Kurzvorstellung

Möglichkeiten zum Schutz vor Makro-Malware

Im ***McAfee® Labs Threat-Report vom November 2015*** werfen wir einen genauen Blick auf Makro-Malware, ein Relikt aus den 1990er Jahren, das derzeit eine Wiederbelebung erfährt, da Unternehmen weiterhin Makros verwenden. Zudem wird Makro-Malware zunehmend mit raffinierteren Social-Engineering-Taktiken kombiniert, die die Verbreitung neuer, unauffälliger Varianten ermöglichen. Ein Makro ist eine Verknüpfung zur Automatisierung einer häufig durchgeführten Aufgabe. Es handelt sich dabei um Code, der in ein Dokument (typischerweise ein Microsoft Office-Dokument) eingebettet und meist in der Programmiersprache Visual Basic für Anwendungen (Visual Basic for Applications) geschrieben wurde. Beim Aufzeichnen eines Makros wird in Wirklichkeit ein Programm in Visual Basic für Anwendungen generiert. Zum Kampf gegen Makro-Malware führte Microsoft zur Makro-Aktivierung eine Berechtigungsabfrage ein, die als Doppelprüfung dient. Microsoft Office deaktiviert jetzt alle Makros standardmäßig, damit sie nur mit Erlaubnis des Benutzers ausgeführt werden. Diese Maßnahme bremste den Eifer der Makro-Malware-Autoren, sodass böswillige Makros an Einfluss verloren. Im vergangenen Jahr nutzten Angreifer jedoch neue, noch unauffälligere Makro-Malware in Kombination mit Social-Engineering-Taktiken für persistente gezielte Angriffe auf Unternehmen. Die Zahl neuer Makro-Malware-Varianten hat den höchsten Stand in sechs Jahren erreicht.

Heute verwenden Makro-Malware-Angreifer hauptsächlich Phishing-E-Mail-Anhänge sowie Spam-Kampagnen, kompromittierte Webseiten und Drive-by-Downloads, um ihre Malware zu verbreiten. Diese Techniken sind heute erheblich raffinierter als in den 1990er Jahren, als Makro-Malware zum ersten Mal auftrat. Für Benutzer ist es inzwischen relativ schwierig, diese Kampagnen zu erkennen, da sie gezielt sowie kurzlebig sind und sorgfältig gestaltete Anhänge enthalten, die der Erkennung entgehen.

intel Security

Mit diesen Richtlinien und Verfahrensweisen können Sie sich vor Makro-Malware-Angriffen schützen:

- Aktivieren Sie die automatische Update-Funktion Ihres Betriebssystems, oder laden Sie die Betriebssystem-Updates regelmäßig herunter, um Ihr Betriebssystem mit Patches für bekannte Sicherheitslücken zu aktualisieren.
- Verwenden Sie aktualisierte Microsoft Office-Software, die besseren Schutz vor solchen Angriffen bietet.
- Stellen Sie sicher, dass die Makro-Sicherheitseinstellungen für alle Microsoft Office-Produkte standardmäßig auf „Hoch“ gesetzt sind.
- Konfigurieren Sie Ihre Malware-Schutz-Software so, dass E-Mail- und Instant-Messaging-Anhänge automatisch gescannt werden. Sorgen Sie dafür, dass E-Mail-Programme Anhänge nicht automatisch öffnen oder Grafiken automatisch darstellen und dass das Vorschaufenster deaktiviert ist.
- Die Sicherheitseinstellungen des Browsers sollten mindestens auf die mittlere Stufe festgelegt werden.
- Seien Sie äußerst vorsichtig, wenn Sie Anhänge öffnen, besonders wenn sie die Endung .DOC oder .XLS haben.
- Öffnen Sie niemals eine E-Mail, die Ihnen unverlangt zugesendet wurde oder einen unerwarteten Anhang enthält – auch dann nicht, wenn die E-Mail von einem bekannten Absender stammt.
- Fallen Sie nicht auf Phishing-Versuche in Spam-Mails herein. Klicken Sie nicht auf Links in E-Mails oder Instant Messages.
- Überwachen Sie unerwartete Ping-Befehle an IP-Adressen wie 1.3.1.2 oder 2.2.1.1 von internen Computern.
- Bedenken Sie, dass Dokumente mit Bestätigungs- oder Rechnungsinformationen normalerweise keine Makros benötigen.
- Gehen Sie vorsichtig vor, wenn Sie leere Dokumente erhalten, die Benutzer dazu auffordern, zum Anzeigen des Inhalts Makros zu aktivieren.

So kann Intel Security vor Makro-Malware schützen

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 Makro-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 Global Threat Intelligence (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.

McAfee VirusScan® Enterprise

Mit **McAfee VirusScan Enterprise** ist das Erkennen und Entfernen von Makro-Malware einfach. McAfee VirusScan Enterprise nutzt das preisgekrönte McAfee Labs-Scan-Modul zum Schutz Ihrer Dateien vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen. Weiteren Schutz erhält Ihr Unternehmen mit McAfee VirusScan Enterprise, da diese Lösung Ports und Dateinamen blockieren, Ordner, Verzeichnisse und Dateifreigaben sperren sowie Infektionen nachverfolgen und blockieren kann.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutztechnologien und Eindringungsschutz können Exploits abgewehrt werden, die mithilfe von Buffer Overflows Schwachstellen in Microsoft-Anwendungen angreifen.
- **Unschlagbare Malware-Erkennung und -Bereinigung:** Die erweiterte Verhaltensanalyse schützt vor Bedrohungen wie Rootkits und Trojanern. Mithilfe von Techniken wie der Blockierung von Ports und Dateinamen, der Sperrung von Ordnern bzw. Verzeichnissen und Freigaben sowie dem Verfolgen und Blockieren von Infektionen wird Malware schon im Ansatz aufgehalten.
- **Echtzeitsicherheit mit McAfee GTI:** Die Plattform für die branchenweit umfassendsten Bedrohungsdaten bietet Schutz vor bekannten und neuen Bedrohungen aus allen Sektoren – Dateien, Web, E-Mails und Netzwerk.

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, erkennt McAfee Advanced Threat Defense nicht nur Dokumente, die mit Makros Malware übertragen, sondern gewährleistet auch Erkennung und Schutz vor Malware, die nach der Ausführung heruntergeladen wurden.

- **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 Makro-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 Makro-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.

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

- **E-Mail-Gateway-Sicherheit:** Makro-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 für jedes Sicherheitssystem ist eine gute Firewall-Technologie. Eine Firewall kann viele Bedrohungen an der Peripherie erkennen, bevor sie in das vertrauenswürdige Netzwerk gelangen.

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