Kurzvorstellung

Schutz vor potenziell unerwünschten Programmen

Potenziell unerwünschte Programme (PUPs) werden ausführlich im **McAfee Labs Threat-Report vom Februar 2015** besprochen. Alle Anwendungen, die von Benutzern als praktisch angesehen werden, jedoch ein messbares Risiko darstellen, können als PUP eingestuft werden. Die Anwendungen informieren die Benutzer im Allgemeinen nicht über diese Risiken. Im Gegensatz zu Trojanern, Viren, Rootkits und anderen Malware-Formen haben PUPs meist nicht das Ziel, Benutzeridentitäten (für soziale Medien, Bankzugangsdaten und andere Anmeldeinformationen) zu stehlen oder Systemdateien zu manipulieren. Sie liegen in einer Grauzone zwischen den Schadkategorien, da sie dem Benutzer einerseits einen Mehrwert bieten, gleichzeitig jedoch ein Risiko darstellen. Sie sind häufig schwer zu erkennen und zu kategorisieren.

PUPs zeigen häufig folgendes Verhalten:

- Sie ändern Systemeinstellungen (z. B. Browser-Konfiguration) ohne Einverständnis des Benutzers.
- Sie verbergen ein nicht erwünschtes Programm innerhalb einer legitimen Anwendung.
- Sie erfassen heimlich Benutzerinformationen, das Surfverhalten und die Systemkonfiguration.
- Sie verbergen die Installation von Anwendungen.
- Sie erschweren die Entfernung.
- Sie werden über irreführende oder betrügerische Werbung verteilt.

PUPs können verschiedene Varianten aufweisen:

- **Adware:** Stellt Werbung vor allem über Browser bereit
- **Kennwort-Cracker/-Anzeiger:** Zeigt das verborgene Kennwort einer Anwendung an
- **Remote-Verwaltungs-Tool (RAT):** Überwacht Benutzeraktivitäten auf dem jeweiligen Computer oder ermöglicht die Fernkontrolle ohne Wissen oder Einverständnis des Benutzers
- **Schlüsselgenerator:** Generiert Produktschlüssel für legitime Anwendungen

intel Security

- **Browser-Hijacker:** Ändert unter anderem die Start- und Suchseite sowie die Browser-Einstellungen
- **Hacker-Tools:** Eigenständige Anwendungen, die Systemeindringungen oder die Kompromittierung wichtiger Daten ermöglichen
- **Proxy:** Leitet Verbindungen um oder verbirgt IP-bezogene Informationen
- **Überwachungs-Tools:** Spyware- oder Keylogger-Anwendungen, die heimlich Benutzereingaben erfassen, die private Kommunikation protokollieren, Online-Benutzeraktivtäten überwachen oder Screenshots erstellen

Folgende wichtige Eigenschaften unterscheiden PUPs von anderer Malware wie Trojanern, Ransomware, Bots und Viren:

Techniken	Potentiell unerwünschte Programme	Andere Malware: Trojaner, Viren, Bots
Installationsmethode	Standardmäßige Vorgehensweise zur Installation von Anwendungen, manchmal mit Lizenzvertrag. Erfordert häufig Einverständnis und Eingaben des Benutzers zur vollständigen Installation auf einem System.	Wird als eigenständiges Programm ohne Benutzereingabe installiert. Agiert meist als unabhängige Datei.
Paket	Gebündelt mit legitimen Anwendungen und heimlich zusammen mit der „sauberen" App installiert.	Eigenständige Dateien mit einigen zusätzlichen Komponenten. Nicht als Installationsprogramme ausgeführt.
Deinstallation	Manchmal enthält das Paket ein Deinstallationsprogramm, das die Entfernung ermöglicht. Häufig ist die Deinstallationsprozedur kompliziert.	Ausführbare Dateien steigern die Komplexität bei der Entfernung von Malware aufgrund von Hooks in andere Prozesse, Prozess-Handler und andere komplexe Verknüpfungen. Da es sich nicht um Installationspakete handelt, werden sie nicht in der Systemsteuerung angezeigt.
Verhalten	Zeigt unangeforderte Werbung, Pop-Up- und Pop-Under-Fenster. Überwacht Browser-Einstellungen, erfasst Benutzer- und Systemdaten oder ermöglicht die Fernkontrolle – ohne Wissen oder Einverständnis des Benutzers.	Stiehlt persönliche Identitäts- und Bankverbindungsdaten, verändert Systemdateien, macht das System unbenutzbar, fordert Lösegeld u. a.
Heimlichkeit	Das Verhalten ist meist nicht heimlich.	Kann Dateien, Ordner, Registrierungseinträge und Netzwerkverkehr verbergen.

Unter all den PUP-Kategorien hat Adware die größte Aufmerksamkeit der Sicherheitsanbieter auf sich gezogen. Der Grund dafür ist nicht die lästige Werbung, sondern der Vertrauensmissbrauch. Im Zuge der Implementierung verschiedener Techniken, die einen dauerhaften Verbleib auf infizierten Systemen gewährleisten sollen, ist Adware raffinierter geworden. Dazu werden unter anderem folgende Methoden genutzt:

- Eigenständiger Prozess, der im Speicher ausgeführt wird
- COM- und Nicht-COM-DLL-Dateien (Component Object Model) mit Funktionen speziell für diese App
- Registrierungsschlüssel für Browserhilfsobjekte
- In Systemprozesse eingeklinkte DLL-Dateien
- Browser-Erweiterungen und Plug-Ins
- Registrierte Systemdienste
- Gerätetreiberkomponenten, die Gerätesteuerungsfunktionen ausführen
- Filtertreiber für die unterste Ebene
- Als Schaddaten übertragene Trojaner

PUPs werden meist verbreitet, indem – wie im **McAfee Labs Threat-Report vom November 2014** beschrieben – das Vertrauen nichts ahnender Benutzer missbraucht wird. Folgende Verbreitungsformen werden für PUPs am häufigsten genutzt:

- Heimliches Anhängen an eine legitime Anwendung
- Social Engineering
- Verkauf von Facebook-Likes
- Veröffentlichung von Betrugsnachrichten auf Facebook
- Kapern von Google AdSense
- Unerwünschte Browser-Erweiterungen und Plug-Ins
- Erzwungene Installation zusammen mit legitimen Anwendungen

So kann Intel Security vor dieser Bedrohung schützen

McAfee Application Control

Mit **McAfee Application Control** kann Ihr Unternehmen kontrollieren, welche Anwendungen in Ihrer Umgebung ausgeführt werden. Dabei kommen dynamische Whitelists und Durchsetzungsrichtlinien für vernetzte und eigenständige Endgeräte zum Einsatz. Die Lösung kann Ihr Unternehmen vor PUPs schützen.

- **Dynamische Whitelists:** Damit kann Ihr Unternehmen Anwendungen, die auf einer Whitelist geführt werden, effektiv verwalten, indem die Whitelist automatisch erweitert wird, sobald die Systeme gepatcht und aktualisiert werden. McAfee Application Control verringert Ihre Anfälligkeit für PUPs, indem es die Ausführung bekannter Adware verhindert.
- **Datei-Reputation:** Durch die Integration von **McAfee Global Threat Intelligence** (McAfee GTI) kann McAfee Application Control Echtzeitinformationen zu gefährlichen, ungefährlichen und unbekannten Dateitypen abrufen und in die Whitelist aufnehmen, sodass Ihr Unternehmen über bekannte PUP-Anwendungen informiert bleibt.
- **Schutz mit und ohne Vernetzung:** Setzen Sie Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten und Geräten mit fester Funktion wie Kassenterminals durch.

McAfee Web Gateway

Malvertising, Drive-by-Downloads und böswillige URLs, die in vertrauenswürdige Webseiten eingebettet sind, sind nur einige der Angriffsmethoden, mit denen PUPs übertragen werden. 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. 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 Echtzeitdienst 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 Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) ist ein umfassender, in Echtzeit funktionierender und Cloud-basierter Bedrohungsanalysedienst, durch den McAfee-Produkte alle Bedrohungsvektoren blockieren können – Dateien, das Web, Nachrichten und das Netzwerk. McAfee GTI schützt proaktiv mithilfe der folgenden Funktionen vor PUPs:

- **Bedrohungsinformationen durch Vektorkorrelierung:** Erfasst und korreliert Daten von und über alle wichtigen Bedrohungsvektoren (Dateien, das Web, E-Mails und das Netzwerk), um kombinierte Bedrohungen wie Werbenetzwerke, die signierte Malware verteilen, zuverlässig zu erkennen.
- **Plattform für umfassende Bedrohungsanalysen:** Erfasst Bedrohungsdaten von Millionen Sensoren auf McAfee-Produkten, die bei Kunden auf Endgeräten, Web-, E-Mail- und Netzwerkeindringungsschutz-Systemen sowie Firewall-Geräten im Einsatz sind.
- **Zertifikat-Reputation:** Die Echtzeitabfrage bekannt guter oder gefährlicher Zertifikate schützt Ihr Unternehmen vor Bedrohungen wie signierte Malware, die durch böswillige Werbenetzwerke verteilt wird.
- **Security Connected:** Die Integration in andere McAfee-Sicherheitsprodukte ermöglicht die branchenweit umfassendsten Daten zu Bedrohungen, die zuverlässigste Korrelation dieser Daten und die vollständigste Produktintegration, damit der Schutz vor Adware gewährleistet bleibt.

McAfee SiteAdvisor® Enterprise

Es ist mit einigem Aufwand verbunden, der wandlungsfähigen Bedrohungssituation einen Schritt voraus zu bleiben. Dies gilt insbesondere dann, wenn Online-Benutzer vor Bedrohungen wie PUPs geschützt werden sollen, ohne dass ihnen die Arbeit durch strikte Richtlinien erschwert werden soll.

- **Einfache Erkennung von Bedrohungen wie böswilligen Webseiten, die sich als legitim ausgeben:** Mit dem intuitiven farbcodierten Bewertungssystem bietet **McAfee SiteAdvisor Enterprise** eine zusätzliche Schutzebene für den Desktop. Die Lösung blockiert alle Verbindungen zu bekannt böswilligen Webseiten und informiert die Benutzer über die Bedrohung.
- **Erweiterte Sicherheit durch McAfee GTI:** McAfee GTI stellt für McAfee SiteAdvisor Enterprise Echtzeitbedrohungsdaten bereit, sodass diese Lösung Webseiten anhand der aktuellsten Informationen einstufen kann.

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 diese Art von Angriffen erheblich verringern.

- **Umfassende Bedrohungsanalysen:** Die umfassenden Bedrohungsdaten von weltweiten Datenquellen können unkompliziert angepasst werden. Dabei kann es sich um Feeds von McAfee GTI oder Drittanbietern handeln, die mit lokalen Bedrohungsdaten aus Echtzeit- und 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 Richtlinien-durchsetzung zurück.

- **Zertifikat-Reputation:** Durch die Integration von McAfee GTI kann sich Ihr Unternehmen in Echtzeit vor Bedrohungen schützen, die signierten Malware-Code verwenden. Dazu ruft der Dienst Echtzeitinformationen zu legitimen und gefährlichen Zertifikaten ab. Mithilfe zentral verwalteter Richtlinien, die zum Schutz vernetzter und eigenständiger Endgeräte ausgebracht werden können, kann McAfee Threat Intelligence Exchange Ihre Endgeräte vor böswilligen Zertifikaten schützen.

McAfee VirusScan® Enterprise

Mit **McAfee VirusScan Enterprise** ist das Erkennen und Entfernen von Malware (darunter Adware) äußerst einfach. McAfee VirusScan Enterprise nutzt das preisgekrönte McAfee-Scan-Modul zum Schutz Ihrer Systeme vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutz-technologien und Eindringungsschutz können Exploits abgewehrt werden, die mithilfe von Buffer Overflows Schwachstellen in 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 der Verfolgung und Blockierung 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.

Der Schutz Ihres Unternehmens vor PUPs, die das herkömmliche Vertrauensmodell mit heimtückischem und unerwünschtem Verhalten unterlaufen möchten, ist häufig nicht einfach. Durch die Kombination aus branchenweit führender Forschung von McAfee Labs mit Intel Security-Technologie kann sich Ihr Unternehmen vor PUPs schützen.

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