SOLUTION BRIEF

Protecting Against Script-Based Malware

Malware authors have made detection challenging through techniques such as polymorphism, implanting watchdogs, revoking permissions, and many others.

During this decade, we have seen attackers leverage features such as 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 because the malicious code can be implanted directly in the registry of a compromised host.

Script-based infections have been around for years. Even though they were considered fileless, previous malware families would drop a small binary on the disk in the initial attack before moving into a system's main memory.

However, the latest evasion techniques used by scripting malware leave no trace on disk, making for harder detection, which generally relies on finding static files. Read our thorough analysis of script-based malware in the *McAfee Labs Threats Report: September 2017.*

Three types of script-based malware are common:

- **Memory resident:** This type of 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.
- **Rootkits:** Some malware hides its presence behind a user- or kernel-level application programming interface (API). A file is present on disk but in stealth mode.
- **Windows registry:** Some advanced script malware types reside in the Windows registry. Malware authors have exploited features in the past such as the Windows thumbnail cache, used to store images for Explorer's thumbnail view. The thumbnail cache acts as a persistence mechanism for the attack. Malware of this type must still enter the victim's system through a static binary. Most use email as the attacking vector 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.

Today, malware authors have cleverly crafted the script malware families 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 deletes itself once the system is ready for the malicious operation.

Policies and Procedures to Protect Against Script-Based Malware

The latest McAfee cyber defense best practices recommend the adoption of the following general threat mitigation strategies for network and endpoints:

- The best way to protect your system from script malware infections is to stop them before they happen. Prevention is the key. The biggest factor in preventing any kind of malware infection on a computer is the user. Users need to be aware of the risks of downloading and installing applications that they do not understand or trust. On top of that, malware could be inadvertently downloaded by unaware users while browsing.
- Apply security updates and patches for your applications and operating system.
- Keep your web browsers and add-ons up to date and antimalware in endpoints and network gateways upgraded and updated to the latest version.
- Never use computers that are not distributed and certified by your corporate IT security group. Script malware could be easily disseminated by unprotected assets connected to your corporate network.
- In case users have local administrator privileges to install applications by themselves, educate them to install only applications with trusted signatures from known vendors. It is very common for "harmless" applications offered online to have embedded rootkits and other script malware types.

- Avoid application downloads from nonweb sources. The likelihood of downloading malware from Usenet groups, IRC channels, instant messaging clients, or peer networks is very high. Links to websites in IRC and instant messages also frequently point to infected downloads.
- Implement an educational program for phishing attack prevention. Malware is commonly distributed by targeted emails.
- Use threat intelligence feeds combined with your antimalware technology. This combination will help you to improve the detection time of emerging and well-known malware threats.

How McAfee Helps Protect Against Script-Based Malware

Outright detection of script 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 this type of malware.

McAfee Endpoint Security

McAfee Endpoint Security (ENS) provides a collaborative security framework that reduces the complexity of endpoint security environments, and offers visibility into advanced threats, such as script malware, that speeds detection and remediation responses. Its extensible architecture provides a framework for security teams that are burdened with multiple solutions to more easily view, respond to, and manage the threat defense lifecycle.

McAfee ENS introduces several new technologies and improvements:

- **Real Protect.** Applies machine learning techniques to identify malicious code based on what it looks like, what it might do (pre-execution analysis), and what it does (dynamic behavioral analysis)—without signatures. Real Protect is a part of an effective defense strategy against script malware.
- **Dynamic Application Containment.** Includes the ability to contain a single instance of a process.
- **McAfee Client Proxy integration.** McAfee Endpoint Security can be combined with Multi-Layered Web Gateway Security, which provides pervasive protection wherever a user travels, eliminating the gap of off-network protection by connecting endpoints to the Web Gateway cloud service.
- **Firewall Module.** The next layer of protection insured by a proactive security strategy is to block the communication between your computer and the servers controlled by cybercriminals.
- **Threat Prevention Module.** On-Demand Scans now include a registry scanning option, useful for protecting against script malware. Administrators can create custom services Access Protection rules, which now include Windows services. Custom Application Exploit Prevention is available along with McAfee-supplied intrusion prevention system (IPS) signatures. Finally, Windows application protection has been added to Exploit Prevention rules.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) 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 ATD will protect against script 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 (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 preceding inspection engines, McAfee ATD 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 Threat Intelligence Exchange

Having an intelligence platform that can adapt over time to suit an environment's needs is important. McAfee Threat Intelligence Exchange (TIE) significantly reduces exposure to script 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 TIE 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 TIE 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 TIE 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-file hashes and immunize your environment against these known threats through policy enforcement. If any of the indicators trigger in the environment, McAfee TIE 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 script malware. McAfee Web Gateway (MWG) is a robust product that will boost your company's protection against this type of threat.

- **Gateway Anti-Malware Engine:** Signatureless intent analysis filters 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 MWG will deny attempts to connect to known malicious websites or websites that use malicious ad networks. In addition to these McAfee products, we recommend two additional classes of security technologies.
  - **Email gateway security:** Most script 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 script malware enters a system through static binaries, many of these attacks can be stopped before they enter systems inside the trusted network.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com