Kurzvorstellung

Schutz vor dateiloser Malware

Im ***McAfee® Labs Threat-Report vom November 2015*** werfen wir einen genauen Blick auf dateilose Malware und stellen technische Details von Kovter vor, das die Erkennung umgeht, indem es die Speicherung von Binärdateien auf der Festplatte verringert oder vollständig vermeidet und stattdessen Code in der Registrierung des kompromittierten Hosts verbirgt. Die Malware-Autoren erschweren die Erkennung zusätzlich durch Polymorphismus, Implantierung von Watchdogs, Widerruf von Berechtigungen und weitere Techniken. Im Jahr 2015 beobachteten wir auch Angriffe, die Funktionen wie Windows-Verwaltungsinstrumentation (WMI, Microsoft Windows Management Instrumentation) und Windows PowerShell nutzen, um Endgeräte zu kompromittieren, ohne jemals eine Binärdatei auf der Festplatte zu speichern. Dadurch wird die Untersuchung solcher Angriffe noch weiter erschwert.

Infektionen mit dateiloser speicherbasierter Malware sind in der Sicherheitsbranche seit Jahren bekannt. Auch wenn diese Malware-Form als dateilos bezeichnet wird, legten frühere Malware-Familien in der ersten Angriffsphase eine kleine Binärdatei auf der Festplatte ab, bevor sie in den Hauptspeicher des kompromittierten Hosts wechselten. Doch die jüngsten Verschleierungstechniken dateiloser Malware-Varianten (z. B. Kovter, Powelike und XswKit) hinterlassen auf der Festplatte keine Spuren, sodass die Entdeckung, die sich in der Regel auf statische Dateien auf der Festplatte stützt, schwieriger wird.

Es gibt drei gängige Arten dateiloser Malware:

- **Speicherresidente Malware:** Diese Form dateiloser Malware verwendet den Speicherbereich einer legitimen Windows-Datei. Diese Malware lädt den eigenen Code in diesen Speicherbereich und verbleibt dort, bis auf den Code zugegriffen oder dieser reaktiviert wird. Obwohl die Ausführung im Speicherbereich einer legitimen Datei erfolgt, gibt es eine ruhende physische Datei, die die Ausführung initiiert oder erneut startet. Dieser Malware-Typ ist somit nicht vollständig dateilos.
- **Rootkits:** Einige Formen dateiloser Malware verbergen ihre Gegenwart hinter einer API (Application Programming Interface) auf Benutzer- oder Kernel-Ebene. Es gibt zwar eine Datei auf der Festplatte, diese befindet sich jedoch in einer Art „Tarnmodus“.
- **Windows-Registrierung:** Einige neue Malware-Typen nisten sich in der Registrierung des Windows-Betriebssystems ein. Malware-Autoren machen sich Features wie den Windows-Cache für Miniaturansichten zunutze, mit dem Miniaturansichten für Windows Explorer gespeichert werden. Der Cache für Miniaturansichten fungiert dabei als Persistenzmechanismus für die Malware. Diese dateilose Malware muss immer noch über eine statische Binärdatei in das System des Opfers eindringen. In den meisten Fällen dient E-Mail als Medium, um das System zu erreichen. Wenn der Benutzer auf den E-Mail-Anhang klickt, schreibt die Malware die vollständige Schaddatendatei in verschlüsselter Form in die Windows-Registrierungshauptstruktur. Anschließend wird die Datei vom System entfernt, indem sie sich selbst löscht.

intel Security

Malware-Autoren haben die Malware-Familien Kovter, Powelike und XswKit geschickt so gestaltet, dass vollständig dateilose Angriffe auf die Windows-Registrierung gestartet werden können, ohne auch nur eine Spur zurückzulassen. Obwohl die Umgebung, in der diese Angriffe ausgeführt werden, durch die Ausführung von Code in einer Datei vorbereitet wird, zerstört sich die Datei selbst, sobald das System für die böswillige Operation bereit ist.

So kann Intel Security vor dateiloser Malware schützen

Die direkte Erkennung einer dateilosen Malware, die in der ersten Phase keine Binärdatei verwendet, kann schwierig sein und ist meist erst durch Untersuchungen von Sicherheitsunternehmen möglich. Zur Abwehr solcher dateiloser Malware bedarf es jedoch geeigneter Kontrollfunktionen, die den Angreifern gleich am Zugangspunkt den Zugriff verwehren.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense ist ein mehrstufiges Produkt zum Aufspüren von Malware, das 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 dateiloser Malware, die in der ersten Stufe eine Binärdatei auf dem Zielsystem ablegt.

- **Erkennung auf Signaturbasis:** Die Lösung erkennt Viren, Würmer, Spyware, Bots, Trojaner, Buffer Overflows sowie komplexe Angriffe. Die umfassende KnowledgeBase wird von McAfee Labs erstellt und gepflegt.
- **Erkennung auf Reputationsbasis:** Durch die Überprüfung der Datei-Reputation mithilfe von McAfee Global Threat Intelligence (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:** Für Dateien, deren Sicherheit nicht mit den oben genannten Untersuchungs-Modulen überprüft werden kann, kann McAfee Advanced Threat Defense den Datei-Code in einer virtuellen Laufzeitumgebung ausführen und das Dateiverhalten beobachten. Virtuelle Umgebungen können so konfiguriert werden, dass sie der jeweiligen Host-Umgebung entsprechen. McAfee Advanced Threat Defense unterstützt benutzerdefinierte Betriebssystem-Abbilder von Windows XP SP2 und SP3, Windows 7 (32-Bit- und 64-Bit-Versionen), Windows 8 (32-Bit- und 64-Bit-Versionen), Windows Server 2003, Windows Server 2008 (64-Bit-Versionen) und Android.

McAfee Threat Intelligence Exchange

Sie benötigen eine Informationsplattform, die sich im Laufe der Zeit an Ihre Umgebung anpassen lässt. Dank der Erkennung unmittelbarer Bedrohungen wie unbekannter Dateien oder Anwendungen, die in der Umgebung ausgeführt werden, kann **McAfee Threat Intelligence Exchange** die Anfälligkeit für Angriffe mit dateiloser Malware erheblich verringern.

- **Umfassende Bedrohungsanalyse:** Die umfassenden Bedrohungsdaten von weltweiten Bedrohungsdatenquellen 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 importiert, damit Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen bekannte immunisiert wird. Wenn diese Indikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit ihnen in Zusammenhang stehen.

McAfee Web Gateway

Drive-by-Downloads und böswillige URLs, die in Phishing-E-Mails eingebettet sind, sind die wichtigsten Methoden zur Übertragung von dateiloser Malware. Der zuverlässige **McAfee Web Gateway** dehnt den Schutz Ihres Unternehmens auf diese Art der Bedrohung aus.

- **McAfee Gateway Anti-Malware Engine:** Die signaturlose Absichtsanalyse filtert in Echtzeit gefährliche Inhalte aus dem Web-Datenverkehr heraus. Emulation und Verhaltensanalyse bieten präventiven Schutz vor Zero-Day-Bedrohungen und gezielten Angriffen. Die McAfee Gateway Anti-Malware Engine untersucht Dateien und blockiert das Herunterladen durch den Benutzer, falls sich die Dateien als böswillig erweisen.
- **Integration von McAfee GTI:** Der Echtzeit-Datendienst McAfee GTI bietet Datei- und Web-Reputation sowie Web-Kategorisierungsinformationen und schützt so vor den neuesten Bedrohungen, da McAfee Web Gateway alle Verbindungsversuche zu bekannt böswilligen Webseiten sowie zu Webseiten blockiert, die böswillige Werbenetzwerke nutzen.

Zusätzlich zu diesen Intel Security-Produkten empfehlen wir zwei weitere Sicherheitstechnologieklassen.

- **E-Mail-Gateway-Sicherheit:** Dateilose Malware gelangt meist über einen E-Mail-Anhang in ein System, sodass zum zuverlässigen Schutz vor diesen Angriffen ein solides E-Mail-Gateway-Sicherheitsprodukt mit Funktionen zum Scannen aller Anhänge auf Malware gehört.
- **Firewall:** Die Grundlage jedes Sicherheitssystems ist eine Firewall-Technologie. Eine Firewall kann viele Bedrohungen an der Peripherie erkennen, bevor sie in das vertrauenswürdige Netzwerk gelangen. Da dateilose Malware über statische Binärdateien in ein System gelangt, können viele dieser Angriffe gestoppt werden, bevor sie in Systeme innerhalb des vertrauenswürdigen Netzwerks gelangen.

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