Kurzvorstellung

Schutz vor Manipulationen von Firmware und BIOS

Im ***McAfee Labs Threat-Report vom Mai 2015*** werfen wir einen genauen Blick auf die „Equation Group“ und ihre Angriffe auf die Firmware von Festplatten (HDD) und Solid State Drives (SSD). Die „Equation Group“, die ihre Bezeichnung aufgrund außerordentlich hochentwickelter Verschlüsselungsmethoden und der dazugehörigen Malware erhielt, zählt mittlerweile zu den auffälligsten und raffiniertesten jemals beobachteten Firmware-Bedrohungen.

Eines der wichtigsten Forschungsergebnisse sind Module zur Umprogrammierung der Firmware von Festplatten und Solid State Drives. Die umprogrammierte Firmware dieser Laufwerke kann bei jedem Neustart zugehörige Malware neu laden, sodass die Bedrohung auch dann bestehen bleibt, wenn die Laufwerke umformatiert oder das Betriebssystem neu installiert werden. Hinzu kommt, dass die umprogrammierte Firmware und die dazugehörige Malware nach der Infektion für Sicherheits-Software unsichtbar bleiben.

In den letzten Jahren beobachtete Intel Security viele Malware-Varianten mit Funktionen zur Manipulation von Firmware oder BIOS. Sie wurden in akademischen PoCs, aber auch in real eingesetzten Exemplaren verwendet, darunter **CIH/Chernobyl**, Mebromi und **BIOSkit**. Zudem sagten wir in den *Bedrohungsprognosen von McAfee Labs für 2012* genau diese Art von Angriffen voraus. Wir stufen die Varianten der „Equation Group“ als die bekanntesten und raffiniertesten jemals beobachteten Beispiele für Firmware-Angriffe ein.

Schutz vor Equation Group-Angriffen

Mit diesen Richtlinien und Verfahrensweisen können Sie sich vor Equation Group-Angriffen schützen:

- Installieren Sie Sicherheits-Software auf allen Endgeräten.
- Aktivieren Sie die automatische Update-Funktion des Betriebssystems, oder laden Sie regelmäßig die Betriebssystem-Updates herunter, um das Betriebssystem vor bekannten Sicherheitslücken zu schützen.
- Installieren Sie Patches anderer Software-Hersteller, sobald diese verfügbar sind.
- Verschlüsseln Sie wichtige Daten und Laufwerke.
- Wehren Sie Massen-Phishing-Kampagnen mithilfe sicherer Gateway-E-Mail-Filterung ab.
- Überprüfen Sie die Absenderidentität, damit sich Internetkriminelle nicht als vertrauenswürdige Parteien tarnen können.

intel Security

- Erkennen und blockieren Sie gefährliche Anhänge mithilfe von hochentwickeltem Malware-Schutz.
- Scannen Sie URLs in E-Mails beim Erhalt der E-Mail und beim Klick auf den Link.
- Überprüfen Sie den Web-Datenverkehr auf Malware, wenn Phishing-Angriffe den Benutzer zu mehreren Mausklicks auffordern.
- Schulen Sie Ihre Benutzer über empfohlene Vorgehensweisen zur Erkennung und Reaktion auf verdächtige E-Mails.
- Implementieren Sie Systeme zur Verhinderung von Datenkompromittierungen und -exfiltrationen bei Dateneinbrüchen.

So kann Intel Security vor Equation Group-Angriffen schützen

Der Schutz vor Manipulationen von Firmware und BIOS sollte zum Sicherheitskonzept jedes Unternehmens gehören. Dabei sind zwei Bereiche von Bedeutung:

- Implementierung von Erkennungsmaßnahmen für die Erstinfektion von Equation Group-Malware. Die bekannten Angriffsvektoren sind Phishing, CDs und USB-Laufwerke. Widmen Sie diesen Bereichen besondere Aufmerksamkeit.
- Schutz von Systemen vor Datenexfiltration. Obwohl das Modul zur Firmware-Umprogrammierung heute noch nicht erkannt werden kann, ist das Ziel des Angriffs sehr wahrscheinlich die Ausspähung. Da zur Ausspähung systematische Kommunikation und die Datenweitergabe an einen Kontroll-Server gehört, ist die Blockierung dieses Schritts unverzichtbar.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense ist eine mehrschichtige Malware-Erkennungslösung, die mehrere Analysemodule kombiniert. Die Module wenden signatur- und reputationsbasierte Analysen, Echtzeit-Emulation, vollständige statische Code- sowie dynamische Sandbox-Analysen an. McAfee Advanced Threat Defense schützt vor hochentwickelter Malware, die von umprogrammierter Firmware immer wieder neu geladen wird.

- **Erkennung auf Signaturbasis:** Erkennt Viren, Würmer, Spyware, Bots, Trojaner, Buffer Overflows sowie komplexe Angriffe. Ihre von McAfee Labs erstellte und gepflegte umfassende Wissensdatenbank umfasst derzeit mehr als 150 Millionen Signaturen.
- **Erkennung auf Reputationsbasis:** Überprüft die Reputation von Dateien mithilfe des McAfee Global Threat Intelligence-Services zur Erkennung neuer Bedrohungen.
- **Statische Analyse und Emulation in Echtzeit:** Bietet statische Echtzeitanalyse und Emulation zur schnellen Erkennung von Malware und Zero-Day-Bedrohungen, die von Signatur- oder Reputations-basierten Verfahren nicht erkannt werden.
- **Vollständige statische Code-Analyse:** Führt ein Reverse Engineering des Datei-Codes durch, um alle Attribute und Anweisungsfolgen zu bewerten und den Quell-Code zu analysieren, ohne ihn dabei auszuführen. Dank umfangreicher Funktionen zum Entpacken aller Arten gepackter und komprimierter Dateien kann Malware vollständig analysiert und klassifiziert werden, sodass Ihr Unternehmen die Bedrohung der spezifischen Malware besser versteht.
- **Dynamische Sandbox-Analyse:** Führt den Datei-Code in einer virtuellen Ausführungsumgebung aus und beobachtet sein Verhalten. Dabei werden die virtuellen Umgebungen so konfiguriert, dass sie mit Host-Umgebungen Ihres Unternehmens übereinstimmen – unabhängig davon, ob Sie benutzerdefinierte Betriebssystemabbilder von Windows 7 (32- oder 64-Bit-Versionen), Windows XP, Windows Server 2003, Windows Server 2008 (64-Bit-Version) oder Android benötigen.

McAfee Threat Intelligence Exchange
Sie benötigen eine Informationsplattform, die sich an Ihre Umgebung anpassen lässt. 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 Richtliniendurchsetzung 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:** Die Hash-Werte bekannt gefährlicher Dateien werden in McAfee Threat Intelligence Exchange importiert, um Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen zu immunisieren. Wenn diese Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit dem Indikator in Zusammenhang stehen.

McAfee VirusScan Enterprise
McAfee VirusScan® Enterprise nutzt das preisgekrönte McAfee-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 Sektoren – Dateien, Web, E-Mails und Netzwerk.

McAfee Network Security Platform

McAfee Network Security Platform ist für die Durchführung tiefgehender Netzwerkdatenverkehr-Überprüfungen ausgelegt. McAfee Network Security Platform setzt auf eine Kombination fortschrittlicher Untersuchungstechniken zur Erkennung sowie Abwehr bekannter und Zero-Day-Angriffe im Netzwerk. Diese Techniken umfassen unter anderem die vollständige Analyse der Protokolle, der Bedrohungs-Reputation und des Verhaltens sowie fortschrittliche Malware-Analyse.

- **Umfassender Malware-Schutz:** Die Lösung kombiniert McAfee GTI-Datei-Reputationsdaten sowie Datei-Tiefenanalysen mit JavaScript-Überprüfungen und umfasst ein signaturloses hochentwickeltes Malware-Analysemodul zur Erkennung und Abwehr von Zero-Day-Bedrohungen, angepasster Malware sowie anderen verborgenen Angriffen.
- **Hochentwickelte Analysetechniken:** Die Lösung umfasst die vollständige Analyse der Protokolle, der Bedrohungs-Reputation und des Verhaltens zur Erkennung sowie Abwehr bekannter und Zero-Day-Angriffe im Netzwerk.
- **Integration von McAfee Global Threat Intelligence:** Kombiniert Echtzeit-Datei-Reputations-, IP-Reputations- und Standort-Feeds mit detaillierten Kontextdaten zu Benutzern, Geräten und Anwendungen, um schnell und präzise auf Angriffe aus dem Netzwerk reagieren zu können.
- **Security Connected:** Dank der zuverlässigen Integration von McAfee Advanced Threat Defense kann die McAfee Network Security Platform verdächtige Dateien, die in überwachtem Datenverkehr gefunden wurden, an McAfee Advanced Threat Defense übermitteln und dann gemäß den von McAfee Advanced Threat Defense zurückgegebenen Angaben zulassen oder ablehnen.

McAfee DLP Monitor

McAfee Data Loss Prevention (DLP) Monitor sammelt, verfolgt und meldet Informationen zum Datenverkehr im gesamten Netzwerk. So können Sie unbekannte Gefahren für Daten erkennen, Maßnahmen zu ihrem Schutz einleiten und Ihr Unternehmen damit vor Dateneinbrüchen bewahren.

- **Überprüfung des Netzwerkverkehrs:** Die branchenweit führende McAfee DLP Monitor-Funktion zum Scannen und Analysieren von Daten unterzieht den Netzwerkverkehr einer Tiefenprüfung.
- **Schnelle Erkennung von Daten:** Mit der Echtzeiterkennung können Sie schnell erfassen, wie Daten verwendet werden, wer sie verwendet und wohin sie übertragen werden. Dadurch verfügen Sie über praktisch verwertbare Informationen. McAfee DLP Monitor kann mehr als 300 über beliebige Ports oder Protokolle übertragene Inhaltstypen erkennen, sodass Ihr Unternehmen jederzeit den vollen Überblick behält.
- **Durchführung detaillierter forensischer Analyse:** Ermöglicht die Durchführung forensischer Analysen zur Korrelation aktueller und vergangener Risikoereignisse sowie zur Erkennung von Risikotrends und Bedrohungen. Dadurch können Sie Situationen schnell erfassen sowie adäquate Richtlinien und Verhaltensweisen entwickeln.

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Prevent stellt sicher, dass Daten nur dann das Netzwerk verlassen, wenn es situationsgerecht ist – unabhängig davon, ob per E-Mail, Internet-E-Mail, Instant Messenger, über Wikis, Blogs, Portale, HTTP/HTTPS- oder FTP-Übertragungen. Die Lösung bietet damit Schutz vor Datenverlusten. Die schnelle Erkennung und Reaktion bei Exfiltrationsversuchen bewahrt Sie nicht nur vor dem Verlust wichtiger Daten, sondern auch vor negativen Schlagzeilen in den Medien.

- **Übersicht bei Sicherheitsvorfällen:** Angepasste Ansichten und Vorfallsberichte bieten eine Zusammenfassung sowie detaillierte Darstellungen von Sicherheitsvorfällen und den ergriffenen Behebungs-Maßnahmen.
- **Präventive Richtliniendurchsetzung bei allen Datentypen:** Gewährleistet die Richtliniendurchsetzung bei offensichtlich sowie weniger offensichtlich vertraulichen Daten. Dank zahlreicher integrierter Richtlinien (z. B. für Compliance, zulässige Nutzung und geistiges Eigentum) können Sie ganze Dokumente oder Teile davon mit einem umfassenden Satz von Regeln abgleichen, sodass alle sensiblen Informationen geschützt werden.

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