Detection of WannaCry using Splunk and Sysmon

Author: Henry Motta
Advisor: Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department

Abstract

Lately, ransomware keeps being an important topic of conversation. Their sophisticated encryption and propagation schemes limit our chances of recovering data to almost zero. I investigate the use of Splunk Enterprise, combined with Sysmon to detect a specific ransomware threat. For proof of concept, I use 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.

Introduction and Motivation

Currently, the ransomware threat is still considered as the main money-making scheme for threat actors. It has evolved from simple scare tactics to where it now targets anything it can get its hands on. Furthermore, ransomware combines the usage of exploits with worm-like spreading mechanisms to propagate itself. For this reason, we need new countermeasures, apart from the traditional approaches.

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. For proof of concept I used a WannaCry sample. To detect this, I use Splunk Enterprise to collect the events that Sysmon sends to the server. After collecting the events, we can identify malicious or anomalous activity and understand how intruders and malware operate on the network.

This research topic became of interest to me over my 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 me how to use Sysmon and Splunk, to monitor their networks for any anomalies. My main objective while there was to find a solution to create alerts using the Sysmon data to better monitor windows systems.

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.

Methodology

I started using a Windows machine which had 2 virtual machines. One was an unsecured windows 10 OS and the other one was a Linux Ubuntu OS which had the Splunk framework installed.

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. Additionally, the information coming in from its forwarders can be used to create dashboards, graphs, alerts, and reports [6]. Sysmon on the other hand, is a windows system service and driver that monitors and logs system activity to the windows event log [5]. Because we are working with a live malware sample, I had to secure the lab.

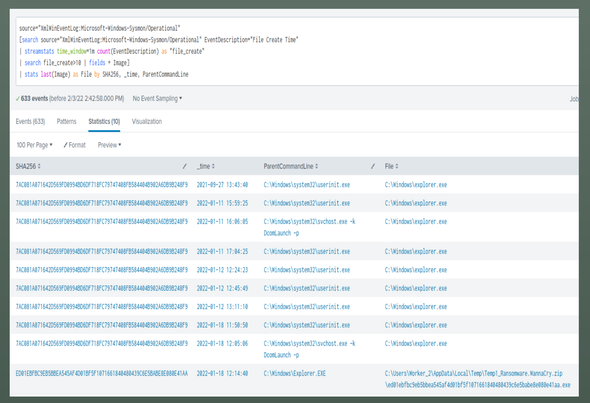
I did this by limiting file swapping between virtual machines.
Using a third party anti-virus software on the host.
Having windows defender alongside the anti-virus on the host.
Updated the host to the latest patches.
Limited network access to the host.
Set-up a private network between the virtual machines.
I disabled the SMB port on the Ubuntu virtual machine since WannaCry uses that port to propagate.
After downloading the malware sample, I used a pen drive to transfer it directly to the windows virtual machine.

When the execution file was run, it unloaded its files as in Figure 1. In this figure we can also see that the malware changed the desktop background to let the user know it has been infected.

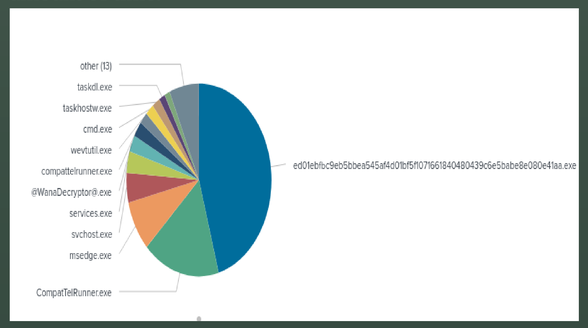
Next, the WannaDecryptor 2.0 window is shown in Figure 2 which gives information about payment. If the ransom is not paid before the first timer expires, the ransom doubles. After the second timer expires, the files become unrecoverable.

Methodology

With Sysmon we can know what happened to our system and with Splunk we can see it. In the case of a ransomware, we want to look for a Sysmon event which creates files in a short amount of time. Using some Splunk queries we can be as specific as needed. The search result shows suspicious activity on the last file. This is the WannaCry ransomware at work.



With these results we can create a report for the next part in incident response and have our teams further investigate. This is important because malware can go undetected in our networks for long periods of time when finally, the attacker decides to execute. Figure 3 better represents how the malware created new files in a short amount of time.



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.

Conclusions and Future Work

The project was successful in detecting the ransomware sample with the process responsible of creating a lot of files in a short amount of time. The detection method is best used with other similar software like Splunk, 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 put normal activity and have greater visibility. Future research can also use whitelists to add the hash of known processes and use this same hash to compare it against a database like VirusTotal [9]. If attackers try 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.

Acknowledgements

This research is based upon work done in my internship at the Jet Propulsion Lab and is supported by the National Science Foundation (NSF) through their Scholarship for Service Award (SFS).

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

[9] VirusTotal. 2021. VirusTotal. [Online]. Available: https://www.virustotal.com/gui/home/search. [Accessed: February, 16, 2022].