Kurzvorstellung

Schutz vor getarnter Malware

Wie im McAfee Labs Threats-Report vom Juni 2017 näher erläutert, maskiert getarnte Malware sich selbst, um der Entdeckung zu entgehen. Sie verbirgt sich, indem sie sich an legitime Anwendungen anhängt oder diese missbraucht. Die Malware erkennt, wenn sie in einer Sandbox analysiert wird und verzögert ihre Ausführung, um erst nach Tagen, Wochen oder sogar Monaten zuzuschlagen.

Erforderlich ist ein Sicherheitsprogramm, das auf drei wichtigen Säulen basiert:

- **Menschen:** Sicherheitsmitarbeiter müssen so geschult werden, dass sie auf Sicherheitsvorfälle angemessen reagieren und mit aktueller Sicherheitstechnologie kompetent umgehen kann. Ferner setzen Angreifer gern Social-Engineering-Taktiken ein, um Benutzer zu infizieren. Unachtsame und nicht entsprechend geschulte Benutzer stellen für Angreifer ein offenes Einfallstor dar.
- **Prozesse:** Es müssen klare Strukturen und interne Prozesse vorhanden sein, damit Sicherheitsbeauftragte effektiv arbeiten können. Bewährte Sicherheitsmaßnahmen (Aktualisierungen, Sicherungen, Governance, Bedrohungsdaten, Vorfallsreaktionspläne usw.) bilden die Grundlagen für ein leistungsfähiges und wirksames Sicherheitsteam.
- **Technologien:** Technologien unterstützen das Team und die Prozesse. Sie sollten gut gepflegt und ständig ausgebaut werden, um mit neuen Bedrohungen Schritt halten zu können.

Konkrete Richtlinien und Vorgehensweisen zum Schutz vor getarnter Malware

- Die wichtigste Verteidigungslinie zum Schutz vor Malware-Infektionen ist der Benutzer. Er muss die Risiken kennen, die mit dem Herunterladen und Installieren von Anwendungen, die aus potenziell riskanten Quellen stammen, verbunden sind. Dem Benutzer muss auch klar sein, dass Malware ungewollt heruntergeladen werden kann, während er im Internet surft.
- Daher müssen Browser und Add-Ons immer auf dem aktuellen Stand gehalten werden 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 Systeme, die mit dem vertrauenswürdigen Netzwerk verbunden sind, können jederzeit getarnte Malware verbreiten.

McAfee™
Together is power.

- Getarnte Malware kann sich auch in seriöser Software verstecken, die zuvor von einem Trojaner kompromittiert wurde. Um erfolgreiche Angriffe dieser Art zu verhindern, empfehlen wir dringend, strenge Mechanismen für die Übertragung und Verteilung von Software zu implementieren. Es ist äußerst sinnvoll, für im Unternehmen eingesetzte Software ein zentrales Repository zu betreiben, aus dem die Benutzer dann genehmigte Software herunterladen können.
- Falls Benutzer auch Anwendungen installieren dürfen, die nicht zuvor von der IT-Sicherheitsgruppe überprüft wurden, sollten sie zumindest dahingehend geschult werden, dass sie nur Anwendungen mit vertrauenswürdigen Signaturen von bekannten Anbietern installieren. Es ist ein gängiger Trick, „harmlose" Anwendungen online anzubieten, in denen dann eine Malware versteckt ist.
- Downloads aus anderen Quellen als dem Web sollten überhaupt vermieden werden. So ist bei Downloads aus Usenet-Gruppen, IRC-Kanälen, Instant-Messaging-Clients oder P2P-Netzwerken die Wahrscheinlichkeit sehr hoch, sich mit einer Malware zu infizieren. 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 Phishing-Angriffe weitergegeben wird.
- Nutzen Sie Bedrohungsdaten-Feeds in Kombination mit Malware-Schutztechnologie, um Bedrohungen schneller zu entdecken.

So schützen McAfee-Produkte vor getarnter Malware

McAfee hat eine neue Generation an Sicherheitsfunktionen entwickelt, die selbst die am besten getarnten modernen Bedrohungen bekämpft. Dank leistungsfähiger Machine Learning-Analysen sowie Tools zur Eindämmung von Anwendungsprozessen können Unternehmen erheblich schneller und mit deutlich weniger Aufwand versteckte Bedrohungen aufdecken sowie blockieren.

Diese Fähigkeiten werden über die folgenden McAfee-Produkte bereitgestellt:

Real Protect

Real Protect ist eine Komponente von McAfee Endpoint Protection und kombiniert statische Analysen vor sowie Verhaltensanalysen nach der Ausführung, um mehr Malware aufzuspüren, als dies mit – ebenfalls in das McAfee-Ökosystem integrierten – signaturbasierten oder ausschließlich statischen Lösungen möglich ist. Dabei kommen modernste Machine Learning-Techniken zum Einsatz, die böswilligen Code identifizieren, indem sie seine statischen Eigenschaften mit umfassenden Analysen (vor der Ausführung) sowie seine Aktivitäten (mithilfe dynamischer Verhaltensanalyse) untersuchen. Hierfür werden keine Signaturen benötigt. Damit lassen sich selbst die neuesten Verschleierungstechniken überwinden und verborgene Zero-Day-Malware aufdecken.

Dynamische Eindämmung von Anwendungsprozessen

Die dynamische Eindämmung von Anwendungsprozessen (Dynamic Application Containment, DAC), die ebenfalls in McAfee Endpoint Protection enthalten ist, schützt „Patient Null"-Endgeräte vor Zero-Day-Malware-Infektionen. Wenn ein Endgerät eine verdächtige Datei entdeckt, blockiert DAC sofort das für Malware typische Verhalten (z. B. Veränderungen in der Registry, Schreibvorgänge in einem temporären Verzeichnis oder das Löschen von Dateien). Im Gegensatz zu anderen Techniken, die die Ausführung der Datei (und damit auch die Benutzer) für mehrere Minuten aufhalten, lässt DAC das Laden der Datei in den Arbeitsspeicher zu, verhindert jedoch bestimmte Veränderungen auf dem Endgerät oder die Ausbreitung auf weitere Systeme, solange noch keine Freigabe erfolgt ist.

Real Protect und DAC sind vernetzt – miteinander, mit Sicherheitslösungen anderer Anbieter (z. B. SPLUNK, Avecto und ForeScout) sowie mit McAfee Endpoint Protection – um selbst vor den am besten getarnten Bedrohungen mehrschichtigen Schutz zu gewährleisten. Dadurch erhält Ihr Sicherheitsteam die Möglichkeit, alle Stufen des Kreislaufs zur Bedrohungsabwehr – Erkennung, Behebung und präventiver Schutz – schnell und automatisiert durchzusetzen.

Real Protect und DAC können für die folgenden Zwecke eingesetzt werden:

- Erkennung von Angriffen durch Aufdeckung von Verschleierungstechniken
- Begrenzung der Auswirkungen von Angriffen: Eindämmung, Abschirmung und Verhinderung von Schäden an Systemen, bevor ein Angriff stattfindet oder bevor es zu unwiderruflichen Schäden kommt
- Überwachung und Anpassung: Nutzung automatisierter und integrierter Schutzmaßnahmen, um ein größeres Spektrum an Sicherheitsprozessen durchzuführen, ohne sie planen oder manuell aktivieren zu müssen

Sehen Sie sich dazu ein Demovideo an, und erfahren Sie, wie getarnte Malware mithilfe von Real Protect und DAC eingedämmt werden kann.

Empfohlene Vorgehensweisen für die Konfiguration der dynamischen Eindämmung von Anwendungsprozessen
DAC-Regeln in der McAfee Default-Richtlinie werden so definiert, dass nur eine Meldung erfolgt, wodurch die Anzahl von False-Positives reduziert wird. Das Modul Adaptiver Bedrohungsschutz stellt zwei weitere vordefinierte DAC-Richtlinien bereit: McAfee Default Balanced (Standard, ausgeglichen) und McAfee Default Security (Standard, Sicherheit). Diese Richtlinien legen empfohlene Regeln für das Sperren auf Grundlage des Sicherheitsprofils fest:

- McAfee Default Balanced bietet Basisschutz und vermeidet dabei viele False-Positives bei den gängigsten unsignierten Installationsprogrammen und Anwendungen.
- McAfee Default Security sorgt für aggressiven Schutz, kann aber bei unsignierten Installationsprogrammen und Anwendungen häufiger zu False-Positives führen.

Sie können die Auswirkungen von DAC-Regeln beurteilen, indem Sie die McAfee Default-Richtlinie verwenden und in den Regeln festlegen, dass Verstöße nur gemeldet werden sollen. Wenn Sie feststellen möchten, ob Installationsversuche blockiert werden sollen, müssen Sie die Protokolle und Berichte überwachen. Nachdem die Ereignisse mit zulässigen DAC-Verstößen (Ereignis-ID 37280) erfasst wurden, legen Sie Reputationen innerhalb des Unternehmens oder DAC-Ausnahmen fest, bevor die McAfee Default Balanced-Richtlinie angewendet wird.

DAC kann Prozesse anhand ihres Namens, MD5-Hash-Wertes, Pfads und ihrer Signaturdaten von der Eindämmung ausschließen. Wenn Ihr Unternehmen intern bereitgestellte Tools signiert, fügen Sie diese Signaturen als Ausnahmen hinzu, um False-Positives zu vermeiden.

Sie können für DAC-Regeln die Anzahl der Ereignisse begrenzen, die pro Stunde, pro Regel bzw. pro Prozess generiert werden sollen. Diese Funktion zur „Flutkontrolle“ verfolgt Prozesse anhand der Prozess-ID nach. Wenn ein Prozess neu gestartet wird, weist ihm das Betriebssystem eine neue ID zu – dadurch wird die Kontrollfunktion zurückgesetzt, obgleich der Prozessname der gleiche ist. Ein Beispiel: Wenn der Prozess A die DAC-Regel A 100 mal pro Stunde verletzt, erhalten Sie ein Ereignis pro Stunde. Wird der Prozess A während dieser Stunde neu gestartet, wird die Kontrollfunktion für den Prozess A zurückgesetzt. Und falls dieser dann weiter gegen die DAC-Regel A verstößt, erhalten Sie ein weiteres Ereignis. Wenn der Prozess B gegen die gleiche DAC-Regel A verstößt, erhalten Sie ein zweites Ereignis (mit den Details zu Prozess B). Hier erhalten Sie weitere Informationen zu empfohlenen Vorgehensweisen für DAC-Regeln, die von McAfee definiert wurden.

Wenden Sie das McAfee-Tool GetClean auf die Standardbereitstellungs-Images für Ihre Produktionssysteme an, um bekannt saubere Dateien zur Kategorisierung an McAfee Global Threat Intelligence (GTI) zu senden. Auf diese Weise gewährleisten Sie, dass McAfee GTI keine falschen Reputationswerte für Ihre Dateien angibt. Weitere Informationen finden Sie im GetClean-Produkthandbuch (PD23191).

McAfee Cloud Threat Detection
Mit McAfee Cloud Threat Detection (CTD) können Sie die von McAfee bereitgestellten Schutzfunktionen noch weiter ausbauen, sodass auch hochentwickelte Malware-Varianten entdeckt und versteckte Bedrohungen enttarnt werden. Nutzen Sie den Zugang zur McAfee ePO Cloud, aktivieren Sie McAfee CTD, und integrieren Sie es in Ihre McAfee-Produkte.

Um die von McAfee CTD bereitgestellten Funktionen in Ihren McAfee-Sicherheitsprodukten nutzen zu können, gehen Sie wie folgt vor:

- Aktivieren Sie McAfee CTD in McAfee ePO Cloud.
- Aktivieren Sie McAfee CTD auf der Benutzeroberfläche Ihres McAfee-Sicherheitsprodukts, und rufen Sie den Bereitstellungsschlüssel ab.
- Generieren Sie auf der Benutzeroberfläche von McAfee ePO Cloud mithilfe des Bereitstellungsschlüssels einen Aktivierungsschlüssel.
- Aktivieren Sie Ihr McAfee-Sicherheitsprodukt mit dem Aktivierungsschlüssel.

Die genaue Vorgehensweise zum Abrufen des Bereitstellungsschlüssels und zum Aktivieren eines Produkts ist vom jeweiligen Produkt abhängig. Detaillierte Informationen dazu, wie Sie McAfee CTD in Ihr McAfee-Produkt integrieren können, finden Sie im jeweiligen Produkthandbuch.

Sobald die integrierten Produkte damit beginnen, Dateien zur Analyse an McAfee CTD zu übermitteln, können Sie Ihre Nutzungsinformationen auf der Seite „Subscriptions“ (Abonnements) in McAfee ePO Cloud einsehen.

McAfee Active Response

- McAfee Active Response ist dafür konzipiert, hochentwickelte Bedrohungen zu finden und darauf zu reagieren. Wenn die Anwendung zusammen mit Bedrohungsdaten-Feeds wie McAfee GTI, Dell SecureWorks oder ThreatConnect eingesetzt wird, können Sie nach evasiven 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 kann mit Auslösern und Reaktionen festlegen, welche Aktionen bei bestimmten Bedingungen ausgeführt werden sollen. Wenn zum Beispiel bestimmte Hash-Werte oder Dateinamen gefunden werden, kann automatisch eine Löschaktion ausgeführt werden.

Weitere Informationen

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (Neutralisierung hochentwickelter Bedrohungen: Kompletter Schutz vor Malware durch mehrschichtige Schutzmaßnahmen)

McAfee Security Advice Center: Die zehn wichtigsten Tipps zum Schutz vor Malware und Trojanern

McAfee Endpoint Security: Häufig gestellte Fragen

McAfee™
Together is power.

3187_0617_brf-protecting-against-evasive-malware
Juni 2017

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de