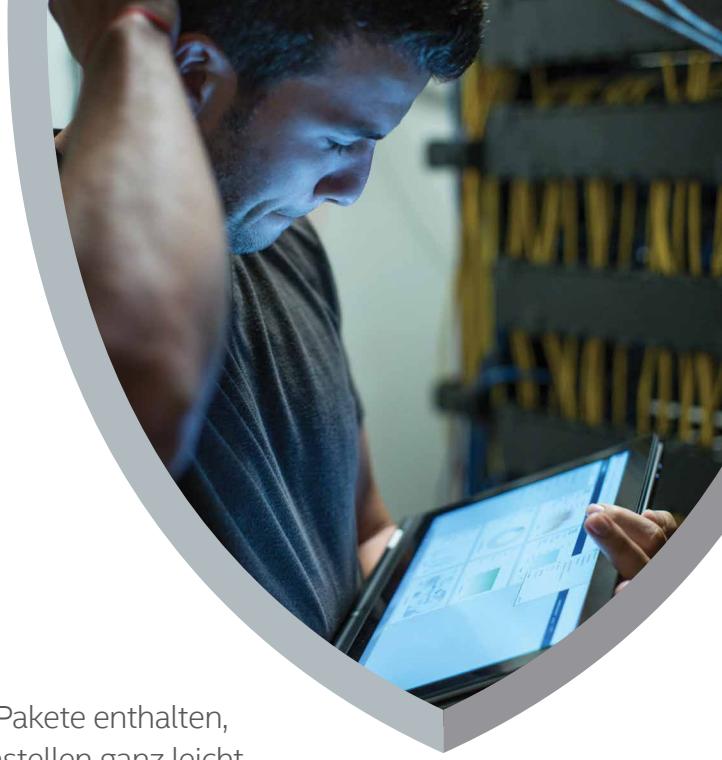
Kurzvorstellung

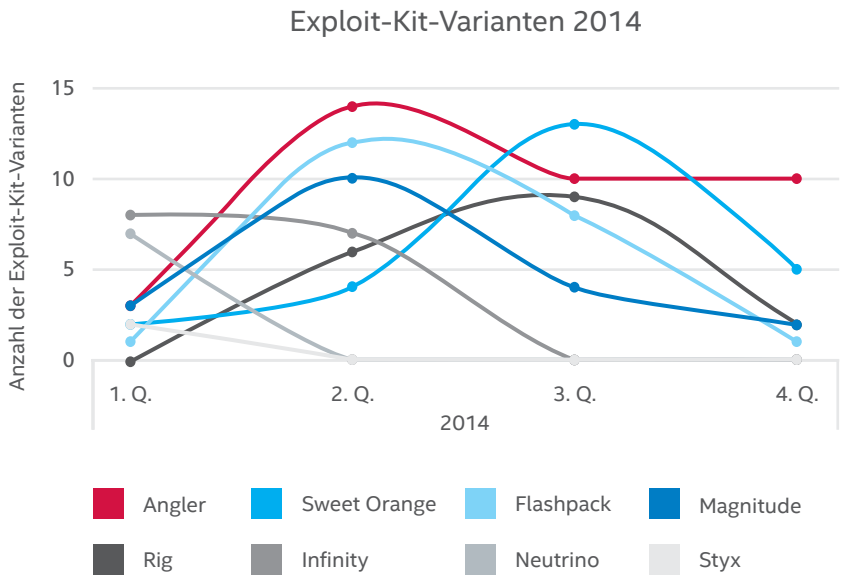


Kampf gegen das Exploit Kit Angler

Exploit-Kits sind Massenprodukte, die komplette Software-Pakete enthalten, mit denen bekannte und unbekannte („Zero-Day“) Schwachstellen ganz leicht für Angriffe ausgenutzt werden können. Diese Toolkits nutzen Client-seitige Schwachstellen aus, meist solche in Web-Browsern und Anwendungen, auf die über den Web-Browser zugegriffen werden kann. Exploit-Kits können auch Infektionsmetriken verfolgen und verfügen über robuste Steuerungsfunktionen.

Was ist das Exploit-Kit Angler?

Das Exploit-Kit Angler wird ausführlich im **McAfee® Labs Threat-Report vom Februar 2015** besprochen. In der zweiten Hälfte 2014 legte Angler bei der Verbreitung und beim Bekanntheitsgrad stark zu, da es über einige neue Funktionen verfügt. So kann es zum Beispiel den Arbeitsspeicher ohne Umweg über Dateien infizieren sowie virtuelle Maschinen und Sicherheitsprodukte rechtzeitig erkennen. Außerdem ist es in der Lage, die unterschiedlichsten Formen von Schaddaten zu übertragen, darunter Banking-Trojaner, Rootkits, Ransomware, CryptoLocker und Backdoor-Trojaner. Besondere Fachkenntnisse setzt Angler nicht voraus. Zudem ist es in zahlreichen einschlägigen Online-Schwarzmärkten erhältlich. So wurde es dermaßen populär:



Quelle: McAfee Labs, 2015

intel Security

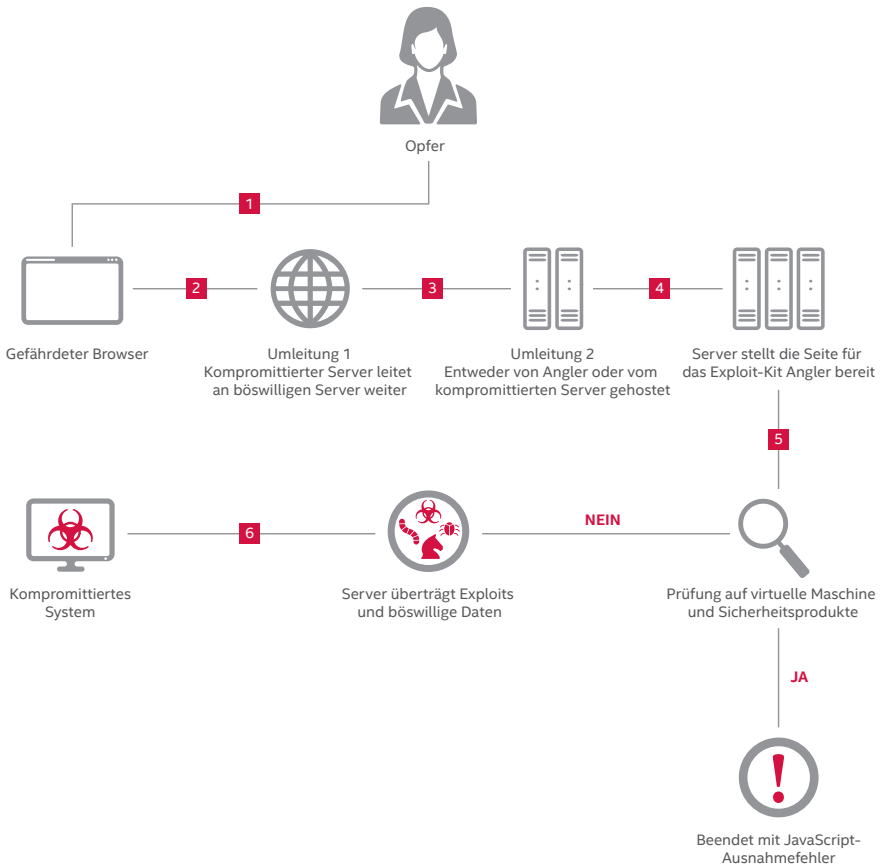
Die Exploit-Kits Angler wechseln häufig ihre Muster und Schaddaten, um sich vor Sicherheitsprodukten zu verbergen. Zum Schutz vor Entdeckung setzt Angler verschiedene Verschleierungstaktiken ein:

- Vor Erreichen der Landing Page setzt es zwei Umleitungsebenen ein.
- Kompromittierte Web-Server, auf denen die Landing Page gehostet wird, können von einer IP-Adresse aus nur einmal besucht werden. Die Hosts werden von den Angreifern sehr aktiv überwacht.
- Es erkennt, wenn auf einem System virtuelle Maschinen oder Sicherheitsprodukte vorhanden sind.
- Es erschwert das Reverse Engineering durch Garbage- und Junk-Aufrufe.
- Es verschlüsselt sämtliche Schaddaten beim Download und entschlüsselt sie auf dem infizierten Computer.
- Es infiziert Computer ohne Umweg über Dateien – direkt aus seinem Arbeitsspeicher heraus.

Eine erfolgreiche Infektion von Systemen durch das Exploit-Kit Angler sieht wie folgt aus:

- Das Opfer greift über einen verwundbaren Browser auf einen kompromittierten Web-Server zu.
- Der kompromittierte Web-Server leitet die Daten an Zwischen-Server weiter.
- Dieser zwischengeschaltete Server wiederum leitet die Verbindung an einen böswilligen Web-Server um, der als Host für die Landing Page aus dem Exploit-Kit dient.
- Die Landing Page prüft, ob der Browser bestimmte Plug-Ins enthält (Java, Flash und Silverlight), und stellt deren Versionsnummern fest.
- Wird eine verwundbare Browser- oder Plug-In-Version gefunden, überträgt das Exploit-Kit die entsprechenden Schaddaten und infiziert den Computer.

Infektionskette beim Exploit-Kit Angler



Schutz vor dem Exploit-Kit Angler

Zum Schutz vor dem Exploit-Kit Angler empfehlen sich die folgenden Maßnahmen:

- Verwenden Sie einen sicherheitsbewussten Internetdienstanbieter (ISP), der starke Prozeduren gegen Spam und Phishing implementiert.
- Aktivieren Sie die automatische Update-Funktion ihres Betriebssystems, oder laden Sie die Betriebssystem-Updates regelmäßig herunter, um Ihr Betriebssystem mit den entsprechenden Patches für bekannte Sicherheitslücken zu aktualisieren. Installieren Sie Patches anderer Software-Hersteller, sobald diese verfügbar sind. Ein mit sämtlichen Patches versehener Computer hinter einer Firewall ist die beste Verteidigung gegen Trojaner- und Spyware-Angriffe.
- Seien Sie äußerst vorsichtig, wenn Sie Anhänge öffnen. Konfigurieren Sie Ihre Virenschutz-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. Öffnen Sie niemals eine E-Mail, die Ihnen unverlangt zugesendet wurde oder die 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 rein. Klicken Sie nicht auf Links in E-Mails oder Instant Messages.
- Installieren Sie ein Browser-Plug-In, das die Ausführung von Skripten und iFrames verhindert.

So kann Intel Security vor dem Exploit-Kit Angler schützen

McAfee Web Gateway

Malvertising, Drive-by-Downloads und böswillige URLs, die in vertrauenswürdige Webseiten eingebettet sind, sind nur einige der Angriffsmethoden, mit denen das Exploit-Kit Angler übertragen wird. 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 Malware, wie sie von Angler übertragen wird, äußerst einfach. McAfee VirusScan Enterprise nutzt das preisgekrönte McAfee-Scan-Modul zum Schutz Ihrer Dateien vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutztechnologien 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.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense ist eine mehrstufige Lösung zum Aufspüren von Malware, die 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 Advanced Threat Defense vor gängigen Exploit-Kits wie Angler und deren Malware.

- **Signatur-basierte Erkennung:** Schützt vor Viren, Würmern, Spyware, Bots, Trojanern, Buffer Overflows und kombinierten Angriffen. Die umfangreiche KnowledgeBase, die derzeit mehr als 150 Millionen Signaturen (inklusive den Angler-Varianten) enthält, wird von McAfee Labs gepflegt.
- **Reputations-basierte Erkennung:** Über das McAfee GTI-Netzwerk werden Informationen zur Datei-Reputation abgerufen, damit auch neue Bedrohungen erkannt werden.
- **Statische Echtzeitanalyse und Emulation:** Bietet statische Echtzeitanalyse und Emulation zur schnellen Erkennung von Malware und Zero-Day-Bedrohungen, die von Signatur- oder Reputations-basierten Verfahren nicht erkannt werden.
- **Vollständige statische Code-Analyse:** Führt ein Reverse Engineering des Datei-Codes durch, um alle Attribute und Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen. 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:** Hierbei wird Datei-Code in einer virtuellen Ausführungsumgebung ausgeführt und das Verhalten beobachtet. Dabei werden die virtuellen Umgebungen so konfiguriert, dass sie mit Host-Umgebungen Ihres Unternehmens übereinstimmen – unabhängig davon, ob Sie benutzerdefinierte Betriebssystemabbilder von Windows 7 (32- und 64-Bit-Versionen), Windows XP, Windows Server 2003, Windows Server 2008 (64-Bit-Version) oder Android benötigen.

McAfee Network Security Platform

McAfee Network Security Platform ist für die Durchführung tiefgehender Netzwerkdatenverkehr-Überprüfungen ausgelegt. McAfee Network Security Platform setzt auf eine Kombination fortschrittlicher Untersuchungstechniken zur Erkennung sowie Abwehr bekannter und Zero-Day-Angriffe im Netzwerk. Diese Techniken umfassen unter anderem die vollständige Analyse der Protokolle, der Bedrohungs-Reputation und des Verhaltens sowie fortschrittliche Malware-Analyse.

- **Umfassender Malware-Schutz:** Die Lösung kombiniert McAfee GTI-Datei-Reputationsdaten sowie Datei-Tiefenanalysen mit JavaScript-Überprüfungen und umfasst ein signaturloses hochentwickeltes Malware-Analysemodul zur Erkennung und Abwehr von Zero-Day-Bedrohungen, angepasster Malware sowie anderen verborgenen Angriffen.
- **Nutzung fortschrittlicher Untersuchungstechniken:** Die Lösung umfasst die vollständige Analyse der Protokolle, der Bedrohungs-Reputation und des Verhaltens zur Erkennung sowie Abwehr bekannter und Zero-Day-Angriffe im Netzwerk.

- **Integration von McAfee GTI:** Kombiniert Echtzeit-Datei-Reputations-, IP-Reputations- und Standort-Feeds mit detaillierten Kontextdaten zu Benutzern, Geräten und Anwendungen, um schnell und präzise auf Angriffe aus dem Netzwerk reagieren zu können.
- **Security Connected:** Dank der zuverlässigen Integration von McAfee Advanced Threat Defense kann die McAfee Network Security Platform verdächtige Dateien, die in überwachtem Datenverkehr gefunden wurden, an McAfee Advanced Threat Defense übermitteln und dann gemäß den von McAfee Advanced Threat Defense zurückgegebenen Angaben zulassen oder ablehnen.

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 und 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 Hashwerte bekannt gefährlicher Dateien werden in McAfee Threat Intelligence Exchange importiert, um Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen zu immunisieren. Wenn diese Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit dem Indikator im Zusammenhang stehen.

Die zunehmende Verbreitung leicht zu bedienender Exploit-Kits wie Angler ist ein warnender Beleg dafür, dass sich die Bedrohungslage ständig ändert. Mit der Technologie von Intel Security kann sich Ihr Unternehmen sowohl auf den Endgeräten als auch im Netzwerk präventiv vor Bedrohungen wie dem Exploit-Kit Angler schützen.

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