Technische Kurzbeschreibung

Schutz vor Ransomware

Verhindern Sie mit Sicherheitsprodukten von Intel® Security Bedrohungen durch neueste Ransomware-Varianten.

Ransomware ist Malware, die die Daten ihres Opfers mittels asymmetrischer Verschlüsselung als Geiseln nimmt. Asymmetrische (öffentlich-private) Verschlüsselung ist eine Form von Kryptografie, bei der ein Schlüsselpaar zum Ver- und Entschlüsseln einer Datei verwendet wird. Der Angreifer generiert das einmalige öffentlich-private Schlüsselpaar für das Opfer, wobei der private Schüssel für die Entschlüsselung der Dateien auf dem Server des Angreifers abgelegt wird. Der Angreifer verspricht dem Opfer, ihm den privaten Schlüssel nach Zahlung eines Lösegeldes auszuhändigen – ein Versprechen, das in der Vergangenheit nicht immer gehalten wurde. Ohne Zugang zu diesem privaten Schlüssel ist es fast unmöglich, die in Geiselhaft genommenen Dateien zu entschlüsseln.

Es gibt viele Ransomware-Formen. Ransomware (und andere Malware) wird häufig über E-Mail-Spam-Kampagnen oder gezielte Angriffe übertragen. Sicherheitsprodukte von Intel® Security nutzen eine Vielzahl an Technologien zur Verhinderung von Ransomware. Die folgenden McAfee®-Lösungen und entsprechenden Konfigurationen sind dafür ausgelegt, viele der Ransomware-Formen abzuwehren.

McAfee VirusScan® Enterprise 8.8 oder McAfee Endpoint Security 10

- Halten Sie DAT-Dateien auf dem neuesten Stand.
- Stellen Sie sicher, dass McAfee Global Threat Intelligence (McAfee GTI) verwendet wird. McAfee GTI enthält mehr als 8 Millionen verschiedene Ransomware-Signaturen.
- Erstellen Sie Zugriffsschutzregeln, um die Installation von Ransomware-Schaddaten zu verhindern. Informationen dazu finden Sie in den Wissensdatenbank-Artikeln KB81095 und KB54812.

McAfee Host Intrusion Prevention

- In diesem Video erfahren Sie, wie Sie McAfee Host Intrusion Prevention konfigurieren, müssen um CryptoLocker-Inhalte abzuwehren.
- Aktivieren Sie die Signatur 3894 von McAfee Host Intrusion Prevention, „Access Protection—Prevent svchost.exe executing non-Windows executables“ (Zugriffsschutz, um zu verhindern, dass „svchost.exe“ ausführbare Dateien ausführt, die nicht von Windows stammen).
- Aktivieren Sie die Signaturen 6010 und 6011 von McAfee Host Intrusion Prevention, um die Injektion sofort zu blockieren.

intel Security

McAfee Host Intrusion Prevention-Regeln
McAfee Host Intrusion Prevention überwacht Aktionen wie das Erstellen, Lesen, Ausführen, Löschen und Umbenennen von Dateien, Ändern von Attributen sowie Erstellen einer festen Verknüpfung. Legen Sie fest, bei welchem Dateipfad/-typ sie (explizit nicht) gewarnt werden möchten und welche ausführbaren Dateien Sie einschließen (bekannte gefährliche Quellen) oder ausschließen (bekannte Auslöser von False-Positives) wollen. Diese Regel stellt unter Umständen einen erheblichen Eingriff dar. Sie sollten daher in Betracht ziehen, die Regel für einen Testzeitraum im informativen/Protokoll-Modus zu verwenden. Beachten Sie, dass Regeln zum Dateischutz die Erstellung einer Datenbank Ihrer vertrauenswürdigen Anwendungen erfordert.

Rule: Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

Beachten Sie, dass im folgenden Beispiel viele Dateierweiterungen auf Grund von Platzbeschränkungen ausgelassen wurden. Achten Sie darauf, alle zutreffenden Dateierweiterungen für Ihre Anwendungen zu prüfen.

Rule {

tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”

Class Files

Id 4001

level 4

files {Include “**.3DS” “**.7Z” “**.AB4” “**.AC2” “**.ACCDB” “**.ACCDE” “**.ACCDR” “***.ACCDT” “**.ACR” “**.ADB” “**.AI” “**.AIT” “**.al” “**.APJ” “**.ARW” “**.ASM” “**.ASP” “**.BACKUP” “**.BAK” “**.BDB” “**.BGT” “**.BIK” “**.BKP” “**.BLEND” “**.BPW” “**.C” “**.CDF” “**. CDR” “**.CDX” “**.CE1” “**.CE2” “**.CER” “**.CFP” “**.SRF” “**.SRW” “**.ST4” “**.ST5” “**.ST6” “**.ST7” “**.ST8” “**.STC” “**.STD” “**. STI” “**.STW” “**.STX” “**.SXC” “**.SXD” “**.SXG” “**.SXI” “**.SXM” “**.SXW” “**.TXT” “**.WB2” “**.X3F” “**.XLA” “**.XLAM” “**.XLL” “**. XLM” “**.XLS” “**.XLSB” “**.XLSM” “**.XLSX” “**.XLT” “**.XLTM” “**. XLTX” “**.XLW” “**.XML” “**.ZIP”}

Executable {Include “*”}

user_name{Include “*”}

directives files:writefiles:renamefiles:delete

}

- Zugriffsschutzregeln: Sie können die Zugriffsschutzregeln auch nutzen, um die McAfee Host Intrusion Prevention-Regel mit dem folgenden flexiblen Platzhalter zu verstärken: **\Users**\AppData***.exe

Hinweis: Bei neueren Versionen von SYSCore, das mit aktualisierten Versionen von McAfee VirusScan Enterprise, McAfee Agent, McAfee Host Intrusion Prevention und McAfee Data Loss Prevention mitgeliefert wird, funktioniert ** zu Beginn des Felds „File or folder name to block“ (zu blockierender Datei- oder Ordnername) nicht mehr. Bei neueren Versionen müssen Sie das folgende Format verwenden:

```
C:\**\AppData\**.exe
```

Damit soll jede beliebige EXE-Datei im Stamm- und jedem Unterverzeichnis eines Ordners mit dem Namen „AppData“ an einem beliebigen Ort auf Laufwerk C: blockiert werden.

Die möglichen Iterationen einer Regel dieser Art sind nahezu unbegrenzt. Bedenken Sie daher sorgfältig alle Aspekte der Regel. Sie sollten alle Aspekte der Regel sowie die Auswirkungen sämtlicher Einträge bedenken und überprüfen, wie die Regeln als Ganzes konfiguriert werden können (siehe folgendes Beispiel):

Process to include: *

Process to exclude: [Leer lassen]

File or folder name to block: <Pfad oder Verzeichnis>

File actions to prevent: [Die gewünschte Aktion. (Wir empfehlen, mit weniger aggressiven Aktionen zu beginnen, um den potenziellen Schaden für das Endgerät zu minimieren.)]

McAfee SiteAdvisor® Enterprise oder McAfee Endpoint Security/Web Protection

- Nutzen Sie die Reputation von Webseiten, um Benutzer vor Webseiten zu schützen oder zu warnen, über die Ransomware verbreitet wird.

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

- Richtlinienkonfiguration bei McAfee Threat Intelligence Exchange:
  - Beginnen Sie im Beobachtungsmodus: Wenn Endgeräte mit verdächtigen Prozessen erkannt werden, nutzen Sie System-Tags, um die Durchsetzungsrichtlinien von McAfee Threat Intelligence Exchange anzuwenden.
  - Säubern bei Reputation „Known malicious“ (Bekannt böswillig).
  - Blockieren bei Reputation „Most-likely malicious“ (Höchstwahrscheinlich böswillig). (Die Blockierung bei Status „Unknown“ (Unbekannt) würde besseren Schutz bieten, aber möglicherweise auch den Anfangsaufwand für Administratoren erhöhen.)
  - Legen Sie für die Option „Submit files to McAfee Advanced Threat Defense“ (Dateien an McAfee Advanced Threat Defense senden) die Statuswerte „Unknown“ (Unbekannt) und darunter fest.
  - McAfee Threat Intelligence Exchange Server-Richtlinie: Akzeptieren Sie die von McAfee Advanced Threat Defense festgelegten Reputationen für Dateien, die von McAfee Threat Intelligence Exchange noch nicht erkannt wurden.
- Manueller Eingriff bei McAfee Threat Intelligence Exchange:
  - Erzwingung der Datei-Reputation (bei Betriebsmodus) Bereinigen/Löschen bei Reputation „Most likely malicious“ (Höchstwahrscheinlich böswillig).
  - Blockieren bei Reputation „Might be malicious“ (Möglicherweise böswillig).
- Die Reputation innerhalb des Unternehmens kann McAfee GTI außer Kraft setzen.
  - Sie können optional festlegen, dass unerwünschte Prozesse blockiert werden (z. B. nicht unterstützte oder anfällige Anwendungen).

  - Kennzeichnen Sie die entsprechende Datei als „Might be malicious“ (Möglicherweise böswillig).
- Oder Sie erlauben einen unerwünschten Prozess zu Testzwecken:
  - Kennzeichnen Sie die entsprechende Datei als „Might be trusted“ (Möglicherweise vertrauenswürdig).

McAfee Advanced Threat Protection

- Integrierte Erkennungsfunktionen:
  - Signaturbasierte Erkennung: Signaturen, die von McAfee Labs gepflegt werden (mehr als 8 Millionen Signaturen, inklusive CTB-Locker, CryptoWall und entsprechende Varianten).
  - Reputationsbasierte Erkennung durch McAfee GTI.
  - Statische Analyse und Emulation in Echtzeit: Werden zur signaturlosen Erkennung verwendet.
  - Benutzerdefinierte YARA-Regeln.
  - Vollständige statische Code-Analyse: Führt ein Reverse Engineering des Datei-Codes durch, um Attribute sowie Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen.
  - Dynamische Sandbox-Analyse.
- Erstellen Sie Analyseprofile für die Bereiche, unter denen Ransomware vermutlich ausgeführt wird:
  - Verbreitete Betriebssysteme, Windows 7, Windows 8, Windows XP.
  - Installieren Sie Windows-Anwendungen (Word, Excel), und aktivieren Sie Makros.
- Internetzugriff für das Analyseprogramm-Profil:
  - Viele Malware-Varianten führen ein Skript aus einem Microsoft-Dokument aus, das eine ausgehende Verbindung herstellt und den Schadcode aktiviert. Dem Analyseprogramm-Profil wird eine Internetverbindung bereitgestellt, was die Erkennungsraten weiter erhöht.

McAfee Network Security Platform

- McAfee Network Security Platform verfügt in seinen Standardrichtlinien über Signaturen zur Erkennung folgender Bedrohungen:
  - Überprüfen Sie, ob die Signatur id=0x4880f900 bei Ihnen vorliegt (typisch für Ransomware).
  - McAfee Network Security Platform verfügt auch über Signaturen zur Erkennung von Tor, das zur Übertragung von Dateien genutzt werden kann, die in Verbindung mit Malware stehen.
- Integration von McAfee Advanced Threat Defense zur Abwehr neuer Angriffsvarianten:
  - Konfigurieren Sie die Integration von McAfee Advanced Threat Defense in der erweiterten Malware-Richtlinie.
  - Konfigurieren Sie McAfee Network Security Platform so, dass EXE-Dateien, Microsoft Office-Dateien, Java-Archivdateien und PDF-Dateien zur Überprüfung an McAfee Advanced Threat Protection gesendet werden.
  - Überprüfen Sie, ob die Konfiguration von McAfee Advanced Threat Protection auf Sensorebene angewendet wird.
- Aktualisieren Sie die Callback-Erkennungsregeln (zum Schutz vor Botnets).

McAfee Web Gateway

- Aktivieren Sie die Analyse durch McAfee Gateway Anti-Malware.
- Aktivieren Sie McAfee GTI für URL- und Datei-Reputation.
- Integrieren Sie McAfee Advanced Threat Defense für Sandbox-Analysen und Zero-Day-Erkennung.

VirusTotal Convicter: Automatischer Eingriff

- Convicter ist ein Python-Skript, das vom automatischen Reaktionssystem von McAfee ePolicy Orchestrator® (McAfee ePO™) ausgelöst wird, um eine Datei, die ein McAfee Threat Intelligence Exchange-Bedrohungsereignis erzeugt, mit VirusTotal abzugleichen.
- Beachten Sie, dass Sie das Skript ändern können, so dass andere Daten zu Bedrohungsanalysen ausgetauscht werden, z. B. GetSusp.
- Wenn der Schwellenwert zum Vertrauen der Community erreicht wird, setzt das Skript automatisch die Unternehmensreputation fest.
- Vorgeschlagener Schwellenwert: 30 % der Anbieter und zwei wichtige Anbieter müssen zustimmen.
- Filter: Target File Name Does Not Contain (Name der Zieldatei enthält nicht): McAfeeTestSample.exe.
- Dies ist ein kostenloses, von der Community unterstütztes Tool (wird von McAfee/Intel Security nicht unterstützt).

McAfee Active Response

Active Response findet hochentwickelte Bedrohungen und reagiert darauf. Wenn die Anwendung zusammen mit Bedrohungsdaten-Feeds wie McAfee GTI, Dell SecureWorks oder ThreatConnect eingesetzt wird, können Sie nach neuen Bedrohungen – einschließlich Ransomware – suchen und diese entfernen, bevor sie die Gelegenheit haben, sich auszubreiten.

- Benutzerdefinierte Kollektoren ermöglichen die Entwicklung spezieller Tools, um mit Ransomware in Verbindung stehende Kompromittierungsindikatoren zu finden und zu identifizieren.
- Der Benutzer legt mit Auslösern und Reaktionen fest, welche Aktionen bei bestimmten Bedingungen ausgeführt werden sollen. Wenn zum Beispiel Hash-Werte oder Dateinamen gefunden werden, kann automatisch eine Löschen-Aktion ausgeführt werden.

Weitere Informationen

Protecting Against Ransomware (Schutz vor Ransomware)

In diesem Wissensdatenbank-Artikel erhalten Kunden aktuelle, detaillierte Informationen dazu, wie sie sich in einer Intel Security-Umgebung vor Ransomware schützen können.

In den folgenden Videos erhalten Sie umfangreiche Informationen zu den verschiedenen CryptoLocker-Ransomware-Varianten, Symptomen, Angriffsvektoren sowie zu möglichen Schutztechniken:

- CrytpoLocker Malware Session (CryptoLocker-Malware-Sitzung)
- CryptoLocker Update (Aktualisierung zu CryptoLocker)

McAfee Labs-Bedrohungshinweise: X97M/Downloader

In diesem Artikel finden Kunden eine detaillierte Analyse der neuesten Ransomware-Versionen.

Keine Chance für Ransomware: Schützen Sie Ihre Daten vor der Geiselnahme

In dieser fünfseitigen Kurzvorstellung wird erläutert, was Ransomware ist und wie einige (nicht alle) Lösungen von Intel Security helfen, Sie davor zu schützen.

Advice for Unfastening CryptoLocker Ransomware (Ratschläge, um sich von CryptoLocker-Ransomware zu befreien)

Detaillierter Blog-Artikel dazu, was ein Kunde nach einem Ransomware-Angriff machen sollte.

Ransomware kehrt zurück: Neue Familien drängen nach vorn

Artikel aus dem Threat-Report von McAfee Labs (Seite 14), in dem neue und sich entwickelnde Ransomware aufgezeigt wird.

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