Detection of WannaCry using Splunk and Sysmon

Henry Motta López
Master in Computer Science
Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract – *Lately, ransomware keeps being an important topic of conversation around the information security communities, as well as politics and economics. It has caused major damage in all these sectors and researchers must keep evolving as ransomware doe finding new ways to detect and remove the threat. Ransomware's sophisticated encryption and propagation schemes limit the security team's chances of recovering data to almost zero. The researcher investigated the use of Splunk Enterprise combined with Sysmon to detect and explore a specific ransomware threat. For proof of concept, the researcher used a WannaCry sample to detect the first time it was executed. This way, an investigation can be done, and alerts can be configured to better aid the incident response team. This solution detects ransomware file creation through the Splunk search query using Sysmon event codes.*

Key Words – *Detection, Ransomware, Splunk, Sysmon.*

INTRODUCTION

Currently, the ransomware threat is still considered as the main money-making scheme for threat actors and the key threat to internet users. They have evolved from simple scare tactics to nowadays the attacks target hospitals, government agencies, and just about anything they can get their hands on. Moreover, ransomware combines the usage of exploits with worm-like spreading mechanisms to propagate itself. With the fast development of ransomware, the design of new countermeasures, apart from the traditional security approaches, is considered an important and trending task in this field.

Using complex malware capable of evasion, attackers now focus on targeted attacks which are more profitable. A vast number of detection mechanisms have been proposed in the literature and this article [1] provides a systematic review of ransomware countermeasures ranging from deployment through to payment via cryptocurrency.

The authors in this article [1] did extensive research on detection mechanisms for ransomware and divided ransomware samples in a multi-phased attack compromising four phases: Delivery, Deployment, Destruction, and Dealing. This project will be focused on the second phase, Deployment. The deployment phase is when the malware infiltrates the system.

Security Information and Event Management (SIEMs) are a part of the security ecosystem. They aggregate data from multiple systems and analyze that data to catch abnormal behavior or potential cyberattacks. The security operations centers (SOCs) invest in this type of software to streamline visibility across the environment, investigate log data for incident response to cyberattacks and data breaches, and adhere to local and federal compliance mandates.

For proof of concept, the researcher used a WannaCry sample. However, the investigator believe that any other ransomware families can be used since they create many files. The researcher investigated the use of Splunk (which is a SIEM) to collect events which helps capture, index, and correlate real-time data in a searchable repository. After the collection of the data, graphs, reports, alerts, dashboards, and visualizations can be created. Then, couple this with Sysmon, which monitors and logs system activity to the windows event log. Finally, with the combination of these two, the researcher can identify malicious or anomalous activity and understand how intruders and malware operate on the network.

The first version of WannaCry, encrypted files by using AES-128 algorithm and did not have any worm component. Later, an improved version was found, which

used a hardcoded dictionary to access SMB shared folders and dropped a tor browser download link in the *cfg* file [2]. To the best of the investigator knowledge, there is no known research regarding the use of Sysmon data analytics combined with Splunk to detect ransomware attacks. There does exist internet forums and blogs where people use Splunk and Sysmon on their company networks. Moreover, the researcher will be using his own experience working with both in his last internship. Since then, the investigator has found interesting to be able to use such powerful monitoring tools to detect anomalous behavior.

BACKGROUND

This research topic became of interest to the researcher over his summer internship at JPL as a Cybersecurity Analyst. JPL is a research and development lab, federally funded by NASA, and managed by Caltech. They taught interns how to use Sysmon, which provides detailed information about process creation, file changes in Windows systems; and Splunk, to monitor their networks for any anomalies. Additionally, interns learned the value of using tools that the company already has at their disposal to combat threats while also keeping overall costs down.

Researcher main objective was to find a solution to create alerts using the Sysmon data to better monitor windows systems. While working there, the investigator realized how useful these two tools were, especially to monitor what is happening in an organization's networks.

Problem

The main problem these days is that attackers use packers and obfuscation techniques to evade detection. Furthermore, antivirus products take more than 8 days to analyze new threats and add them to their definition files [3]. This is bad news, especially if analysts leave the antivirus solutions to do the job. When employing detection tools coupled with Sysmon, security teams have a bird's eye view of our network. If malware goes undetected for long periods of time, they can know the when, where, and how it came into the organization's systems and create custom alerts for the security operations team to deal with the threat with an abundance of detail.

Term Definitions

4.1 Ransomware

Ransomware is a malicious software that holds the victims' data hostage and proceeds with the release if the ransom payment was made in time. This is done with the exchange of the decryption key to restore the encrypted files. There are two types of ransomwares that infect computers: locking and crypto ransomware.

- Locking ransomware does not alter data but blocks access to the computer.
- Crypto ransomware encrypts files from the file system, making recovery difficult, if not impossible. This type of ransomware is also divided into subparts because it depends if the encryption was symmetric or asymmetric.

The phases of ransomware are explained [4]:

1. Exploitation and Infection

Malicious files are executed on a computer through common infection vectors like phishing emails or exploit security holes in software applications. In the case of WannaCry, through a dropper known as EternalBlue. It exploits a vulnerability in the Service Message Block (SMB), which allows the malware to spread to all unpatched Windows systems from XP to 2016. Apart from this, the ransomware can also infect via social engineering techniques which will evidence the first vector of infection.

2. Delivery and Execution

The actual execution of ransomware is done in the victims' machine. Depending on network latency, this can take a couple of seconds. It is most often executed in %APPDATA% or %TEMP% folder in the user profile.

3. Back-up Spoliation and File Encryption

The ransomware removes back-up files and folders to prevent restoring from back-up. In Windows systems, it is often seen the *vssadmin* command being used to remove the volume shadow copies from the system. With WannaCry, after it encrypts all files with the format shown in Figure 1, the decrypted program attempts to delete any of the shadow copies using the mentioned command.

4. User Notification and Clean-up

After everything is done, the demand instructions for extortion and payment are presented. In this case, the instructions are presented in the desktop background using an image named b.wnry, in the encrypted files folder, and through the "Wanna Decryptor" 2.0 program.

Sysmon

System Monitor (Sysmon) is a windows system service and device driver that monitors and logs system activity to the windows event log. It gives researchers information on process creations, network connections, and file creation, which is very important for the detection of ransomware [5].

Splunk

Splunk is a tool for log management and analysis that is used for searching, monitoring, visualizing, and analyzing machine data in a real-time basis. It gives security teams visibility, efficiency and context, flexibility, and behavioral analytics. Additional to this, the information coming in from its forwarders can be used to create dashboards, graphs, alerts, and reports [6].

METHODOLOGY

3.1 Lab Setup

Researcher started using a Windows machine consisting of Ryzen 5, 32 GB RAM, NVIDIA 3080 10GB GPU, and approximately 150 GB of storage. The Virtual Machines are made up of Windows 10 and the Splunk Framework VM. The Splunk server, which is the framework, is installed on an ubuntu machine. Although, it can be installed on either operating system. Next, the Windows machine has the Splunk Forwarder installed which forwards the data it gathers from its hosts.

3.2 Splunk and Sysmon Installation

Splunk

Researcher started off downloading the server part of Splunk. This is where all the logs and forwarders will send traffic. Then, the investigator installed it by using the command "dpkg -i splunk-8.1.0-f57c09e87251-linux-2.6-amd64.deb. It is then enabled on boot; setup the credentials; and finally, set the service to start. Next, researcher configured the indexers and made sure that the server was listening for traffic. The default port 9997 was used for this test. Additionally, other ports can be configured for other services. The Universal Forwarder contains the essential parts needed to forward data. These forwarders are the ones installed on the hosts. In this case, the Windows 10 host. With this done, the researcher can now view event logs within the dashboard using the search query.

Sysmon installation

First, the researcher installed the Sysmon Add-on for Splunk, which provides a data input and CIM-compliant field extractions [7]. This means that the events that Sysmon generates are pre-categorized which makes it easier to search. Sysmon must be modified to control the logging of many events since the investigation uses the free version. SwiftOnSecurity has a configuration file template with default high-quality event tracing while also not including needless events that take up most of the space [8]. The free version of Splunk: Splunk ES Free edition is limited to 500 MB per day. Because of this limitation, the researcher limited the experiment to one host. After this, Sysmon was installed on the Windows 10 machine.

3.3 Securing the Lab

The lab was secured by implementing some common measures to ensure there was little chance of the malware leaking out. Swapping files between the machines and the host system was limited to a shared file folder with read-only permissions; using a third-party anti-virus software (Malwarebytes); having windows defender alongside the main antivirus software; updated to the latest patches; and limited network access to the host establishing a private network between the virtual machines. The Splunk framework virtual machine had the SMB port disabled because WannaCry attempts lateral movement through this port. The WannaCry malware strain was downloaded using theZoo. This is installed on a linux machine and downloaded through the terminal. It was then transferred to a USB pen drive. From this pen drive, the zip file was moved to the windows machine and executed the edjnfona.exe file.

3.4 Infection

Multiple samples of the WannaCry dropper have been identified, and although they share similar functionality, the samples differ slightly. The Researcher used the encryption component with the SHA256 encryption ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa. This ransomware makes use of EternalBlue, which exploit a vulnerability in the SMB protocol, which allows the malware to spread to all unpatched windows systems on a network that has this protocol enabled. When the execution file was run, it unloaded its files, and continued to encrypt any important files it finds with the extensions listed in Figure 1.

Figure 1

The user will see the background of the desktop change as in Figure 2 and a window open with the information of what just happened to the computer as in Figure 3. The latter will have the information needed to make the ransomware payment. If no payment is received, then the ransom is raised. After the second clock runs out, all files will be encrypted beyond recovery.

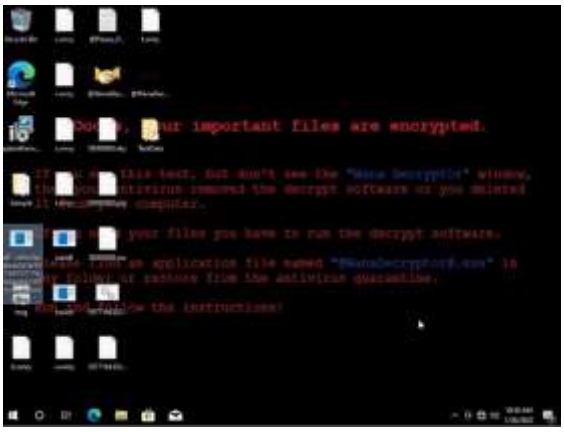

Figure 2

Figure 3

3.5 Detection

Sysmon and Splunk makes it easy to detect ransomware. The Splunk Add-on for Microsoft Sysmon makes it easier because it makes detection, events, and incidents available to be streamed to the Splunk environment. With this, it can search for new file creation since ransomware creates many new files. In Figure 4, researcher used streamstats command to search for a file name that creates many files in a short amount of time [6]. The values of the streamstats search are fed back to Splunk to find the SHA256 of the file that is generating the file creation event. The last result, shown in Figure 4, is an indicator of suspicious activity since it is not a common executable. This is WannaCry at work. Hashes found in this manner can then be compared against other ransomware samples in virustotal for example. Furthermore, with these results, a report can be made for the next step in the incident response process. In Figure 5, can be seen a pie chart of a search that displays the

processes that used the file creation event during the time which the ransomware exe was first run.

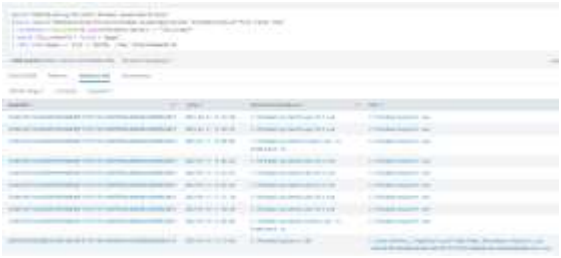

Figure 4

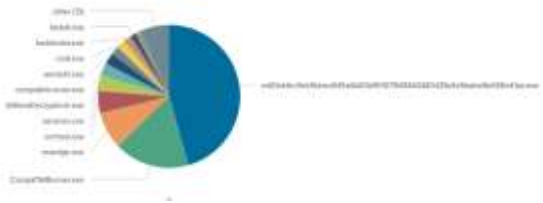

Figure 5

RESULTS

The results indicated that the combination of Splunk and Sysmon indeed helps in detecting malware from the first instance of infection. Furthermore, it gives wealth of information which can be narrowed down from where the infection first started and how much the infection has spread. With the help of Sysmon Event IDs, security teams can reduce any search query to fit the on-going projects, add them to a dashboard for easy access, and create an alert for the next step. The next step would involve the incident response team using all this information to remove the threat.

CONCLUSION

The project was successful in detecting the WannaCry ransomware sample. The investigation evidenced this when the process responsible for creating all the malware files in a short amount of time was found.

The sample used in this research project was real. It was downloaded from theZoo repository and safely executed inside a virtual machine. The solution used by combining a SIEM, Splunk, and Sysmon data proved useful. Although, the data can get very noisy, especially in big companies. It is important to first filter out unnecessary logs to be able to detect successfully. Sysmon gives tons of useful data for the security operations center to investigate and take appropriate action. Once the alerts and dashboards are configured, the detection process can be monitored easily.

This detection method is best used with other incident response strategies. It can even be used with other SIEM software, the important part is to be able to effectively parse Sysmon logs to get a full understanding of the network. Additional parameters can be used to filter out normal activity and have greater visibility. Future research can also use whitelists to add the hash of known processes. This way, if attackers attempt to disguise their malware via common windows processes, security teams will be immediately alerted by it. Moreover, lateral movement attacks inside the network can be investigated and can also test whether this method works with other strains of WannaCry or any other ransomware.

REFERENCES

[1] R. Moussaileb, N. Cuppens, J.-L. Lanet and H. Le Boulder, "A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms: Case Closed?," *ACM Computing Surveys*, vol. 54, no. 6, p. 35, July 2021.

[2] LogRythm Labs Research Group, "A Technical Analysis of WannaCry Ransomware," 16 May 2017. [Online]. Available: https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/. [Accessed: December, 12, 2021].

[3] L. Whitney, "Why traditional malware detection can't stop the latest security threats," *TechRepublic*, 16 March 2021. [Online]. Available: https://www.techrepublic.com/article/why-traditional-malware-detection-cant-stop-the-latest-security-threats/. [Accessed: November, 3, 2021].

[4] R. Brewer, "Ransomware attacks: detection, prevention, and cure.," *Network Security*, pp. 5-9, 2016.

[5] M. Russinovich and T. Garnier, "Sysmon Documentation," 16 December 2021. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon. [Accessed: September, 27, 2021].

[6] Splunk, "Splunk Documentation," [Online]. Available: https://docs.splunk.com/Documentation. [Accessed: August, 12, 2021].

[7] SwiftOnSecurity, "sysmon-config | A Sysmon configuration file for everybody to fork. [Online]. Available: github.com/SwiftOnSecurity: https://github.com/SwiftOnSecurity/sysmon-config. [Accessed: July, 22, 2021].

[8] Splunk, "Splink Add-On for Microsoft Sysmon. [Online]. Available: https://splunkbase.splunk.com/app/1914/#/details. [Accessed: July, 14, 2021].