CYLANCE

BUSINESS BRIEF

FILELESS MALWARE

Detect and stop fileless malware with local endpoint artificial intelligence (AI) models, preventing these sophisticated cyberattacks from ever being successful.

Read more about fileless malware executables

WHAT IT IS

Fileless malware gets its name by not leaving files on disk. Instead, it stays memory resident and executes commands that already exist on the machine. Often, fileless malware uses a tool like PowerShell to coordinate attacks and uses a Meterpreter[1] payload that employs in-memory DLL injection stagers to set up additional attacks. Because fileless malware leaves no trace on disk, detection by standard antivirus (AV) tools, which often use signature files to identify static files on disk, is much more difficult.

WHO IS AFFECTED

Think of fileless malware as a cyberattack that uses a cloak of invisibility. That is, even if you are looking right at something malicious, unless you see the wallet being stolen off the table, it's hard to recognize something bad is happening. This means that organizations using traditional endpoint security based on signatures will unfortunately be most susceptible to being victimized by a fileless malware attack.

WHY THIS MATTERS

Two families of fileless malware, Poweliks and Kovter, use similar techniques to infect a system. First, JavaScript code is written into the registry under the Run key along with an AutoRun entry that is used to read and decode the encoded JavaScript. In the second stage of the attack, PowerShell is used to decrypt and inject a malicious .dll into a standard Windows process. This technique allows the malware to stay resident in memory and evade traditional AV defenses.

Fileless, memory-based malware has been known for years in the security industry, but increasingly is being used for significant monetary gain. Several attacks detected over the past few months that rely heavily on PowerShell, open-source tools, and fileless malware techniques might be the work of a single group of attackers.[2] A few high-profile examples of recent fileless malware attacks include:

- **Target**[3] **—** The fileless malware injected itself into running processes to identify credit card data and copy it during a narrow window of opportunity before the data was scrambled. Approximately 110,000,000 records worth of payments, transactions, and other personally identifiable data were intercepted.

About Cylance

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

- **Democratic National Committee**[4] **—** This attack was carried out almost entirely using PowerShell and Windows Management Instrumentation, a set of specifications from Microsoft for consolidating the management of devices and applications in a network.

Detect and stop fileless malware with local endpoint artificial intelligence models, preventing these sophisticated cyberattacks from ever being successful.

RECOMMENDED ACTIONS

The human interaction element at most endpoints render them the weakest link in any security chain. The endpoint, however, can be secured with AI based advanced endpoint protection that predicts and prevents attacks before they can execute.

Enterprises worldwide have already protected thousands of endpoints throughout their network with CylancePROTECT.® Using machine learning to predict, prevent, and stop malware and cyberattacks, including fileless malware, Cylance AI recognizes how attackers attempt to exploit computers and thus can stop attacks before they can execute.

CylancePROTECT includes a feature called Memory Protection, which scans and monitors running processes to protect devices from malware that takes advantage of software vulnerabilities that exploit running processes or executes from within memory space. Fileless malware that uses memory injection or stack pivot attack techniques is quickly prevented using Cylance's Memory Protection capabilities.

- Read more about fileless malware executables
- Learn more about CylancePROTECT Memory Protection
- IDC reports that when "prevention capabilities are enabled, CylancePROTECT has the ability to stop all Windows PowerShell, active scripts, and a variety of malicious macro actions." Read the full IDC report
- Want to know if you've been breached? Engage Cylance Consulting for a Compromise Prevention Assessment to determine if a security breach has happened or is actively occurring in your environment

[1] *"About the Metasploit Meterpreter," Offensive Security*

[2] *"String of fileless malware attacks possibly tied to single hacker group," March 17, 2017, Network World*

[3] *"How Cybercriminals Attacked Target: Analysis," January 20, 2014, Security Week*

[4] *"Nothing to see here? Banks' latest cybersecurity concern," February 8, 2017, American Banker*

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE™