Investigating Fileless Malware

by

David Snow

A Capstone Project Submitted to the Faculty of

Utica College

August 2021

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

The purpose of this capstone project was to review and detail what fileless malware is, what proactive measures can be done to protect organizations from the threat of fileless malware, and how to respond when a fileless malware infection has taken place. Fileless malware typically does not leave evidence of its existence on a hard drive of a computer system. It can maintain persistence by hiding and altering the registry, task scheduler, or by using Windows Management Instrumentation (WMI). Currently, the main solutions that exist to prevent an infection are antivirus and Endpoint Detection and Response solutions (EDR). When a cybersecurity team responds to the threat of fileless malware it will be pivotal to understand how it is working and how to stop it and clean the system's infection. This study examines the proactive protection solutions available and how a cyber security team can recover their systems using incident response procedures. Additionally, this project highlights how using current tools available today; cybersecurity teams can clean a threat from their system.

Keywords: Cybersecurity, Professor Carmen Mercado, fileless malware, antivirus, RAM forensics, filesystem forensics.

Acknowledgements

I would like to acknowledge all of the people that gave me support and encouragement throughout my time at Utica College, and through the Capstone Project. To my parents thank you for passing your love of education on to me and instilling in me the importance of an education. To my friend Nate Roberts for giving me the idea to attend Utica College, and taking the time to listen to me and help me throughout out my time attending Utica College and for being my second reader. Most importantly I would like to thank my best friend and confidant Anna Zambrano for supporting me and always being patient with me throughout the most difficult times that was I felt that I was facing through the program.

Table of Contents

Investigating Fileless Malware

Defining the Problem

Fileless malware is a type of malicious software built in such a specific way that it can be challenging to detect. In 2020, PurpleSec, a cybersecurity consulting firm, released their cybersecurity trends report for 2021, in which they stated that, on average, it costs a cybersecurity team fifty days to remediate a malware infection with an average cost of 2.4 million dollars ("2021 Cyber Security Trends Report," n.d.). This report included findings for all forms of malware to contain traditional or file-based and fileless malware. Fileless malware can be more challenging to detect and remediate, increasing the loss of revenue that organizations may experience due to fileless malware's design to avoid detection by Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Antivirus. This research project aimed to identify problems caused by fileless malware in an enterprise environment, how organizations can prevent the infection of fileless malware, and how forensic techniques can aid organizations in identifying and remediating infections.

Justification of the Problem

Fileless malware is a form of malware that can infect systems in various ways to evade antivirus solutions by not writing any code to disk where antivirus solutions would scan and detect the malware. Traditionally, antivirus works by maintaining a database of previously seen malware indicators (Dulaney, 2018). When a computer system interacts with new software, the antivirus examines the new software. It scans the new software to identify whether it contains any known malware indicators maintained in its database of known bad entries. Fileless malware can avoid detection because its code or processes get written directly into random access RAM

(RAM) rather than running on a disk where antivirus can scan and identify it as malicious (Andrews, 2018).

To better understand how fileless malware works, knowing how file-based malware infects a system is beneficial. The entry point for malware is typically an attachment in an email or a malicious file downloaded from a website. In either case, a computer system downloads a file to disk (Tancio, 2019). In the event of fileless malware, a computer system may download a file to initiate the infection process; however, by leveraging tools approved to run on a computer system such as Microsoft PowerShell, fileless malware can launch attacks from RAM (Tancio, 2019).

Fileless malware typically has three stages during its lifecycle: point of entry, fileless code, and fileless persistence (Tancio, 2019). During the point of entry phase, the fileless malware may exploit a vulnerability in a computer system that allows an attacker to load shellcode directly to RAM, eliminating code on disk. Another entry method for a user to download a malicious file from is a compromised website or opening a malicious attachment in a malicious email. The infected file, attachment, or uniform resource locater (URL) contains malicious code that relies on a scripting language such as PowerShell to write the malicious code to RAM. If the source of infection comes from an attachment, it is fileless only after storing malicious code in RAM. Finally, during the persistence phase, the malicious code needs to maintain its persistence by saving a script to a location that would be hard for a computer user to locate; otherwise, a reboot of the infected machine would clear the infection.

Understanding how fileless malware operates makes it easy to understand why fileless malware is becoming adopted widely amongst cybersecurity attackers. WatchGuard, a cybersecurity research company, produced a report of its quarter-four findings for 2020, detailing that when comparing 2020 to the previous year, 2019, they saw a rise in fileless malware infection rates by 888 percent (*Internet Security Report -Q4 2020*, n.d.). During the same year, Red Canary, a cybersecurity research company, released a threat detection report that detailed that 48.7 percent of organizations had been affected by malicious PowerShell scripts (*2021 Threat Detection Report*, n.d.).

There are multiple methods an infection can occur using fileless malware once the malware is on the system. One such method is scripting and is the easiest to understand since it is the one that is the most like file-based malware. Once a user opens a malicious attachment received through a malicious email, the script will be launched and run directly in RAM. When run, these scripts will be allowed to run due to them being whitelisted and permitted in the environment, as is the case with PowerShell, a tool commonly used in enterprise information technology (IT) environments for administrative purposes (Tancio, 2019). When the initial script runs, it works as a downloader, enabling the download of another script, binary or final payload from a malicious site. The original file or downloader used to download the secondary file will erase itself, at which point the second file will run in RAM. It can be challenging for scripts to be identified as malicious because they are commonly encoded or obfuscated, making them difficult to read.

A second method that fileless malware will use to evade detection is living-off-the-land techniques (Tancio, 2019). Living-off-the-land techniques abuse tools that already exist on a system and can execute in the environment for administrative purposes. Once an attacker gains access to an organization’s environment, they can use these tools to perform malicious activities throughout the network without detection. Using these tools, an attacker can move from computer system to computer system, performing asset discovery, data exfiltration, or download additional tools or malware.

The third method fileless malware may use is code injection, which involves compromising a legitimate process and executing malicious code (Tancio, 2019). Having malicious code hide in legitimate processes allows the malicious code to remain undetected on the system as it appears to be legitimate. Additionally, since the legitimate processes are approved to operate in an organization’s environment, they can go undetected by antivirus.

It is important to understand how fileless malware can avoid detection on systems, as antivirus solutions do not work and whitelisting programs or applications allow for the applications’ utilization in attacks against organizations, as is the case with PowerShell. The old methods that organizations are using to protect themselves against fileless malware need to be improved. There is a solution for prevention, to deploy a more recent classification of a tool called Endpoint Detection and Response (EDR) (Liggett, 2018). EDR tools rely on looking for indicators of compromise (IOC) and indicators of attack (IOA). An IOC is an artifact that acts as evidence that an intrusion or other malicious activity has taken place on a network or computer system (Trend Micro, n.d.). To find IOCs, cybersecurity teams can look at event logs and applications and system services logs. Some examples of IOCs are unusual traffic in and out of an organization’s network, unknown files or applications on a system, suspicious activity using administrator accounts. In contrast, an IOA is a series of computer actions that indicate something malicious is happening on a system or network (Crowdstrike, 2021). As Liggett identified during his research on the Evolution of Endpoint Detection and Response Platforms, to successfully identify an IOA, a specialized cybersecurity analyst will need to manually search