Solution Brief

Protecting Against Fileless Malware

In the ***McAfee® Labs Threats Report: November 2015,*** we take an in-depth look into fileless malware and a technical dive into Kovter, which evades detection by reducing or eliminating the storage of any binaries on disk and instead hides its code in the registry of a compromised host. Malware authors have made detection challenging through techniques such as polymorphism, implanting watchdogs, revoking permissions, and more. Also in 2015, we have seen attackers leverage features like Microsoft Windows Management Instrumentation (WMI) and Windows PowerShell to compromise endpoints without ever storing a binary on disk, ensuring that an attack remains hard to track down.

Fileless memory-based infections have been known for years in the security industry. Even though they were considered fileless, previous malware families would drop a small binary on the disk in the initial attack before moving into the main memory of the compromised host. However, the newest evasion techniques used by fileless malware—Kovter, Powelike, and XswKit, for example—leave no trace on disk, thus making detection, which generally relies on static files on disk, more difficult.

Three types of fileless malware are common:

- **Memory resident**: This type of fileless malware uses the memory space of a legitimate Windows file. It loads its code into that memory space and remains resident until it is accessed or reactivated. Although execution occurs within the legitimate file's memory space, there is a dormant physical file that initiates or restarts the execution. As a result, this malware type is not completely fileless.
- **Rootkits**: Some fileless malware hides its presence behind a user- or kernel-level application programming interface (API). A file is present on disk but in a stealth mode.
- **Windows registry**: Some new fileless malware types reside in the registry of the Windows operating system. Malware authors have exploited features such as the Windows thumbnail cache used to store images for Windows Explorer's thumbnail view. The thumbnail cache acts as a persistence mechanism for the malware. Fileless malware of this type must still enter the victim's system through a static binary. Most use email as the medium to reach the system. Once the user clicks on the attachment, the malware writes the complete payload file in an encrypted form in the Windows registry hive. It then disappears from the system by deleting itself.

intel Security

Malware authors have cleverly crafted the fileless malware families Kovter, Powelike, and XswKit to execute completely fileless Windows registry attacks without leaving any trace on the file system. Although the environment to carry out these attacks is prepared by executing code in a file, the file destroys itself once the system is ready for the malicious operation.

How Intel Security Helps Protect Against Fileless Malware

Outright detection of fileless malware that does not involve an initial binary can be tricky and is often driven by security organizations' investigative efforts. However, ensuring that proper controls are in place to deny attackers an entry point is the key to stopping fileless malware.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection product that combines multiple inspection engines. By combining multiple inspection engines that apply signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing, McAfee Advanced Threat Defense will protect against fileless malware that initially drops a binary on its target system.

- **Signature-based detection**: Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledgebase is created and maintained by McAfee Labs.
- **Reputation-based detection**: Looks up the reputation of files using McAfee Global Threat Intelligence (McAfee GTI) to detect newly emerging threats.
- **Real-time static analysis and emulation**: Provides real-time static analysis and emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.
- **Full static-code analysis**: Reverse engineers file code to assess all its attributes and instruction sets and fully analyzes the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by specific malware.
- **Dynamic sandbox analysis**: For a file whose safety cannot be established through the inspection engines above, McAfee Advanced Threat Defense can execute the file code in a virtual runtime environment and observe the resulting behavior. Virtual environments can be configured to match host environments. McAfee Advanced Threat Defense supports custom operating system (OS) images of Windows XP SP2 and SP3, Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows Server 2003, Windows Server 2008 (64-bit), and Android.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt over time to suit an environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to fileless malware attacks thanks to its visibility into immediate threats such as unknown files or applications being executed in the environment.

- **Comprehensive threat intelligence**: Easily tailor comprehensive threat intelligence from global threat intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.

- **Execution prevention and remediation**: McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to the product's powerful central management and policy enforcement capabilities.
- **Visibility**: McAfee Threat Intelligence Exchange can track all packed executable files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process actions, from installation to the present, enables faster response and remediation.
- **Indicators of compromise**: Import known bad files hashes and immunize your environment against these known threats through policy enforcement. If any of the indicators trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the indicators of compromise.

McAfee Web Gateway

Drive-by-downloads and malicious URLs embedded in phishing emails are the main attack methods used to deliver fileless malware. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway Anti-Malware Engine**: Signatureless intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protect against zero-day and targeted attacks. The Gateway Anti-Malware Engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee GTI**: Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

In addition to these Intel Security products, we recommend two additional classes of security technologies.

- **Email gateway security**: Most fileless malware enters a system through an attachment to an email message, so a robust email gateway security product that scans all attachments for malware should be part of a solid defense against this type of attack.
- **Firewall**: Foundational to any security system is firewall technology. A firewall can detect many threats at the perimeter—before they enter the trusted network. Because fileless malware enters a system through static binaries, many of these attacks can be stopped before they enter systems inside the trusted network.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com