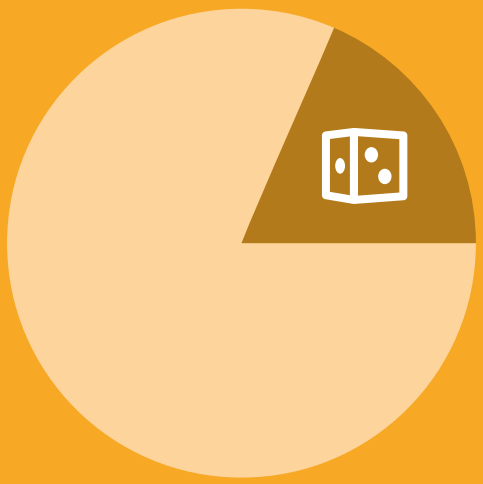
Gefahrenbericht: H2/2015

SIMPLY SECURE

G DATA PC Malware Report

Hostländer bösartiger Webseiten:
USA auf Platz 1 mit 57,2 %
Deutschland auf Platz 3 mit 3,9 %



18,7 % der bösartigen Websites fallen unter die Kategorie Glücksspiel

5.143.784

neue Signaturvarianten im Jahr 2015 (im Schnitt alle 6 Sekunden eine neue)

Inhalte

G DATA PC Malware Report

Auf einen Blick

- Im zweiten Halbjahr 2015 verzeichneten die Experten der G DATA SecurityLabs 2.098.062 neue Signaturvarianten. Die Zahl fällt damit um 31% geringer aus als in H1 2015.
- Mit 5.143.784 liegt die Gesamtzahl der neuen Signaturvarianten 2015 nur vermeintlich knapp unter dem Wert von 2014.
- Ein Blick auf die gemeldeten Angriffe zeigt: 39,6% aller Meldungen finden sich in den TOP 10 des Gefahrenmonitors wieder. PUP und Adware sind dabei weiterhin dominant.
- Script.Adware.Dealply.G belegt Platz 1 der Auswertung, mit 22,9% aller ausgewerteten Angriffe. Das häufig unbeabsichtigt installierte Browser Add-On versendet und verarbeitet Benutzerdaten, die dann von der Entwicklerfirma für verschiedene Zwecke gebraucht werden können.
- Bei der Kategorisierung bösartiger Webseiten tut sich die Kategorie Glücksspiele besonders hervor: Sie sprang innerhalb der letzten sechs Monate von Platz 13 auf Platz 1 (18,7%) der Auswertung.
- Mit Blick auf die Länder, in denen die Server von bösartigen Webseiten stehen, liegen die USA auch in diesem Halbjahr vorn: rund 57% der registrierten Angriffe haben hier ihren Ursprung. Deutschland belegt Platz 3, mit 3,9%.
- Der Banking-Trojaner Swatbanker, der noch im März 2015 für die höchsten Anzahl an abgewehrten Angriffen seit Beginn der Aufzeichnungen geführt hatte, verschwand quasi vollständig von der Bildfläche.
- Zum Ende des Jahres wurden erneut massive Angriffe durch Dridex verzeichnet. Der Banking-Trojaner war schon zuvor aufgefallen und es ist davon auszugehen, dass er auch weiterhin aktiv bleibt.
- Die Auswertung nach Zielen von Banking-Trojanern bestätigt die Beobachtung, dass der anglophone Sprachraum nach wie vor das Hauptziel der Angreifer ist: 80% aller identifizierten Ziel-Seiten stammten aus englischsprachigen Ländern.
- Im zweiten Halbjahr 2015 waren insbesondere die Exploit Kits Neutrino, Angler, Nuclear und Magnitude von Bedeutung.
- Die Angriffe auf Hacking Team hatten zur Folge, dass Informationen über bis dahin unbekannte Sicherheitslücken in die Hände von Cyber-Kriminellen gelangten und, in Exploits Kits verbaut, für eine von mehreren Angriffswellen sorgten.
- Auffällig war in diesem Halbjahr, dass zwei große Angriffswellen (im Fall des Hacking Teams nachweislich, im Fall von APT28 mutmaßlich) auf staatlich genutzte Angriffswerkzeuge zurückgehen, die von Cyber-Kriminellen adaptiert wurden.

Neue Signaturvarianten: pendelt sich alles wieder ein?

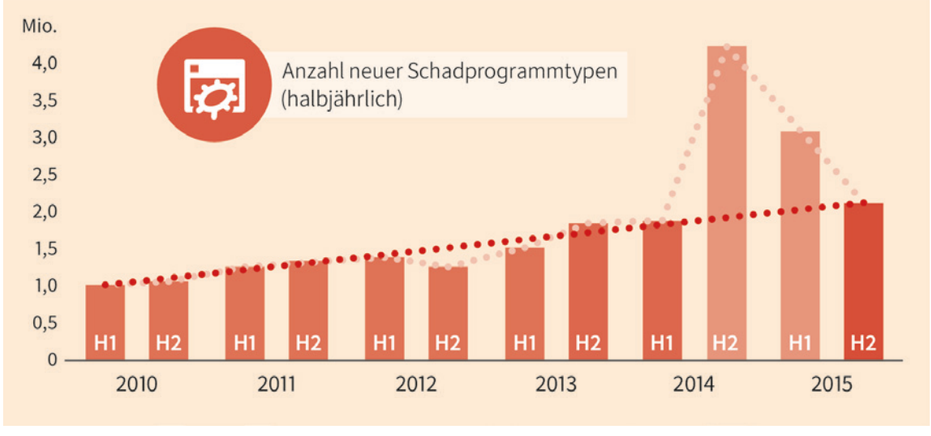
Im zweiten Halbjahr 2015 konnten wir einen erneuten Abfall der Zahlen neuer Signaturvarianten verzeichnen: 2.098.062 zu 3.045.722 in H1 2015 und somit ein Einbruch um 31%. Noch deutlicher wird der Rückgang der aktuellen Zahlen im Vergleich zum zweiten Halbjahr 2014 – ein Rückgang um 49,5%! Dieser Rückgang bedeutet jedoch weder eine Entwarnung in Bezug auf die Gefahr für Computernutzer, noch deutet sie an, dass der klassische Virenscanner[1] bald ausgedient hat.

Betrachten wir alle Halbjahreszahlen der letzten fünf Jahre, dann gab es in den letzten anderthalb Jahren deutliche Ausreißer nach oben. Eben genau die oben beschriebenen, die für den jetzt starken Negativtrend der Werte zuständig sind. Betrachtet man die Halbjahreszahlen jedoch ohne die beiden starken Abweichungen des zweiten Halbjahres 2014 und des ersten Halbjahres 2015, dann ergibt sich ein konsistenteres Bild. In dieser Betrachtung kann man die Steigerung der Werte beinahe linear beschreiben (unten). Es wird deutlich, dass die Zahl neuer Signaturvarianten keineswegs einem so stark abnehmenden Trend unterliegt, den man ob der vorgenannten Ausreißer vermuten könnte. Im Gegenteil, es lässt sich die These aufstellen, dass sich die Masse der neuen Signaturvarianten nun wieder auf ein Maß einpendeln wird, was im Rahmen des Erwartbaren liegt. Diese Einschätzung lehnt sich an die Betrachtung der Jahresgesamtzahlen an:

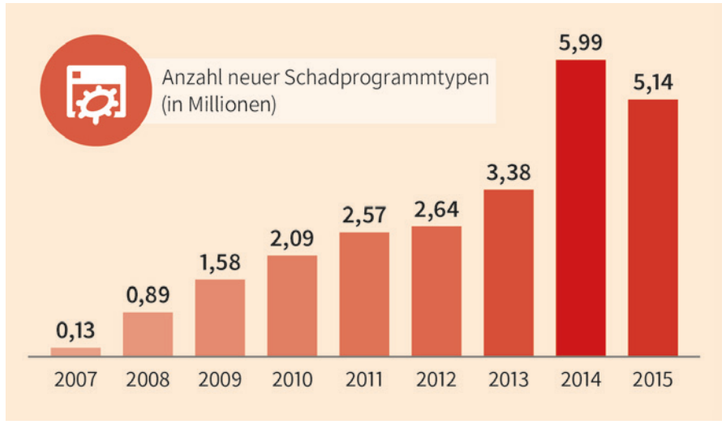
5.143.784

#DidYouKnow
In 2015 zählte GDataSoftwareAG 5,14 Mio. neue Schadprogramm-Typen!

Mit 5.143.784 liegt die Gesamtzahl des Jahres 2015 nur vermeintlich knapp unter dem Wert von 2014 – ein Minus von 14,3%, jedoch immer noch ein unbestritten sehr hohes Niveau des Schadpotentials. Zudem darf man dabei nicht außer Acht lassen, dass eine einzige Signaturvariante für die Erkennung von entweder exakt einer Datei zuständig ist oder aber auch die Erkennung von tausenden schädlichen Dateien ermöglichen kann.



[1] https://www.gdata.de/securitylabs/was-ist-eigentlich/virenscanner



Die Anzahl der tatsächlich schädlichen Dateien ist also höher als die Zahl der Signaturvarianten. Viren, Würmer und Trojanische Pferde sind nach wie vor eine Gefahr für Computernutzer.

Immer wieder werden Rufe laut: „Virenscanner sind tot“[2] und sie werden als überholt deklariert. Bei solchen Aussagen wird jedoch leider häufig der Begriff „Virenscanner“ als gesamte Sicherheitslösung interpretiert, was in der heutigen Zeit lange nicht mehr zutrifft. Die Erstellung von Signaturen für die Signatur-Engines ist nach wie vor ein sehr wichtiger Baustein für das Funktionieren einer umfassenden Sicherheitslösung, aber sie sind eben nur ein Bestandteil. Heutzutage kommt kein Top-AV-Produkt mehr ohne pro-aktive Technologien und cloudbasierten Schutz aus.

Und genau diese Weiterentwicklung der pro-aktiven Technologien kann ein entscheidender Faktor in der scheinbar so stark gesunkenen Anzahl der neuen Signaturvarianten sein. Die Weiterentwicklung des Cloud-Schutzes führt dazu, dass Bedrohungen an einer früheren Stelle abgefangen werden können – schon bevor sie den Rechner erreichen. Schnelle Reaktionszeiten auf neue Angriffsszenarien sind hier ebenfalls ein großer Vorteil gegenüber klassischen Signaturen. Durch die Auswertung von schon einigen Vorfällen, z.B. aus der Malware Information Initiative, kann sofort Schutz für die gesamte G DATA Community gewährt werden. Und die gewonnenen Erkenntnisse fließen dann weiter in die zahlreichen anderen Schutztechnologien der Produkte ein.

#DidYouKnow
Pro-aktive Technologien & cloudbasierter Schutz sind heute Standard in der #itsicherheit

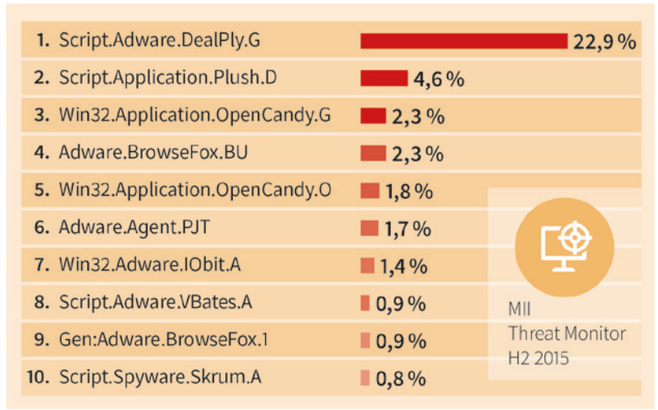
https://secure.gd/dl-de-pcmwr201502

[2] https://blog.gdata.de/2014/05/23813-weiterentwicklung-von-virenschutzlosungen-halt-an

Gefahren-Monitor

Der Gefahren-Monitor gibt die Top 10 der abgewehrten Angriffe gegen Computernutzer mit G DATA Sicherheitslösungen und aktiviertem Feedback[3] an. Nachfolgend werden die am häufigsten abgewehrten Attacken aus dem zweiten Halbjahr 2015 dargestellt. Eine Aufstellung für die einzelnen Monate ist immer aktuell auf der G DATA SecurityLabs Webseite[4] zu finden.

Die Zählweise in diesem Bereich unterscheidet sich von der für die Gesamtzahl der neuen Signaturvarianten (siehe Seite 4). Im aktuellen Kapitel werden die Zahlen tatsächlicher Angriffe ausgewertet und nicht die Zahlen neuer Schadprogrammtypen. Ein einziger Schadprogrammtyp kann bei der Zählung der Angriffe einen massiven Effekt haben, auch wenn die Familie unter Umständen nur wenige (neue) Varianten hervorbringt.



Die Top 10 des vergangenen Halbjahres machen 39,6% aller Schadprogramm-Meldungen aus. Damit setzt sich der Trend aus H1 2015 fort: die Varianz der gemeldeten Schädlinge nimmt erneut zu. Eine weitere Beständigkeit zu den Vormonaten zeigt sich in der Meldung von Script.Adware.Dealply.G. Erneut waren G DATA Kunden mit aktiviertem MII-Feedback Funktionen dieses potentiell unerwünschten Programms (PUP) am häufigsten ausgesetzt.

Der Anteil dieser Signatur ist erneut um 6,7% gestiegen. Schauen wir uns die Hintergründe zu Script.Adware.Dealply.G an:

DealPly ist ein Browser Add-On, das dem Benutzer helfen soll, beim Einkauf per Browser Vergleichsangebote zum aktuell aufgerufenen Produkt zu bekommen.

Die israelische Entwicklerfirma DealPly Technologies Ltd. erklärt, dass das Add-On „nur Deals und Einkaufsangebote anzeigt, wenn sie relevant sind für die Seite, die man gerade besucht. Für diese Seiten sendet DealPly dann gerade genügend nicht-identifizierbare Daten an den Server, um den Produkttyp von Interesse zu identifizieren.“[5] Der selbsternannte Einkaufs-Assistenz-Service verdient natürlich auch etwas daran.

[3] Die Malware Information Initiative (MII) setzt auf die Kraft der Online-Community und jeder Kunde von G DATA Sicherheitslösungen kann daran teilnehmen. Vorrausetzung hierfür: Er muss diese Funktion in seiner G DATA Sicherheitslösung aktivieren. Wird ein Angriff eines Computerschädlings abgewehrt, so wird dieser Vorfall vollkommen anonym an die G DATA SecurityLabs übermittelt. Die Informationen über die Schädlinge werden in den G DATA SecurityLabs gesammelt und statistisch ausgewertet.

[4] https://www.gdata.de/securitylab/statistiken/top10-malware.html

[5] http://www.dealply.com/faq.html

Spätestens dann, wenn der Kunde auf ein vom Add-On eingeblendetes Angebot klickt. In eigenen Worten der Firma heißt das: „Wenn Sie einen Kauf über DealPly machen, dann bezahlen uns einige Händler eine kleine Kommission.“[6]

Im Grunde genommen freut sich natürlich jeder Einkäufer, wenn er ein Produkt günstiger erhalten kann, doch leider werden solche Add-Ons in einer Vielzahl von Fällen nicht freiwillig vom Nutzern in den Browser integriert, sondern kommen Huckepack mit Installationsdateien (Installer) von anderen Programmen. Eine Möglichkeit ist, dass ein Benutzer sich eine Software aus dem Internet lädt, aber dafür nicht die Originaldatei von der Seite des Herstellers wählt, sondern ein beliebiges Downloadportal eines Drittanbieters. Drittanbieter bündeln die eigentliche Software häufig mit eben solchen Huckepack-Programmen, da sie selbst dadurch Profite pro Einrichtung verzeichnen können. Der unbedarfte Benutzer wird dann nach dem Start häufig von der Zugabe der potentiell unerwünschten Programme abgelenkt.

Es gibt auch Fälle, in denen ihm die Information zur Installation der Zusatzsoftware sogar aktiv vorenthalten wird. Was in den allermeisten Fällen gegen ethische Grundsätze verstößt, ist jedoch leider gängige Praxis im Web.

Die Gefahren und Plagen sind bei PUP und bei der eben beschrieben Software vielfältig:

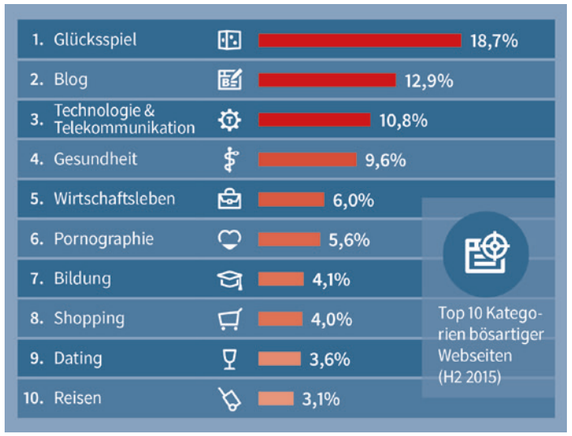
- Daten des Benutzers werden ungefragt an den Server der Entwickler oder einer Zwischenfirma gesendet. Ohne Recherche wird ein Nutzer nicht erfahren, um welche Daten es sich handelt und wo sie landen. DealPly Technologies gibt auf seiner Webseite immerhin Auskünfte darüber.
- Um zu entscheiden, welche Webseiten für das Add-On relevant sind (siehe oben), müssen alle aufgerufenen Seiten untersucht werden. Hier könnte durch die Betreiberfirma ein „Bewegungsprofil“ des Benutzers erstellt werden. Wird das Add-On im Firmenkontext benutzt, könnten also auch interne URLs und Adressen bekannt werden.
- PUPs sind für den Benutzer besonders innerhalb des Browsers zu bemerken, doch nicht immer beschränken sie sich darauf, sich nur dort einzunisten. Mit der Entfernung der Browser Add-Ons ist es häufig nicht getan, denn immer wieder aufgerufene Installationsroutinen lassen die Plagegeister in vielen Fällen wieder erscheinen. Nicht selten lauten Suchanfragen daher „Wie kann ich Dealply entfernen?“ oder auch „Adware.Dealply Was ist das?“ Das kostenfreie G DATA CLEAN UP[7] hilft bei der Bereinigung hartnäckiger Adware, Toolbars und Plug-Ins.

[6] http://www.dealply.com/eula.html

[7] https://www.gdata.de/clean-up/

Kategorien bösartiger Webseiten

Zum zweiten Mal, nach dem ersten Halbjahr 2014, steht die Kategorie Glücksspiele an der Spitze dieser Auswertung. Im ersten Halbjahr 2015 wurde sie nur auf Platz 13 verzeichnet und gehört somit definitiv zu den erwähnenswerten Themen bösartiger Webseiten der letzten sechs Monate.



Online-Glücksspiele und Online-Wetten vereinen sich zu einem Markt, der in 2015 mehr als 40 Milliarden US-Dollar Einnahmen verzeichnete[8]; mehr als eine Verdreifachung innerhalb der letzten 10 Jahre. Bald feiert diese Industrie ihr 20-jähriges Bestehen.

Nicht selten kommt es vor, dass Angreifer Webspace von kleineren Anbietern und weniger populären Seiten missbrauchen und dort Malware oder Phishing-Seiten hinterlegen. Schlagen die Systeme der Sicherheitslösungen dann darauf an, wird eine neue bösartige Seite in der passenden Kategorie verbucht. In der zweiten Jahreshälfte gab es beispielsweise mindestens eine groß angelegte Kampagne, bei der in mehreren Casino-Webseiten ein IFrame zu Malware-Domains eingebunden war, der Besucher unbemerkt einer Exploit-Kit-Attacke (siehe Seite 16) ausgesetzt hat. Nun könnte man meinen, dass die Zahl der Besucher von diesen Online-Casino Webseiten nicht so hoch wäre, jedoch kamen viele der Opfer gar nicht freiwillig auf die Glücksspiel-Seite: Sie wurden über einen infizierten Werbebanner (Malvertising) quasi unfreiwillig dorthin gebracht. Und die Reichweite von Werbebannern ist mitunter extrem hoch.

Im oben beschriebenen Fall wurden die verhängnisvollen Werbebanner auf Webseiten mit Kopien urheberrechtlich geschützten Materialien eingeblendet. Doch auch ganz legitime Seiten und vor allem Blogs finanzieren sich häufig über das Ausspielen von Werbung – die Kosten für Domains, Server und redaktionelle Arbeit wollen/müssen refinanziert werden, vor allem wenn das Webangebot der Seite an sich kostenlos ist.

#DidYouKnow
Von Glücksspiel (22,9%) bis Reise-Webseiten (3,1%), Angriffe lauern überall

https://secure.gd/dl-de-pcmwr201502
via @GDataSoftwareAG

[8] https://www.statista.com

Dabei nehmen aber die meisten Anbieter die Auswahl der angezeigten Werbungen nicht selbst in Hand, sondern bieten Platz auf ihrer Webseite zur Vermarktung in Werbenetzwerken an und verlassen sich damit auf Dritte. Die Werbenetzwerke liefern täglich Milliarden von Werbebannern aus und viele kleinere Netzwerke können die Prüfungen und Sicherheitsvorkehrungen nicht realisieren, wie die ganz großen Anbieter. Doch selbst dort passieren Fehler, wie wir schon im April im G DATA SecurityBlog[9] berichteten. 2015 gehörten Yahoo!, YouTube und auch der Britische eBay-Webauftritt zu den populären Opfern von Malvertising – sie dienten also ungewollt als Verbreiter von schädlichen Werbungen.

Ein Blick zurück auf die Kategorien bösartiger Webseiten und Platz Nummer 2, die Blogs. Diese populäre Art der Publikationsplattform wird von Millionen von Benutzern geführt – professionell und privat. Alleine mit Wordpress-Blogs werden pro Monat 56 Millionen neue Posts[10] erzeugt. Leider hat die häufig offene Art des Systems nicht nur Vorteile: Viele Benutzer können Plug-Ins und Verbesserungen für das System zur Verfügung stellen, doch diese enthalten häufig auch Sicherheitslücken. Die Grundprodukte, z.B. die Wordpress Basis-Plattform, haben inzwischen ein hohes Maß an Sicherheit und Code-Qualität. Die Plug-Ins und anderweitigen Erweiterungen sind hier viel eher das Problem.

Ob der Popularität der großen Anbieter bedeutet das im Umkehrschluss, dass eine Sicherheitslücke dann in sehr, sehr vielen Systemen gleichzeitig existiert. Das ist eine willkommene Angriffsfläche für Cyber-Kriminelle. Sie können fast automatisiert nach Blogs mit Schwachstellen suchen und diese dann manipulieren, zur Auslieferung von Malware oder auch Phishing, zum Redirect auf andere Seiten oder sonstige Aktionen.

ANGRIFFE AUS DEM INTERNET

Das Surfen im Internet stellt eine der größten Gefahren für Computernutzer dar und es gibt vielfältige Angriffsmöglichkeiten für Cyber-Kriminelle. Hier sind zwei der populärsten Angriffe:

Phishingseiten

Meist eine 1:1-Kopie einer Webseite mit dazugehörigem Login-Formular, z.B. eine Webseite einer Bank, eines E-Mail-Providers oder eines Bezahldienstleisters. Eingegebene Anmeldedaten werden jedoch nicht an das eigentliche Unternehmen/den eigentlichen Service zum Einloggen gesendet, sondern an die Server der Angreifer. Datenmissbrauch und Identitätsdiebstahl sind hier neben anderen möglichen Problemen vorprogrammiert.

Drive-by-Infektionen

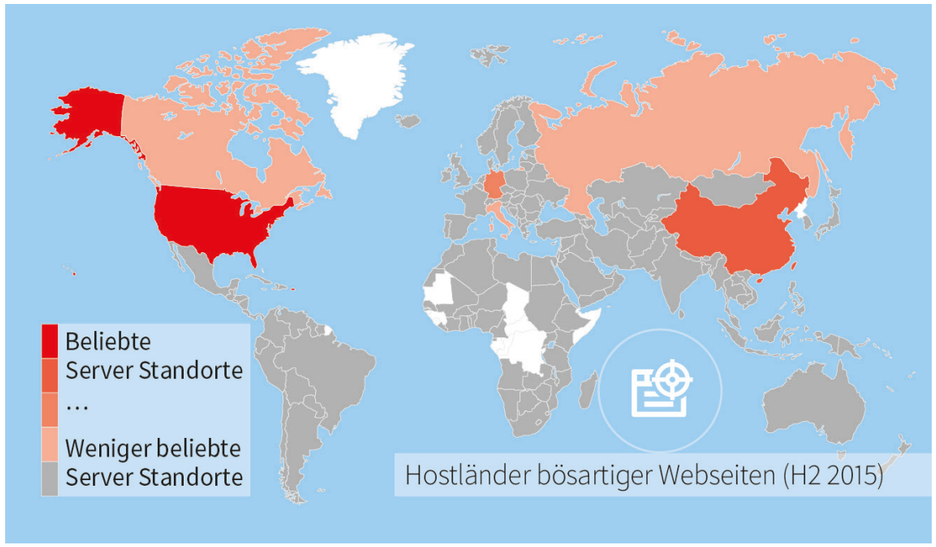
Wie der Name schon verrät, passiert dieser Angriff „im Vorübergehen" und meist unbemerkt vom Nutzer. Manipulierte Webseiten spähen zunächst die Konfiguration des Rechners auf angreifbare Anwendungen aus (Browser, Betriebssystem, Software, ...). Wird eine geeignete Lücke entdeckt, wird ein passender Exploit an den Client gesendet, der die gefundene Sicherheitslücke ausnutzt, um danach oft weiteren Schadcode auf den angegriffenen Rechner zu laden und auszuführen, z.B. FakeAV, Backdoors, Spionage-Trojaner, Ransomware, etc.

[9] https://blog.gdata.de/2015/04/24246-augen-auf-beim-bannerkauf-googles-werbedienst-zur-malwareverbreitung-missbraucht
[10] https://wordpress.com/activity/

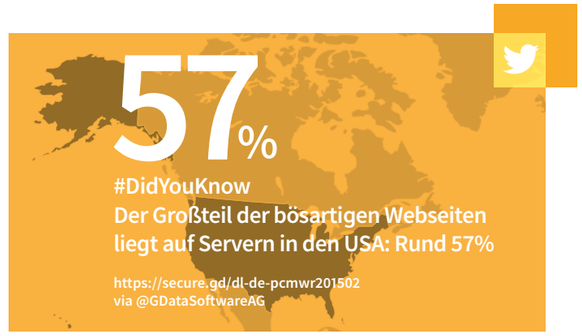
Kategorisierung nach Server-Standort

Die G DATA SecurityLabs stellen nicht nur die thematische Einordnung von schadhaften Webseiten dar, sondern auch deren Verteilung auf der ganzen Welt.

Die folgende Auswertung zeigt, wo auf der Welt die Mehrzahl der bösartigen Webseiten liegt, die in den G DATA SecurityLabs im zweiten Halbjahr als schädlich oder Phishing gemeldet wurden.



Die obige Grafik zeigt an, in welchem Land der Ursprung der Attacke liegt, also wo der Webseiten-Server steht, wobei nicht zwischen Phishing- und Malwareseiten unterschieden wird. Dabei ist es nicht entscheidend, welche Top Level Domain (z.B. .com, .de oder andere) an einer Webseite steht, sondern in welchem Land die Rechner für den Webspace stehen. So kann es zum Beispiel sein, dass eine schädliche Webseite auf .de endet, jedoch der Inhalt der Webseite auf einem Server in den USA liegt. In diesem Fall würde in der Statistik ein Fall in den USA registriert.

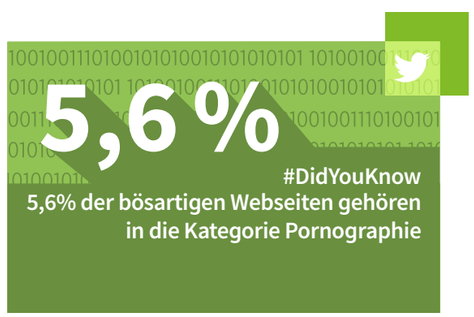


Insgesamt ist die Anzahl der als bösartig klassifizierten Webseiten um 45% gestiegen, was deutlich unterstreicht, dass Angriffe aus dem Web eine der größten und auch wachsenden Gefahren für Computernutzer darstellen. Tatsächlich wurden rund 57% der registrierten Angriffe über Ressourcen durchgeführt, die in den USA untergebracht waren – das ist eine deutliche Mehrheit. Außerdem ist es eine erneute Steigerung im Vergleich zum vorherigen Halbjahr, in denen wir 43,3% der bösartigen Webseiten in den Vereinigten Staaten registrierten.

Auch China, Hong Kong, Russland und Kanada (zusammen 14,4%) finden sich unter den Top-Plätzen der Hostländer. Europa ist in H2 2015 relativ wenig in Erscheinung getreten – lediglich Deutschland und Italien sind unter den ersten sieben zu finden und sind für zusammen 6% Anteil verantwortlich.

Hier liegt die Vermutung nahe, dass Cyber-Kriminelle zwar das in weiten Teilen erstklassig ausgebaute Kommunikationsnetz schätzen und nutzen, aber innerhalb der EU eben auch mehr gegen Straftaten im Netz getan wird als in anderen Ländern.

Unterstützt wird diese Einschätzung durch die kürzlich von der Europäischen Kommission veröffentlichte Agenda zur „Bekämpfung von Terrorismus, organisierter Kriminalität und Computerkriminalität“ [11]. Die EU-Mitgliedsstaaten sollen demnach noch intensiver und organisierter zusammenarbeiten, um gegen die genannten Delikte vorzugehen. „Dringlichste Aufgabe ist der Abbau von Hindernissen, die der Ermittlung von Online-Straftaten im Wege stehen, insbesondere in Bezug auf die Zuständigkeit und Vorschriften über den Zugang zu Beweisen und Informationen“ – so lautet eine der Maßnahmen für den Zeitraum 2015 bis 2020.

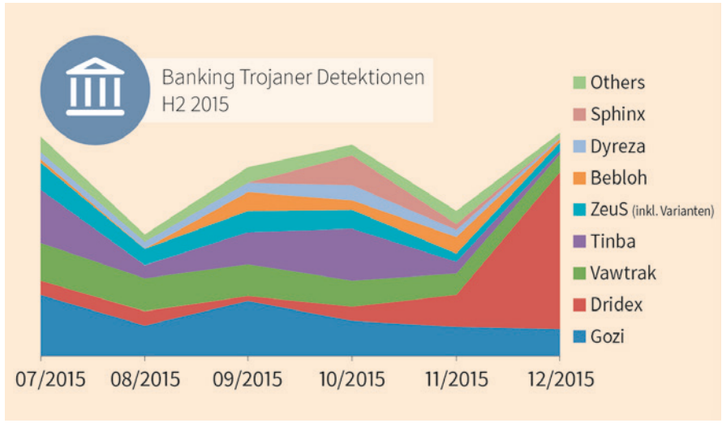


[11] http://europa.eu/rapid/press-release_IP-15-4865_de.htm

Banking

Banking-Trojaner Trends

Zu Beginn des zweiten Halbjahres 2015 machte es zunächst den Anschein als wenn Angriffe durch Banking-Trojaner deutlich abnehmen würden. Der zuvor dominante Swatbanker aus der Cridex-Gruppe, der noch im März 2015 für die höchsten Anzahl an abgewehrten Angriffen seit Beginn der Aufzeichnungen geführt hatte, verschwand aus unbekannten Gründen quasi vollständig von der Bildfläche.



Die zu diesem Zeitpunkt registrierten Schädlinge verteilten sich auf relativ niedrigem Niveau, wie die obige Grafik zeigt: Im Juli wurde ein Viertel weniger Angriffe registriert als noch im Vormonat und diese Zahl halbierte sich im August nochmals.

Im weiteren Verlauf der zweiten Jahreshälfte kam es jedoch zu einer erneuten Verschärfung der Angriffs-Situation. Einen Teil dazu trug eine neue Crimeware namens Sphinx bei.[12] Hierbei handelt es sich um eine neue Variante des altbekannten Banking-Trojaners ZeuS, bei der der gesamte Netzwerkverkehr über das Anonymisierungsnetzwerk Tor abgewickelt wird. Diese Idee ist allerdings nicht neu; eine ähnlich operierende Schädlings-Variante konnte von G DATA bereits 2012 identifiziert[13] werden. Letztlich blieb Sphinx eine kurzlebige Randerscheinung.

Zu Beginn des Halbjahres erreichte kein Trojaner eine besondere Vormachtstellung. In Summe wurde im Oktober jedoch wieder das Infektionsniveau des Julis erreicht.

[12] http ://securityaffairs.co/wordpress/39592/cyber-crime/sphinx-variant-zeus-trojan.html
[13] https://blog.gdata.de/2012/09/23891-in-tor-versteckter-botnet-command-server

Im November wurde ein bedeutender russischer Cyber-Crime-Ring gesprengt.[14] Pikante Randnotiz: Als Tarnung für die kriminelle Organisation diente offenbar eine Filmproduktionsfirma, die gerade an einem Film über Cyber-Crime arbeitete. Es wird über eine Verbindung zum Dyreza-Trojaner spekuliert, dessen Aktivitäten nach dem Ausheben der Gruppe praktisch erloschen. Aber auch Tinba sowie ZeuS mitsamt seiner Varianten konnten danach deutlich seltener registriert werden, so dass das Angriffsniveau im November wieder nur knapp über dem von August lag.

Im Dezember nahm dann mit Dridex ein bereits bekannter Banking-Trojaner eine deutliche Führungsposition ein, der sich über massenhaft versendete E-Mails mit angeblichen Rechnungen[15] verbreitete. Insgesamt lag das Infektionsniveau schlussendlich wieder auf dem Niveau des Julis.

Die weitere Entwicklung der bisherigen Akteure ist schwer vorherzusehen. Fraglich ist beispielsweise, ob die Angreifer hinter Swatbanker in absehbarer Zeit mit der vorherigen Intensität zurückkehren. Die Angreifer hinter Dridex verbreiten ihre Schadsoftware wie zuvor die Swatbanker-Angreifer, vor allem mit Spam-Mails. Allerdings scheinen die Angriffe hier konstanter zu erfolgen, und nicht stoßweise, wie bei Swatbanker. Wir erwarten, dass Dridex auch weiterhin einen bedeutenden Anteil an den Erkennungen der kommenden Monate haben wird. Gozi war eine weitere Konstante, so dass auch hier mit weiteren Angriffen zu rechnen ist.

Das geringer werdende Angriffsvolumen könnte letztlich auch auf einen Paradigmenwechsel der Angreifer hindeuten: Während die Angriffe in den letzten Jahren vor allem auf eine breite Masse abgezielt haben, könnte sich der Fokus eher auf wenige, dafür aber besonders lukrative Angriffsziele verlagern, insbesondere auf Unternehmenskonten.

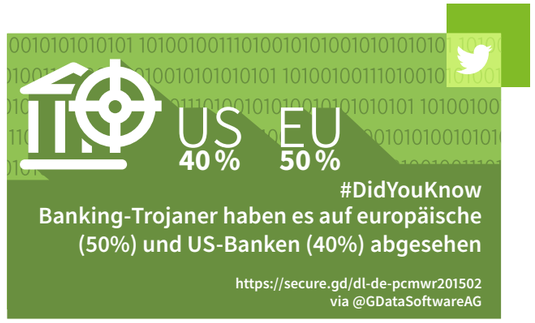
[14] http://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS
[15] https://blog.gdata.de/2015/12/24310-dridex-das-stehaufmannchen

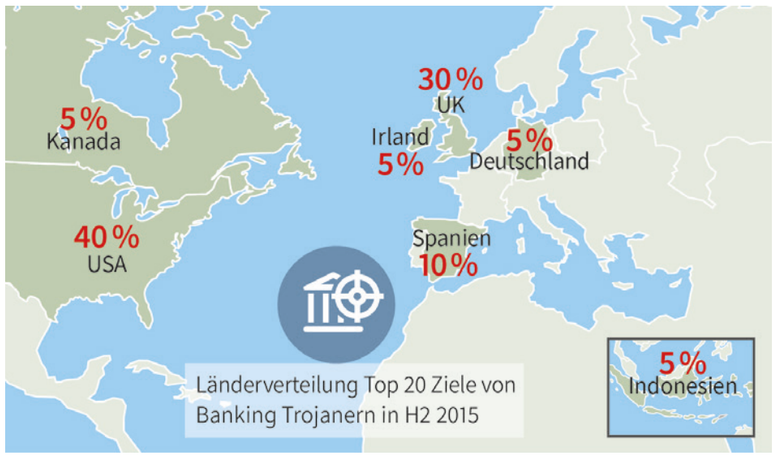
Die Ziele von Banking-Trojanern

Jeder Banking-Trojaner greift je nach Konfiguration bestimmte Ziele an. Ziele bedeutet in diesem Fall, dass der Banking-Trojaner seine Angriffe durchführt, wenn ein Nutzer des infizierten PCs eine festgelegte Webseite aufruft. Dann entfaltet der Schädling seine jeweils an das Ziel angepasste Wirkung.

Wie bereits in früheren Reports zeigt sich auch diesmal wieder die Vorliebe der Cyber-Kriminellen für den anglophonen Sprachraum. 80% aller identifizierten Ziel-Seiten stammten aus diesen Ländern.

Es tauchten – mit Ausnahme des Zahlungsdienstleisters PayPal – ausschließlich Banken in der Liste der häufigsten Ziele auf. Platz 1 der Auswertung belegt die Santander-Gruppe, eine Bank mit Ursprung außerhalb des angolophonen Sprachraums, wobei Angriffe auf dieses Ziel sowohl das spanische, als auch das englische Portal der Bank mit einbezogen. In vorangegangenen Untersuchungen war die Santander-Bank als Ziel eher nachrangig in Erscheinung getreten.





Methodik

Insgesamt wurden 4.422 Konfigurationsdateien der Familien Vawtrak, Tinba, ZeuS (inkl. Varianten, u.a. Citadel), Bebloh und SpyEye entschlüsselt und analysiert. Bebloh wurde dabei hinzugefügt, und Swatbanker entfernt, da er nicht mehr in Erscheinung trat (siehe Seite 12). In den Konfigurationsdateien dieser Banking-Trojaner befindet sich eine Liste von Zielseiten (d.h. Webseiten von Banken, Bezahldienstleistern etc.). Werden diese Seiten vom infizierten Rechner aus aufgerufen, tritt speziell auf die Seite abgestimmter Schadcode (sog. Webinjects) in Aktion. [16]

Der errechnete prozentuale Wert entspricht der Wahrscheinlichkeit, dass ein Ziel bei Infektion mit einem Banking-Trojaner auch in der Liste der Angriffsziele steht. Dabei wurde auch der Verbreitungsgrad der jeweiligen Trojaner-Familie einbezogen. Weil mit Swatbanker kein übermäßig dominanter Trojaner mehr vorkam, wurde auf eine Errechnung der Liste bei angenommener Gleichverteilung der Trojaner verzichtet. Den Top 20 wurden zudem Herkunftsländer zugeordnet. [17]

	Land	Rating (Markenwert nach Brand Finance)	Angriffswahrscheinlichkeit (Basierend auf der Analyse von 4.422 Banking-Trojanern der Familien Vawtrak, Tinba, ZeuS (inkl. Varianten, u.a. Citadel), Bebloh und SpyEye
Santander Group gruposantander.es, santander.co.uk		10	45,00 %
Lloyds Banking Group lloydstsb.co.uk, halifax-online.co.uk, ...		35	35,86 %
RBS Group rbs.com, natwest.com, ulsterbank.co.uk, ...		60	35,81 %
Barclays barclays.co.uk		13	34,99 %
Allied Irish Banks aib.ie		181	25,75 %
HSBC hsbc.com, hsbc.co.uk, ...		3	25,48 %
The Co-operative bank co-operativebank.co.uk		114	25,32 %
PayPal paypal.com, paypal.co, paypal.co.mx, ...		-	25,03 %
Nationwide nationwide.co.ukcom.sg		94	22,64 %
Bank Central Asia klikbca.com		147	19,00 %
BBVA bbvanetoffice.com, bbva.es, ...		28	17,79 %
Bank of America bankofamerica.com		6	17,57 %
Wells Fargo wellsfargo.com		1	17,25 %
Chase chase.com, chasecanada.ca, chaseonline.com		7	17,01 %
Citi citibank.com, citibank.com.au, citibank.com.sg		5	16,87 %
U.S. Bancorp usbank.com		46	16,56 %
Citizens Bank citizensbankonline.com		264	16,51 %
Fifth Third Bank 53.com		111	16,37 %
TD Bank td.com, tdcanadatrust.com		18	15,80 %
DKB Bank dkb.de		176	14,64 %

Kategorie: = Bank = E-Payment = Auktion

TOP 20 Angriffsziele von Banking-Trojanern in H2 2015 (nach Trojaner-Verteilung)

[16] Bei Webinjects mit sogenannten Wildcards oder regulären Ausdrücken wurden diese auf andere Webinjects ohne Wildcards abgebildet, soweit möglich. Wenn solche Webinjects auf mehrere Domänen passten, wurden daraus Gruppen gebildet, wobei diese manuell auf Plausibilität geprüft wurden. Im weiteren Verlauf wurden die Domänen aus den Zielseiten extrahiert und auf Gültigkeit überprüft. Schließlich wurde gezählt, welche Domänen (bzw. Gruppen) in wie vielen Samples vorkommen.

[17] Dazu wurden die firmeneigenen Angaben auf den jeweiligen Seiten genutzt. Bei Gruppierungen wurde im Zweifelsfall der Standort des Mutterhauses als Herkunftsland angenommen. Das Brand Rating stammt von Brand Finance (http://www.rankingthebrands.com/PDF/Brand%20Finance%20Global%20Banking%20500,%202015.pdf), wobei hier ohne eigenes Rating das Rating des Mutterhauses übernommen wurde. Existierten mehrere Labels für Domänengruppen, wurde die höchstplatzierte Marke zu Grunde gelegt.

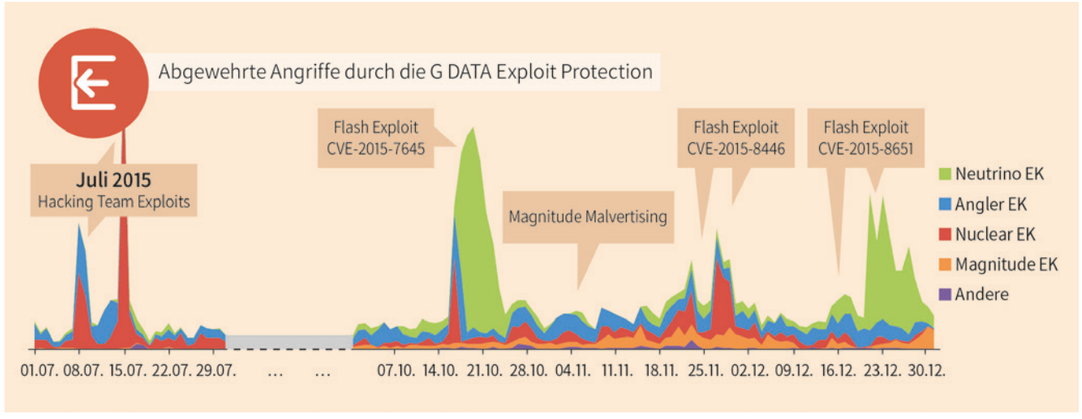
Exploit Kits

Bei Exploit Kits handelt es sich um im Untergrund gehandelte Werkzeuge zur automatisierten Suche und Ausnutzung von Schwachstellen. Die PC-Sicherheitslösungen von G DATA enthalten mit dem Exploit-Schutz eine Komponente, die sich auf die pro-aktive Abwehr von Exploits spezialisiert hat. Dabei abgewehrte Angriffe wurden in dieser Untersuchung auf bekannte Exploit Kits abgebildet.

Im zweiten Halbjahr 2015 waren insbesondere die Exploit Kits Neutrino, Angler, Nuclear und Magnitude von Bedeutung. Die meisten abgewehrten Angriffe konnten erneut von Angler registriert werden.

Es gab dabei allerdings keine deutliche Dominanz wie noch im vorherigen Halbjahr; Neutrino lag praktisch auf Augenhöhe. Außerdem konnten Angriffe von Huanjuan, Niteris, RIG und Fiesta festgestellt werden, die aber weitestgehend Randerscheinungen blieben. Wie schon im vorherigen Halbjahr war Adobe Flash der bevorzugte Angriffsvektor der Kriminellen.

Eine erste große Welle geht letztlich auf einen Angriff auf das Hacking Team zurück. [18] Dabei handelt es sich um eine Firma, die mehr oder weniger legitim Angriffswerkzeuge herstellt und verkauft, zum Beispiel an Regierungsorganisationen.



[18] https://en.wikipedia.org/wiki/Hacking_Team#2015_data_breach

Bei dem Angriff wurden ironischerweise praktisch sämtliche Daten des Hacking Teams durch Hacker gestohlen und am 5. Juli der Öffentlichkeit zugänglich gemacht. Neben pikanten Informationen zum Kundenkreis, zu dem auch Pariastaaten gehörten, wurden ebenfalls die Angriffswerkzeuge des Hacking Teams vollständig veröffentlicht. Dazu gehörten unter anderem Exploits für mehrere bisher unbekannte Flash-Schwachstellen, sogenannte Zero-Days. Der Begriff Zero-Day wirkt hier allerdings beinahe komisch, denn tatsächlich war das Hacking Team bereits seit Oktober 2013 im Besitz der Exploits.

Auf die Veröffentlichung der Daten wurden natürlich auch Cyber-Kriminelle aufmerksam. Diese integrierten die Angriffsmethoden innerhalb kürzester Zeit, ab dem 7. Juli, in ihre Exploit Kits. Die Anzahl abgewehrter Angriffe schoss danach in die Höhe. G DATAs Exploit Protection schützte vor sämtlichen dieser Angriffe, inklusive denen des Hacking Teams. Die Angriffe dauerten bis zum 10. Juli an, bis Adobe einen Patch zur Verfügung stellte.

Danach war die Lage für einige Monate relativ ruhig, bis am 13. Oktober. ein neuer Flash-Exploit (CVE-2015-7645 / APSA15-05) [19] aus dem Exploit Kit einer Gruppe namens APT28, alias Sofacy, publik wurde.

Dabei handelt es sich um eine mutmaßlich mit der russischen Regierung verbundene Gruppe, die auch schon auf die Angriffe auf den deutschen Bundestag verantwortlich gewesen sein soll. [20]

Die Cyber-Kriminellen adaptierten den Angriff wieder innerhalb kurzer Zeit, in drei Tagen, woraufhin in der G DATA Exploit Protection entsprechende abgewehrte Angriffe festgestellt werden konnten. Adobe konnte praktisch zeitgleich zu den beginnenden Angriffen der Cyber-Kriminellen ein Update zur Behebung der Schwachstelle zur Verfügung stellen. Vermutlich half dabei, dass die Schwachstelle bereits zwei Wochen vorher von einer Sicherheitsforscherin entdeckt und an Adobe gemeldet wurde. [21]

Da es eine gewisse Zeit dauert, bis Updates auch tatsächlich an die Nutzer verteilt sind, wurden letztlich trotzdem ähnlich viele Angriffe registriert wie bei den Exploits, die nach den Attacken auf Hacking Team in die Angriffswerkzeuge integriert wurden.

[19] https://helpx.adobe.com/security/products/flash-player/apsa15-05.html
http://malware.dontneedcoffee.com/2015/10/cve-2015-7645.html

[20] https://en.wikipedia.org/wiki/Sofacy_Group

[21] https://twitter.com/natashenka/status/655083143456665600

Die Personen hinter dem Magnitude Exploit Kit stiegen erst relativ spät auf den Zug auf, und begannen am 9. November eine Kampagne mit CVE-2015-7645, die durch sogenanntes Malvertising flankiert wurde.[22] Dabei wird das Exploit Kit über Werbebanner in Webseiten eingebettet, die an sich gar nicht bösartig sind und dem Nutzer zudem unverdächtig erscheinen. Da der eingesetzte Exploit Anfang November jedoch nicht mehr gänzlich neu war, war die Angriffsintensität nicht so deutlich wie die der initialen Welle der anderen Exploit Kits. Im Vergleich zu den Magnitude-Angriffen der Vormonate verzeichneten wir aber immer noch eine deutliche Steigerung.

Flash war im Laufe des Halbjahres noch zwei Mal im Fokus der Angreifer: Einmal ab dem 13. November (CVE-2015-8446 / APSB15-32)[23]. Die Angriffswelle begann im Gegensatz zu den vorherigen erst einige Tage nach dem Release des Sicherheitsupdates von Adobe und fiel entsprechend schwächer aus. Eine weitere Angriffswelle begann am 21. Dezember und zielte auf die Schwachstelle, die in CVE-2015-8651 / APSB16-01[24] beschrieben ist. Sie wurde insbesondere vom Neutrino Exploit Kit ausgenutzt, bis Adobe am 28. Dezember ein Sicherheitsupdate veröffentlichte. Da die Schwachstelle eine Woche lang offen war, waren hier wieder deutlich mehr Angriffe zu verzeichnen.

Wie schon zuvor ist Flash der bedeutendste Angriffsvektor für Exploit Kits. Neben Angler hat in diesem Jahr vor allem Neutrino eine tragende Rolle gespielt, in geringerem Maße auch Nuclear. Bei Angler und Neutrino war insbesondere die schnelle Adaption von Angriffen auffällig. Von Magnitude wurden größere Angriffswellen als zuvor registriert, insbesondere im Kontext von Malvertising. Die Menge der registrierten Angriffe reicht aber nicht an die Dimension der anderen Exploit Kits heran.

2

#DidYouKnow
2 Exploit Kit Angriffswellen basierten auf staatlich genutzten Angriffswerkzeugen

https://secure.gd/dl-de-pcmwr201502

Auffällig war in diesem Halbjahr, dass zwei große Angriffswellen (im Fall des Hacking Teams nachweislich, im Fall von APT28 mutmaßlich) auf staatlich genutzte Angriffswerkzeuge zurückgehen, die von Cyber-Kriminellen adaptiert wurden.

Das Risiko, dass solche Angriffswerkzeuge in die Hände von Cyber-Kriminellen gelangen können, wird dabei schon seit langer Zeit von Sicherheitsforschern diskutiert. Die Existenz dieses Risikos hat sich nun bestätigt.

[22] https://blog.malwarebytes.org/exploits-2/2015/11/magnitude-exploit-kit-activity-increases-via-malvertising-attacks/
[23] https://helpx.adobe.com/security/products/flash-player/apsb15-32.html
[24] https://helpx.adobe.com/security/products/flash-player/apsb16-01.html

G DATA PC Malware Report

Über G DATA

Die G DATA Software AG ist der Antivirus-Pionier. 1985 gegründet, entwickelte das Bochumer Unternehmen bereits vor 30 Jahren die erste Software gegen Computerviren. Heute gehört G DATA zu den führenden Anbietern von Internetsicherheitslösungen und Virenschutz mit weltweit mehr als 400 Mitarbeitern.

GDATA PC Malware Report H2 2015 DE V3 • 5710110316