Fileless Malware{

authorName = Matko Antun Bekavac
lenght = 37
deathByPowerPoint = true

}

Table of Contents

Definition

Fileless malware is a type of malicious software that operates entirely in memory without leaving any traces on a computer's hard drive.

Instead of relying on traditional file-based methods to infect systems, fileless malware uses various techniques to inject itself into legitimate system processes, registry keys, or even firmware, making it harder to detect and remove.

Brief history

Fileless malware is not a new concept, but its use has increased significantly in recent years due to the rise of cloud computing and the availability of new attack tools and techniques.
In the past, fileless malware was mostly used by advanced threat actors, such as nation-states and cybercriminals with sophisticated skills. Today, fileless malware is more accessible to a wider range of attackers, including script kiddies and hacktivists.

A growing threat

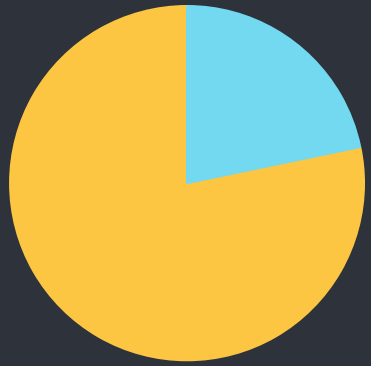
Evades traditional antivirus and endpoint protection solutions. According to various reports, fileless attacks accounted for ~50% of successful attacks in 2020, and the trend continued in 2021 and beyond. In addition, fileless malware attacks are often more difficult to detect and remediate, which can lead to longer dwell times and greater damage to the victim's systems and data.

A growing threat

77%

Fileless

77% of successful ransomware attacks were from fileless techniques that completely bypassed the victim company’s antivirus.



23%

File based

*

https://purplesec.us/resources/cyber-security-statistics/

How fileless malware works

Fileless malware uses various techniques to evade detection by traditional antivirus and endpoint protection solutions.
One of the most common techniques is process injection, which involves injecting the malicious code into a legitimate process, such as explorer.exe or svchost.exe. This allows the malware to blend in with the legitimate system processes and avoid detection.
Other techniques include reflective DLL injection, registry-based malware, and script-based malware.

Different types

There are several types of fileless malware, each with its own unique characteristics and methods of operation.

One of the most common types is in-memory malware, which runs entirely in memory without leaving any traces on the hard drive. Other types include PowerShell malware, macro malware, and JavaScript malware.

Comparison vs Traditional Malware

Delivery

Fileless

Often delivered via social engineering techniques, such as spear-phishing emails or malicious websites

Traditional

Typically delivered via email attachments, downloads, or physical media

Comparison vs Traditional Malware

Persistence

Fileless

Uses legitimate system tools and processes, such as PowerShell or WMI, to run malicious code directly in memory without leaving any traces

Traditional

Usually relies on files or registry keys to maintain persistence on a system

Comparison vs Traditional Malware

Detection

Fileless

Can be more difficult to detect, as it does not leave any files on disk and may not exhibit any obvious malicious behavior

Traditional

Relatively easy to detect using signature-based antivirus software or behavior-based detection techniques

Comparison vs Traditional Malware

Evasion techniques

Fileless

Uses advanced evasion techniques, such as anti-forensic techniques or "living off the land" tactics, to blend in with legitimate system activity

Traditional

May use simple evasion techniques, such as packing or obfuscation, to avoid detection

Comparison vs Traditional Malware

Attack surface

Fileless

Can attack any system or device that can run PowerShell or other system tools, including endpoints, servers, and IoT devices

Traditional

Can attack both endpoints and networks, typically relying on vulnerabilities or weaknesses in software or systems

Comparison vs Traditional Malware

Impact

Fileless

Can be equally damaging as a traditional malware, with the added risk of being more difficult to detect and remove

Traditional

Can cause significant damage to systems and data, potentially spreading across networks and causing widespread disruption

Comparison vs Traditional Malware

Prevention

Fileless

Requires more advanced prevention techniques, such as behavioral analysis, application whitelisting, and user training

Traditional

Can be prevented using traditional security measures, such as antivirus software, firewalls, and intrusion detection systems

Comparison vs Traditional Malware

Mitigation

Fileless

Requires advanced mitigation techniques, such as threat hunting, network segmentation, and response planning

Traditional

Can be mitigated using incident response procedures, backups, and recovery plans

Real-world examples

/01

PowerGhost malware

/02

FIN7 malware

/03

DarkHotel malware

PowerGhost malware

The PowerGhost malware is a fileless malware that targeted corporate networks in 2018. It exploited vulnerabilities in Microsoft Office and PowerShell to infect systems and evade detection.

The malware was able to move laterally across networks, steal credentials, and execute commands, making it difficult to detect and remediate. The PowerGhost malware infected thousands of systems worldwide, causing significant damage and financial loss.

FIN7 malware

The FIN7 malware campaign is another example of fileless malware in action. FIN7, a notorious hacking group, used fileless techniques to steal credit card data from over 100 companies in the US and Europe.

The malware was delivered via phishing emails and exploited vulnerabilities in Microsoft Office and PowerShell to infect systems. FIN7 used the stolen credit card data to make fraudulent purchases and steal money from victims, causing significant financial harm.

DarkHotel malware

The DarkHotel malware is a fileless malware that targets high-profile individuals and organizations, such as government agencies and corporate executives.

The malware is delivered via spear-phishing emails and exploits vulnerabilities in Adobe Flash and other software to infect systems. Once infected, the malware can steal sensitive data, including passwords, credentials, and confidential documents.

Detection and prevention techniques

One of the most effective ways to prevent fileless malware is to limit administrative privileges on systems. By reducing the number of users with administrative access, organizations can reduce the risk of malware spreading and limit the damage that malware can cause.

Using behavioral-based detection techniques

Traditional signature-based antivirus solutions are often ineffective against fileless malware. Behavioral-based detection techniques, such as anomaly detection and machine learning, can be more effective at detecting fileless malware. These techniques analyze system behavior and network traffic to identify suspicious activity and flag potential threats.

Keeping software up to date

Fileless malware often exploits vulnerabilities in software to infect systems. Keeping software up to date with the latest security patches and updates can help prevent these vulnerabilities from being exploited.

Network segmentation

Network segmentation can help contain the spread of fileless malware by dividing the network into smaller segments with different levels of access. This can limit the scope of an attack and make it easier to detect and remediate.

User education and awareness

User education and awareness are critical for preventing fileless malware. Employees should be trained on how to recognize phishing emails and other social engineering tactics used by attackers to deliver fileless malware.

Challenges in defending against fileless malware

One of the biggest challenges in defending against fileless malware is the difficulty in detection and attribution. Fileless malware can be difficult to detect using traditional antivirus solutions, and it often leaves little or no trace on the infected system. This makes it challenging to identify the source of the attack and attribute it to a specific attacker or group.

Evolving techniques and tactics

Fileless malware is constantly evolving, with attackers developing new techniques and tactics to evade detection and improve their success rate. This means that defenders need to stay up to date with the latest threats and constantly adapt their defenses to stay ahead of attackers.

Lack of visibility and control

Fileless malware often operates in memory or uses legitimate system processes, making it difficult for defenders to detect and respond to attacks. This lack of visibility and control can make it challenging for defenders to contain and remediate attacks.

Complexity of remediation

Remediating a fileless malware attack can be complex and time-consuming. Because fileless malware often uses legitimate processes and tools, it can be difficult to determine what is malicious and what is legitimate. This can make it challenging to remove the malware without causing further damage to the system.

Insider threats

Fileless malware attacks can also be carried out by insiders, such as disgruntled employees or contractors with access to sensitive systems. These attackers can be difficult to detect and may have legitimate access to systems, making it challenging to prevent or remediate attacks.

Conclusion

-It’s not rare anymore
-It’s hard to detect
-It’s here to stay

Further reading

"The Evolution of Fileless Malware: How it Works and Strategies to Combat Attacks" by Carbon Black

"Fileless Malware: An Overview" by Palo Alto Networks

"Fileless Malware: A Detailed Analysis of Techniques and Defenses" by FireEye