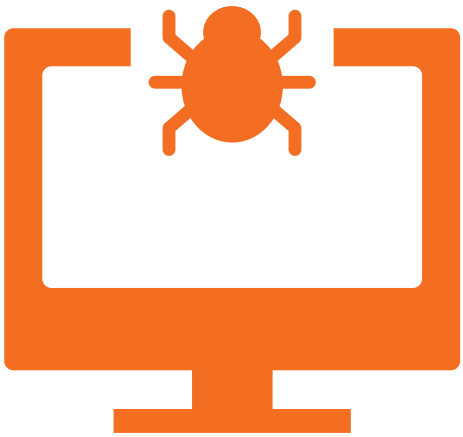
SOPHOS



Die fünf Phasen eines Web-Malware-Angriffs

Ein Leitfaden zu Web-Angriffen, mit Besprechung von Technologien, Tools und Taktiken für wirksamen Schutz

Autor: **Chris McCormack,** Senior Product Marketing Manager

Moderne Web-Angriffe sind extrem ausgefeilt und facettenreich. Ihr Nährboden ist eine immer stärker wachsende Schattenwirtschaft, die mit kompromittierten Computern und Benutzerdaten handelt. In diesem White Paper erfahren Sie, wie solche Angriffe genau funktionieren. Dazu haben wir den Ablauf eines Angriffs in fünf Phasen unterteilt – vom Eintritt bis zur Ausführung der Schadsoftware.

Wir erklären Ihnen die hochentwickelten Verfahren, mit denen Hacker die Systeme von Internetbenutzern infizieren, um an ihre Daten und ihr Geld zu gelangen. Außerdem zeigen wir Ihnen, warum die meisten Web-Security-Produkte keinen ausreichenden Schutz bieten. Sie erhalten Informationen dazu, welche Schutzschichten Sie benötigen, sowie eine Checkliste, mit der Sie Ihre Richtlinien und die Sicherheitsfunktionen Ihrer Webschutz-Lösung bewerten können.

Inhaltsverzeichnis

Web-Malware in Zahlen

Das Internet ist ein gefährlicher Ort. Die SophosLabs verzeichnen täglich rund 30.000 neue Schad-URLs. Zu 80 % handelt es sich dabei um eigentlich seriöse Webseiten, die jedoch manipuliert wurden. 85 % aller Malware-Schädlinge – u. a. Viren, Würmer, Spyware, Aware und Trojaner – stammen aus dem Internet.

Außerdem bieten sich Hackern mit kriminellen Absichten immer mehr Gelegenheiten. Denken Sie nur daran, wie groß das Internet ist und wie viele von uns es täglich nutzen. Jeden Tag sind mehr als 2,7 Mrd. Nutzer online und stellen 3 Mrd. Suchanfragen.[1] Es gibt schätzungsweise 700 Mio. Webseiten und ihre Anzahl steigt jährlich um 10 %.[2]

Vielleicht haben Sie selbst noch keine Probleme mit Web-Malware oder Schad-Webseiten gehabt. Täglich sind jedoch Millionen von Internetnutzern betroffen und Infektionen im Netz breiten sich immer weiter aus. Laut Googles Transparency Report liegt die Zahl der Nutzer,[3] denen Browser-Warnungen angezeigt werden, konstant bei zig Millionen pro Woche.

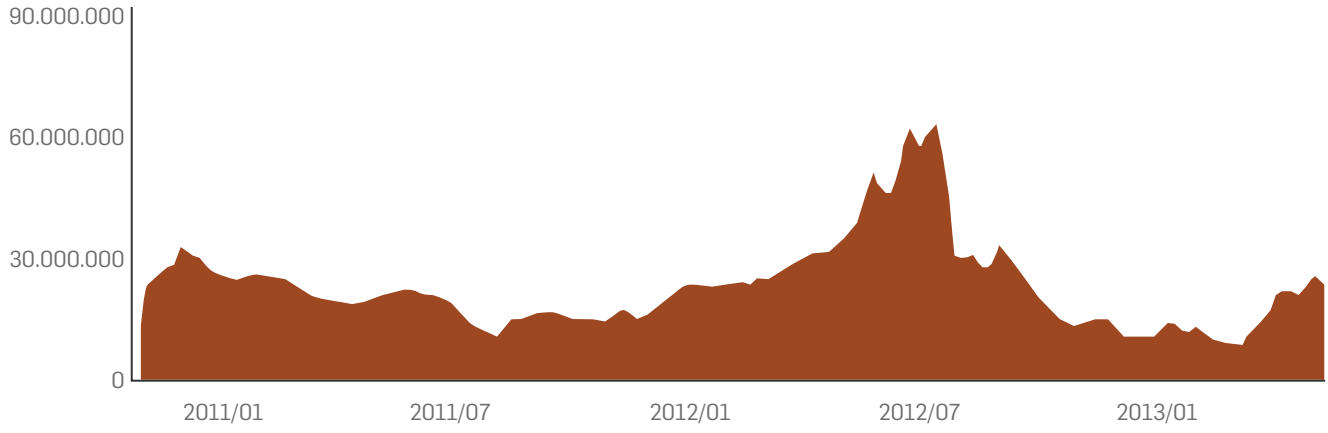


Abbildung 1: Anzahl an Nutzern, die wöchentlich Warnungen von Google Safe Browsing angezeigt bekommen
Quelle: Google Transparency Report.

1 Infografik: The Incredible Growth of Web Usage [1984-2013], WhoIsHostingThis, 21. August 2013, http://www.whoishostingthis.com/blog/2013/08/21/incredible-growth-web-usage-infographic/
2 Internet 2012 in numbers, Royal Pingdom, 16. Januar 2013, http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/
3 Safe Browsing Transparency Report, Google, http://www.google.com/transparencyreport/safebrowsing/

Wie Web-Angriffe funktionieren – die fünf Phasen

In diesem Abschnitt erklären wir, wie moderne Web-Angriffe funktionieren. Dazu teilen wir den Ablauf eines Angriffs in fünf Phasen ein: Eintritt, Umleitung, Exploit, Infektion und Ausführung.

Ihre Lieblings-Webseite

1. Eintritt	Ein Drive-By-Download von einer infizierten Webseite oder aus einer E-Mail mit Schadlink verschafft sich die Kontrolle über den Browser des Benutzers.
2. Umleitung	Malware leitet den Browser des Benutzers zu einer Schad-Webseite um, je nach verwendetem Browser und Betriebssystem.
3. Exploit	Das System des Benutzers wird mit einem Exploit-Kit auf eine Reihe von Schwachstellen untersucht.
4. Infektion	Ein schädlicher Payload wird heruntergeladen und infiziert das System des Benutzers mit Malware.
5. Ausführung	Die Malware überträgt sensible Daten an ihren Host oder versucht, vom Benutzer Geld zu erpressen (Ransomware).

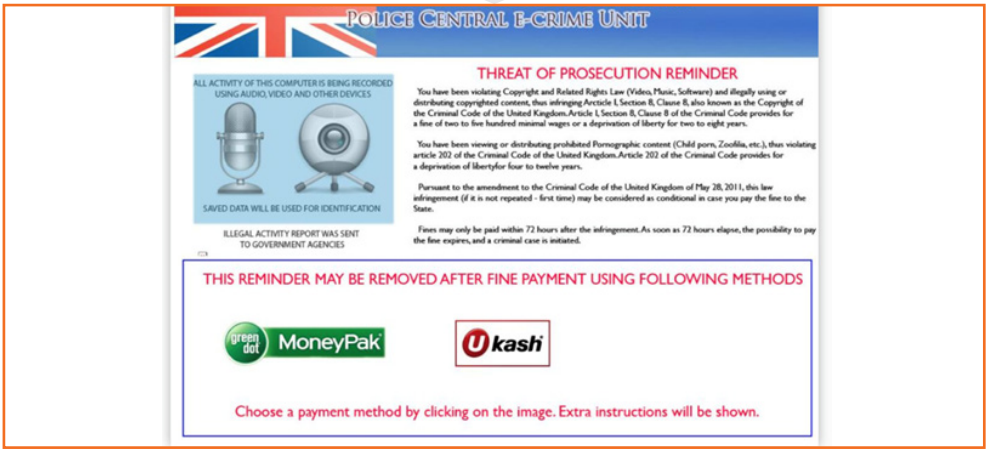


Abbildung 2: Infografik zu den fünf Phasen eines Web-Angriffs

Phase 1: Eintritt

In der ersten Phase eines Web-Angriffs kommt ein Drive-by-Download ins Spiel, der über einen so genannten Eintrittspunkt, also z. B. eine manipulierte Webseite oder eine E-Mail mit einem Schadlink, ausgelöst wird.

Drive-by-Downloads

Ein Drive-by-Download beschreibt einen Vorgang, bei dem schädlicher Webcode allein durch den Besuch einer Webseite ungewollt heruntergeladen wird. Der Drive-by-Download läuft automatisch ab, ohne dass der Nutzer es bemerkt.

Am häufigsten treten Drive-By-Downloads in Form unsichtbarer 0x0-Pixel-iFrames auf, die schädlichen JavaScript-Code enthalten. Dieses hochentwickelte JavaScript kann verschleiert (d. h. unleserlich gemacht) werden oder polymorph sein (Code wird bei jedem Aufruf der Webseite geändert). Herkömmliche Antivirus-Lösungen auf Signaturbasis sind gegen solche Code-Tricks machtlos.

Wie seriöse Webseiten manipuliert werden

Webserver wie Apache und IIS sowie ihre Content-Management-Systeme haben Schwachstellen. Hacker können diese Schwachstellen mit Website-Exploit-Tools ausnutzen und Schadcode in Webseiten einbinden.

Ein besonders beliebtes Exploit-Tool heißt Darkleech. Dabei handelt es sich um ein bösartiges Apache-Modul, mit dem Angreifer schädliche iFrames auf Webseiten einbinden können, die auf den betroffenen Webservern gehostet werden. Von Oktober 2012 bis Juli 2013 infizierte Darkleech mehr als 40.000 Webseiten.[4]

Viele Hacker verschaffen sich außerdem über gestohlene Zugangsdaten die Kontrolle über Webseiten. Die Zugangsdaten vieler Wordpress-Webseiten lassen sich z. B. leicht erraten oder durch Brute-Force-Angriffe ermitteln. Sobald die Hacker an die Zugangsdaten Ihrer Webseite gelangt sind, können sie beliebig Malware einschleusen.

Technologien, Tools und Taktiken für wirksamen Schutz

Jahrelang hielt sich die These, die meisten Bedrohungen lauerten in den weniger seriösen Bereichen des Internets (z. B. pornografische, Glücksspiel- und Hacking-Webseiten). Wenn dies der Wahrheit entspräche, würde es ausreichen, sich mit einem URL-Filter zu schützen, der solche Webseiten blockiert. Leider ist es in der Realität jedoch wesentlich komplizierter.

Innerhalb der 10 am häufigsten infizierten Webseiten-Kategorien belegen pornografische Webseiten mit nur 2 % den letzten Platz. Kategorien wie Blogs, Hosting und geschäftliche Internetauftritte sind wesentlich anfälliger für Malware.[5]

4 Rampant Apache website attack hits visitors with highly malicious software, Ars Technica, 3. Juli 2013, http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/
5 Surprise! The Most Dangerous Web Sites Aren't Porn Sites, TechNewsDaily, 4. Juni 4 2012, http://www.technewsdaily.com/4365-porn-dangerous-web-site.html

Die zehn am häufigsten infizierten Webseiten-Kategorien

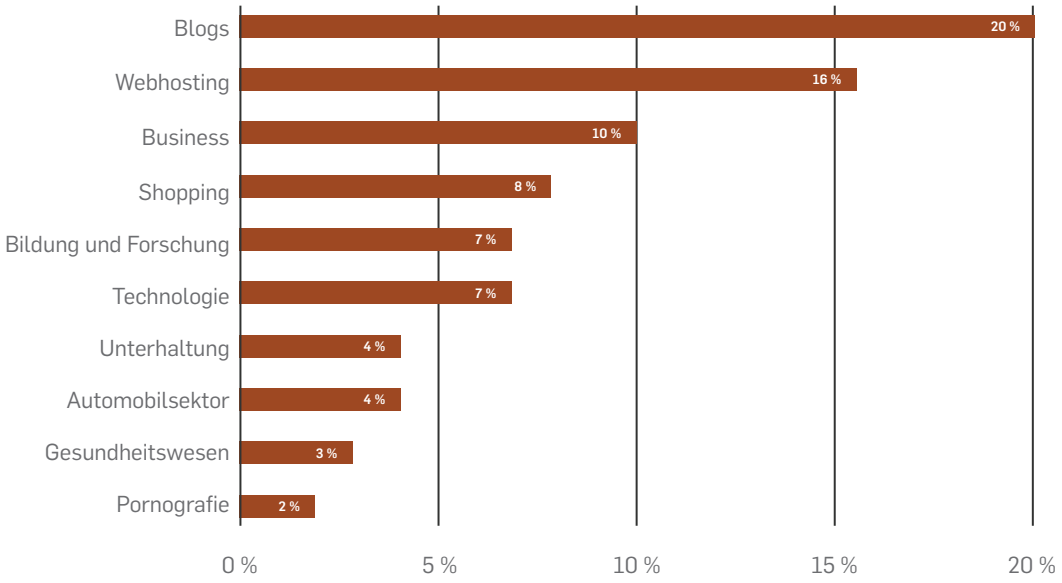


Abbildung 3: Die zehn führenden Kategorien von Schad-Webseiten Quelle: TechNewsDaily

Noch schlimmer ist, dass Malware-Werbekampagnen (auch Malvertising genannt) häufig auf zahlreichen manipulierten Webseiten auftauchen. Auch deshalb ist dem Problem mit einer einfachen URL-Filterung kaum Herr zu werden.

Wie können Sie sich nun wirksam schützen? Eine URL-Filterung ist nach wie vor wichtig. Bessere Lösungen besitzen jedoch zusätzlich eine **Live-Reputationsfilterung**. Diese wird laufend aktualisiert, um so auch Webseiten zu entdecken, die gerade erst infiziert wurden. Außerdem ist eine **Richtlinie für sicheres Internetsurfen** nur dann wirksam, wenn sie nicht einfach umgangen werden kann. Stellen Sie deshalb sicher, dass Sie die Nutzung anonymisierender Proxy-Server unterbinden können.

Die vielleicht wichtigste Technologie, die Sie benötigen, um Web-Bedrohungen auf dieser Ebene und darüber hinaus abzuwehren, ist ein **Schutz vor moderner Web-Malware**. Sie benötigen einen Bedrohungsschutz der neuesten Generation, der alle heruntergeladenen Webinhalte mittels moderner Verfahren wie JavaScript-Emulation auf Malware scannt und verdächtigen und schädlichen Code bereits erkennt, bevor dieser in den Browser gelangt. Ein solcher Schutz ist nicht nur an Ihrem Netzwerk-Gateway unerlässlich, sondern sollte außerdem auf Ihren Endpoints oder in Ihrem Desktop-Antivirus vorhanden sein, damit Benutzer auch außerhalb des Büros geschützt sind.

Des Weiteren sollten Sie einen Browser verwenden, der Googles Safe Browsing API (https://developers.google.com/safe-browsing/) unterstützt, z. B. Chrome, Firefox oder Safari. Diese Browser können Schad-Webseiten in den Suchergebnissen erkennen und den Benutzer warnen, bevor er Gefahr läuft, eine infizierte Webseite zu besuchen.

Investieren Sie außerdem in **Schulungen zum sicheren Internet-Surfen**, um computertechnisch weniger versierte Benutzer darüber aufzuklären, worauf sie achten müssen und wie sie üblichen Social-Engineering-Tricks und offensichtlichen E-Mail-Betrügereien aus dem Weg gehen können.

Darüber hinaus sollten Sie unbedingt sicherstellen, dass Ihre eigene Webseite nicht zur Problematik beiträgt. Verwenden Sie für Ihr Webseiten-CMS und Ihre Wordpress-Blogs sichere Passwörter. Prüfen Sie außerdem den Code Ihrer Webseite auf potenzielle Schwachstellen. Schützen Sie Ihre Webseite mit einer **Web Application Firewall**, mit der Formulare gesichert und Angriffe vermieden werden können.

Phase 2: Umleitung

Sobald der Drive-By-Download den Browser erreicht hat, wird der ahnungslose Benutzer zum Download eines Exploit-Kits umgeleitet. Anstatt den Benutzer jedoch auf bekannte Exploit-Kit-Webseiten zu verweisen, erstellen ausgeklügelte Traffic Distribution Systems (TDS) eine Vielzahl von Umleitungen, deren Nachverfolgen und Blacklisten praktisch unmöglich ist.

Einige TDS sind seriös, z. B. solche, die für Werbe- und Empfehlungsnetzwerke verwendet werden. Aber wie bei jeder Software besteht auch bei seriösen TDS-Lösungen die Gefahr einer missbräuchlichen Nutzung durch Hacker, die damit Datenverkehr auf Malware-Webseiten umleiten.

So nutzen Cyberkriminelle das TDS „Sutra", um den durch Drive-by-Downloads erzeugten Internetverkehr auf die spezifischen Eigenschaften des Benutzers auszurichten und so eine höhere Infektionsrate zu erreichen. Als Daten dienen hierfür die IP-Geolocation, das Betriebssystem, der genutzte Browser oder andere aussagekräftige Metadaten. Hacker können die aktuelle Version von Sutra TDS 3.4 für gerade einmal 100 $ erwerben und erzielen damit auf einem Low-End-Server mehr als eine Million Klicks pro Stunde.

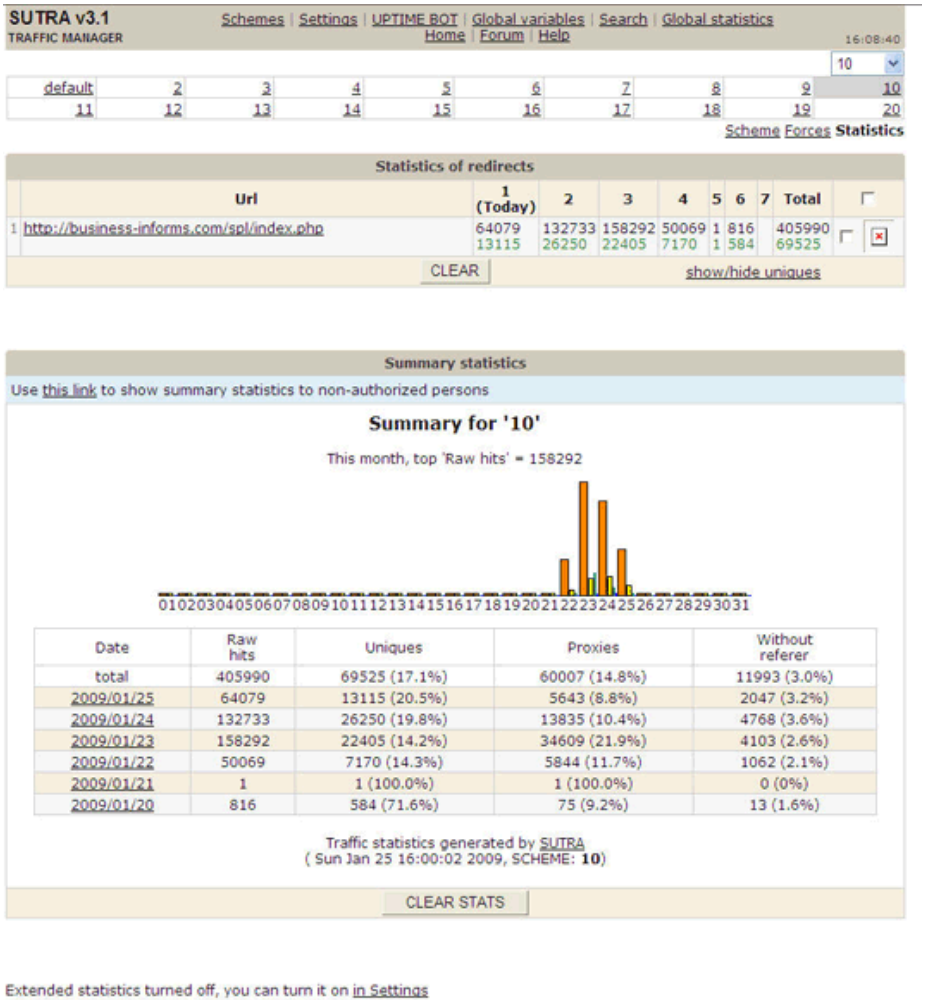


Abbildung 4: Kommerzielle TDS wie Sutra dienen Hackern häufig dazu, ihre Malware-Webseiten hinter einer komplexen Infrastruktur zur Umleitung von Datenverkehr zu verbergen.

Außerdem filtern TDS-Netzwerke häufig den Internetverkehr, damit ihre Webseiten vor Suchmaschinen und Sicherheitsanbietern verborgen bleiben. Sie nutzen außerdem Fast-Flux-Netzwerke, um damit Domains über tausende verschiedene IP-Adressen erreichbar zu machen. So verhindern sie, dass ihre Malware-Webseiten auf einer Blacklist landen.

Technologien, Tools und Taktiken für wirksamen Schutz

Die Verschleierungstaktiken der TDS-Netzwerke stellen die Sicherheit so auf eine echte Probe. Für den Benutzer ist es unmöglich, eine Umleitungskette zu unterbrechen, da diese sofort im Hintergrund in Gang gesetzt wird, ohne dass der Benutzer es bemerkt. Selbst für die meisten Sicherheitsunternehmen ist es extrem schwierig, hier Schritt zu halten.

Deshalb sollte Ihre Lösung zur Netzwerksicherheit und Web-Filterung unbedingt von einem Anbieter stammen, der sich mit TDS auskennt und in Verfahren investiert, mit denen ein TDS-Missbrauch unterbunden werden kann. So ist es mit der richtigen Ausstattung beispielsweise möglich, die Reputation von DNS-Registrars zu kontrollieren und nachzuverfolgen, um so Hackern immer einen Schritt voraus zu sein und Proxyserver und Umleitungen schon zu blockieren, bevor sie überhaupt online gehen.

Phase 3: Exploit

In der nächsten Phase eines modernen Web-Angriffs erfolgt der Download eines Exploit-Kits von der Malware-Webseite. Exploit-Kits führen eine Vielzahl von Exploits aus. Dabei nutzen sie Schwachstellen in Webbrowsern und angeschlossenen Plug-ins wie Java, PDF-Readern und Media-Playern.

Exploit-Kits

Cyberkriminelle kaufen Exploit-Kits meist auf dem Schwarzmarkt und spülen damit Geld in die Kassen der Entwickler. Seit seiner Veröffentlichung Ende 2010 ist Blackhole zu einem der berüchtigsten Exploit-Kits geworden. Die Entwickler haben rund um das Kit ein professionelles Geschäftsmodell aufgezogen und bieten Blackhole für 500 $ im Monat an. Die Blackhole-Betreiber haben sogar eine webbasierte Management-Konsole im Angebot und leisten technischen Support über das Internet.

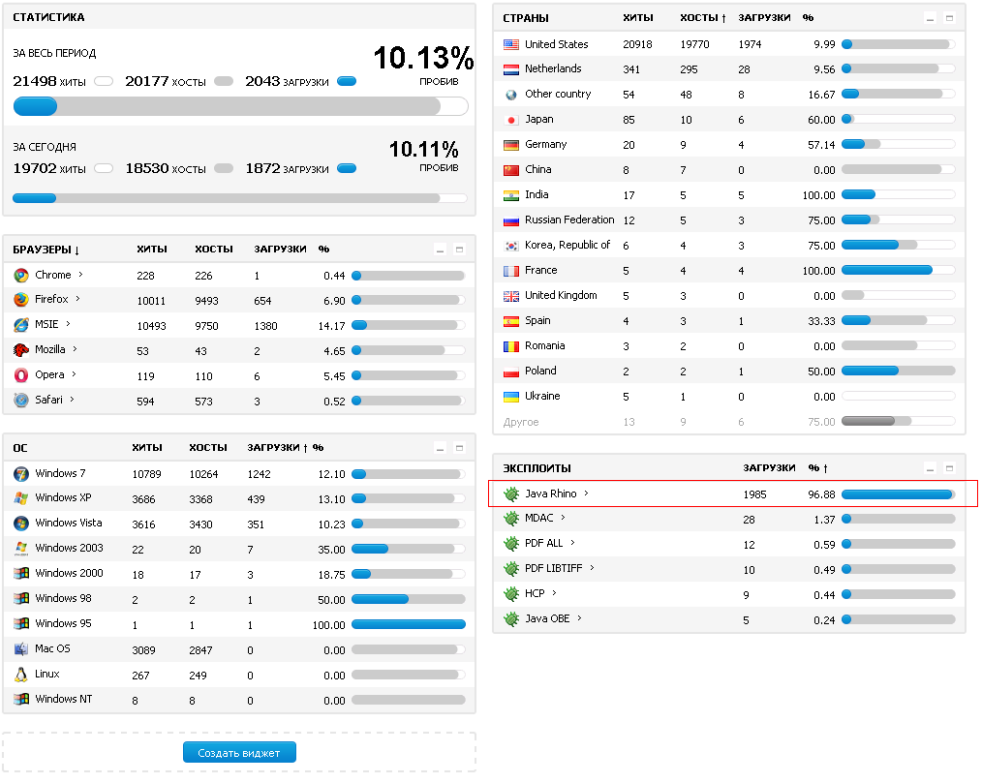


Abbildung 5: Blackhole-Dashboard

Der Ausschnitt des Blackhole-Dashboards in Abbildung 5 zeigt, wie Cyberkriminelle folgende Parameter nachverfolgen können: ihre Erfolgsrate bei Infektionen, die Anzahl der Webseiten, die Malware hosten, die betroffenen Systeme sowie den geografischen Standort der infizierten Webseiten.

Sobald der Browser eines Benutzers auf eine Webseite mit einem Blackhole-Exploit-Kit gelangt ist, werden Dateien geladen. Diese Dateien nutzen gezielt die spezifischen Schwachstellen des Betroffenen aus, die dank frei verfügbarer Informationen im Browser bekannt sind. Zur Ausnutzung von Schwachstellen auf Benutzersystemen werden besonders häufig die folgenden vier Dateitypen verwendet:

- **PDF:** PDF-Dateien mit eingebettetem JavaScript versuchen, bekannte Schwachstellen im Adobe Reader auszunutzen.
- **Flash:** Zwei unterschiedliche Arten von Flash-Dateien mit speziell entwickeltem Code werden häufig geladen, um Schwachstellen im Adobe Flash Player auszunutzen.
- **Java:** JAR-Dateien mit JavaScript- oder Applet-Code sind beim Auffinden von Schwachstellen meist am erfolgreichsten.
- **HTML/JS/VBS:** Laufzeitcode kann heruntergeladen werden, um gezielt Schwachstellen im Hilfe- und Supportcenter von Microsoft auszunutzen.

Natürlich sind die Skripts, Codes und Inhalte, die während der Exploit-Kit-Phase geladen werden, genau wie alle anderen Elemente eines Web-Angriffs hoch verschleiert und polymorph, um nicht erkannt zu werden.

Java Rhino

Leider ist Java für Hacker ein Traum. Milliarden Geräte und Browser werden mit Java ausgeliefert und die Programmiersprache ist auf praktisch allen Plattformen vorhanden. Einer der beliebteren und erfolgreicheren Exploits heißt Java Rhino und ist ein Java-Skriptmodul, das dazu missbraucht werden kann, willkürlichen Code außerhalb der Java-Sandbox auszuführen. Der Exploit funktioniert auf einer Vielzahl von Clients, auf denen Java 7 oder ältere Versionen installiert sind. Obwohl es mittlerweile einen Patch gibt, ist der Exploit nach wie vor sehr erfolgreich. Denn laut Qualys werden auf 80 % aller Unternehmenssysteme veraltete, nicht gepatchte Java-Versionen ausgeführt.[6]

Technologien, Tools und Taktiken für wirksamen Schutz

Eine leistungsstarke Web-Malware-Erkennung ist unbedingt erforderlich, um den Exploit-Code schon beim Download zu blockieren, bevor er Schwachstellen ausnutzen kann. Die Entwickler der Exploit-Kits nutzen jedoch Verschleierungs- und Polymorphismus-Taktiken, um nicht von Antivirus-Engines erkannt zu werden.

Wirksame Sicherheitslösungen gegen Web-Malware können mehr, als Schädlinge bloß anhand von Signaturen zu erkennen: Sie kombinieren eine URL-Filterung zur Blockierung bekannter Malware-Seiten mit einer intelligenten **Malware-Analyse**, die Exploit-Kits kontinuierlich kontrolliert und testet, um Erkennungsalgorithmen zu bestimmen.

Eine weitere wichtige Strategie, um die Angriffsfläche zu verkleinern, sind engmaschige Kontrollen der Browser und Anwendungen (z. B. PDF-Reader), die Ihre Benutzer verwenden. Beschränken Sie die zugelassenen Browser und Anwendungen auf ein Minimum und spielen Sie für diese regelmäßig Patches ein. So können Sie die Zahl der Schwachstellen, die sich durch Exploit-Kits ausnutzen lassen, entscheidend reduzieren.

Traurig, aber wahr: 90 % aller Angriffe auf Anwendungsschwachstellen könnten durch eine Installation bereits vorhandener Patches verhindert werden.[7] Leider sind viele Benutzer schlicht zu bequem, ihre Systeme regelmäßig zu **patchen**. Glücklicherweise gibt es Lösungen, die sich in Ihre Desktop-Sicherheitslösung integrieren lassen, um Endbenutzer-Anwendungen zu kontrollieren und Sicherheitspatches identifizieren und priorisieren können.

Bei der Ausarbeitung einer **Richtlinie für Webclientsoftware** sollten einige wichtige Sicherheitsaspekte berücksichtigt werden:

- **Browser:** Wenn möglich, sollten Sie sich auf einen Standard-Browser beschränken, der Googles Safer Browsing API unterstützt (z. B. Google Chrome, Mozilla Firefox oder Apple Safari). Gängige Browser sind zwar anfälliger für Exploits, ihre Anbieter halten jedoch auch mehr Ressourcen zur Behebung von Schwachstellen vor und stellen häufiger Patches bereit.
- **Java:** Wenn Sie Java nicht für unternehmensrelevante Webanwendungen benötigen, entfernen Sie die Software am besten von den Computern Ihrer Benutzer oder erlauben sie nur denjenigen Benutzern, die Java auch tatsächlich benötigen.

6 The Dark Side Of Java, Dark Reading, 1. Dezember 2011
http://www.darkreading.com/attacks-breaches/the-dark-side-of-java/232200604

7 Improving Your 2011 Security Bang for the Buck: Patching Depth and Breadth, Gartner blog, 4. Januar 2011, http://blogs.gartner.com/neil_macdonald/2011/01/04/improving-your-2011-security-bang-for-the-buck-patching-depth-and-breadth/

- **PDF-Reader:** Verwenden Sie nur einen einzigen Standard-PDF-Reader. Patchen Sie diesen regelmäßig, stellen Sie sicher, dass die Auto-Update-Funktion aktiviert ist, und sorgen Sie dafür, dass Benutzer neue Patches sofort installieren.
- **Plug-ins, Add-Ons und Toolbars:** Vermeiden Sie grundsätzlich Browser-Plug-ins und Toolbars. Diese vergrößern lediglich Ihre Angriffsfläche.

Phase 4: Infektion

Sobald der Angreifer eine Anwendungsschwachstelle ausgenutzt und sich Kontrolle über das betreffende System verschafft hat, wird ein schädlicher Payload heruntergeladen und das System infiziert. Der Payload ist die eigentliche Malware oder der Virus, der letztendlich die Daten stiehlt oder Geld vom Benutzer erpresst.

Hacker können dabei aus einer ganzen Reihe unterschiedlich infektiöser Payloads wählen. Nachfolgend sind einige der momentan beliebtesten Payloads aufgeführt.

Zbot	**25 %**	Backdoor	**6 %**
Ransomware	**18 %**	ZAccess	**6 %**
PWS	**12 %**	Downloader	**2 %**
Sinowal	**11 %**	Sonstige	**9 %**
FakeAV	**11 %**		

Abbildung 6: Aufschlüsselung von Blackhole-Payloads während eines Zeitraums von zwei Monaten (August und September 2012). Quelle: SophosLabs

- **Zbot (Zeus):** Zeus ist ein Trojaner, der persönliche Daten stiehlt, indem er Tastatureingaben aufzeichnet und Frames im Browser abfängt. Zbot-Angriffe zielten zunächst auf Windows, aber es wurden mittlerweile auch Varianten beobachtet, die mobile Android-Geräte infizieren.
- **Ransomware:** Ransomware sperrt Benutzer aus ihrem eigenen Computer oder von bestimmten Dateien aus und verlangt zur Freigabe ein Lösegeld. Ransomware-Angriffe zielen vornehmlich auf Windows ab. In jüngster Vergangenheit ist allerdings auch eine weniger gefährliche, jedoch ähnlich lästige Mac-Variante aufgetaucht.
- **PWS:** PWS ist ein passwortstehlender und remote zugreifender Trojaner, der Windows-Computer infiziert .
- **Sinowal (Torpig):** Torpig ist eine Botnet-Infektion, die auf Microsoft-Windows-Computer abzielt. Der Schädling verwendet ein Rootkit, um Zugangsdaten zu stehlen und einen Remotezugriff einzuräumen.
- **FakeAV:** FakeAV (gefälschter Virenschutz) installiert gefälschte Sicherheitssoftware, die sich als legitime Antivirus-Desktopanwendung ausgibt. Diese meldet zahlreiche angebliche Viren und erpresst den Benutzer, für die Entfernung der Viren zu zahlen. In der Vergangenheit waren vor allem Windows-Systeme betroffen. In jüngster Zeit geraten allerdings auch zunehmend Macs in den Fokus.

Technologien, Tools und Taktiken für wirksamen Schutz

Wie eben besprochen, wird in dieser Phase die Malware auf den Computer des Opfers heruntergeladen. In diesem Stadium des Angriffs vertrauen Sie auf **Web-Malware-Scans** und eine **Inhaltsfilterung**, der es bislang nicht gelungen ist, den Angriff zu erkennen.

Nun können Sie lediglich hoffen, dass der Payload nicht genauso geschickt ist wie der Schadcode, der in den vorhergehenden Phasen unerkannt bleiben konnte. Von einer verlässlichen Abwehr kann so natürlich keine Rede sein. Die weitaus klügere Strategie ist es, sich einen besseren **Schutz vor Web-Malware** zuzulegen, der Malware bereits in einem früheren Stadium des Angriffs unschädlich machen kann.

Phase 5: Ausführung

In Phase 4 des Angriffs wurde der Payload heruntergeladen und auf dem System des Opfers installiert. In Phase 5 besteht seine Aufgabe nun darin, dem Kriminellen, der hinter dem Payload steckt, Geld einzubringen. Dieses Ziel kann auf unterschiedliche Art und Weise erreicht werden: Durch das Abfangen von Zugangsdaten, den Klau von Online-Banking- oder Kreditkartendaten, die auf dem Schwarzmarkt veräußert werden können, oder durch eine direkte Erpressung des Benutzers. Sowohl bei Ransomware als auch FakeAV handelt es sich um Malware-Varianten, die Geld von Benutzern erpressen. Einige aktuelle Ransomware-Arten und ihre Vorgehensweisen sehen wie folgt aus:

Verschlüsselnde Ransomware: Diese Art bedient sich immer geschickterer Verschlüsselungsmethoden, um Dateien bis zur Zahlung des Lösegelds (meist um die 100 $) unzugänglich zu machen. 2013 tauchte eine neue Variante namens Cryptolocker auf, die alle privaten und beruflichen Dateien verschlüsselt und sie erst nach Begleichen einer Gebühr in Höhe von 300 $ wieder entschlüsselt. Die Verschlüsselung ist dabei so komplex, dass dem Opfer nichts anderes übrig bleibt, als das Lösegeld zu begleichen – oder eine komplette Neuaufsetzung des Systems vorzunehmen.

Nicht verschlüsselnde Ransomware: Hier gibt es verschiedene Varianten, die den Benutzer aus seinem eigenen Computer aussperren und so Lösegeld erpressen. Eine Variante zeigt eine gefälschte Windows-Aktivierungsnachricht und Zahlungsoption an. Eine andere, noch arglistigere Version sperrt den Benutzer nicht nur aus, sondern zeigt auch eine gefälschte Meldung an, die vorgibt, von einer Strafverfolgungsbehörde zu stammen, und die Zahlung eines Bußgelds wegen des Besitzes illegaler Software oder Kinderpornografie einfordert. Diese neueren Ransomware-Varianten unternehmen große Anstrengungen, um seriös zu erscheinen, und sind in unterschiedlichsten Sprachen erhältlich, um möglichst viele Opfer zu erreichen.

Abbildung 7: Eine typische Ransomware-Forderung

Abbildung 8: In verschiedene Sprachen übersetzte Lösegeldforderungen

Ransomware für Mac: Da Apple Macs sowohl in Unternehmen als auch privat immer beliebter werden, verwundert es kaum, dass es nun auch eine Ransomware speziell für Mac gibt. Sie funktioniert etwas anders und verwendet ein einfaches JavaScript, das die Kontrolle über den Browser übernimmt und unabhängig von der Reaktion des Benutzers immer wieder die gleiche Seite mit einer Lösegeldforderung lädt. Diese Mac-Ransomware (Abbildung 7) lässt sich recht einfach unschädlich machen. Jedoch wissen das die meisten Benutzer nicht und zahlen entnervt das Lösegeld (oft 300 $ pro Vorfall), was diese Malware so effektiv und lukrativ macht.

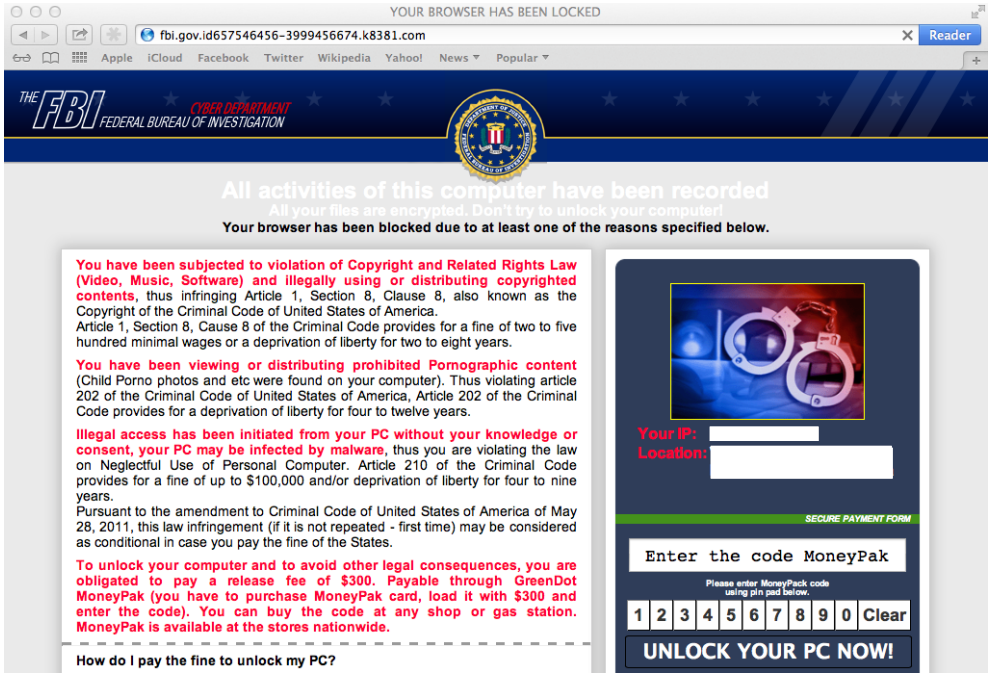


Abbildung 9: Eine Mac-Ransomware-Meldung gibt vor, vom FBI zu stammen
Quelle: Malwarebytes, http://blog.malwarebytes.org/intelligence/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/

Technologien, Tools und Taktiken für wirksamen Schutz

Ein Angriff in der Ausführungsphase gelangt an Ihrem Web-Schutz vorbei bis zu Ihrer letzten Verteidigungslinie – Ihrem **Desktop-Antivirus**. In dieser Phase besteht der Angriff aus einer ausführbaren Datei, einem Rootkit oder einer anderen Malware, die auf dem betroffenen System präsent ist und versucht, sensible Daten zu stehlen, Dateien zu verschlüsseln oder Benutzer aus ihren Computern auszusperren. Wenn der Angriff es bis hierhin geschafft hat, kann die Infektion nur noch durch einen Endpoint-Schutz mit Echtzeit-Updates und ein modernes **Host Intrusion Prevention System (HIPS)** verhindert werden.

In der Vergangenheit stützte sich die Virenerkennung auf Signaturen. Sobald eine neue Bedrohung entdeckt war, wurde eine neue Signatur als Update veröffentlicht, mit der sich der Virus erkennen lässt. Heutige Bedrohungen sind jedoch viel zu komplex und werden ständig modifiziert, so dass herkömmliche Antivirus-Updates keinen zuverlässigen Schutz mehr bieten.

Zur Erkennung moderner Malware ist daher HIPS notwendig. HIPS kann Bedrohungen abfangen, gegen die normale Antivirus-Engines machtlos sind, da es sich nicht auf Signaturen stützt, sondern in der Lage ist, bösartige Verhaltensweisen zu erkennen. HIPS-Engines beinhalten einen erweiterten Regelsatz, mit dem verdächtiges Systemverhalten rechtzeitig aufgedeckt, kommuniziert oder sofort unterbunden werden kann. Besonders wirksam sind dabei HIPS, bei denen die Regelsätze bereits auf Grundlage bewährter Branchenpraxis vorkonfiguriert und sofort einsatzbereit sind, um einerseits False Positives zu verhindern und andererseits neue Malware abzufangen.

Eine weitere Methode, die Infektionen in dieser Phase bekämpfen kann, ist eine **Call-Home-Erkennung**. Bei der Call-Home-Erkennung handelt es sich um eine Funktion, die in einigen Secure-Web-Gateway-Lösungen enthalten ist und infizierte Computer daran erkennen kann, dass sie bekannte Malware-Command-and-Control-URLs anfragen. Diese Funktion kann zwar keine Infektionen verhindern, kann Ihnen aber dabei helfen, infizierte Systeme in Ihrem Netzwerk zu finden.

Checkliste: Technologien, Tools und Taktiken für wirksamen Web-Schutz

Zu einer wirksamen Webschutzstrategie gehören Richtlinien zur Verkleinerung der Angriffsfläche, geeignete Tools und Technologien zur Durchsetzung dieser Richtlinien sowie ein Schutz zum Stoppen von Angriffen auf allen Ebenen.

Möchten Sie herausfinden, wie gut Ihre Richtlinien und Ihr Web-Schutz wirklich sind? Dann laden Sie hier unsere Checkliste zu Technologien, Tools und Taktiken für wirksamen Web-Schutz herunter.

Zum Download

Web-Schutz von Sophos

Der Web-Schutz von Sophos ist einfach zu installieren, zu verwalten und zu warten. Unsere erschwinglichen Suites enthalten alles, was Sie brauchen, um sich wirksam vor aktuellen Web-Bedrohungen zu schützen. Wir bieten den branchenweit besten Schutz und Support. Denn unsere umfassenden Lösungen werden ergänzt durch die Experten in unseren SophosLabs, die Bedrohungen pausenlos analysieren, und durch unser Support-Team, das rund um die Uhr für Sie im Einsatz ist.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA

12/13 NP

SOPHOS