Kurzvorstellung

„Trojanisierte“ legitime Software

Verhindern Sie mit Sicherheitsprodukten von Intel® Security die Infektion durch Bedrohungen sowie deren Ausbreitung

Die Mechanismen zur Verteilung von Software über das Internet können als Angriffsvektor für Malware und Viren missbraucht werden. Die raffinierten Distributoren legitimer Software, die vor oder während der Verteilung „trojanisiert“ wurde, haben kaum noch etwas gemein mit den ursprünglichen böswilligen Binder-Programmen, die vor einem Jahrzehnt aufkamen.

Unabhängig davon, wie raffiniert ein Trojaner ist, sind die grundlegenden Schritte stets die gleichen:

- Die Software wird in eine Waffe verwandelt: Die Malware wird in eine Anwendung eingefügt, die übertragen werden soll.
- Übertragung: Die Software mit dem unerkannten Trojaner wird an das Ziel übertragen.
- Ausnutzung: Der Trojaner-Code wird ausgeführt und versucht dabei unerkannt zu bleiben.
- Installation: Der Trojaner setzt sich fest und versucht sich innerhalb des Netzwerks weiterzubewegen.

Die neueste Angriffstechnik basiert auf einem hochentwickelten Mechanismus, bei dem der Code während der Übertragung in einen legitimen Download injiziert wird, um unerkannt zu bleiben. Das Angriffsprinzip besteht darin, den böswilligen Code mit der ursprünglichen Anwendung verschmelzen zu lassen.

Diese Angriffstechnik kann zwei Komponenten verwenden, um einen erfolgreichen Eindringungspunkt in das Ziel zu finden: Ein „Listener“ erfasst sowie modifiziert die HTTP-Download-Anfrage, und ein „Binder“ infiziert sowie verteilt die Binärdateien.

Aktuelle Algorithmen verwenden Malware-Infektionsroutinen und Netzwerkumleitungen, ohne dabei den Code der Anwendung zu ändern. Damit öffnet sich ein Einfallstor für den Missbrauch kommerzieller oder Open-Source-Software, der sich auch auf ausführbare Dateien mit einer eingebetteten Signatur erstrecken kann. Der Angriff kann nur gestoppt werden, wenn die Signatur vor der ersten Ausführung automatisch und vollständig überprüft wurde.

Nach dem Start der trojanisierten Anwendung auf dem Zielsystem erstellt ein „Binder“-Prozess eine eigene Datei für weitere eingebettete, ausführbare Dateien, in denen der gesamte injizierte Code zur weiteren Ausführung wiederhergestellt wird. Auf diese Weise werden alle Sicherheitskontrollen umgangen. Da die ursprüngliche Anwendung unverändert bleibt, muss sich die Malware lediglich an eine beliebige Datei mit einer Signatur anhängen, um erfolgreich zu sein.

intel Security

Richtlinien und Vorgehensweisen

Die neuesten empfohlenen Vorgehensweisen von Intel Security zur Abwehr von Cyber-Bedrohungen umfassen folgende allgemeine Strategien zum Schutz für Netzwerke und Endgeräte:

- Verwenden Sie bei Verbindungen mit einem nicht vertrauenswürdigen Netzwerk stets ein VPN. Administratoren sollten die Sicherheits-Software auf dem neuesten Stand halten und sich auf starke Indikatoren für Vertrauenswürdigkeit konzentrieren, anstatt auf solche, die für einen Angriff gefälscht werden können. Anwendungen sollten signiert und mit einer Vertrauenskette verifiziert werden. Im Rahmen forensischer Analysen sollten Hash-Werte mit vertrauenswürdigen Quellen korreliert werden.
- Da statische Scans nur eine begrenzte Wirksamkeit haben, sollte die verwendete Sicherheits-Software dynamische Analysen durchführen können, um böswillige Aktionen unabhängig von der ursprünglichen Binärdateienuntersuchung aufzudecken. Verhaltensüberwachung, Web- und IP-Reputation, Speicher-Scans sowie Anwendungsisolierung sind wichtige Komponenten in einer vollständigen Lösung.
- Anbieter-Downloads sollten über abgesicherte Verbindungen erfolgen, und jeglicher Code sollte signiert sein. Dies verringert erheblich die Erfolgsrate von Man-in-the-Middle-Angriffen. Software-Anbieter sollten in ihren Anwendungen Funktionen zur Selbstüberprüfung einschließen, ihren Code regelmäßig überprüfen, Tools zur statischen Code-Analyse nutzen und Peer Reviews durchführen. Sinnvoll ist die Erstellung eines zentralen Repositorys vertrauenswürdiger Unternehmensanwendungen, das für Benutzer als einzige Installationsquelle für Anwendungen verwendet werden darf.
- Konfigurieren Sie Malware-Schutz-Software so, dass „Binder"-Programme erkannt werden.
- Nutzen Sie Anwendungen zur Erkennung sowie Verhinderung von Host-Eindringungsversuchen, und konfigurieren Sie sie so, dass Pakete auf Schaddaten überprüft werden.
- Verwenden Sie ausschließlich vertrauenswürdige Virtualisierungsarchitekturen in Kombination mit angemessener Netzwerksegmentierung. Vertrauenswürdige Virtualisierungsarchitekturen nutzen einen sicheren und verifizierbaren Startvorgang. Mit der richtigen Netzwerksegmentierung können Sie den Datenverkehr überwachen und Anwendungen im Falle einer erfolgreichen Ausnutzung isolieren. Diese Kombination verhindert außerdem die Ausbreitung der Malware in Ihrem Netzwerk.
- Überwachen Sie ausgehenden Datenverkehr auf Malware, die durch trojanisierte Software übertragen wird. Auf diese Weise können Sie infizierte Systeme identifizieren und weiter untersuchen.

Intel Security

Intel Security-Sicherheitsprodukte können trojanisierte legitime Software identifizieren, die eingebettete Malware-Bedrohung erkennen und blockieren, Kompromittierungen aufdecken sowie schnell reagieren:

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 erkennt mehr als 600 Millionen verschiedene Malware-Signaturen.
- Erstellen Sie Zugriffsschutzregeln, um die Installation und Inhalte von Malware zu stoppen:
  - Informationen dazu finden Sie in den Wissensdatenbank-Artikeln KB81095 und KB54812.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee VirusScan Enterprise 8.8: PD22940.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention unterstützt Sie dabei, die Ausbreitung der Malware zu verhindern. Dank benutzerdefinierter IPS-Signaturen können Sie Regeln erstellen, mit denen von der Malware generierte Dateiaktionen (z. B. Erstellen, Schreiben, Ausführen, Lesen) blockiert werden.
- 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.
- Dies erreichen Sie mit zwei Unterregeltypen:

1. Erstellen Sie im Files-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
   - Name: <Namen einfügen>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <Pfad/Dateiname der Malware>
     - Der Dateiname muss einen Pfad enthalten. Wenn Sie im Pfad Platzhalter verwenden möchten, beginnen Sie den Dateinamen mit „**\“ bzw. „?:\“, wenn sich der Platzhalter auf den Laufwerkbuchstaben beziehen soll (z. B. „**\Dateiname.exe“ oder „?:\Dateiname.exe“).
     - Sie können für den Parameter „Files“ keine MD5-Hash-Werte, sondern nur Pfad/Dateiname verwenden.
     - Sie können den Laufwerktyp angeben, um den Pfad auf ein bestimmtes Laufwerk zu beschränken (z. B. Festplatte, CD-ROM, USB, Netzwerk, Diskette).
   - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf bestimmte Prozesse beschränken möchten, die die Dateiaktion ausführen (z. B. explorer.exe oder cmd.exe).
2. Erstellen Sie im Program-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
   - Name: <Namen einfügen>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <leer lassen>
   - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf einen bestimmten Prozess als ausführbare Quelle beschränken möchten (z. B. wenn Sie verhindern möchten, dass „explorer.exe“ ein Target Executable (z. B. notepad.exe) ausführen kann).
   - Target Executables: Definieren Sie die ausführbaren Eigenschaften, für die Sie die Ausführung verhindern möchten (z. B. wenn Sie die Ausführung von „notepad.exe“ blockieren möchten, geben Sie Pfad/Dateiname der ausführbaren Datei an). Die ausführbare Datei kann mit mehreren Kriterien definiert werden (Dateibeschreibung, Dateiname, Fingerabdruck, Signaturgeber).

McAfee SiteAdvisor® Enterprise oder McAfee Web Protection

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

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

- Richtlinienkonfiguration bei McAfee Threat Intelligence Exchange:
  - Starten 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:
  - Durchsetzung der Datei-Reputation (bei Betriebsmodus). „Most likely malicious“ (Höchstwahrscheinlich böswillig): Säubern/löschen.
  - „Might be malicious“ (Möglicherweise böswillig): Blockieren.
- 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 Defense

- Integrierte Erkennungsfunktionen:
  - Erkennung auf Signaturbasis: McAfee Labs erkennt mehr als 600 Millionen Signaturen.
  - 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 trojanisierte Software vermutlich ausgeführt wird:
  - Verbreitete Betriebssysteme, Windows 7, Windows 8, Windows 10.
  - 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 den Standardrichtlinien über Signaturen zur Erkennung des Netzwerks 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.
- Sie können das Skript so ändern, 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 Intel Security nicht unterstützt).

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response findet und reagiert auf hochentwickelte Bedrohungen. Wenn die Anwendung zusammen mit Bedrohungsdaten-Feeds von McAfee Labs, Dell SecureWorks oder ThreatConnect eingesetzt wird, können Sie nach neuen Bedrohungen suchen und diese entfernen, bevor sie die Gelegenheit haben, sich auszubreiten.
- Benutzerdefinierte Kollektoren ermöglichen die Entwicklung spezieller Tools, um mit trojanisierten Anwendungen 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

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak (Empfohlene Vorgehensweisen für die Verwendung von McAfee Host Intrusion Prevention-Regeln bei einem Malware-Ausbruch): KB84507

Wissensdatenbank-Artikel mit detaillierten Informationen zur Infektion und zu den Verbreitungsvektoren des Trojaners Trojan-Powelike: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors (Koordinierung von SIEM: Koordinierung deckt Hinweise auf Malware-Infektionen und anormales Verhalten auf): PD24830

Whitepaper: *Sicherheit auch ohne Signatur*

FAQs for Network Security Platform: Advanced Malware Detection (Häufige Fragen und Antworten zu McAfee Network Security Platform: Erkennung hochentwickelter Malware): KB75269

Produkthandbuch zu McAfee Web Gateway: Webseiten-Filter: PD26339

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