Solution Brief

Protecting Against GPU Malware

In the **McAfee® Labs Threats Report: August 2015**, we take an in-depth look into malware that deviates from the norm of leveraging an endpoint's system memory or CPU and instead attacks the graphics processing unit (GPU).

Malware that attacks or leverages an endpoint's GPU is not new. Bitcoin-mining Trojans that leverage the GPU's throughput to increase the potential payouts from the compromised system have been in the wild for at least four years. However, the release of proof-of-concept code that claims to leverage GPU capabilities in never-before-seen ways has once again brought GPU-based malware into the spotlight. The claims, which are discussed at length in the report, can be distilled into four main points:

- CPU host memory access from the GPU.
- Subsequent deletion of CPU host files.
- Persistence across warm reboots.
- Absence of GPU analysis tools.

GPU threats are a real concern, although malware performing this type of attack is still only a proof-of-concept. We have not yet seen any proliferation in the wild. The absence of tools that can conduct forensic analysis on GPUs has led to a situation in which reverse engineering and forensic analysis of GPU threats is a much more complex and challenging task than analyzing attacks that leverage memory or CPUs. Attackers have diminished the detection surface by moving malicious code off the CPU and memory, though not entirely because trace elements of their activity often remain on the endpoint.

Undoubtedly there will be more advancements in GPU-based malware from attackers, and only time will tell how prolific these types of attacks will become.

Safeguarding Against GPU Malware

McAfee Labs recommends several ways to protect systems against GPU attacks:

- Enable automatic operating system updates or download OS updates regularly to keep systems patched against known vulnerabilities.
- Install patches from other software manufacturers as soon as they are distributed.
- Place endpoint security software on all endpoints and keep anti-malware signatures up to date.
- Consider application whitelisting to stop the execution of unauthorized applications.
- Avoid running applications in administrator mode whenever possible.

How Intel Security Can Help Protect Against GPU Malware

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection solution 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 helps protect against advanced malware.

- **Signature-based detection:** Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. McAfee Advanced Threat Defense includes a comprehensive knowledgebase that is created and maintained by McAfee Labs and currently includes more than 150 million signatures.
- **Reputation-based detection:** Looks up the reputation of files using the McAfee Global Threat Intelligence (McAfee GTI) service 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 to fully analyze 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 the specific malware.
- **Dynamic sandbox analysis:** Executes the file code in a virtual runtime environment and observes the resulting behavior. Virtual environments can be configured to match your company's host environments and supports custom operating system (OS) images of Microsoft Windows 7 (32-/64-bit), Windows XP, Windows Server 2003, Windows Server 2008 (64-bit), and Android.

McAfee VirusScan Enterprise

McAfee VirusScan® Enterprise uses the award-winning Intel Security scanning engine to protect files from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks:** Integrates anti-malware technology with intrusion prevention to protect against attacks that leverage buffer overflow exploits targeted at vulnerabilities in applications.
- **Unbeatable malware detection and cleaning:** Protects against threats such as rootkits and Trojans with advanced behavioral analysis. It stops malware in its tracks through multiple techniques, including port blocking, filename blocking, folder/directory lockdown, file-share lockdown, and infection trace and block.
- **Real-time security with McAfee GTI integration:** Protects against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform on the market.

McAfee Threat Intelligence Exchange

An intelligence platform that can adapt to suit your environment's needs is essential. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks, thanks to its visibility into immediate threats such as unknown files or applications.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global 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 executing 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 its powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into the actions of an application or process, from installation to the present state, enables faster response and remediation.
- **Indicators of compromise (IoCs):** IoCs often import known bad files hashes. McAfee Threat Intelligence Exchange can immunize your environment against these known bad files through policy enforcement. If any of the IoCs trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the IoC.

McAfee Application Control

McAfee Application Control lets your business control which applications are allowed to run in your environment through dynamic whitelisting and enforcement policies on both connected and disconnected endpoints—ensuring your organization is protected against vulnerable or known malicious applications.

- **Dynamic whitelisting:** Enable your organization to efficiently manage your whitelisted applications by developing your whitelist automatically as systems are patched and updated.
- **File reputation:** Integration with McAfee GTI allows McAfee Application Control to query real-time feeds of known good, bad, and unknown file types to help with whitelisting and keep your company aware of vulnerabilities or attacks from applications that may have been altered.
- **Protection whether connected or disconnected:** Enforce controls on connected or disconnected servers, virtual machines, endpoints, and fixed-function devices such as point-of-sale terminals.

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