# Schutz vor skriptbasierter Malware

Angreifer erschweren die Erkennung von Malware durch Polymorphismus, die Einschleusung von Watchdogs, den Widerruf von Berechtigungen und zahlreiche weitere Techniken.

In diesem Jahrzehnt 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. Die Untersuchung solcher Angriffe wird zusätzlich dadurch erschwert, dass der böswillige Code direkt in die Registrierung des kompromittierten Hosts eingeschleust werden kann.

Skriptbasierte Infektionen sind seit Jahren im Umlauf. 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 sich in den Hauptspeicher des kompromittierten Systems bewegten.

Da die neuesten Vertreter skriptbasierter Malware Verschleierungstechniken einsetzen, die keinerlei Spuren auf der Festplatte hinterlassen, ist die Bedrohungserkennung – meist auf der Suche nach statischen Dateien basierend – erheblich schwieriger. Weitere Informationen zu skriptbasierter Malware finden Sie im *McAfee Labs Threats-Report vom September 2017*.

Es gibt drei gängige Arten skriptbasierter Malware:

- **Speicherresidente Malware:** Diese Malware-Form verwendet den Speicherbereich einer legitimen Windows-Datei. Die 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.
- **Rootkits:** Einige Malware-Formen 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 hochentwickelte skriptbasierte Malware-Formen nisten sich in der Windows-Registrierung ein. In der Vergangenheit machten Malware-Autoren sich Features wie den Windows-Vorschau-Cache zunutze, in dem Vorschauen von Windows Explorer gespeichert werden. Dieser Cache fungiert dabei als Persistenzmechanismus für den Angriff. Diese Malware-Form muss immer noch über eine statische Binärdatei in das System des Opfers eindringen. In den meisten Fällen dienen E-Mails 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-Registrierungs-hauptstruktur. Anschließend wird die Datei vom System entfernt, indem sie sich selbst löscht.

Heute gestalten Malware-Autoren die Malware-Familien so geschickt, 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, löscht die Datei sich selbst, sobald das System für die böswillige Operation bereit ist.

## Richtlinien und Vorgehensweisen zum Schutz vor skriptbasierter Malware

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

- Am besten schützen Sie Ihr System vor skriptbasierten Malware-Infektionen, indem Sie sie von vornherein verhindern. Das Zauberwort heißt Vorbeugung. Der wichtigste Faktor bei der Verhinderung jeder Art von Malware-Infektion auf einem Computer ist der Benutzer. Er muss die Risiken kennen, die mit dem Herunterladen und Installieren von Anwendungen, die er nicht versteht oder denen er nicht vertraut, verbunden sind. Zudem kann Malware auch beim Surfen im Internet von Benutzern unbemerkt heruntergeladen werden.
- Wenden Sie Sicherheits-Updates und Patches für Anwendungen und Betriebssystem an.
- Web-Browser und Add-Ons müssen immer auf dem aktuellsten Stand und Malware-Schutzprodukte auf Endgeräten sowie Netzwerk-Gateways immer in der neuesten Version gehalten werden.

- Im vertrauenswürdigen Netzwerk dürfen ausschließlich Systeme zugelassen werden, die von der firmeneigenen IT-Sicherheitsgruppe verteilt oder zertifiziert wurden. Ungeschützte Ressourcen, die mit Ihrem Unternehmensnetzwerk verbunden sind, können jederzeit Skript-Malware verbreiten.
- Falls Benutzer lokale Administratorberechtigungen besitzen, um Anwendungen eigenständig zu installieren, sollten sie zumindest dahingehend sensibilisiert werden, dass sie nur Anwendungen mit vertrauenswürdigen Signaturen von bekannten Anbietern installieren. Es ist ein gängiger Trick, „harmlose“ Anwendungen online anzubieten, in denen dann Rootkits oder andere skriptbasierte Malware eingebettet sind.
- Downloads aus anderen Quellen als dem Web sollten generell vermieden werden. Die Wahrscheinlichkeit, Malware aus Usenet-Gruppen, IRC-Kanälen, Instant-Messaging-Clients oder Peer-Netzwerken herunterzuladen, ist sehr hoch. Links zu Webseiten in IRC oder Sofortnachrichten führen ebenfalls häufig zu infizierten Downloads.
- Stellen Sie ein Schulungsprogramm zur Verhinderung von Phishing-Angriffen auf, da Malware häufig über gezielte E-Mails verbreitet wird.
- Nutzen Sie Bedrohungsdaten-Feeds in Kombination mit Malware-Schutztechnologie, um die Erkennungszeit für neue und bekannte Malware-Bedrohungen zu verkürzen.

## So kann McAfee vor skriptbasierter Malware schützen

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

### McAfee Endpoint Security

Mit McAfee Endpoint Security (ENS) erhalten Sie ein kooperatives Sicherheits-Framework, das die Komplexität von Endgeräte-Sicherheitsumgebungen verringert und den Überblick über hochentwickelte Bedrohungen (z. B. skriptbasierte Malware) bietet, die Sie zur schnellen Erkennung und Reaktion benötigen. Für Sicherheitsteams, die durch den Einsatz mehrerer Lösungen überlastet sind, stellt die erweiterbare Architektur ein Framework bereit, mit dem der Kreislauf zur Bedrohungsabwehr einfacher angezeigt, behandelt und verwaltet werden kann.

In McAfee ENS sind zusätzlich folgende neue Technologien und Verbesserungen enthalten:

- **Real Protect:** Nutzt Machine Learning-Techniken, die böswilligen Code identifizieren, indem sie seine möglichen Aktionen (per Analyse vor der Ausführung) sowie seine tatsächlichen Aktivitäten (per dynamischer Verhaltensanalyse) untersuchen. Hierfür werden keine Signaturen benötigt. Real Protect ist Bestandteil einer effektiven Strategie zum Schutz vor skriptbasierter Malware.

- **Dynamische Eindämmung von Anwendungsprozessen:** Bietet die Möglichkeit, eine einzelne Instanz eines Prozesses einzudämmen.
- **McAfee Client Proxy-Integration:** McAfee Endpoint Security kann mit mehrschichtigem Web-Gateway-Schutz kombiniert werden, damit Benutzer überall und jederzeit geschützt werden. Durch die Vernetzung der Endgeräte mit dem Web-Gateway-Cloud-Dienst schließt sich die Schutzlücke, die immer dann entsteht, wenn Endgeräte nicht mit dem Unternehmensnetzwerk verbunden sind.
- **Firewall-Modul:** Im Rahmen einer proaktiven Sicherheitsstrategie besteht die nächste Schutzebene darin, Kommunikation zwischen Computer und von Cyber-Kriminellen kontrollierten Servern zu blockieren.
- **Bedrohungsschutzmodul:** On-Demand-Scans umfassen jetzt eine Option zum Scannen von Registrierungseinträgen, die für den Schutz vor skriptbasierter Malware besonders wichtig ist. Administratoren können Zugriffsschutzregeln für eigene sowie Windows-Dienste erstellen. Zusätzlich zu den von McAfee bereitgestellten Eindringungsschutz-Signaturen (IPS) ist Exploit-Schutz für eigene Anwendungen verfügbar. Außerdem decken die Exploit-Schutzregeln auch Windows-Anwendungsschutzregeln ab.

## McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) ist ein mehrschichtiges 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 ATD vor skriptbasierter 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 Wissensdatenbank wird von McAfee Labs erstellt und gepflegt.
- **Erkennung auf Reputationsbasis:** Durch die Überprüfung der Datei-Reputation mithilfe von McAfee Global Threat Intelligence (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 Befehlssätze bewertet sowie 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 Untersuchungsmodulen überprüft werden kann, kann McAfee ATD 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 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 (TIE) die Anfälligkeit für Angriffe mit skriptbasierter 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 TIE 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 TIE 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 TIE 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 Bedrohungen immunisiert wird. Wenn diese Indikatoren in der Umgebung entdeckt werden, kann McAfee TIE alle Prozesse und Anwendungen, die mit ihnen in Zusammenhang stehen, blockieren.

## McAfee Web Gateway

Drive-by-Downloads und böswillige URLs, die in Phishing-E-Mails eingebettet sind, sind die primären Methoden zur Übertragung skriptbasierter Malware. Das zuverlässige McAfee Web Gateway (MWG) dehnt den Schutz Ihres Unternehmens auf diese Art der Bedrohung aus.

- **Gateway Anti-Malware Engine:** Die signaturlose Absichtsanalyse filtert gefährliche Inhalte in Echtzeit 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-Bedrohungsdatendienst McAfee GTI bietet Datei- und Web-Reputation sowie Web-Kategorisierungsinformationen und schützt so vor den neuesten Bedrohungen, da MWG alle Verbindungsversuche zu bekannt böswilligen Webseiten sowie zu Webseiten, die böswillige Werbenetzwerke nutzen, blockiert. Zusätzlich zu diesen McAfee-Produkten empfehlen wir zwei weitere Sicherheitstechnologiekategorien.
  - **E-Mail-Gateway-Sicherheit:** Skriptbasierte 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 skriptbasierte Malware über statische Binärdateien in ein System gelangt, können viele dieser Angriffe gestoppt werden, bevor sie Systeme innerhalb des vertrauenswürdigen Netzwerks erreichen.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de