COMPHONE UND
IT-Systemhaus - Lösungen für IT-Integration

SOPHOS
Security made simple.

Security Threat Report 2014

Malware: So raffiniert, tückisch und gut getarnt wie nie zuvor

Inhalt


SMS

Vorwort

Betrachtet man die Sicherheits- und Bedrohungslandschaft der vergangenen zwölf Monate, fällt eine Entwicklung besonders auf: Malware-Autoren werden immer geschickter darin, ihre Angriffe zu tarnen. Da Quellcode für ausgefeilte Botnets und Exploit-Kits im Netz mittlerweile weit verbreitet ist, sind immer mehr Malware-Autoren in der Lage, verschiedenste innovative Angriffsmethoden zu entwickeln.

Cyberkriminelle nutzen zunehmend Online-Marketing, um ihre Dienstleistungen auf dem Schwarzmarkt zu bewerben und zu verkaufen. Im Jahr 2012 veränderte das Exploit-Kit Blackhole die Bedrohungslandschaft massiv. 2013 wurde Blackhole durch mehrere neue Exploit-Kits abgelöst, die auf dem Original basieren und Teile seines Codes verwenden. Die daraus entstandenen Botnets haben zu einer starken Zunahme von Ransomware geführt, deren gefährlichster Vertreter Cryptolocker ist.

Bei moderner Malware geht es vor allem um Tarnung. Advanced Persistent Threats (APTs), eine besonders gefährliche Variante solcher als seriös getarnter Bedrohungen, richten ihre Angriffe gezielt gegen bestimmte Personen, Unternehmen, Regierungen und deren Daten. APTs sind hoch entwickelte, raffinierte Angriffe, die zielgerichtet konkrete Missionen im Netz ausführen. Datenlecks, in Verbindung mit Spionage und veröffentlichten Unternehmensdaten, waren ein großes Thema im vergangenen Jahr.

Die APT-Angriffe im Jahr 2013 waren gut geplant, sorgfältig ausgearbeitet und wurden von hoch motivierten, technisch sehr versierten Kriminellen ausgeführt. Das Perfide an APTs: Selbst nach erfolgreichem Abschluss der eigentlichen Mission bleiben sie oft noch aktiv, um zusätzliche Informationen zu sammeln. Die Abwehr solcher APTs ist kompliziert und nur mit einem gut organisierten Ansatz möglich, der sowohl die betreffenden Systeme als auch das Netzwerk einbezieht.

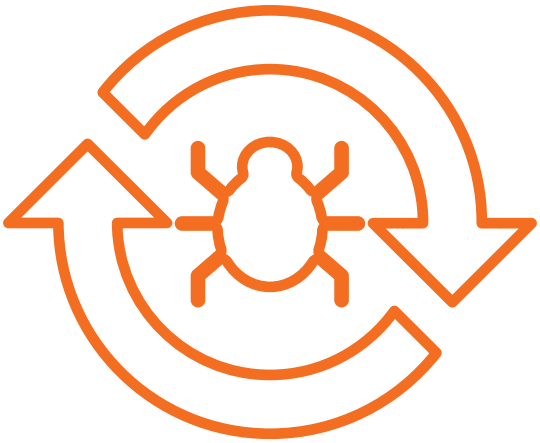
IT-Sicherheit ist deshalb mittlerweile kein Pluspunkt mehr, sondern absolute Notwendigkeit. Unternehmen und Regierungen, die sich zu Recht Sorgen um Datenschutz und die Sicherheit sensibler Daten machen, müssen jetzt noch besser über Sicherheitsprobleme Bescheid wissen, die in wichtigen Infrastrukturen auftreten können. So selbstverständlich wir mit dem Flugzeug fliegen, Geld am Automaten abheben oder uns auf die Versorgung mit Strom und Wasser verlassen – wir können nicht mehr automatisch davon ausgehen, dass die Sicherheit all dieser Systeme gewährleistet ist. Angriffe auf die Infrastruktur dieser entscheidenden Netzwerke und Steuerungssysteme führen uns deutlich vor Augen, dass es Sicherheitslücken in der lebenswichtigen Infrastruktur unserer Gesellschaft gibt. Im nächsten Jahr könnten Systeme mit Smart-Grid-Infrastruktur zunehmend das Ziel von Cyberkriminellen werden.

Die zunehmende Popularität des „Internets der Dinge“ (z. B. mobile Geräte, Anwendungen, soziale Netzwerke oder vernetzte Gadgets und Geräte) macht es fast unmöglich, mit den immer wieder neuen Bedrohungen Schritt zu halten. Mobile Plattformen werden fortwährend mit neuen Technologien ausgestattet, wie z. B. der Near Field Communication (NFC). Neue Bedrohungen lassen da nicht lange auf sich warten. Die innovative Nutzung von GPS-Diensten, um die digitale Welt mit unserer realen Welt zu verbinden, bietet Cyberkriminellen neue Sicherheitslücken und Möglichkeiten, in unsere Privatsphäre einzudringen.

Solche Systeme könnten Angriffe lancieren, die Auswirkungen auf jeden einzelnen von uns haben. Im Jahr 2014 erwarten uns nicht nur Weiterentwicklungen bereits bekannter Angriffsarten, sondern auch völlig neue Bedrohungen, für die es gilt, wirksame Abwehrmechanismen zu entwickeln.

Mit freundlichen Grüßen

Gerhard Eschelbeck
CTO, Sophos



Malware entwickelt sich 2013 entscheidend weiter

Seit unserem letzten Security Threat Report haben Malware-Angriffe und andere IT-Sicherheitsbedrohungen zugenommen und sind ausgefeilter geworden. Zudem werden die Entwickler und Herausgeber von schädlichen Codes und Webseiten immer kreativer, wenn es darum geht, ihre Bedrohungen zu tarnen.

Im Jahr 2013 gab es zahlreiche Innovationen bei Botnets und Exploit-Kits. Denn während früher nur absolute Experten in der Lage waren, solche Innovationen zu entwickeln, können neue Malware-Autoren jetzt aus den Erfahrungen und dem veröffentlichten Quellcode ihrer Vorgänger lernen. Cyberkriminelle sind geschickter darin geworden, unerkannt zu bleiben. Dazu nutzen sie vermehrt Kryptographie und platzieren ihre Server immer häufiger im Darknet – in geschlossenen, anonymen Bereichen des Internets, in denen sich unbeobachtet agieren lässt.

Da Benutzer ihr Augenmerk weiterhin auf mobile Geräte und Web Services legen, tun Malware-Autoren genau dasselbe. Android-Angriffe wurden 2013 komplexer und ausgereifter und gut getarnte Angriffe wie Darkleech haben Tausende Webserver unter Fremdkontrolle gebracht. Gleichzeitig blicken Benutzer älterer Windows-Systeme mit Sorge auf den 8. April 2014, denn ab diesem Zeitpunkt stellt Microsoft keine Sicherheitsupdates mehr für Windows XP und Office 2003 zur Verfügung. Man darf gespannt sein, welche gefährlichen Zero-Day-Forever-Angriffe dies zur Folge haben wird.

Wie andere innerhalb der IT-Sicherheitsbranche beobachten auch wir bei Sophos immer mehr Bedrohungen, die sich ganz gezielt auf bestimmte Unternehmen, Branchen oder Regierungsbehörden konzentrieren. Außerdem nehmen Bedrohungen zu, die sich einst auf Osteuropa beschränkten – solche, deren Ziel Bankkonten und Finanztransaktionen sind.

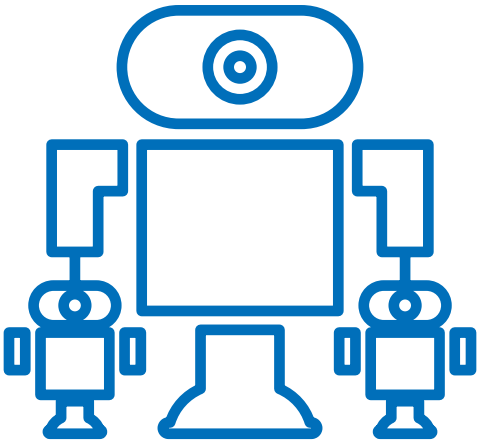
Manche Bedrohungen treten weiterhin zyklisch auf – sie verschwinden für einige Jahre und schlagen dann erneut zu. So gab es beispielsweise ein Comeback von Spam-Mails, die nach dem so genannten Pump-and-Dump-Schema arbeiten und eigentlich von der US-Börsenaufsicht vor einigen Jahren so gut wie ausgemerzt worden waren.

2013 trat außerdem eine gefährliche neue Version der Ransomware Cryptolocker auf. Zwar gibt es Ransomware bereits seit fast einem Vierteljahrhundert, doch diese neueste Version nutzt eine sehr starke Verschlüsselung, um die Benutzer aus ihren eigenen Dateien auszusperren und so Geld von ihnen zu erpressen.

Glücklicherweise gab es jedoch auch ein paar gute Schlagzeilen zu vermelden. Der mutmaßliche Entwickler des Exploit-Kits Blackhole wurde im Oktober festgenommen: ein Beweis dafür, dass kriminelle Malware-Organisationen zur Rechenschaft gezogen werden. Google machte 2013 vom technischen Standpunkt betrachtet Fortschritte bei der Sicherung der Android-Plattform. Zudem verschärfte das Unternehmen seine Regeln zur Einschränkung vieler aggressiver potentiell unerwünschter Apps.

Gleichzeitig leisten die Experten in unseren weltweiten SophosLabs Pionierarbeit bei der Entwicklung neuer Ansätze zur Erkennung und Bekämpfung von Angriffen. Dabei nutzen sie die derzeit leistungsfähigsten, modernsten Cloud- und Big-Data-Technologien.

Egal, ob Sie ein großes oder kleines Unternehmen besitzen, einer Schule oder einer Regierungsbehörde angehören oder ein einzelner Benutzer sind – unser gemeinsamer Kampf gegen Malware geht weiter. Um diesen Kampf zu gewinnen, arbeiten wir auch weiterhin unermüdlich daran, Sie mit den besten Technologien umfassend zu schützen.



Botnets: Größer und immer besser getarnt

In den letzten 12 Monaten haben sich Botnets weiter ausgebreitet, sind resistenter geworden und haben ihre Tarnung verbessert. Dazu nehmen sie offenbar neue Ziele ins Visier.

Normalerweise halten die Entwickler von Botnets ihren Quellcode streng geheim. Denn wenn Cyberkriminelle die Botnets nicht mehr aktiv nutzen möchten, können sie den Code häufig zu hohen Preisen verkaufen. In den letzten Jahren wurde jedoch immer mehr Botnet-Quellcode öffentlich. Dadurch können Nachahmer ihre eigenen Botnets erstellen und diese so raffiniert weiterentwickeln, wie es die ursprünglichen Programmierer nie für möglich gehalten hätten.

So führte das Bekanntwerden des Zeus-Codes vor ein paar Jahren zur Entwicklung der Variante Gameover. Diese nutzt zur Kommunikation im Gegensatz zum ursprünglichen Zeus nicht mehr einen zentralen "Command-and-Control"-Server (C&C), sondern ein weitflächiges Peer-to-Peer-Netzwerk aus infizierten Geräten. Gameover integrierte Backup-Mechanismen zur Kommunikation, setzte vermehrt auf Verschlüsselung und bot mehr Möglichkeiten, das Botnet flexibel für unterschiedliche Zwecke einzusetzen, z. B. für DDoS-Angriffe.[1]

Botnets sind resistenter geworden

Botnets verfügen mittlerweile über verschiedene Backup-Mechanismen zur Kommunikation und Steuerung. Kann sich ein infizierter Client wie Gameover beispielsweise nicht mit Adressen anderer infizierter Computer im Netzwerk verbinden, nutzt er einfach integrierte Algorithmen zur Generierung von Domänen. Wenn diese Algorithmen auch nur einen der neu eingerichteten C&C-Server entdecken, kann der Client seine aktive Rolle im Botnet wiederherstellen.[2]

Außerdem reagieren die Botnet-Betreiber zunehmend schneller und effektiver auf Gegenmaßnahmen. So hatte ein Antivirus-Unternehmen die Kontrolle über einen Teil des Botnets ZeroAccess erlangt und den Traffic von 500.000 infizierten Clients auf einen eigenen Server umgeleitet (bekannt als Sinkholing).[3] Im Gegenzug steigerten die Besitzer des Botnets mit Hilfe verbundener Netzwerke im Nu die Anzahl neuer Viren-Dropper, die sie auf den Clients platzierten. Innerhalb weniger Wochen hatten sie die verloren gegangenen Clients ersetzt. Diese waren nun außerdem immun gegen diese Maßnahme.

Weitere Informationen

Video-Demo zu Cryptolocker (englisch)

Botnets verbreiten immer tückischere Ransomware

Da Internet-Nutzer falsche Warnmeldungen und Antivirus-Scams immer häufiger erkennen, konzentrieren sich Botnets nun verstärkt auf Ransomware. Bei dieser Art Malware erhalten die Benutzer Forderungen, enorme Geldsummen zu zahlen, um wieder auf ihre eigenen Daten zugreifen zu können.

Das vermutlich gefährlichste und bekannteste Beispiel ist Cryptolocker. Diese Ransomware fügt sich selbst der Liste von Windows-Programmen hinzu, die beim Start ausgeführt werden. Sie macht einen infizierten Server ausfindig, lädt eine kleine ID-Datei von Ihrem Computer, kontaktiert den Server, der einen öffentlichen Schlüssel generiert (und einen entsprechenden privaten Schlüssel speichert) und verschlüsselt schließlich alle Daten- und Bilddateien auf dem Rechner.

Sobald die Daten verschlüsselt wurden, können Sie diese nur mit dem privaten Schlüssel wieder entsperren, der bei den Kriminellen gespeichert ist. Um den Schlüssel zu erhalten, müssen Sie eine Zahlung leisten (wovon wir abraten).[4]

Cryptolocker wird manchmal durch Spam-Mails verbreitet, weit häufiger jedoch durch Botnets, die bereits einen PC infiziert haben. Die Bots reagieren dabei einfach auf einen Upgrade-Befehl, der es den Kriminellen ermöglicht, die Malware zu bearbeiten, die sie bereits auf dem PC platziert haben. Sie können diese aktualisieren, austauschen oder ihr etwas hinzufügen. Der Nutzer bemerkt in der Regel erst etwas, wenn es bereits zu spät ist.[5]

Immer mehr Botnets mit Banking-Malware

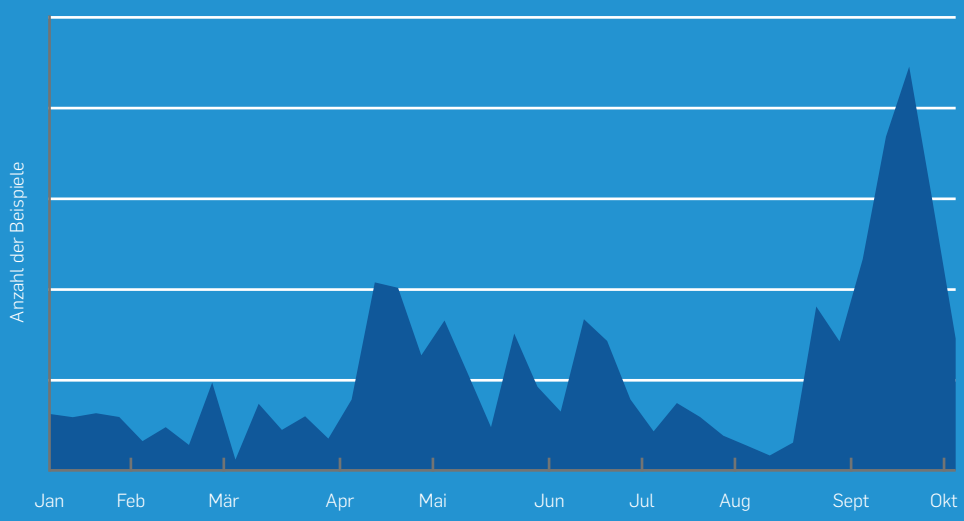
Der Quellcode von Carberp, einem Botnet-Kit, das es auf Banken abgesehen hat, wurde Mitte 2013 im Netz veröffentlicht. Carberp stiehlt Anmeldedaten und wurde von Kriminellen genutzt, um insgesamt mehr als 200 Millionen Euro von Finanzinstituten und deren Kunden zu erbeuten.[6] Während der Trojaner lange Zeit vor allem in Russland aktiv war, taucht er mittlerweile weltweit auf, und Teile der veröffentlichten Software findet man nun auch in anderen Botnets. Dazu zählt ein auf Power Loader basierender Code – ein Code, der einige der ausgefeiltesten Techniken umfasst, die bisher entwickelt wurden, um die Erkennung durch IT-Sicherheitsprogramme zu vermeiden, während Malware auf einem Computer platziert wird.[7]

Zeitgleich haben viele Benutzer in Europa Begegnung mit Shylock/Caphaw gemacht, einer durch ein Botnet verbreiteten Banking-Malware, die besonders Kunden weltweiter, großer Banken im Visier hat, unter anderem Kunden von Barclays, der Bank of America, Capital One, der Citi Private Bank und Wells Fargo.[8]

ZeroAccess-Trend 2013: Durch Sinkholing zunächst eingedämmt, dann jedoch mehr Infektionen als je zuvor

Dank Sinkholing-Maßnahmen von Antivirus-Unternehmen gab es im Juli und August 2013 wesentlich weniger Endpoints, auf denen Sophos eine ZeroAccess-Infektion feststellte. Doch die Eigentümer von ZeroAccess gingen energisch in die Offensive, und im September entdeckten wir mehr infizierte Endpoints als je zuvor.

Quelle: SophosLabs



Botnets lassen sich schwerer außer Gefecht setzen

Bei einigen Botnets ist die erste C&C-Check-in-Adresse, die ein infizierter Client zu kontaktieren versucht, nicht Teil eines Botnets, sondern eine seriöse (aber manipulierte) Domäne, die nicht so einfach gesperrt werden kann.

Mittlerweile ist der erste Check-in eines Botnet-Clients häufig ein PPP-Server (eine Art Remote Access Server) im Proxy-Modus, der die Verbindung wiederum weiterleitet. Nimmt man den ersten Server vom Netz, hat man dadurch lediglich einen Proxy deaktiviert. Die eigentliche Kommandozentrale des Botnets macht man damit jedoch nicht unschädlich.

Botnets verlassen sich zunehmend auf das „Darknet“

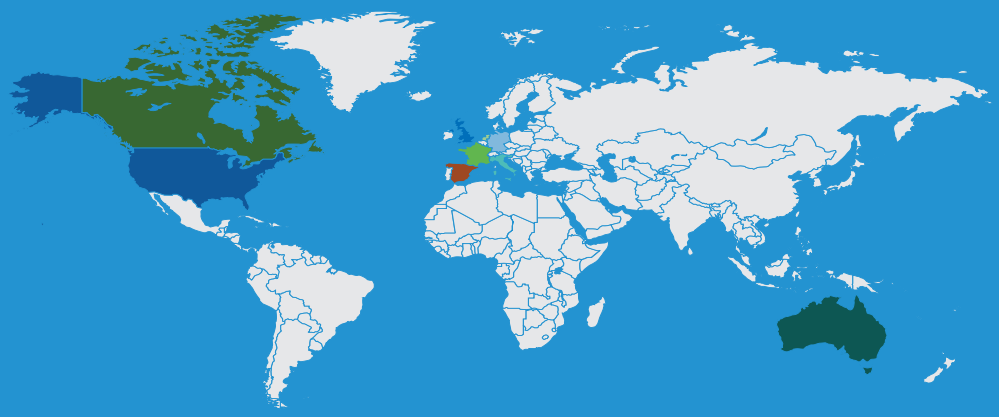
Botnets nutzen immer häufiger versteckte Netzwerke wie Tor, die Verbindungsdaten anonymisieren und entwickelt wurden, um sich der Kontrolle im Netz zu entziehen.[9] Tor wurde vor allem bekannt als wichtiges Instrument von Wikileaks und anderen Gruppierungen, die ihre Quellen schützen wollen. Ebenfalls ein Thema war Tor als Host des Online-Schwarzmarkts Silk Road.

Botnets können C&C-Server als verdeckte Dienste im Tor-Netzwerk speichern, sodass es extrem schwierig ist, sie aufzuspüren. Viele Unternehmen verbieten ihren Mitarbeitern deshalb, Tor zu verwenden, und setzen auf eine Application-Control-Technologie, um die Browser-Client-Software von Tor zu blockieren.

ZeroAccess-Infektionen nach Ländern

Im Zeitraum bis Oktober 2013 waren Tausende Endpoints in den USA und Großbritannien mit ZeroAccess infiziert. Auch in Deutschland, Australien und Italien fanden sich zahlreiche Infektionen.

Infizierte Endpoints	
Vereinigte Staaten	6.754
Großbritannien	1.625
Deutschland	747
Australien	622
Italien	458
Kanada	360
Frankreich	340
Niederlande	170
Spanien	110
Sonstige	1.014



Quelle: SophosLabs

Bitcoin-Mining per Botnet: eine neue Einnahmequelle für Malware

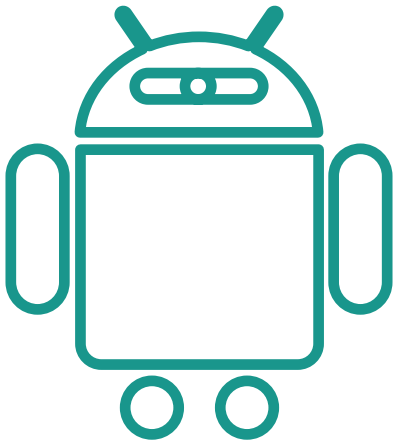
Botnet-Betreiber sind ständig auf der Suche nach neuen Einnahmequellen. Mit Bitcoin-Mining wurden 2013 große Gewinne erzielt. Bitcoins sind eine rein digitale Währung, die keiner Kontrolle durch eine Regierung unterliegt. Der Wert eines Bitcoin ist in der Vergangenheit stark geschwankt, in den letzten Monaten bewegte er sich allerdings meist zwischen 150 und 200 US-Dollar.[10]

Neue Bitcoins werden erstellt, indem komplexe mathematische Probleme gelöst werden, die eine enorm starke Computer-Rechenleistung erfordern – die Art von Leistung, die sich große globale Botnets zunutze machen können.

Von Mai 2012 bis Februar 2013 und weitere drei Wochen im April 2013 wurden infizierte Clients auf dem ZeroAccess-Botnet „versklavt“, um neue Bitcoins zu fördern.[11]

Obwohl der Wert der Bitcoins in diesem Zeitraum stark anstieg, deaktivierte ZeroAccess letztlich diese Funktion. Warum? Das wissen wir nicht so genau. Möglicherweise erregte das System zu viel Aufmerksamkeit. Oder die Kriminellen machten damit nicht so viel Gewinn wie durch Klickbetrug. Einige Beobachter sehen den Grund darin, dass neuere, speziell für Bitcoin-Mining entwickelte Hardware dabei wesentlich erfolgreicher ist als Botnets.[12]

Während ZeroAccess also kein Bitcoin-Mining mehr betreibt, haben andere Botnet-Besitzer diesen Traum noch nicht aufgegeben. So entdeckte der Sicherheitsexperte Brian Krebs beispielsweise im Mai 2013 verstärkte Bitcoin-Mining-Aktivitäten des russischen Botnets FeodalCash.[13]



Android-Malware: Neue Formen, mehr Raffinesse

Android-Malware entwickelt sich ständig weiter und schlägt dabei Wege ein, die wir bereits von Windows-Malware kennen. Doch auch bei der Sicherung der Plattform gibt es Fortschritte.

Seit der ersten Entdeckung von Android-Malware im August 2010 haben die SophosLabs über 300 Malware-Familien verzeichnet. Außerdem ist am Ökoystem der Android-Malware deutlich zu erkennen, dass dieses viele Wege einschlägt, die vor Jahren von Windows-Malware beschritten wurden.

Schwierig zu entdecken und zu entfernen

Android-Malware hat in der letzten Zeit viele neue Methoden entwickelt, mit denen sie aktiv verhindert, dass sie erkannt wird. Ein gutes Beispiel hierfür ist Ginmaster. Dieses mit einem Trojaner versehene Programm, das erstmals im August 2011 in China auftauchte, wird in viele seriöse Apps injiziert, die auch über Drittanbieter verteilt werden.

Ab 2012 konnte Ginmaster mit verschiedenen Methoden erfolgreich verhindern, erkannt zu werden: durch die Verschleierung von Klassennamen, die Verschlüsselung von URLs und C&C-Anweisungen sowie die allmähliche Nutzung der Polymorphismus-Verfahren, die bei Windows-Malware mittlerweile zum Standard gehören. 2013 implementierten die Entwickler von Ginmaster dann eine Verschleierung und Verschlüsselung, die noch weitaus komplexer und raffinierter ist. Dadurch wurde es wesentlich schwieriger, die Malware aufzuspüren oder ein Reverse Engineering vorzunehmen.[14] Gleichzeitig ist die Zahl der erkannten Ginmaster-Infektionen seit Anfang 2012 kontinuierlich jedes Quartal gestiegen – auf über 4.700 zwischen Februar und April 2013.

Neue Android-Botnets

Jüngst tauchten Berichte über ein groß angelegtes Botnet auf, das die Kontrolle über Android-Geräte übernimmt und dabei ganz ähnlich vorgeht wie Botnets auf PCs. Dieses Botnet, das Sophos als Andr/GGSmart-A identifiziert, scheint sich bisher nur auf China zu beschränken. Es verwendet einen zentralen C&C, um Anweisungen an alle infizierten Geräte zu schicken, z. B. die Anweisung, kostenpflichtige SMS-Nachrichten zu senden, die dem Besitzer des Geräts in Rechnung gestellt werden. Im Gegensatz zu typischen Android-Angriffen kann dieses Botnet Elemente steuern und ändern – darunter kostenpflichtige SMS-Nummern, Inhalte und sogar Affiliate-Systeme innerhalb seines gesamten weitflächigen Netzwerks. Dadurch ist Andr/GGSmart-A besser organisiert und potenziell gefährlicher als die meiste Android-Malware, die wir bisher kennen.[15]

Ransomware jetzt auch unter Android

Ransomware ist keine neue Entwicklung – die ersten Versionen gab es bereits vor 25 Jahren. Im Juni 2013 entdeckte Sophos Experte Rowland Yu den ersten Ransomware-Angriff auf Android-Geräte. Diese hybride Fake-Antivirus-/Ransomware-App namens Android Defender verlangt eine Zahlung von 99,99 $, um den Zugriff auf das gekaperte Android-Gerät wiederherzustellen.

Android Defender nutzt verschiedene Social-Engineering-Tricks, tarnt sich durch ein ausgesprochen seriös wirkendes Erscheinungsbild, und startet mehrfach Versuche, die Administratorrechte für das Gerät zu erhalten. Erhält die App diese Rechte, kann sie den Zugriff auf alle anderen Anwendungen einschränken, sodass es unmöglich ist, Anrufe zu tätigen, Einstellungen zu ändern, Tasks zu beenden, Apps zu deinstallieren oder das Gerät auf Werkseinstellungen zurückzusetzen. Auf dem Bildschirm erscheint eine Warnmeldung zur Infektion, egal, was der Benutzer tut. Android Defender kann sogar die Schaltflächen „Zurück" und „Home" deaktivieren und bei einem Reboot erneut starten, um so der Entfernung vom System zu entgehen. Das einzige, was die Malware momentan noch nicht macht, ist die Verschlüsselung von Daten.[16] Ehrlich gesagt würde es uns jedoch sehr überraschen, wenn wir in unserem Threat Report 2015 nicht über Verschlüsselungsangriffe von Android Defender berichten.

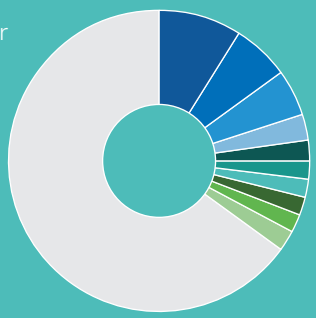
Plünderung des Bankkontos über Smartphones

Im September 2013 haben wir eine neue Form von Banking-Malware entdeckt, die konventionelle Man-in-the-Browser-Angriffe gegen Windows mit Social Engineering kombiniert, um Android-Geräte zu infizieren und den Diebstahl über das Smartphone durchzuführen. Manchmal auch Qadars genannt, haben wir sie als Andr/Spy-ABN identifiziert. Momentan ist diese Malware noch relativ inaktiv, aber es gab bereits Angriffe auf französische, niederländische und indische Finanzinstitute.

Die am häufigsten erkannte Android-Malware im Oktober 2013

Momentan lässt sich keine einzelne Android-Malware-Familie erkennen, die dominant ist. Die heutzutage am häufigsten erkannte Malware ist Andr/BBridge-A. Dieser Trojaner verwendet eine Rechteausweitung zur Installation weiterer schädlicher Apps auf Ihrem Gerät. Andr/BBridge-A hat Hartnäckigkeit bewiesen: Auf unserer Liste der Android-Infektionen belegte diese Malware bereits im Juni 2012 den zweiten Platz.[17]

Andr/BBridge-A	9 %	Andr/Adop-A	2 %	Andr/SmsSend-BE	2 %
Andr/Fakeins-V	6 %	Andr/Boxer-D	2 %	Andr/MTK-B	2 %
Andr/Generic-S	5 %	Andr/SmsSend-BY	2 %	Sonstige	65 %
Andr/Qdplugin-A	3 %	Andr/DroidRt-A	2 %		



Hinweis: Die Prozentangaben wurden auf die nächsten ganzen Prozent gerundet
Quelle: SophosLabs

Weitere Informationen
Mobile Geräte im Sicherheitsvergleich

Kostenloses Tool
Sophos Mobile Security für Android

Wie der Vorgänger Zeus startet Andr/Spy-ABN die Angriffe über Windows. Die Malware schleust ihren Code in den Internet Explorer, um Benutzerinformationen abzufangen, bevor diese verschlüsselt und an Finanzinstitute weitergeleitet werden. Außerdem erfasst sie persönliche Zertifikate und Cookies des Browsers.

Nach der Authentifizierung wird den Benutzern dann mitgeteilt, dass ihre Bank eine neue Smartphone-App hat, die ab sofort genutzt werden muss. Die Begründung dafür ist mehr als ironisch: Die neue App solle die Benutzer vor Betrug schützen. Der Benutzer wird nach seiner Telefonnummer sowie dem Gerätemodell gefragt und erhält eine SMS mit einem Link zum Download der schädlichen App. Als ob dies nicht schon schlimm genug wäre, verhindert der installierte Code auch noch, dass die Benutzer auf ihre Konten zugreifen können, bis die Malware installiert ist und ein Aktivierungscode bereitgestellt wird.[18]

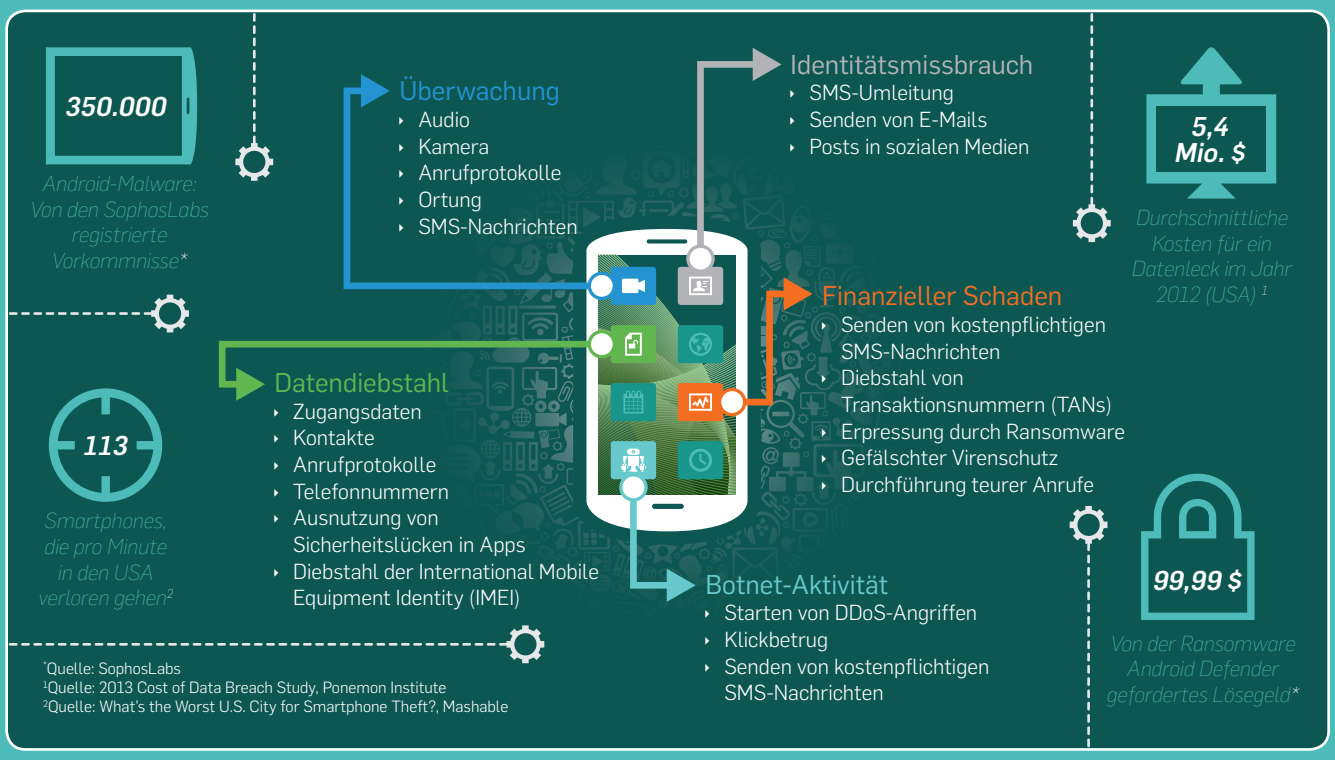
Android sichern

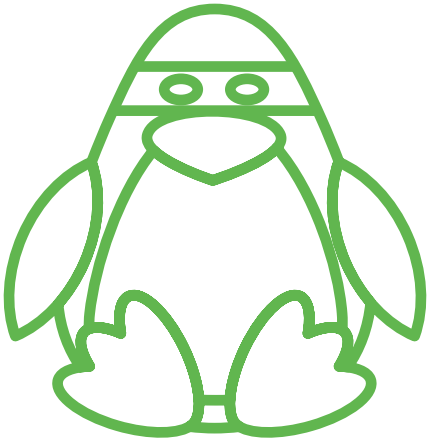
Erfreulicherweise hat Google in den letzten Monaten einige wichtige Maßnahmen ergriffen, um die Android-Plattform sicherer zu machen. Zum einen gibt es in Android 4.3 keine automatischen App-Downloads mehr, wie sie in älteren Versionen üblich waren. Zum anderen hat Google seine Vorgaben für Entwickler verschärft, insbesondere bezüglich potenziell unerwünschter Apps (PUAs). Bei diesen Apps handelt es sich zwar nicht direkt um Malware, sie räumen sich jedoch meist einen Zugriff auf Daten und Funktionen ein, der viel weitreichender ausfällt, als es den Benutzern lieb ist.

Daher hat Google beschlossen, bestimmte Verhaltensweisen von Apps und Frameworks nicht mehr zuzulassen. So dürfen Entwickler in Zukunft keine Werbung und Links von Dritten mehr auf der Startseite platzieren, die Browser-Homepage nicht mehr ändern und den Bereich der Systemmeldungen nicht mehr für Zwecke nutzen, die keinen direkten, sinnvollen Verwendungszweck für diesen Bereich haben.[19]

Anatomie eines gehackten mobilen Geräts: Was ein Hacker alles mit Ihrem Smartphone anstellen kann

Auch wenn Sie Ihrem Android-Smartphone nichts anmerken, kann es infiziert sein und sich unter der Kontrolle von Kriminellen befinden. Diese können Sie über das Telefon überwachen, Ihre Identität missbrauchen, Ihr Gerät für gefährliche Botnet-Aktivitäten nutzen, Ihre persönlichen Daten abfangen oder Geld von Ihnen stehlen.[20]





Linux: Oft verwendet, daher interessant für Kriminelle

Die Linux-Plattform ist Ziel von Angriffen, da Linux-Server oft für die Bereitstellung von Webseiten und Webinhalten verwendet werden.

Zwar ist die Anzahl der Angriffe auf Linux verschwindend gering im Vergleich zu Angriffen auf Windows oder Android, Angriffe auf Linux durch Malware-Programme und Skripte lassen sich jedoch stetig beobachten. Außerdem verzeichnen wir zahlreiche Fälle, in denen Dienste angegriffen werden, die im Grunde plattformunabhängig sind, aber häufig auf Linux-Servern ausgeführt werden.

Linux-basierte Webserver sind aus mehreren Gründen ein lohnendes Ziel für Kriminelle geworden, die den Datenverkehr an ihre kriminellen Kits umleiten möchten. Erstens ist Linux das Betriebssystem, auf dem ein großer Prozentsatz aller Webserver des Internets ausgeführt wird. Dazu zählen auch viele der weltweit bedeutendsten Webseiten mit dem höchsten Zugriffsvolumen und permanenter Erreichbarkeit. Zweitens wird gemeinhin angenommen, Linux-Server seien sicherer als andere Betriebssysteme, sodass sie manchmal als mögliches Ziel für Infektionen einfach übersehen werden. So kann ein Linux-Server unter Umständen über Monate oder Jahre hinweg unbemerkt infiziert sein und kriminellen Vereinigungen einen hohen finanziellen Nutzen bringen.

Als Ergebnis zeigt unsere Untersuchung, dass die überwiegende Mehrheit der infizierten Server, die Datenverkehr auf die Landing Pages krimineller Kits senden, Linux-Server sind. Daher sollten Malware-Infektionen von Linux-Administratoren als Bedrohung ernst genommen werden, auch wenn das Malware-Aufkommen für Linux vergleichsweise gering ist.

Zurzeit identifizieren wir jeden Monat zehntausende Fälle, in denen verdächtiger PHP-Code (eine serverseitige Skriptsprache, die häufig für Webseiten verwendet wird) auf Linux-Servern ausgeführt wird. Und das, obwohl die Malware-Autoren sich größte Mühe geben, ihre PHP-Skripte zu verschleiern und so eine Erkennung zu verhindern. Häufig verschleiern sie ihre Skripte mehr als 50 Mal hintereinander, um sicherzugehen.

Weitere Informationen

Naked Security: Linux (englisch)

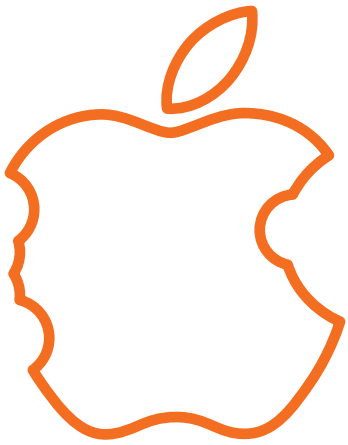
Außerdem sind zahlreiche schädliche PHP-Skripte im Umlauf, die Linux anvisieren: Ihr Ziel ist der Missbrauch von Linux-Servern als Knoten in einem größeren Traffic Distribution System, das viele Eigenschaften eines traditionellen Botnets besitzt. Dadurch kann das System andere gefährliche Payloads ausführen, z. B. DDoS-Angriffe. (Angriffe auf Webserver, z. B. Darkleech und Redkit werden auf Seite 16 noch genauer besprochen.)

Manipulierte PHP-Skripte werden häufig auf anfälligen Plattformen ausgeführt, beispielsweise auf unzureichend gepatchten Versionen von WordPress.[21] So entdeckte man 2013 einen Exploit in der PHP-Engine, auf der das CMS-System Plesk ausgeführt wurde. Über einen bestimmten Post Command war es Kriminellen theoretisch möglich, Zugriff auf diese Engine zu erhalten und auf ihr jedes beliebige PHP-Skript auszuführen.[22]

Fügen Administratoren mehr Skripte und Services von Dritten hinzu, vergrößern sie dadurch natürlich die Angriffsfläche ihrer Linux-Systeme. Umso wichtiger ist es deshalb, Patches sofort einzuspielen und mit einem umfassenden, mehrschichtigen Ansatz für eine Härtung sowohl des Linux-Betriebssystems als auch der Dienste darauf zu sorgen.

Linux-Dateiserver hosten häufig Malware, die auf Windows und andere Betriebssysteme ausgerichtet ist. So kann ein Linux-Server, auch wenn er selbst vielleicht nicht infiziert ist, trotzdem andere Geräte infizieren, die Dateien von ihm erhalten.

2013 fanden wir erstmals auch eine Vielzahl von Android-Malware auf Linux-Systemen. Ist ein Linux-Server, Scripting-Host oder Webserver mit Malware infiziert, ist es für diese Malware technisch gesehen kein Problem, HTTP-Anfragen von Android-Geräten zu erkennen und die Android-Malware entsprechend zu verbreiten. Daher sollten Linux-Systeme, die Services für Windows oder andere Clients bereitstellen, unbedingt eine Anti-Malware-Software nutzen.



Mac OS X: Ein Jahr vieler kleiner Angriffe

2013 gab es zwar keine groß angelegten Angriffe auf Mac OS X, wir beobachteten jedoch kontinuierlich kleinere, sehr kreative Angriffe, die zeigen, dass Mac-User auf der Hut sein sollten.

Angriffe auf die Mac-OS-X-Plattform entwickelten sich 2013 stetig weiter. Allerdings gab es keine großen, globalen Angriffe, die vergleichbar wären mit dem Trojaner Flashback im Jahr 2012. Unter den beobachteten Angriffen auf Mac-Computer waren Trojaner, Angriffe auf Schwachstellen in der Java-Plattform und in Microsoft-Word-Dokumenten, aggressive Browser-Plugins, schädliche Java- und Python-Skripte sowie Malware, die mit einer Apple Developer-ID signiert ist, um den Gatekeeper-Schutz von Apple zu umgehen und Benutzern vorzutäuschen, es handele sich um eine seriöse Software.

Im Februar 2013 beispielsweise berichtete Reuters, dass die Macs der Apple-Mitarbeiter von Hackern über eine weitere Zero-Day-Java-Schwachstelle angegriffen wurden. Es handelte sich dabei um dieselbe Schwachstelle, der auch Facebook eine Woche zuvor zum Opfer gefallen war[23] und die kurz darauf die Mac-Geschäftssparte von Microsoft angriff.[24] Dieser über eine Seite für Software-Entwickler verbreitete "Watering Hole"-Angriff zeigt möglicherweise eine Erkenntnis der Hacker: Manchmal ist es einfacher, Unternehmen über kleinere Seiten anzugreifen, die von ihren Mitarbeitern besucht werden, als direkt über die gut geschützte Infrastruktur des Unternehmens.

Mac-Trojaner

Letztes Jahr identifizierten AlienVault und Sophos Backdoor-Trojaner, die Macintosh-Computer in Asien über Word-Dokumente infizierten. Die Trojaner waren in Dokumente eingebettet, die vorgaben, Menschenrechtsverletzungen in Tibet zu thematisieren. Dies löste Spekulationen darüber aus, ob der Angriff möglicherweise aus Quellen stammte, die der chinesischen Regierung nahestehen.[25]

Im Februar waren ähnliche Angriffe in Dokumenten versteckt, die über vermeintliche Menschenrechtsverstöße gegen die Uiguren in Ost-Turkestan berichteten. All diese Angriffe nutzten eine Schwachstelle von Word 2004/2008, für die Microsoft seit langem Patches bereitgestellt hat (MS09-027).[26] Falls Sie also mit diesen Word-Versionen arbeiten und die Sicherheitspatches nicht installiert haben, sollten Sie dies umgehend nachholen.

Doch es gab noch weitere, ähnlich zielgerichtete Angriffe. Im September 2013 tauchte OSX/Bckdr-RQV auf, ein neuer Backdoor-Angriff, der nach der Installation verschiedene Informationen des infizierten Systems weiterleitet. Laut Intego versuchen einige Versionen, ein Bild der Syrian Electronic Army herunterzuladen, einer Gruppe von Hackern, der man nachsagt, einen Cyberkrieg zugunsten des syrischen Regimes Bashar al-Assads zu führen.[27]

Kostenloses Tool
Sophos Antivirus für Mac

Angriffe unter Ausnutzung der Apple Developer ID

Bei den neuesten Versionen von OS X erlaubt das Gatekeeper-Tool von Apple standardmäßig die Installation von OS-X-Software, die aus dem Apple Store stammt oder mit einer aktiven Apple Developer ID versehen ist. Aber wie sieht es aus, wenn Malware mit einer Developer ID signiert ist? Das war zwischen Dezember 2012 und Februar 2013 der Fall, als schädliche E-Mails Weihnachtskarten-Apps verschickten, die mit der Signatur des Apple-Entwicklers Rajinder Kumar versehen waren. Bevor Apple die ID von Kumar widerrufen konnte, hatten bereits einige Benutzer den Spear Phishing-Payload OSX/HackBack-A ausgeführt: eine Malware, die komprimierte Versionen der Dokumentdateien der Nutzer auf einen Remote-Server hochlud.[28]

Die Weihnachtskarten-App war nicht die einzige Mac-Malware mit der Signatur eines Apple Developers: Im Sommer 2013 nutzte der Python-basierte Trojaner Janicab den gleichen Trick.[29] Möglicherweise gibt es weitere Angriffe, die auf aktiven Apple Developer IDs basieren, aber nicht gemeldet wurden. Und selbst wenn nicht, ist es sehr wahrscheinlich, dass noch mehr derartige Angriffe kommen werden.

Adware und Ransomware

Wie bei Android entdeckten wir 2013 auch bei OS X mehr aggressive Browser-Adware-Plugins – Software, bei der es fraglich ist, ob sie nur als potenziell unerwünschte App oder als echte Malware einzustufen ist. Diese Adware-Plugins verwenden oft ein aggressives Installationsprogramm (das sogar Benutzereinstellungen ignorieren kann), tarnen sich als Video-Codecs, die der Benutzer vielleicht benötigt (OSX/FkCodec-A),[30] oder nutzen andere Tricks, um den Benutzer zur Installation zu bringen.

Auch eine arglistige Ransomware nahm 2013 Apples Browser Safari ins Visier. Wie bei Ransomware meist üblich, gibt sich auch diese als eine von der Justiz gesendete Nachricht aus, die behauptet, der Benutzer sei beim Anzeigen oder Abrufen von illegalen Inhalten erwischt worden, und verlangt die sofortige Zahlung einer Strafe. Anders als die tückischste Ransomware im Jahr 2013 (Cryptolocker; befällt nur Windows) verschlüsselt diese Mac-Malware die Dateien auf dem Computer nicht, sondern führt JavaScript-Code aus, der Browser-Inhalte und -eingaben erfasst und selbst nach einem Neustart des Browsers nicht verschwindet. Glücklicherweise lässt sich dieses JavaScript laut Malwarebytes ganz einfach und ohne schädliche Folgen entfernen, indem man im Menü des Browsers „Safari zurücksetzen“ wählt. [31]

Zu guter Letzt bergen Mac-OS-X-Server (und manchmal auch Clients) eine ähnliche Gefahr wie Linux-Server: Sie hosten häufig Windows-Malware, die so lange inaktiv ist, bis sie auf ein Windows-System übertragen wird. Außerdem führen viele Nutzer Windows auf virtuellen Maschinen innerhalb OS X aus, z. B. mit der Software Parallels Desktop. Diese virtuellen Windows-Maschinen sind genauso anfällig für Malware wie jedes andere Windows-System. Mac-Benutzer, die nur gelegentlich mit Windows arbeiten, schützen ihre virtuellen Windows-Maschinen unter Umständen nicht – ein Fehler, den Sie unbedingt vermeiden sollten.

4 einfache Schritte, mit denen Sie Ihren Mac schützen

Malware ist auf Macs nicht so stark verbreitet wie auf Windows oder Android. Und doch gibt es immer wieder Fälle infizierter Macs. Sie sollten daher nicht einfach hoffen, dass es Sie nicht treffen wird, sondern sich aktiv gegen mögliche Gefahren schützen. Mit ein paar einfachen Schritten können Sie das Risiko einer Infektion deutlich reduzieren.

Entfernen Sie Java von Ihrem Mac, wenn Sie es nicht unbedingt benötigen. Falls Sie Java nicht komplett entfernen können, schalten Sie es zumindest in Ihrem Browser aus, denn dort lauern die meisten gefährlichen Java-Bedrohungen. Neuerdings macht Apple es den Benutzern einfacher, Java zu vermeiden. OS X Lion und neuere Versionen installieren Java nicht standardmäßig. Falls Sie es dennoch installieren, wird es automatisch deaktiviert, wenn Sie es länger als fünf Wochen nicht verwenden.[32]

Sorgen Sie dafür, dass Ihre Software immer über die neuesten Sicherheitspatches verfügt. Hacker finden immer noch zahlreiche Opfer, indem sie Angriffe nutzen, die sich bereits vor Jahren hätten ausschalten lassen. Das soll nicht heißen, dass es keine neuen Schwachstellen gibt, die zu beheben sind: Das im September 2013 veröffentlichte Apple-Update OS X 10.8.5 schloss Sicherheitslücken in mehreren Bereichen des Systems, die für eine Remote Code Execution ausgenutzt werden konnten, von CoreGraphics und ImageIO bis hin zu PHP und QuickTime.[33]

Wenn Ihre OS-X-Version es erlaubt, lassen Sie bei Ihrem Mac nur die Installation von Apps aus dem Mac App Store zu. Sie können die Einschränkung gezielt dann aufheben, wenn Sie wissen, dass Sie eine seriöse App von einem sicheren Ort herunterladen. Mit dieser Vorgehensweise sorgen Sie für einen wertvollen zusätzlichen Schutz.

Nutzen Sie auf Ihrem Mac unbedingt einen Virenschutz. Wenn Sie bisher noch keinen Virenschutz für Ihren Mac haben, testen Sie die Sophos Antivirus für Mac Home Edition. Die Software steht kostenlos zum Download zur Verfügung und stoppt Malware-Bedrohungen mit derselben erstklassigen Technologie, die unsere Firmenkunden schützt. Damit sind Sie auch sicher vor Bedrohungen durch neueste webbasierte Malware.

Webbasierte Malware: Noch ausgereifter, vielseitiger und schwerer zu erkennen

Gefährliche, schwer zu erkennende Webserver-Angriffe und Exploit-Kits haben 2013 zugenommen und zu mehr Drive-By-Angriffen auf anfällige Webclients geführt.

Wie beim Thema Linux-Malware schon kurz erwähnt, konnten wir eine deutliche Zunahme von Angriffen beobachten, die in Form von schädlichen Apache-Modulen auftreten. Sind diese Module einmal auf manipulierten seriösen Webseiten installiert, starten sie Drive-By-Angriffe über Webbrowser mit bekannten Sicherheitslücken.

Darkleech greift Webserver an

Das bekannteste Beispiel im vergangenen Jahr war Darkleech. Die Malware infizierte (laut einem Bericht) bis Mai 2013 über 40.000 Domains und IP-Adressen von Webseiten, 15.000 davon allein im Mai. Sogar Webseiten wie die der Los Angeles Times oder von Seagate waren Berichten zufolge betroffen. Mit Darkleech infizierte Server waren für die Verbreitung extrem gefährlicher Malware-Varianten verantwortlich. Dazu gehörte auch die Ransomware Nymaim, die Benutzerdateien verschlüsselte und ein Lösegeld von 300 $ für die Bereitstellung des Schlüssels verlangte.[34] Unsere Nachforschungen ergaben, dass 93 % der von Darkleech infizierten Webseiten Apache ausführten.[35]

Im März 2013 waren Darkleech und verwandte Angriffe die häufigsten Bedrohungen aus dem Internet, die auf Kunden-Endpoints und Web Appliances festgestellt wurden, und machten beinah 30 % aller gefundenen Bedrohungen aus.

Einige dieser Angriffe sind außerdem so ausgeklügelt, dass sie sich nur sehr schwer kopieren lassen. So werden sie möglicherweise nur in einem von zehn Fällen ausgelöst, wodurch misstrauische Administratoren zu dem Schluss kommen, das Problem bestehe entweder gar nicht oder habe nichts mit dem lokalen System zu tun. Darkleech führte Blacklists, um sicherzustellen, dass eine schädliche Weiterleitung nur einmal an eine bestimmte IP gesendet wird. Viele Angreifer entscheiden sich auch dafür, die Weiterleitung nicht zu injizieren, wenn sie auf eine IP stoßen, die vermutlich aus der Security Community oder von einer Suchmaschine stammt.

Weitere Informationen
Die fünf Phasen eines Web-Malware-Angriffs

Angriffe auf Webserver zeigen, wie wichtig es ist, dass Sicherheits- und Hosting-Unternehmen enger zusammenarbeiten, damit komplexe und gut versteckte Angriffe wie Darkleech besser aufgespürt werden können. Schon rein technisch betrachtet sind diese Angriffe sehr schwierig zu erkennen. Wir haben bereits eng mit mehreren betroffenen Hosting-Anbietern zusammengearbeitet, um ihre Server von Infektionen zu befreien. Doch aufgrund der geringen Gewinnspanne, die Hosting-Unternehmen haben, erstellen diese bei Entdeckung eines infizierten Servers oft nur eine neue virtuelle Server-Instanz, anstatt der Infektion auf den Grund zu gehen. Da auf diese Weise weder sie selbst noch ihre Sicherheitsanbieter wissen, was eigentlich genau passiert ist, sind die neuen Instanzen oftmals direkt wieder infiziert.

Kunden sollten sich erkundigen, welche Maßnahmen ihre Host-Provider im Fall einer Infektion ergreifen, und auch fragen, was die Provider tun, um eine erneute Infektion zu vermeiden.

Zunahme von Malvertising

Bei Malvertising handelt es sich um schädliche Werbeanzeigen, die über seriöse Werbenetzwerke und -Webseiten verbreitet werden. Malvertising ist schon seit einigen Jahren in Umlauf, doch 2013 konnten wir eine starke Zunahme verzeichnen. Manche der schädlichen Anzeigen fanden sich sogar auf bekannten Seiten wie YouTube.

Aktuell tritt Malvertising häufig in Form von schädlichen Flash-Inhalten auf. Klickt ein Benutzer auf eine Flash-Werbeanzeige, kann es passieren, dass er über ActionScript-Code auf eine schädliche Webseite weitergeleitet wird. Ein gutes Beispiel hierfür ist der neue Trojaner Troj/SWFRed-D. Dieser Trojaner, der sich 2013 verstärkt in YouTube-Anzeigen fand, leitet Benutzer zum Exploit-Kit Stys um, was unter anderem die weite Verbreitung des Kits erklärt (siehe Diagramm unten).

In einigen Fällen können Flash-Benutzer sich sogar infizieren, ohne überhaupt umgeleitet zu werden, da die Flash-Werbeanzeige selbst Exploit-Code enthält, der auf Sicherheitslücken im eigenen Flash Player des Clients abzielt.

Jenseits von Blackhole: die Welt der Exploit-Kits

Im Threat Report des vorigen Jahres berichteten wir ausführlich über Blackhole, ein neuartiges, fertig zusammengestelltes Exploit-Kit , mit dem es für Malware-Autoren viel einfacher wurde, nahezu jeden gewünschten Payload bereitzustellen. Blackhole ist immer noch im Umlauf. So kam es beispielsweise bei den oben besprochenen Darkleech-Angriffen zum Einsatz. Doch Blackhole ist nicht mehr einzigartig.

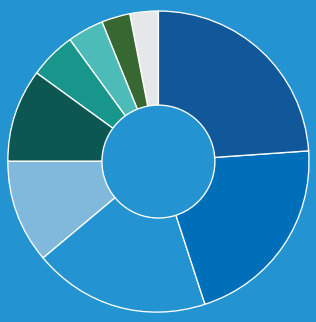
Mehreren Gruppen ist es gelungen, selbst ohne ein Reverse Engineering von Blackhole neue leistungsstarke Exploit-Kits zu erstellen, die auf den Innovationen von Blackhole aufbauen. Bei unserer letzten Studie rangierte Blackhole nur noch auf Platz 8, was die Verbreitung angeht. Und nach der Verhaftung des mutmaßlichen Hauptautors von Blackhole (Paunch) im Oktober 2013[36] wird der Einsatz von Blackhole möglicherweise noch weiter zurückgehen. Die Verhaftung zeigte deutlich die am Markt herrschenden Mechanismen: Berichten zufolge erhöhte einer der Konkurrenten, Neutrino, sofort seine Preise.[37]

Exploit-Kits: Blackhole verliert gegen effektivere Programme

2012 war Blackhole das weltweit am meisten genutzte Exploit-Kit, doch 2013 liefen ihm neuere Kits wie Neutrino und Redkit den Rang ab.

Neutrino	24 %	SweetOrange	11 %	Nuclear	4 %
Unbekanntes Kit	21 %	Styx	10 %	Blackhole/Cool	3 %
Redkit	19 %	Glazunov/Sibhost	5 %	Sonstige	3 %

Hinweis: Die Prozentangaben wurden auf das nächste ganze Prozent gerundet
Quelle: SophosLabs



Der Aufstieg von Redkit

Während Blackhole Schwachstellen in Java, Adobe PDF und Flash nutzt, konzentrieren sich viele neue Kits ausschließlich auf Java und finden dort mehr als genug Gelegenheiten. Ein führendes Beispiel ist Redkit, das seriöse Webseiten zum Ziel hat und im Februar 2013 zum Hacken der NBC-Webseite benutzt wurde.[38] Redkit tauchte auch auf in Verbindung mit Spam-Kampagnen, die auf die Bombenanschläge des Boston Marathon folgten. Bis Juli 2013 hatte Redkit Platz 1 unter allen Exploit-Kits erreicht, was die Verbreitung angeht: Es war verantwortlich für 42 % aller in diesem Monat entdeckten Exploit-Kit-Vorkommnisse.

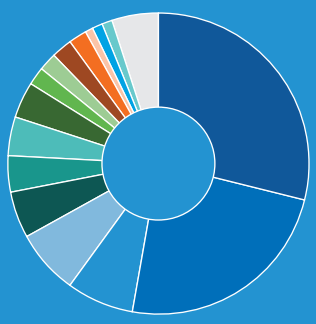
Wie konventionelle Drive-by-Downloads leitet auch Redkit die Benutzer von einer seriösen Webseite auf eine schädliche Exploit-Webseite um. Allerdings nimmt Redkit noch einen Zwischenschritt vor: Zuerst erfolgt eine Umleitung zu einem anderen seriösen, jedoch infizierten Server. Danach folgt eine zweite Umleitung. Bei dieser landet das Opfer auf einer infizierten HTM- oder HTML-Landing Page, von der es schädliche Inhalte in Form einer Java JAR-Datei (ein Dateiformat, das häufig zur Verteilung von Java-Applets verbreitet wird) erhält.

Für den betroffenen Nutzer sieht es so aus, als ob der schädliche Inhalt von dem infizierten Webserver stammt, der in der zweiten Phase der Umleitung verwendet wird. Um eine Entdeckung zu erschweren, wird der schädliche Inhalt jedoch nie dort gespeichert. Stattdessen führen die mit Redkit infizierten Webserver ein PHP-Shell-Skript aus, das sich mit einem Remote-Redkit-C&C-Server verbindet. Dieses Skript aktualisiert die Liste infizierter Webseiten stündlich, kümmert sich um die Umleitung der Opfer an die richtigen Orte und stellt sicher, dass die neuesten schädlichen Inhalte von ihrer echten Quelle aus verbreitet werden.[39]

Exploit Pack Payloads im Juni 2013: In Exploit-Kits kann alles Mögliche enthalten sein – die Übersicht zeigt, was sie tatsächlich enthalten

Das Ziel von Exploit-Kits ist der Transport verschiedenster Payloads. Seit Juni 2013 transportieren sie am häufigsten Ransomware oder das Botnet ZeroAccess.

Ransomware	29 %	Karagany	4 %	Tobfy	1 %
ZeroAccess	24 %	FakeAV	4 %	Tranwos	1 %
Fareit	7 %	Simda	2 %	Andromeda	1 %
Moure	7 %	Dofoil	2 %	Sonstige	5 %
Shylock	5 %	Medfos	2 %		
Zbot	4 %	Redyms	2 %		



Hinweis: Die Prozentangaben wurden auf das nächste ganze Prozent gerundet
Quelle: SophosLabs

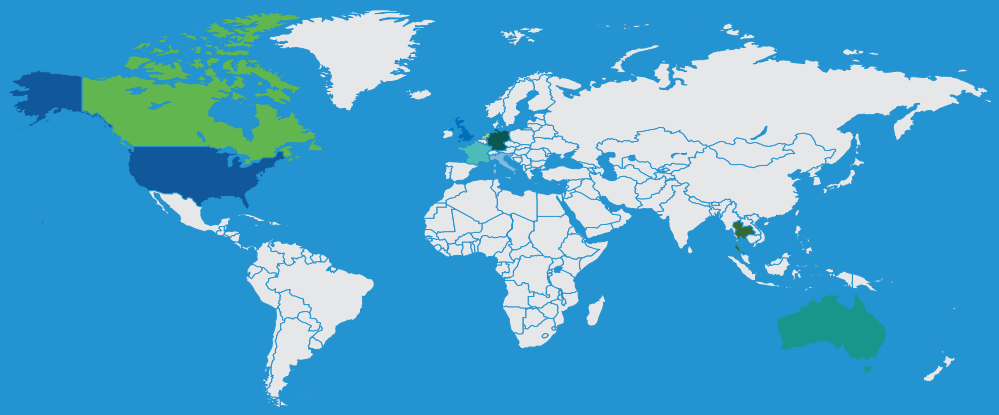
Redkit nutzt bestimmte Botnet-Attribute, um Webserver zu steuern, die mit Tausenden (oder sogar Millionen) von Benutzern interagieren. Da diese Webserver rund um die Uhr laufen und so viele Benutzer erreichen, sind sie sehr wertvoll für jeden, der vorhat, DDoS-Angriffe auszuführen oder Malware in besonders großem Umfang zu verbreiten.

Doch Redkit ist nicht das einzige neue Exploit-Kit, das Webserver zum Ziel hat. So haben wir beispielsweise das Kit Glazunov auf Hosting-Providern überall auf der Welt entdeckt. Wie das Diagramm auf Seite 15 zeigt, war Glazunov für 5,47 % aller erkannten Exploit-Kit-Vorkommnisse im dritten Quartal 2013 verantwortlich. Dieses Exploit-Kit ist berüchtigt für die Verbreitung gefährlicher Ransomware. Zwei weitere neue Exploit-Kits, Sibhost und Flimkit, sind Glazunov so ähnlich, dass sie möglicherweise aus derselben Quelle stammen.

Zbot-Verteilung weltweit

Der verbreitete Exploit-Kit-Payload Zbot breitete sich 2013 in Europa, den USA und Australien aus. 31 % der erkannten Infektionen befanden sich in den USA, weitere 23 % in Großbritannien und 12 % in Italien.

Infizierte Endpoints	
Vereinigte Staaten	2.322
Großbritannien	1.749
Italien	884
Deutschland	693
Australien	365
Frankreich	188
Thailand	156
Kanada	144
Niederlande	135
Singapur	84
Sonstige	795



Quelle: SophosLabs

So schützen Sie Webserver und Clients

Bauen Sie auf einen mehrschichtigen Schutz. Kombinieren Sie moderne Malware-Erkennung mit Web Filtering und Laufzeiterkennung/Host Intrusion Prevention.

Patchen Sie alles – und zwar möglichst schnell. Zero-Day-Angriffen wird viel Aufmerksamkeit geschenkt. Die meisten Angriffe nutzen jedoch ältere Schwachstellen, die längst behoben sein könnten, wenn die Nutzer Patches installieren würden.

Nutzen Sie Java auf dem Client nur eingeschränkt oder entfernen Sie es. 2013 konzentrierten sich die Autoren von Botnets und Exploit-Kits oft nicht mehr auf Flash und PDF, sondern nahmen stattdessen Java ins Visier. In Java sehen die Malware-Autoren die größten Sicherheitslücken. Daher sollten Sie sich gut überlegen, ob Sie Java auf Ihren Clients wirklich benötigen.

Reduzieren Sie die Angriffsfläche, indem Sie unnötige Website-Plugins vermeiden oder entfernen, z. B. WordPress-Plugins, die Sie nicht verwenden.

Schützen Sie die Anmeldeinformationen Ihrer Website. Verwenden Sie individuelle Passwörter und vergewissern Sie sich, dass Sie alle voreingestellten Administrator-Passwörter ersetzt haben.

Gezielte Angriffe auf Bankkonten

Wir verzeichnen immer hartnäckigere und gezieltere Angriffe – viele von ihnen haben es offenbar auf Bankkonten abgesehen.

Die Zahl der Angriffe hat nicht direkt zugenommen. In den SophosLabs beobachten wir jedoch, dass die Angriffe immer hartnäckiger werden und ganz gezielt bestimmte Unternehmen oder Einrichtungen ins Visier nehmen, darunter auch solche, die man bisher nicht als interessante Ziele einstufte. Diese Angriffe scheinen es zunehmend auf Bankkonten abgesehen zu haben. Cyberkriminelle, denen es um die Erbeutung von Geld geht, interessieren sich offenbar zunehmend für Bereitstellungsmethoden, die bisher bei APT-Angriffen (Advanced Persistence Threat) eingesetzt wurden.

Wölfe im Schafspelz: Plugx, Blame und Simbot

Einige der gezielten Angriffe versuchen, sich als seriöse Anwendungen zu tarnen. Wir beobachten insbesondere gefährliche Angriffe, bei denen Zertifikate gestohlen und einwandfreie, signierte Komponenten von Windows oder Drittanbietern verwendet werden, um schädliche Komponenten zu laden. Der schädliche Code wird anschließend von einem vertrauenswürdigen Prozess ausgeführt. Wenn also eine Firewall ausgehenden Datenverkehr erkennt, hält sie diesen unter Umständen für seriös.

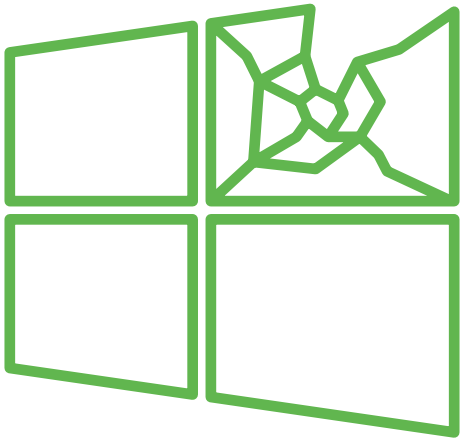
Der leitende Sophos Experte Gabor Szappanos präsentierte jüngst neueste Erkenntnisse zu diesen gezielten Angriffen. Er erklärte, dass die Angriffe für Monate oder gar Jahre unentdeckt bestehen können, da sie das System bewusst nur minimal beeinträchtigen, nahezu alles in verschlüsselter Form belassen und sich unauffällig in die Liste der seriösen Anwendungen einreihen. Diese Techniken zeigen, wohin der Weg führt: In Zukunft werden Angriffe noch schwieriger zu entdecken sein.[40]

So nutzt Plugx beispielsweise digital signierte, seriöse Anwendungen missbräuchlich für seine eigenen Zwecke. Die Malware nutzt die bekannte DLL-Load-Order-Schwachstelle von Windows aus und legt ihre schädliche Bibliothek neben der Anwendung ab. Wird die Anwendung ausgeführt, lädt sie nun die Malware-DLL aus dem aktuellen Ordner anstelle der eigentlichen DLL, die sich im Systemordner befindet.[41] Diese Schwachstelle betrifft eine Entscheidung, die Microsoft vor vielen Jahren bei der Entwicklung des Windows-Systems getroffen hatte. Würde Microsoft hier Änderungen am System vornehmen, hätte dies mit großer Wahrscheinlichkeit zur Folge, dass viele zulässige Anwendungen nicht mehr funktionieren.[42] Daher werden wir wohl noch länger mit dieser Schwachstelle zu tun haben.

Eine weitere Spezies namens Blame versteckt ihren schädlichen Inhalt tief in einer DLL, die aus verschiedenen Open-Source-Projekten kompiliert wurde. Dazu zählt der weit verbreitete LAME MP3-Encoder, der als Köder fungiert und ausreichend sauberen Code hinzufügt, um den schädlichen Code zu verbergen.

Eine dritte Spezies namens Simbot beschreibt ein neues Angriffsmodell: BYOT (Bring your own target). Simbot beinhaltet eine saubere, jedoch anfällige Anwendung, die mit einer extrem langen Befehlszeile gestartet wird. Nach dem Start kommt es zur Ausführung eines schädlichen Shellcodes, der den eigentlichen Payload entschlüsselt und lädt.

Die missbräuchliche Nutzung anfälliger Anwendungen ist zwar keine neue Taktik, doch die Art, wie Simbot vorgeht, ist außergewöhnlich: Die oben beschriebene Taktik wird auf bereits infizierten Systemen bei jedem Start angewandt, um sicherzustellen, dass nur eine saubere Anwendung ausgeführt wird und die Ausführung des schädlichen Codes ausschließlich über den Exploit erfolgt. Dadurch, dass Simbot die Anwendung gleich mitliefert, ist es nicht davon abhängig, dass die Anwendung bereits auf dem System installiert ist. Auch wenn die Schwachstelle in einer neueren Version der Anwendung behoben wurde, ist Simbot dadurch nicht aufzuhalten. Der Ansatz von Simbot hinterlässt so gut wie keine Spuren.



Windows: Das zunehmende Risiko nicht gepatchter Systeme

Ab April 2014 wird es keine neuen Patches mehr für Windows XP und Office 2003 geben. Gleichzeitig hat sich gezeigt, dass Windows-Patching ein großes Problem in spezialisierten Märkten ist, z. B. bei Kassensystemen (PoS-Systeme) oder medizinischen Geräten.

Die Aufmerksamkeit richtet sich deshalb gerade verstärkt auf Android und das Internet. Dabei wird häufig vergessen, dass mehr als eine Milliarde Computer noch mit Windows arbeiten. Das Tool von Microsoft für automatisierte Updates hält zwar viele dieser Systeme auf dem neuesten Stand, dennoch gibt es große, besorgniserregende Lücken. Drei dieser Probleme greifen wir hier heraus: Das bevorstehende Auslaufen des Microsoft-Supports für Windows XP und Office 2003, Kassensysteme, die nicht gepatcht sind oder nicht gepatcht werden können, sowie die weite Verbreitung von Malware auf ungepatchten medizinischen Geräten, die mit verschiedenen Windows-Versionen arbeiten.

Laut NetMarketShare liefen im September 2013 noch über 31 % aller PCs unter Windows XP,[43] der sehr beliebten Windows-Version, die 2001 eingeführt wurde. Microsoft hat mehrfach wiederholt, dass es den Support und die Sicherheits-Updates für Windows XP am 8. April 2014 einstellen wird.[44]

Wenn Sie ein Windows-XP-System in Betrieb haben oder für Systeme anderer Personen verantwortlich sind, auf denen noch Windows XP läuft, stellt dies ein echtes Problem dar. Denn wie Microsoft selbst anmerkt, sind einige Schwachstellen in neueren Windows-Versionen rückwärtskompatibel mit Windows XP. Das bedeutet, wenn Microsoft diese Schwachstellen in Windows Vista, Windows 7 oder Windows 8 behebt, wird dadurch die Aufmerksamkeit darauf gelenkt, dass diese Sicherheitslücken auch bei Windows XP bestehen.[45] Hier können sie jedoch nicht mehr behoben werden und öffnen daher Angreifern Tür und Tor.

Weitere Informationen

Fünf Tipps zur Eindämmung moderner Web-Bedrohungen

Das Auslaufen des Supports für XP betrifft Kassensysteme und medizinische Geräte

Mit zunehmender Sorge um ungepatchte Systeme richtet sich die Aufmerksamkeit jetzt auf andere Geräte, auf denen Windows zum Einsatz kommt, und die oft nicht regelmäßig gepatcht werden. Manche dieser Geräte laufen unter Windows XP (oder noch älteren Windows-Versionen wie Windows 2000). Für diese Systeme werden keine Patches mehr verfügbar sein, auch nicht in Unternehmen oder sonstigen Einrichtungen, die regelmäßige Patching-Prozesse eingeführt haben. Andere Geräte wiederum laufen mit neueren Windows-Versionen, für die es zwar weiterhin Patches gibt, deren Eigentümer oder Hersteller sich aber nicht aktiv um das Einspielen von Patches kümmern.

Kassensysteme laufen häufig unter Windows und führen Finanztransaktionen durch, u.a. mit Kreditkarten. Trotz branchenüblicher Standards, nach denen Sicherheitspatches schnell zu installieren sind, werden einige dieser Systeme nicht regelmäßig aktualisiert. Dies ist insbesondere bei kleineren Einzelhändlern der Fall, die über keine umfassende IT-Abteilung verfügen.[46] Da Windows XP so beliebt und schon so lange in Betrieb ist, wird es immer noch auf vielen Kassensystemen genutzt. Einige dieser Systeme können auf neuere Windows-Versionen aktualisiert werden. Laut Walter Conway, einem führenden Berater der Branche, gibt es jedoch auch Systeme, deren Betrieb nur unter Windows XP getestet und zugelassen wurde.[47]

Die Risiken bestehen keineswegs nur in der Theorie. Im Dezember 2012 wurden Händler von Visa vor der gefährlichen Windows-Malware Dexter gewarnt. Ziel dieser Malware war es, Kassensysteme zu befallen, Magnetstreifendaten zu stehlen und diese an einen zentralen Command-and-Control-Server zu senden.[48]

Besorgniserregende Windows-Sicherheitsrisiken sind auch in medizinischen Geräten aufgetreten. Im Juni 2013 entdeckte die US-Bundesbehörde zur Lebens- und Arzneimittel-Überwachung weit verbreitete Schwachstellen in medizinischen Geräten, die „durch Malware infiziert oder funktionsuntüchtig“ waren. Darunter befand sich Malware, die in der Lage ist, „auf Patientendaten, Überwachungssysteme und implantierte Geräte zuzugreifen“.[49]

Ein Grund für diese Sicherheitslücke liegt darin, dass zahlreiche Hersteller, deren Geräte unter Windows und anderen PC-Plattformen laufen, nicht rechtzeitig Sicherheits-Updates und -Patches bereitgestellt haben. Genau wie bei den Kassensystemen ist auch bei den medizinischen Geräten für das versäumte Einspielen der Patches nicht Microsoft verantwortlich. Hier sind es die Hersteller der Geräte, die sicherstellen müssen, dass ihre Geräte zuverlässig mit den neuesten Fehlerbehebungen von Microsoft funktionieren. Wenn Microsoft jedoch die Sicherheitsupdates für Windows XP einstellt, stehen auch Herstellern, die ihre Prüfprozesse verbessern, keine neuen Patches mehr zur Verfügung.

Soweit die Theorie. Doch wie sieht es in der Praxis aus? Einem Bericht der MIT Technology Review Ende 2012 zufolge sind medizinische Geräte zunehmend „mit Malware gespickt“.[50] Im renommierten Beth Israel Deaconess Medical Center in Boston „laufen 664 medizinische Geräte unter älteren Windows-Betriebssystemen. Die Hersteller haben nicht vor, dies zu ändern, und erlauben dem Krankenhaus nicht, selbst Änderungen vorzunehmen, nicht einmal, um Antiviren-Software zu installieren. Daher sind [die Geräte] häufig mit Malware infiziert, und ein oder zwei Geräte müssen jede Woche vom Netz genommen und bereinigt werden.“

Und noch ein Punkt ist erwähnenswert: Windows XP ist nicht das einzige Microsoft-Produkt, für das ab dem 8. April 2014 keine Sicherheits-Updates mehr zur Verfügung stehen. Microsoft Office 2003 ist ebenfalls betroffen. Das immer noch häufig genutzte Office 2003 war die letzte Office-Version, die auf den alten Dokumentformaten von Microsoft basiert. Diese Formate gelten heutzutage selbst nach drei Service Packs immer noch als unsicher. Office 2003 läuft auch unter Vista und Windows 7. Für Sie besteht daher selbst dann Gefahr, wenn Sie mit zwar mit diesen neueren Windows-Versionen arbeiten, aber noch Office 2003 nutzen. Denn so können Sie zwar Ihr Windows zuverlässig patchen, besitzen durch die ältere Office-Version aber trotzdem Schwachstellen, die Angreifer nutzen können.

Spam erfindet sich neu

Ein weiteres Jahr voller Spam. Und auch in Zukunft wird es vermutlich nicht besser.

So lange E-Mails gesendet werden, wird wohl auch Spam in den Posteingängen landen. Einige Spam-Mails sind einfach nur lästig. Bei anderen versuchen sich die Absender an Finanzbetrügereien, auf die mittlerweile wohl die meisten Nutzer nicht mehr hereinfallen. Und dann gibt es Spam-Mails, die Links zu wirklich gefährlicher Malware enthalten.

Manche Taktiken der Spammer lassen sich scheinbar nicht ausrotten. So zum Beispiel bildbasierter Spam (Versuche, gefälschte Rolex-Uhren zu verkaufen, sind ein Dauerbrenner) und Spam, der im Zusammenhang mit aktuellen Ereignissen auftritt (z. B. nach dem Anschlag beim Boston Marathon im April 2013).

Bei anderen Formen ist ein zyklisches Auftreten zu beobachten: Sie verschwinden von der Bildfläche, treten dann aber Jahre später erneut in Erscheinung. So feierte 2013 z. B. klassischer Pump-and-Dump-Spam ein Comeback.

Die Rückkehr des Pump-and-Dump-Spams

Pump-and-Dump-Mails versprechen, dass eine Kleinaktie demnächst stark anziehen wird. Sobald einige Empfänger darauf hineinfallen, verkaufen die Absender und streichen den gesamten Gewinn ein. Vor ein paar Jahren machte Pump-and-Dump-Spam an manchen Tagen über 50 % aller Spam-Nachrichten aus, doch nach dem Durchgreifen der US-Börsenaufsichtsbehörde verschwanden diese Mails nahezu vollständig.

Anfang 2013 ließ sich jedoch wieder eine Zunahme beobachten: Pump-and-Dump machte vom 17. bis 31. Januar 1-7 % aller Spam-Mails aus, vom 16. bis 20. Februar 5-15 % und im März 5-20 %. Bis Ende Juni beruhigte sich die Situation. Doch dann stieg das Spam-Volumen sprunghaft an: Im Juli, August und September verzeichneten wir tägliche Volumen von 10-20 %. Pump-and-Dump-Spam machte dabei an manchen Tagen 50 % aller Spam-Nachrichten aus.

Weitere Informationen
Wer liest Ihre E-Mails mit?

Zwei Themen, für die sich immer genügend Interessenten finden, sind gesunde Ernährung und einfache Abnehm-Methoden. Es wundert also nicht, dass sich die zweite große Spam-Kampagne, die wir seit einiger Zeit beobachten, genau diese Themen zunutze macht. Die Spam-Nachrichten bewerben grüne Kaffeebohnen als Wundermittel zum Abnehmen. Sie versuchen, seriöse Newsletter zu fälschen, und zitieren häufig prominente TV-Ärzte, um glaubwürdiger zu wirken. Wer jedoch auf die Links in diesen Mails klickt, landet auf Webseiten, die einzig für Call-to-Action-Zwecke der Spam-Kampagne registriert sind und den Nutzer auf die Hauptseiten umleiten, auf denen die Produkte beworben werden.

Verteilte Server und Snowshoe-Spam

Spammer müssen immer fürchten, dass ihre Spambots und Server zerstört werden. Genau wie andere Malware-Entwickler setzen sie deshalb alles daran, ihre Spuren zu verwischen.

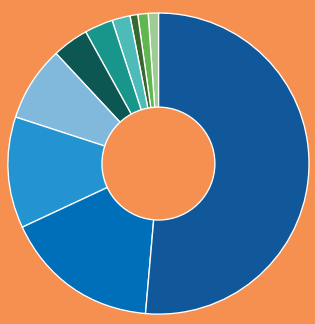
2013 konnten wir erneut viele Spammer beobachten, die das so genannte Snowshoe-Verfahren anwenden. Glücklicherweise sind unsere Spam-Filter so gut, dass sie dieses Vorgehen in der Regel erkennen und entsprechend reagieren. Der Begriff „Snowshoe-Spam“ (Schneeschuh-Spam) beschreibt die Vorgehensweise der Spammer: Sie verteilen ihr Spam-Volumen über eine größere Fläche, um nicht einzubrechen, wenden also das gleiche Prinzip an wie die Träger von Schneeschuhen.

Snowshoe-Spammer verteilen ihren Spam über viele verschiedene IP-Adressen, Websites und Sub-Netzwerke. Einige lassen unter Umständen große Mengen für eine kurze Zeit über eine einzelne IP-Adresse laufen. Danach wechseln sie zu einer anderen IP-Adresse, die sich häufig in der Nachbarschaft befindet. Mit dieser Strategie wird versucht, Erkennungsmechanismen auszutricksen, die Spam anhand des Volumens aufspüren und von großen E-Mail-Hosts verwendet werden.[51] In Unternehmen und Einrichtungen mit unzureichender Spam-Filterung macht Snowshoe-Spam oft die überwiegende Mehrheit der Junk-Mails aus, die es durch die Filter schaffen.

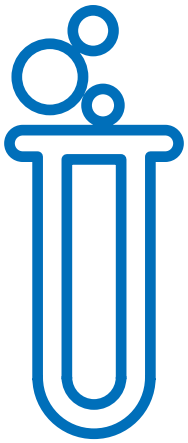
Spam-Anhänge im Juni 2013: Alles andere als harmlos

Im Juni 2013 waren die beiden Loader Fareit und Andromeda die häufigsten in Spam-Anhängen eingebetteten Malware-Formen. Fareit (auch bekannt als Pony oder Ponik) lädt oftmals P2P Zeus herunter, sammelt aber auch Passwörter, die in bestimmter Software gespeichert sind, z. B. in Mail- und FTP-Clients. Andromeda lädt weitere Malware herunter, wie P2P Zeus, Spambots und ZeroAccess, und lädt manchmal auch eigene Module herunter, um Netzlaufwerke und externe Speichermedien zu infizieren.

Fareit	52 %	Donx	4 %	DarkComet	1 %
Andromeda	17 %	Bublik	3 %	Banload	1 %
Zbot	12 %	Ransomware	2 %		
Dofoil	8 %	DnetBckdr	1 %		



Hinweis: Die Prozentangaben wurden auf das nächste ganze Prozent gerundet
Quelle: SophosLabs



SophosLabs: Raffinierten Angriffen immer einen Schritt voraus

Auf die zunehmend raffinierten, schwer zu entdeckenden Malware-Angriffe müssen Sicherheitsunternehmen mit noch schnelleren, flexibleren und klügeren Gegenmaßnahmen reagieren. Genau dies tun die SophosLabs.

Früher konzentrierten sich Anti-Malware-Unternehmen vor allem darauf, die Signaturen der Schadsoftware zu identifizieren. Dann begannen die Angreifer mit polymorphen Angriffen, die einzigartige Malware-Versionen für jeden Computer generieren, den sie infizieren. Die statische Erkennung wurde damit weit weniger effektiv.

Manche polymorphe Angriffe sind leicht zu verhindern. So kann eine E-Mail-Filterung nahezu immer Angriffe verhindern, die über E-Mail-Anhänge verbreitet werden. Heute bestehen die gefährlichsten Angriffe jedoch aus komplexen Ketten von Angriffskomponenten, die breit im Internet verstreut sind. Außerdem nutzen die Kriminellen wie bereits beschrieben raffinierte neue Techniken, um unentdeckt zu bleiben.

Als Reaktion darauf setzen wir bei Sophos in unseren Produkten auf mehrere Schutzschichten. Beispielsweise liegt einer unserer Schwerpunkte auf der Erkennung und Blockierung von Webseiten, die Exploit-Kits oder andere schädliche Inhalte hosten. Wir haben Schutzschichten entwickelt, deren Ziel es ist, bestimmte Exploit-Kit-Komponenten aufzuspüren, darunter verschleierte JavaScript-Umleitungen, manipulierte Java JARs und infizierte Dokumente. Alleine kann keine der Schichten perfekten Schutz bieten, zusammengenommen sind sie jedoch höchst effektiv.

Und wir arbeiten kontinuierlich an der Entwicklung neuer Techniken, die noch effektiver sind.

Weitere Informationen
Bedrohungsanalyse in den SophosLabs

Beispielsweise konzentrieren wir uns auf kontextbasierte Erkennungsmechanismen, die zwei Informationen miteinander kombinieren: die Dateien, die gerade heruntergeladen werden, und die Webseiten, von denen die Dateien stammen. Einzeln betrachtet ist eine Datei oder ihre Quelle unter Umständen nicht so auffällig, dass sie markiert wird. Betrachtet man jedoch Datei und Quelle zusammen, zeigen sich häufig Muster, die auf Bedrohungen hinweisen. Daraufhin reagiert unsere Software, und wir riskieren keine False Positives.

Für den seltenen Fall, dass alle Schutzschichten versagen, haben wir eine zusätzliche Abwehrschicht eingebaut: die Laufzeiterkennung. Wir halten nach Signalen Ausschau, die auf eine aktive Malware hindeuten können. Zum Beispiel beobachten wir, ob sich ein Programm anders verhält, als es seriöse Programme normalerweise tun. Diese Abfrage kombinieren wir mit vorherigen Analysen der Programmdatei. Eine Datei, die beim Herunterladen vielleicht nur ein wenig suspekt erschien, verhält sich u. U. so, dass wir argwöhnischer werden und sie direkt blockieren.

Neue Versionen unserer UTM-Lösung verwenden ähnliche Techniken zum Blockieren von Geräten, deren Verhalten auf eine Malware-Infektion hinweist. Dazu zählen Geräte, die offenbar unter der Kontrolle eines Botnets stehen. Sophos UTM 9.2 inspiziert nicht nur Netzwerkpakete und macht Endpoints ausfindig, die versuchen, illegale Domains zu erreichen. Die Lösung erkennt auch schädliche Konfigurationsdateien, die von Botnets über HTTP an infizierte Endpoints weitergeleitet werden.

Infizierte C&C-Webserver und Malware verändern sich mit rasender Geschwindigkeit. Daher gehören zum Umfang der Sophos Produkte mittlerweile auch cloudbasierte Updates, die sofort bereitgestellt werden.

Die SophosLabs verarbeiten mittlerweile unzählige Daten, die erforderlich sind, um den modernen Angreifern stets einen Schritt voraus zu sein. Täglich erfassen wir mehrere Milliarden Datenpunkte von Millionen Endpoints auf der ganzen Welt. Dank unserer hochmodernen Dateninfrastruktur können wir diese Daten schnell zu wertvollen Informationen verarbeiten. Unter anderem müssen wir große Datenmengen, die von geschützten Endpoints und Servern stammen, miteinander in Beziehung setzen, um neue Angriffe zu erkennen. Ebenfalls wichtig ist das Sammeln von Binärdateien, URLs und Telemetriedaten, damit wir unsere Schutzmechanismen weiter verbessern können.

Rein technisch betrachtet baut unsere Infrastruktur auf Hadoop auf. Diese Open-Source-Software basiert auf Ideen, die bei Google und Yahoo entwickelt wurden. Sie ist optimal für Unternehmen, die schnellstmöglich große Datenmengen analysieren müssen, also z. B. für Facebook, Twitter, eBay und eben auch für Sophos.

Trends für 2014

Von den SophosLabs

Wichtige technologische Entwicklungen sowie eine Reihe von Enthüllungen über die NSA machten 2013 zu einem interessanten Jahr für Trend-Beobachter. In unserer Zusammenfassung der Entwicklungen 2013 haben wir einige Trends herausgegriffen, die wir wahrscheinlich auch im nächsten Jahr beobachten werden.

Angriffe auf Unternehmensdaten und private Daten in der Cloud

Da Unternehmen zunehmend Cloud-Dienste nutzen, um Kundendaten, interne Projektpläne und Vermögenswerte zu verwalten, rechnen wir mit einer Zunahme von Angriffen auf Endpoints, mobile Geräte und Anmeldeinformationen. Ziel dieser Angriffe ist es, Zugriff auf die Clouds von Unternehmen oder Privatpersonen zu erhalten.

Es lässt sich schwer vorhersagen, in welcher Form zukünftige Angriffe auftreten werden. Allerdings können wir uns Ransomware vorstellen, die Sie nicht nur aus Ihren lokal gespeicherten Dokumenten aussperrt, sondern auch von allen möglichen Daten, die in der Cloud gespeichert sind. Diese Angriffe erfordern nicht unbedingt eine Datenverschlüsselung und könnten in Form von Erpressungen auftreten, d. h. als Drohungen, Ihre vertraulichen Daten zu veröffentlichen.

Strenge Richtlinien für den Einsatz von Passwörtern und für den Zugriff auf Daten in der Cloud sind wichtiger als je zuvor. Sie sind immer nur so sicher, wie es Ihre größte Schwachstelle ist. Diese Schwachstelle dürfte in vielen Fällen Ihr Windows-Endpoint und das Sicherheitsbewusstsein Ihrer Benutzer sein.

APTs treffen auf Finanz-Malware

Advanced Persistent Threats sind sehr erfolgreich beim Ausführen von Angriffen, die zur Industriespionage dienen. Wir gehen davon aus, dass dieser Erfolg andere Gruppen anspornen wird, diese Techniken ebenfalls anzuwenden. Interessant könnte dies z. B. für Gruppen sein, die bisher mit weniger ausgefeilter Finanz-Malware arbeiten. Schon jetzt beobachten wir, dass Exploit-Techniken von APT-Gruppen genutzt werden, um Malware zu verbreiten.

Da Sicherheitsanbieter immer effektivere Abwehrmechanismen entwickeln, Betriebssysteme sicherer werden und das Sicherheitsbewusstsein der Benutzer steigt, wird es für Cyberkriminelle immer schwieriger. Sie müssen höhere finanzielle Gewinne von einer kleineren Anzahl Opfer erzielen. Neue Angriffe, die von Betreibern gewöhnlicher Malware angestoßen werden, könnten künftig Komponenten und Bereitstellungsmechanismen enthalten, die noch genauer auf eine ganz spezifische Zielgruppe ausgerichtet sind. Die Grenze zwischen APT und gewöhnlicher Malware wird 2014 weiter verschwimmen.

Android-Malware: Zunehmend komplex und auf der Suche nach neuen Zielen
2013 konnten wir einen enormen Zuwachs an Android-Malware verzeichnen, nicht nur gemessen an der Zahl einzelner Familien und Versionen, sondern auch an der Zahl der weltweit betroffenen Geräte.

Zwar gehen wir davon aus, dass sich die neuen Android-Sicherheitsfunktionen mit der Zeit positiv auf die Infizierungsrate auswirken werden. Allerdings wird es eine Weile dauern, bis diese Funktionen greifen, und bis dahin bleiben die meisten Benutzer ohne Schutz gegen einfache Social-Engineering-Angriffe. Cyberkriminelle werden auch weiterhin nach neuen Methoden suchen, um mit Android-Malware Geld zu verdienen. Auch wenn Angreifer auf dieser Plattform weniger Möglichkeiten haben als auf Windows, so bieten mobile Geräte doch eine attraktive Ausgangsbasis für Angriffe, deren Ziel soziale Netzwerke und Cloud-Plattformen sind.

Dämmen Sie das Risiko ein, indem Sie eine BYOD-Richtlinie durchsetzen, die das Side-Loading mobiler Apps aus unbekannten Quellen verhindert und einen Malware-Schutz vorschreibt.

Malware wird vielfältiger und spezialisierter
Finanz-Malware stellt sich immer stärker auf Unterschiede ein, die zwischen verschiedenen geografischen und ökonomischen Regionen bestehen. Dies zeigt sich an länderspezifischen Social-Engineering-Techniken, verschiedenen Möglichkeiten, die genutzt werden, um Geld zu erbeuten, sowie an den unterschiedlichen Zielsetzungen der Angriffe. Malware, die in vielfältigen Variationen für unterschiedliche Zielgruppen auftritt, wird 2014 vermutlich weiter zunehmen, insbesondere, um zwischen privaten und geschäftlichen Nutzern zu unterscheiden. Außerdem wird es wohl Angriffe geben, die dahingehend spezialisiert werden, wie hoch die Sicherheitslevel und wie lukrativ die anvisierten Ziele sind.

Gefahr für persönliche Daten durch mobile Apps und soziale Netzwerke
Die Sicherheit mobiler Geräte wird auch 2014 ein wichtiges Thema bleiben. Da immer wieder neue Apps für die private und geschäftliche Kommunikation genutzt werden, vergrößert sich die Angriffsfläche ständig. Dies gilt insbesondere für Social-Engineering-Scams und für Versuche, Daten zu stehlen. Ihr Adressbuch und Ihre sozialen Netzwerke sind ein wahrer Schatz für Cyberkriminelle. Überlegen Sie sich deshalb gut, wem Sie Zugriff gewähren und warum. Mit Lösungen, die geschäftlichen Nutzern Schutz für mobile Geräte und Webanwendungen bieten, lässt sich das Risiko deutlich minimieren.

Neue Waffen gegen Schutzmechanismen
Im niemals endenden Kampf zwischen Cyberkriminellen und Sicherheitsanbietern werden neue Waffen zum Einsatz kommen, die auf die neuesten Mechanismen der Cyber-Verteidigung gerichtet sind. Reputationsdienste, Cloud Security-Datenbanken, Whitelisting und Sandboxing werden neuartigen, gefährlichen Angriffen ausgesetzt sein. Außerdem wird es eine Zunahme geben bei Malware mit gestohlenen digitalen Signaturen, Versuchen, Sicherheitsdaten und telemetrische Analysen zu manipulieren, neuen Techniken, um Sandboxing zu erkennen und zu umgehen, sowie bei der Nutzung seriöser Tools zu schädlichen Zwecken.

64-Bit-Malware
Wegen der zunehmenden Verbreitung von 64-Bit-Betriebssystemen auf PCs rechnen wir mit mehr Malware, die nicht auf 32-Bit-PCs ausgeführt werden kann.

Exploit-Kits weiterhin die Hauptbedrohung für Windows
Zwar hat Microsoft bei seinem Windows-Betriebssystem technologische Fortschritte gemacht, mit denen es für Exploit-Entwickler deutlich schwerer wird. Doch das Unternehmen hat den Kampf noch nicht gewonnen.

Mit dem Ende des Supports für Windows XP nach 12 Jahren wird das Betriebssystem ein lukratives Ziel für Angreifer. Wird sich Windows 7 genauso viele Jahre halten können wie XP? Wie lange wird es dauern, bis die Mehrheit aller Endpoints auf neuere Windows-Versionen mit verbesserten Sicherheitsfunktionen migriert?

Bedrohungen, die eine Interaktion der Benutzer erfordern (Social Engineering), werden weiterhin eine Hauptquelle für Infektionen sein. Doch Malware-Autoren werden ihre Techniken verfeinern müssen, um die Benutzer zur Ausführung der Payloads zu bringen, da die Anwender immer besser lernen, zwischen schädlichen und harmlosen Inhalten zu unterscheiden. Autoren von Massen-Malware stehen daher vor der Herausforderung, ihre Köder gezielter und überzeugender zu gestalten.

Angriffe auf zentrale Hardware, Software und Infrastrukturen
Die Enthüllungen im Jahr 2013 über Spionage-Angriffe und den Einsatz von Backdoors durch Regierungsbehörden (und auch durch kommerzielle Organisationen) zeigten der Welt, dass Angriffe auf die zentrale Infrastruktur, die uns alle betrifft, nicht nur möglich sind, sondern auch tatsächlich stattfinden. Wir werden neu bewerten müssen, wie sicher unsere Technologien sind und wem wir vertrauen können.

Die bekannt gewordenen Vorfälle sind jedoch nur die Spitze des Eisbergs, und wir können uns 2014 sicherlich auf viele weitere Geschichten dieser Art gefasst machen. Die meisten Unternehmen werden nicht über die Ressourcen oder das Know-how verfügen, nach Backdoors zu suchen. Doch es empfiehlt sich, die Arbeit der Sicherheitsexperten und der Medien aufmerksam zu verfolgen, was neue Enthüllungen angeht.

Vor Hackern ist nichts mehr sicher
Wir nutzen immer mehr unterschiedliche Geräte, auf denen oft auch sensible Unternehmensdaten gespeichert sind. Die Sicherheitssysteme dieser Geräte sind einfach noch nicht so gut wie die einer traditionellen PC-Umgebung.

Für diejenigen, die uns Schaden zufügen möchten, sind die eingebetteten Geräte bei uns zu Hause, in unseren Büros und sogar in Städten interessante Angriffsziele. Und da es neue elektronische Währungen und Zahlungstechniken gibt, sollten wir nicht nur unsere Kreditkarten gut im Auge behalten.

Wir erwarten zwar nicht, dass sich Angriffe gegen das „Internet der Dinge“ 2014 flächendeckend ausbreiten werden, doch wir rechnen mit mehr Berichten über Schwachstellen und mehr Proof-of-Concept-Exploits.

Abschließende Worte

Die Urheber von Malware, Exploit-Kits und Botnets sind 2013 raffinierter und aggressiver geworden. Sie haben neue Angriffsformen entwickelt, neue Wege für die Wiederverwendung älterer Ansätze entdeckt sowie neue Ziele und neue Techniken zur Verschleierung ihrer Aktivitäten gefunden.

Um uns erfolgreich gegen diese neuen Angriffsformen zur Wehr zu setzen, müssen wir ebenfalls umdenken und neue, noch effektivere Methoden anwenden. Bei Sophos arbeiten wir rund um die Uhr daran, noch bessere Erkennungsmechanismen zu entwickeln, Updates in der Cloud in Echtzeit bereitzustellen und Sie dabei zu unterstützen, eine neue Generation mobiler Geräte zu sichern – egal, ob in Ihrem Unternehmen nur bestimmte Geräte zulässig sind oder ob Ihre Mitarbeiter beliebige private Geräte mitbringen und nutzen dürfen.

Ganz gleich, ob Sie selbst im IT-Bereich arbeiten, ein Unternehmen besitzen oder als Nutzer im Internet unterwegs sind: Machen Sie sich mit dem Thema IT-Sicherheit vertraut. Stellen Sie sicher, dass all Ihre Systeme geschützt sind, egal auf welcher Plattform sie laufen. Verkleinern Sie die Angriffsfläche, indem Sie Programme entfernen, die Sie nicht wirklich benötigen (z. B. Java). Installieren Sie aktuelle Sicherheits-Patches immer sofort, denn die meisten Angriffe nutzen ältere Sicherheitslücken. Beachten Sie außerdem grundlegende Sicherheitsregeln: Verwenden Sie sichere Passwörter und geben Sie vertrauliche Informationen nicht leichtfertig im Internet preis.

IT-Sicherheit wird auch weiterhin ein großes Thema bleiben und es werden immer neue Bedrohungen lauern. Wenn Sie jedoch wachsam bleiben, bewährte Maßnahmen anwenden, neueste Sicherheitstechnologien einsetzen und die richtige Hilfe in Anspruch nehmen, können Sie sich und Ihr Unternehmen erfolgreich schützen. Mit Sophos haben Sie einen Partner an Ihrer Seite, der Ihnen zuverlässigen Rundumschutz bietet – einfach, effektiv und überall.

Quellen

1. ZeuS-P2P Monitoring and Analysis, v2013-06, NASK/CERT Polska, http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf
2. An Analysis of the Zeus Peer-to-Peer Protocol, Dennis Andriesse and Herbert Bos, VU University Amsterdam, The Netherlands, Technical Report IR-CS-74, rev. May 8, 2013, http://www.few.vu.nl/~da.andriesse/papers/zeus-tech-report-2013.pdf
3. Symantec Uses Vulnerability to Take Out Part of the ZeroAccess Botnet, CSO, http://www.csoonline.com/article/740626/symantec-uses-vulnerability-to-take-out-part-of-the-zeroaccess-botnet
4. CryptoLocker Ransomware - See How It Works, Learn about Prevention, Cleanup and Recovery, Sophos Naked Security, http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
5. Destructive Malware "CryptoLocker" on the Loose - Here's What to Do, Sophos Naked Security, 12 October 2013, http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/
6. With Carberp Source Code's Release, Security Pros Expect the Worst, CSO Online, 27 June 2013, http://www.csoonline.com/article/735569/with-carberp-source-code-s-release-security-pros-expect-the-worst
7. Carberp: The Never Ending Story, We Live Security, 25 March 2013, http://www.welivesecurity.com/2013/03/25/carberp-the-never-ending-story/
8. Shylock Financial Malware Back and Targeting Two Dozen Major Banks, ThreatPost, 18 September 2013, http://threatpost.com/shylock-financial-malware-back-and-targeting-two-dozen-major-banks
9. Cyber-thieves Blamed for Leap in Tor Dark Net Use, BBC News, 6 September 2013, http://www.bbc.co.uk/news/technology-23984814
10. Bitcoincharts.com, http://bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv
11. Back Channels and Bitcoins: ZeroAccess' Secret C&C Communications, James Wyke, Senior Threat Researcher, SophosLabs, Virus Bulletin, October 2013, http://www.sophos.com/en-us/medialibrary/PDFs/technical papers/Wyke-VB2013.pdf
12. The Delicate War Between Bitcoin Miners and Botnet Miners, Red Orbit, 28 March 2013, http://www.redorbit.com/news/technology/1112812519/bitcoin-miners-versus-botnet-miners-032813/
13. Botcoin: Bitcoin Mining by Botnet, Krebs on Security, 18 July 2013, http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/
14. GinMaster: A Case Study in Android Malware, Rowland Yu, SophosLabs Australia, Virus Bulletin, October 2013, http://www.virusbtn.com/pdf/conference_slides/2013/Yu-VB2013.pdf
15. Billion Dollar Botnets, Cathal Mullaney, Symantec, presented at Virus Bulletin, October 2013, http://www.virusbtn.com/conference/vb2013/abstracts/Mullaney.xml
16. Hey Android, Are You Frightened of FakeAV plus Ransomware? Rowland Yu, SophosLabs, October 2013
17. Revealed! The Top Five Android Malware Detected in the Wild, Graham Cluley, Sophos Naked Security, 14 June 2012, http://nakedsecurity.sophos.com/2012/06/14/top-five-android-malware/
18. Qadars: A New Banking Malware With a Fraudulent Mobile Application Component, 2 October 2013, http://www.lexsi-leblog.com/cert-en/qadars-new-banking-malware-with-fraudulent-mobile-application-component.html
19. Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html
20. Graphic inspired by The Scrap Value of a Hacked PC, Revisited, Krebs On Security, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/
21. CVE Details: WordPress Vulnerabilities, http://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/
22. Hacker Publishes Alleged Zero-Day Exploit for Plesk, Parity News, 6 June 2013, http://www.paritynews.com/2013/06/06/1112/hacker-publishes-alleged-zero-day-exploit-for-plesk/
23. Exclusive: Apple, Macs Hit by Hackers Who Targeted Facebook, Reuters, 19 February 2013, http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219
24. Microsoft Also Victim of Recent Watering Hole Attack, Help Net Security, 25 February 2013, https://www.net-security.org/secworld.php?id=14482
25. Mac Backdoor Trojan Embedded Inside Boobytrapped Word Documents, Sophos Naked Security, 30 March 2012, http://nakedsecurity.sophos.com/2012/03/30/mac-malware-backdoor/
26. Chinese Uyghur Dissidents Targeted by Mac Malware, Ben Weitzenkorn, TechNewsDaily, 15 February 2013, http://www.technewsdaily.com/16937-china-uyghur-attacks.html
27. New Mac Trojan Discovered Related to Syria, Intego, 17 September 2013, http://www.intego.com/mac-security-blog/new-mac-trojan-discovered-related-to-syria/
28. Mac Spyware: OSX/KitM (Kumar in the Mac), F-Secure, 22 May 2013, http://www.f-secure.com/weblog/archives/00002558.html
29. New Signed Malware Called Janicab, http://www.thesafemac.com/new-signed-malware-called-janicab/
30. OSX/FkCodec-A, Detailed Analysis, Sophos, 11 June 2013, https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/OSX~FkCodec-A/detailed-analysis.aspx
31. FBI Ransomware Now Targeting Apple's Mac OS X Users, Malwarebytes, 15 July 2013, http://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/
32. Apple Gets Aggressive - Latest OS X Java Security Update Rips Out Browser Support, Paul Ducklin, Sophos Naked Security, 18 October 2012, http://nakedsecurity.sophos.com/2012/10/18/apple-gets-aggressive-latest-os-x-java-security-update-rips-out-browser-support/
33. Apple Ships OS X 10.8.5 Security Update - Fixes "sudo" Bug At Last, Paul Ducklin, Sophos Naked Security, 13 September 2013, http://nakedsecurity.sophos.com/2013/09/13/apple-ships-os-x-10-8-5-security-update-fixes-sudo-bug-at-last/
34. Rampant Apache Website Attack Hits Visitors With Highly Malicious Software, Ars Technica, 3 July 2013, http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/
35. Rogue Apache Modules Pushing Iframe Injections Which Drive Traffic to Blackhole Exploit Kit, Fraser Howard, Sophos Naked Security, 5 March 2013, http://nakedsecurity.sophos.com/2013/03/05/rogue-apache-modules-iframe-blackhole-exploit-kit/
36. Blackhole Malware Toolkit Creator 'Paunch' Suspect Arrested, ZDNet, 9 October 2013, http://www.zdnet.com/blackhole-malware-toolkit-creator-paunch-arrested-7000021740/
37. Blackhole Exploit Kit Author Arrested in Russia, ComputerWorld, 8 October 2013, http://www.computerworld.com/s/article/9243061/Blackhole_exploit_kit_author_arrested_in_Russia
38. Lifting the Lid on the Redkit Exploit Kit, Fraser Howard, Sophos Naked Security, 3 May 2013, http://nakedsecurity.sophos.com/2013/05/03/lifting-the-lid-on-the-redkit-exploit-kit-part-1/
39. The Four Seasons of Glazunov: Digging Further into Sibhost and Flimkit, Fraser Howard, Sophos Naked Security, 2 July 2013, http://nakedsecurity.sophos.com/2013/07/02/the-four-seasons-of-glazunov-digging-further-into-sibhost-and-flimkit/
40. Hide and Seek - How Targeted Attacks Hide Behind Clean Applications, Gabor Szappanos, SophosLabs Hungary, October 2013, Virus Bulletin, http://www.virusbtn.com/conference/vb2013/abstracts/LM1-Szappanos.xml
41. Plugx "Malware Factory" Celebrates CVE-2012-0158 Anniversary with Version 6.0, Gabor Szappanos, Principal Researcher, SophosLabs, May 2013, http://sophosnews.files.wordpress.com/2013/05/sophosszappanosplugxmalwarefactoryversion6-rev2.pdf
42. The Windows DLL Loading Security Hole, Dr Dobbs Journal, 9 September 2010, http://www.drdobbs.com/windows/the-windows-dll-loading-security-hole/227400009
43. NetMarketShare, http://www.netmarketshare.com/
44. Windows XP SP3 and Office 2003 Support Ends April 8, 2014, Microsoft, http://www.microsoft.com/en-us/windows/endofsupport.aspx
45. The Risk of Running Windows XP After Support Ends, Tim Rains, Microsoft Security Blog, April 2014, http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx
46. Windows XP End of Life Affects PCI Compliance, Credit Card Processing Space, 6 March 2013, http://www.creditcardprocessingspace.com/windows-xp-end-of-life-affects-pci-compliance/
47. Windows XP End-of-Life Could Cripple PCI Compliance, Walter Conway, 6 February 2013, Storefront Backtalk, http://storefrontbacktalk.com/securityfraud/windows-xp-end-of-life-could-cripple-pci-compliance/
48. Dexter Malware Targeting Point-of-Sale (POS) Systems, Visa Data Security Alert, December 2012, http://usa.visa.com/download/merchants/alert-dexter-122012.pdf
49. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks, U.S. Food and Drug Administration, 13 June 2013, http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm
50. Computer Viruses Are "Rampant" on Medical Devices in Hospitals, MIT Technology Review, 17 October 2012, http://m.technologyreview.com/computing/41511/
51. Following the Tracks: Understanding Snowshoe Spam, Brett Cove, SophosLabs, http://sophosnews.files.wordpress.com/2011/10/vb2011-snowshoe2.pdf

COMPHONE UND
IT-Systemhaus - Lösungen für IT-Integration

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

Oxford, GB | Boston, USA

1091-11.13DD.de.simple

SOPHOS