Best Practices to Detect and Prevent File-Less and Click-Less Malware

By Fob H. James, IV May 2018

Hackers are clever at exploiting weaknesses in an organization's systems. They are also efficient. After an organization installs robust cybersecurity controls, hackers will typically look for an easier target or they will adjust their tactics to exploit remaining leaks in an organization's environment. Unless organizations want to get eaten by a shark, they should constantly adjust and improve their cybersecurity controls.

What is File-less or Click-less Malware?

File-less or Click-less malware is a hacking strategy that has become more popular over the last several years (and often overlooked by IT departments). This type of malware is unique because it does not download "software" on the victim's hard drive, and it does not install or run a conventional .exe type program.

Machines typically become infected through two methods: (1) when a user clicks on a link in an email, document or website; or (2) when a user's mouse hovers over a link (but does not click the link) in a macro enabled program like PowerPoint or Word. In these instances, a file is not downloaded to the hard drive nor is a program executed. The malware generally operates by using Windows PowerShell to load Base64 code directly from system memory (which cannot be scanned using heuristics). PowerShell is a command-line shell and scripting language built on top of the Windows .NET framework, so it has a trusted signature along with access to the registry, the operating system, and other Windows APIs. In layman's terms, this means that PowerShell is a powerful weapon in a hacker's war chest.

Detection Is Difficult

PowerShell has permission to use legitimate Windows processes (e.g., iexplorer.exe), which renders detection by conventional cybersecurity controls ineffective. Because the malware operates in system memory, there are no signatures for an Anti-Virus ("AV") program to detect and other common software centered cybersecurity controls such at whitelisting or blacklisting are futile.

Detection is further hindered by the hacker's use of obfuscated command code, which can shield the unexecuted malicious code from view. The event logs in PowerShell Version 2 reflect when a PowerShell event starts and stops but nothing else. The inability to view the unexecuted code in these instances makes it extremely difficult to determine what the malware is doing. For example, the unexecuted

command code may reveal that the script is exporting certain data to a suspicious external domain or accessing a critical system. Later versions of PowerShell have better security features but hackers will try to downgrade PowerShell to Version 2.

Best Practices for Prevention

Organizations should consider implementing the following practices to prevent intrusion by File-less and Click-less malware:

1) Keep Windows systems, operating systems, anti-malware, and anti-virus software updated and install the latest patches;
2) **Download PowerShell Version 5 and disable Version 2;**
3) **Activate the logging feature in PowerShell Version 5, which will allow viewing of the malicious script's code before execution;**
4) Activate Constrained Language Mode to restrict access to sensitive language elements that can be used to invoke arbitrary Windows APIs (malicious scripts like Invoke-Mimikatz generally will not work with Constrained Language enabled);
5) Disable unnecessary components within the Windows framework;
6) Use AppLocker (included in Windows 10 Enterprise) to create executable rules that will limit which files can be executed by file path or by signature;
7) Incorporate a behavior monitoring mechanism that can help detect unusual modifications;
8) Adopt a policy of the principle of least privilege;
9) Train and educate employees/users on the features of File-less and Click-less malware and how to detect and report suspicious links and documents;
10) Develop and implement sound email security controls (e.g., spam traps, SPF checking, email access logging and monitoring, IP address monitoring and blacklisting) to reduce suspicious emails that could be a malware trap.

Best Practices for Detection and Response

Organizations should consider the following practices and tools to detect and respond to a File-less or Click-less malware incident:

1) Check task manager on any machine of interest for native system processes that are logging unreasonable CPU resources;
2) Run Microsoft Safety Scanner on machines of interest;

3) Identify any remote IP address and domains that a machine's processes may be attempting to communicate with and block them with the main firewall to your organization's environment;

4) With the logging feature enabled in PowerShell Version 5, review logs and pre-executed command code for suspicious code;

5) Maintain a list of commands that are likely to be used by malicious scripts (e.g., "Hidden", "^", "Bypass") and train your IT staff to be cognizant of these commands; and

6) Use sandboxing to analyze malware in a controlled environment.

Importantly, these practices are not exhaustive, and there is no silver bullet to prevent malware intrusions. There are techniques to get around each control listed in this article, and some controls can be used against your organization. The point being, as your organization's systems and data change, and as hackers adjust their techniques, so should your cybersecurity controls and practices.

I recommend that organizations develop and install a Malware section in their infosec policies and that they regularly update their cybersecurity practices. It is a war out there. Hackers will likely stay miles ahead of defenses, and intrusions will occur. But success from a legal standpoint is often obtainable when an organization can demonstrate that they implemented reasonable data security practices and made a good faith effort to protect data. Plus, if you make the attackers lift a finger, there is a decent chance they will pass you over and breach someone else instead.

For more information, please contact:

Fob James
Birmingham, AL
P. (205) 458-5311
E. fjames@burr.com

BURR FORMAN LLP
results matter