Kurzvorstellung

Stoppen von Backdoor-Trojanern

Das Remote-Verwaltungs-Tool Adwind (Remote Administration Tool, RAT) ist ein in Java geschriebener Backdoor-Trojaner, der verschiedene Plattformen angreift, die Java-Dateien unterstützen. Adwind nutzt keine Schwachstellen aus. Damit eine Infektion stattfindet, muss der Benutzer die Malware ausführen, indem er auf die meist als E-Mail-Anhang eintreffende JAR-Datei doppelklickt oder ein infiziertes Microsoft Word-Dokument öffnet. Für eine erfolgreiche Infektion muss die Java-Laufzeitumgebung (Java Runtime Environment) installiert sein. Sobald die böswillige JAR-Datei erfolgreich auf dem Zielsystem ausgeführt wurde, installiert sich die Malware im Hintergrund und verbindet sich mit einem Remote-Server über einen vorkonfigurierten Port, auf dem sie aus der Ferne Befehle vom Angreifer erhält und weitere böswillige Aktivitäten durchführt.

Ein kurzer Ausflug in die Geschichte

Adwind ist eine Weiterentwicklung von Frutas RAT. Frutas ist ein Java-RAT, das Anfang 2013 entdeckt und vor allem für Phishing-E-Mail-Kampagnen gegen bekannte Anbieter aus den Bereichen Telekommunikation, Bergbau, Finanzwesen sowie gegen Behörden in Europa und Asien genutzt wurde.

Seit Anfang des 1. Quartals 2015 registriert McAfee® Labs einen erheblichen Anstieg bei eingesendeten JAR-Dateien, die als Adwind identifiziert wurden.

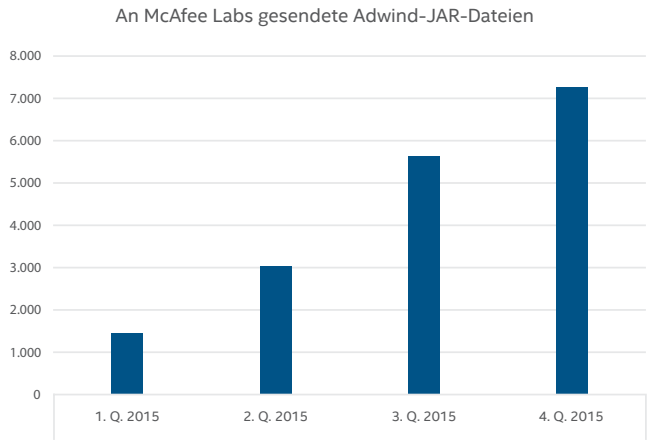

Abbildung 1. Die Anzahl der Adwind-JAR-Dateieinsendungen an McAfee Labs stieg von 1.388 im 1. Quartal 2015 auf 7.295 im 4. Quartal 2015. Das entspricht einer Zunahme von 426 Prozent.

intel Security

Infektionskette

Adwind verbreitet sich meist durch Spam-Kampagnen, bei denen Malware-verseuchte E-Mail-Anhänge, kompromittierte Webseiten sowie Drive-by-Downloads zum Einsatz kommen. Seine Verbreitungsmethode hat sich weiterentwickelt: Frühere Spam-Kampagnen dauerten mehrere Tage oder Wochen und verwendeten stets den gleichen Betreff sowie Anhangnamen. Dank dieser Konsistenz konnten Sicherheitsanbieter Adwind schnell erkennen und minimieren. Heute laufen Spam-Kampagnen jedoch nur für einen kurzen Zeitraum. Zudem ändern sie die Betreffzeilen und die sorgfältig erstellten Anhänge, damit Adwind der Erkennung entgehen kann.

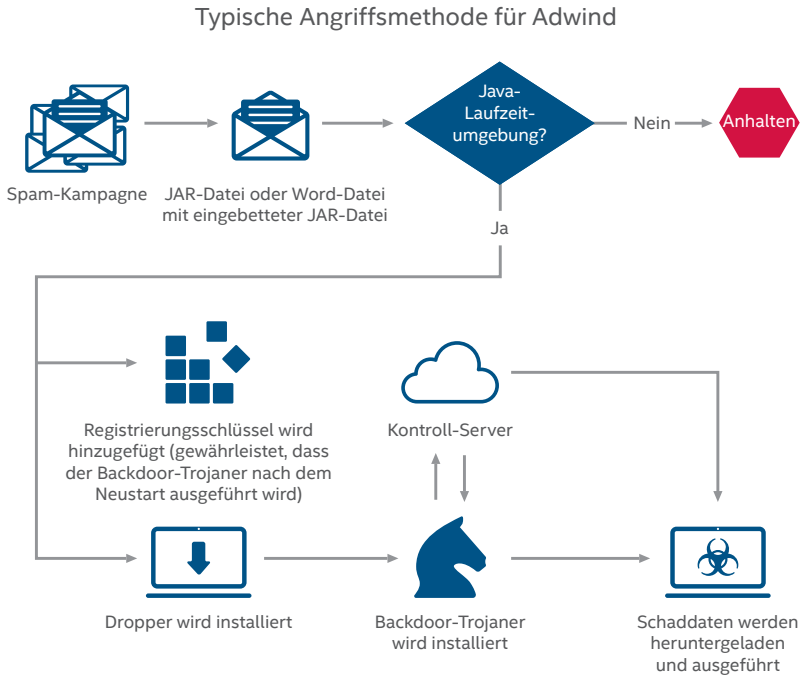

Abbildung 2. Die Adwind-Infektionskette.

Nach der erfolgreichen Infektion eines Systems durch Adwind haben wir beobachtet, dass die Malware Tastatureingaben aufzeichnet, Dateien ändert und löscht, weitere Malware herunterlädt und ausführt, Screenshots erstellt, auf die Systemkamera zugreift, die Kontrolle über Maus und Tastatur übernimmt, sich aktualisiert usw.

So kann Intel Security vor Adwind und anderen Backdoor-Trojanern schützen

Intel Security-Technologie kann vor Backdoor-Trojanern wie Adwind schützen. Dazu stehen unter anderem folgende Produkte zur Verfügung.

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 Gefahr durch Backdoor-Trojaner erheblich verringern.

- **Umfassende Bedrohungsanalyse:** Die umfassenden Bedrohungsdaten von weltweiten Bedrohungsdatenquellen können unkompliziert angepasst werden. Dabei kann es sich um Feeds von **McAfee Global Threat Intelligence** (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 Advanced Threat Defense

McAfee Advanced Threat Defense ist ein mehrstufiges Produkt zum Aufspüren von Malware, das über mehrere Untersuchungsmodule verfügt. Die Module führen signatur- und reputationsbasierte Untersuchungen, Echtzeitemulationen sowie vollständige statische Code- und dynamische Sandbox-Analysen verdächtiger Objekte durch, um vor Malware zu schützen, 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:** Über McAfee GTI werden Informationen zur Datei-Reputation abgerufen, damit auch neue Bedrohungen erkannt werden.
- **Statische Analyse und Emulation in Echtzeit:** Statische Echtzeitanalyse und Emulation ermöglichen die schnelle Erkennung von Backdoor-Trojanern und Zero-Day-Bedrohungen, die von signatur- oder reputationsbasierten 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 Untersuchungsmodulen 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 Microsoft Windows XP (32-Bit- und 64-Bit-Versionen), 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 Network Security Platform

McAfee Network Security Platform ist eine besonders intelligente Sicherheitslösung, die hochentwickelte Bedrohungen im Netzwerk findet und blockiert. Mit hochentwickelten Erkennungs- und Emulationstechniken geht diese Lösung über Musterabgleich hinaus, um Stealth-Angriffe äußerst zuverlässig abzuwehren. Unser offener, integrierter Ansatz für die Sicherheitsverwaltung kombiniert die Echtzeit-Feeds von McAfee GTI mit umfangreichen Kontextdaten zu Benutzern, Geräten und Anwendungen, damit Sie schnell und präzise auf Angriffe über das Netzwerk reagieren können. Dadurch erreichen Sie optimierte Sicherheitsabläufe.

- **Signaturloser Schutz:** Hochentwickelte und unbekannte Bedrohungen wie Stealth-Malware, hochentwickelte hartnäckige Bedrohungen (APTs), Bots und Zero-Day-Angriffe sind häufig in der Lage, signaturbasierte Schutzmaßnahmen zu umgehen. Die McAfee Network Security Platform verfügt über mehrere hochentwickelte Module, die keine Signaturen benötigen, um vor hochentwickelten und unbekannten Bedrohungen zu schützen. Die signaturlose Erkennungsfunktion emuliert und analysiert das Verhalten von Web-Inhalten, PDF- und Flash-Dateien sowie JavaScript-Objekten praktisch in Echtzeit.
- **Endpoint Intelligence Agent:** McAfee Network Security Platform korreliert Endgeräte-Datenverkehr individuell in Echtzeit. Der Agent verknüpft die Verhaltensanalyse des Netzwerk-Datenverkehrs mit Erkenntnissen aus mehreren Reputationsdatenquellen. Diese Technologie nutzt Informationen aus dem Netzwerk sowie von allen Microsoft Windows-Hosts, um Beziehungen zwischen ausführbaren Dateien auf Endgeräten und Netzwerk-Datenflüssen zu ermitteln. Dadurch können böswillige Netzwerkverbindungen und ausführbare Dateien in Echtzeit überführt werden. Der Agent nutzt detaillierte Prozesskontextinformationen zu Angriffen, blockiert böswillige Kommunikationen, verhindern die Ausbreitung von hochentwickelter Malware und isoliert sowie repariert kompromittierte Host-Systeme.

McAfee Web Gateway

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

- **Gateway Anti-Malware Engine:** Die signaturlose Absichtsanalyse filtert in Echtzeit gefährliche Inhalte aus dem Web-Datenverkehr heraus. Emulation und Verhaltens-analyse bieten präventiven Schutz vor Zero-Day-Bedrohungen und gezielten Angriffen. Der Gateway 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 als Kontroll-Server fungieren.

Zusätzlich zu diesen Intel Security-Produkten empfehlen wir eine weitere Sicherheitstechnologieklasse.

- **E-Mail-Gateway-Sicherheit:** Backdoor-Trojaner gelangen 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.

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