Kurzvorstellung

Schutz vor GPU-Malware

Im **McAfee® Labs Threat-Report vom August 2015** werfen wir einen genauen Blick auf Malware, die nicht wie üblich den Systemspeicher oder die CPU von Endgeräten ausnutzt, sondern stattdessen den Grafikprozessor (Graphics Processing Unit, GPU) angreift.

Malware, die die GPU von Endgeräten angreift oder ausnutzt, ist nicht neu. So sind bereits seit mindestens vier Jahren Bitcoin-Mining-Trojaner bekannt, die die enorme Rechenleistung der GPU ausnutzen, um auf kompromittierten Systemen Bitcoins berechnen zu lassen. Die Veröffentlichung von Proof-of-Concept-Code, der GPU-Funktionen angeblich in völlig neuer Form nutzen kann, hat GPU-basierte Malware wieder in den Mittelpunkt gerückt. Die genauen Aussagen, die im Bericht ausführlich diskutiert werden, können zu folgenden Kernpunkten zusammengefasst werden:

- Zugriff von der GPU auf den CPU-Host-Speicher
- Anschließende Löschung der CPU-Host-Dateien
- Übersteht Systemneustarts („Warm Reboots“)
- Keine GPU-Analyse-Tools

Auch wenn entsprechende Malware bisher nur als Proof-of-Concept existiert, stellen GPU-Angriffe eine echte Bedrohung dar. Bisher sind uns noch keine tatsächlichen Angriffe dieser Art bekannt geworden. Da es keine Tools zur forensischen GPU-Analyse gibt, sind Reverse Engineering und forensische Untersuchungen von GPU-Bedrohungen erheblich komplexer und schwieriger als die Analyse von Angriffen, die Systemspeicher und CPUs nutzen. Angreifer konnten die Erkennungsmöglichkeiten dadurch verringern, dass sie den böswilligen Code von der CPU und dem Speicher verschoben. Dies gelang ihnen jedoch nicht vollständig, sodass sie häufig noch Spuren ihrer Aktivitäten auf dem Endgerät hinterlassen.

Zweifellos werden die Angreifer GPU-basierte Malware weiter verbessern, und die Zukunft wird zeigen, wie sehr sich entsprechende Angriffe verbreiten werden.

Möglichkeiten zum Schutz vor GPU-Malware

McAfee Labs empfiehlt verschiedene Methoden zum Schutz von Systemen vor GPU-Angriffen:

- Aktivieren Sie die automatische Update-Funktion des Betriebssystems, oder laden Sie regelmäßig die Betriebssystem-Updates herunter, um das System vor bekannten Sicherheitslücken zu schützen.
- Installieren Sie Patches anderer Software-Hersteller, sobald diese verfügbar sind.
- Setzen Sie auf allen Endgeräten Endgerätesicherheits-Software ein, und halten Sie die Malware-Schutzsignaturen auf dem neuesten Stand.

intel Security

- Nutzen Sie Anwendungs-Whitelists, um die Ausführung nicht autorisierter Anwendungen zu verhindern.
- Vermeiden Sie nach Möglichkeit die Ausführung von Anwendungen im Administratormodus.

So kann Intel Security vor GPU-Malware schützen

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense ist eine mehrstufige Lösung zum Aufspüren von Malware, die über mehrere Untersuchungsmodule verfügt. Durch die Kombination mehrerer Module, die Signatur- und Reputations-basierte Untersuchungen, Echtzeitemulationen sowie vollständige statische Code- und dynamische Sandbox-Analysen durchführen, schützt McAfee Advanced Threat Defense vor hochentwickelter Malware.

- **Erkennung auf Signaturbasis:** Die Lösung erkennt Viren, Würmer, Spyware, Bots, Trojaner, Buffer Overflows sowie komplexe Angriffe. McAfee Advanced Threat Defense beinhaltet eine umfassende Wissensdatenbank, die von McAfee Labs erstellt sowie gepflegt wird und derzeit mehr als 150 Millionen Signaturen umfasst.
- **Erkennung auf Reputationsbasis:** Durch die Überprüfung der Datei-Reputation mithilfe des McAfee Global Threat Intelligence-Services (McAfee GTI) werden neue Bedrohungen erkannt.
- **Statische Analyse und Emulation in Echtzeit:** Statische Echtzeitanalyse und Emulation ermöglichen die schnelle Erkennung von Malware und Zero-Day-Bedrohungen, die von Signatur- oder Reputations-basierten Verfahren nicht erkannt werden.
- **Vollständige statische Code-Analyse:** Mithilfe von Reverse Engineering des Datei-Codes werden alle Attribute und Anweisungsfolgen bewertet und der Quell-Code analysiert, ohne den Code ausführen zu müssen. Umfassende Entpackfunktionen öffnen gepackte und komprimierte Dateien jedes Typs, um Malware vollständig zu analysieren und einzustufen, sodass Ihr Unternehmen weiß, welche Gefahren von einer bestimmten Malware ausgehen.
- **Dynamische Sandbox-Analyse:** Bei der Sandbox-Analyse wird der Datei-Code in einer virtuellen Ausführungsumgebung ausgeführt und sein Verhalten beobachtet. Dabei werden die virtuellen Umgebungen so konfiguriert, dass sie mit Host-Umgebungen Ihres Unternehmens übereinstimmen – unabhängig davon, ob Sie benutzerdefinierte Betriebssystemabbilder von Microsoft Windows 7 (32- und 64-Bit-Versionen), Windows XP, Windows Server 2003, Windows Server 2008 (64-Bit-Version) oder Android benötigen.

McAfee VirusScan Enterprise

McAfee VirusScan® Enterprise nutzt das preisgekrönte Intel Security-Scan-Modul zum Schutz von Dateien vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutztechnologien und Eindringungsschutz können Angriffe abgewehrt werden, die mithilfe von Buffer Overflows Schwachstellen in Anwendungen angreifen.
- **Unschlagbare Malware-Erkennung und -Bereinigung:** Die erweiterte Verhaltensanalyse schützt vor Bedrohungen wie Rootkits und Trojanern. Mithilfe von Techniken wie der Blockierung von Ports und Dateinamen, der Sperrung von Ordnern bzw. Verzeichnissen und Freigaben sowie der Verfolgung und Blockierung von Infektionen wird Malware schon im Ansatz aufgehalten.
- **Echtzeitsicherheit mit McAfee GTI:** Die Plattform für die branchenweit umfassendsten Bedrohungsdaten bietet Schutz vor bekannten und neuen Bedrohungen aus allen Vektoren – Dateien, Web, E-Mails und Netzwerk.

McAfee Threat Intelligence Exchange

Eine Plattform zur Bedrohungsanalyse, die sich an die Anforderungen Ihrer Umgebung anpassen kann, ist für Ihr Unternehmen unverzichtbar. Dank der Erkennung unmittelbarer Bedrohungen wie unbekannter Dateien oder Anwendungen kann **McAfee Threat Intelligence Exchange** die Anfälligkeit für diese Art von Angriffen erheblich verringern.

- **Umfassende Bedrohungsanalyse:** Die umfassenden Bedrohungsdaten von weltweiten Datenquellen können unkompliziert angepasst werden. Dabei kann es sich um Feeds von McAfee GTI oder Drittanbietern handeln, die mit lokalen Bedrohungsdaten aus Echtzeit- sowie Verlaufsereignissen kombiniert und über Endgeräte, Gateways sowie andere Sicherheitskomponenten weitergegeben werden.
- **Ausführungsschutz und Behebung:** McAfee Threat Intelligence Exchange kann unbekannte Anwendungen daran hindern, in der Umgebung ausgeführt zu werden. Wenn eine Anwendung, die sich später als böswillig herausstellt, zuvor ausgeführt wurde, kann McAfee Threat Intelligence Exchange die laufenden Prozesse dieser Anwendung in der gesamten Umgebung deaktivieren. Dabei greift die McAfee-Lösung auf ihre leistungsfähigen Funktionen zur zentralen Verwaltung und Richtlinien-durchsetzung zurück.
- **Sichtbarkeit:** McAfee Threat Intelligence Exchange kann alle gepackten ausführbaren Dateien und deren Start in der Umgebung sowie alle anschließend stattfindenden Veränderungen verfolgen. Dieser Einblick in die Aktionen von Anwendungen oder Prozessen ab der Installation bis zur Gegenwart ermöglicht schnellere Reaktionen und Behebungsmaßnahmen.
- **Kompromittierungsindikatoren:** Kompromittierungsindikatoren importieren häufig Dateien mit gefährlichen Hash-Werten. McAfee Threat Intelligence Exchange kann Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen immunisieren. Wenn bekannte Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit dem Indikator in Zusammenhang stehen.

McAfee Application Control

Mit **McAfee Application Control** kann Ihr Unternehmen mit dynamischen Whitelists und Durchsetzungs-richtlinien für vernetzte und eigenständige Endgeräte kontrollieren, welche Anwendungen in Ihrer Umgebung ausgeführt werden. Dadurch kann Schutz vor Schwachstellen oder bekannten böswilligen Anwendungen gewährleistet werden.

- **Dynamische Whitelists:** Damit kann Ihr Unternehmen Anwendungen, die auf einer Whitelist geführt werden, effektiv verwalten, indem die Whitelist automatisch erweitert wird, sobald die Systeme gepatcht und aktualisiert werden.
- **Datei-Reputation:** Durch die Integration von McAfee GTI kann McAfee Application Control Echtzeitinformationen zu gefährlichen, ungefährlichen und unbekannten Dateitypen abrufen, sodass Ihr Unternehmen eine Whitelist erstellen kann und stets über neue Schwachstellen oder Angriffe von Anwendungen informiert ist, die möglicherweise geändert wurden.
- **Schutz mit und ohne Vernetzung:** Setzen Sie Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten und Geräten mit fester Funktion wie Kassen-terminals durch.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com