Protect Against Invisible Threats: Fileless Malware

Deploying the exploit-prevention capability of Cisco AMP for Endpoints

Anatomy of fileless attacks

2017 was the year of fileless malware: 77 percent of compromised attacks were deemed to be fileless and encompassed a rate of being nearly 10 times as successful as file-based attacks.*

Although security solutions are becoming more efficient at detecting threats, attackers are also becoming more sophisticated and persistent. By developing precisely targeted and stealthier malware, criminals gained the ability to penetrate a business's networks and endpoints without leaving a trace. Their tactics evolved from using file-based malware to initiating attacks that operate on the memory level to avoid detection. Unlike traditional malware, these types of attacks do not have signatures, making them more difficult to detect and prevent.

Unfortunately, creating a fileless attack is simple, but the results are incredibly damaging. These memory-level attacks target our day-to-day applications and can infiltrate an organization's endpoints by exploiting vulnerabilities in software and operating system processes. Even with traditional endpoint security solutions, applications are still highly vulnerable to these advanced attacks.

A typical fileless attack scenario

Most businesses do not have complete control of what their employees access on the internet. As a result, they can easily fall victim to fileless attacks. Let's break down how a fileless attack typically enters a business.

1. Users receive a spoofed message that appears legitimate, which contains a link to a malicious website.
2. Users click the link and enter the site.
3. The malicious site loads and exploits a vulnerability in Adobe Flash technology.
4. Windows PowerShell is then launched with the capability to run instructions through the command line on the memory level.
5. PowerShell run scripts from a command-and-control server.
6. Attackers then gain full control and can locate scripts and steal the users' data.

Fileless attacks make use of particular applications that are installed on a user's computer and known to be safe. Most commonly, these attacks' exploit kits target frequently used applications such as Web browsers, Microsoft Office, Adobe Reader, and more. This allow attackers to run malicious code that can exploit and inject code into a device's memory level; making fileless attacks more persistent and difficult to detect.

Three reasons why traditional endpoint solutions fall short

Traditional endpoint solutions consist of detection, remediation, application control, and antivirus tools. But here are three crucial reasons why those are not enough to protect your organization against fileless attacks:

They can't defend against unknown threats: Traditional endpoint solutions tend to only protect devices and files against known threats. The knowledge base behind unknown threats is limited. Attackers leverage tools like packers, which compress and obfuscate malware to bypass defenses. In many cases, traditional endpoint solutions even allow these threats to enter a device or network.

They have limited visibility: Once it's in, it's in. Users have limited visibility into a file or application once it enters a device. Traditional endpoint solutions do not continuously monitor files and applications. Nowadays, many advanced threats have capabilities that are triggered after a certain time, making them difficult for traditional solutions to detect.

Automation is inefficient: In security, timing is everything. Unfortunately, traditional endpoint solutions are unable to push out automated responses and remediation, making detecting and resolving attacks inefficient and time consuming.

Attackers are evolving their methods. Using solutions that were built to detect and protect against yesterday's threats are not efficient against fileless attacks. Organizations need to shift to a more dynamic approach in order to strengthen their defenses against adversaries who are constantly changing and advancing their attacks.

Attack types and exploit techniques

Threats are constantly evolving. With attackers adapting to security trends, threats can now evade detection. Here are just some of many attack types and exploit techniques that cybercriminals are using to infiltrate businesses' networks and devices.

Exploit technique	Description
Shellcode	Shellcode is designed to be copied into an arbitrary memory address and run from that address. However, the key parts of shellcode are the Dynamic-Link Libraries (DLLs) that enable users to make system calls. This can allow malicious actions to happen on the system.
Process injection techniques	These techniques allow attackers to run malicious code within the address space of another process. They help attackers evade detection and achieve persistence.
Memory corruption exploits	Many exploits fall under the category of memory corruption, including buffer overflows, integer overflows, and use after free.
Stack-based exploit techniques	Using a stack buffer overflow, attackers can overwrite the stack with attacker-controlled data. Modern protection mechanisms against these types of attacks, such as data-execution prevention and address-space layout randomization, can be bypassed by attackers.
Packer-based malicious attacks	In packer-based malware, code is obfuscated and compressed, making it harder to detect using traditional antivirus signatures.

In order for businesses to effectively protect against these attacks, they need to implement a defense mechanism that can stop and prevent attacks early in the attack chain.

AMP for Endpoints' exploit-prevention engine

To defend against threats that target vulnerabilities in applications and operating system processes, the exploit-prevention engine built into Cisco® AMP for Endpoints can change memory structure before attacks even begin. This type of prevention is lightweight, effective, and less costly. Moreover it helps to decrease the time to detect an attack, which is essential for organization's security posture.

Exploit prevention is a true preventive engine that does not require policy tuning, prior knowledge, or rules to operate. When it stops an attack, it stops the application from running and logs contextual data in the AMP for Endpoints device trajectory. Users can see exactly where and how the malware entered a device.

Conclusion

To counter fileless malware, one of the stealthiest malware of all time, businesses need a solution that can protect against it. When malware bypasses the first layers of defense, continuously monitoring your processes and applications is highly effective, because fileless malware attacks at the memory level.

Cisco AMP for Endpoints stops potential fileless attacks before they even begin. It provides users with deep visibility into a threat's journey, allowing you to easily track malware propagation and stay ahead of the hunt.

For more information

Interested in a demo? Please visit here.

For more information on Cisco AMP for Endpoints, please visit here.

* Maria Korolov, "What is a fileless attack? How hackers invade systems without installing software," CSO, October 9, 2017, https://www.csoonline.com/article/3227046/malware/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html.

C11-740455-00 04/18