SIMPLY
SECURE

G DATA SECURITYLABS MALWARE REPORT

HALBJAHRESBERICHT

JANUAR – JUNI 2015

G DATA SECURITYLABS

INHALT

AUF EINEN BLICK

- Im ersten Halbjahr 2015 sind 3.045.722 neue Schädlinge registriert worden. Das liegt zwar um etwas mehr als ein Viertel (26,6%) unter dem Rekordwert des letzten Halbjahrs. Es liegt aber knapp zwei Drittel (+64,8%) über dem Ergebnis des Vorjahreszeitraums. Im Durchschnitt entdecken die G DATA Sicherheitsexperten 12 neue Schädlinge pro Minute. Für das kommende Jahr erwarten wir, dass die Gesamtzahl neuer Schädlinge über der des Vorjahres liegt.
- Die Gesamtzahl aller Schädlinge seit 2006 liegt nun bei 22.393.098.

- Die Top 10 der abgewehrten Malware-Angriffe wird weiterhin dominiert von Adware und Potentiell Unerwünschten Programmen (PUP). Besonders auffällig in diesem Umfeld sind die Familien DealPly und Graftor.

- Das Thema Gesundheit war mit 26,6% das dominanteste Thema der als bösartig klassifizierten Webseiten. Unter anderem wurden auf Seiten dieser Kategorie Kampagnen lanciert, die einen dubiosen Geldsegen versprechen.
- Die Kategorie "Persönliche Werbung und Dating" ist neu in den Top 10. Seiten dieses Themas bieten an, kostenpflichtige Dienste abzuschließen oder Services durch Premium-Rufnummern zu nutzen.
- Schädliche und betrügerische Webseiten liegen weiterhin am häufigsten auf Servern in den USA, in China und in Frankreich. Als Neueinsteiger landet die Ukraine mit 5% auf Platz 4. Es ist unklar, ob es einen Zusammenhang mit den politischen Wirren in dieser Region gibt.

- Die Anzahl der Angriffe von Banking-Trojanern wird 2015 voraussichtlich erstmals seit 2012 wieder steigen.
- Die Swatbanker-Familie sorgte im März mit immer neuen E-Mail-Kampagnen für ein Allzeithoch, was die Anzahl abgewehrter Angriffe von Banking-Trojanern angeht. Die Aktivitäten dauerten bis Juni an. Swatbanker hatte vor allem Kunden von Banken in Deutschland, Österreich und Polen im Visier.
- Im ersten Halbjahr übersteigt die Summe der durch BankGuard verhinderten Schäden die Marke von 100 Millionen Euro.

- Exploits für Sicherheitslücken werden nach wenigen Tagen in die Exploit Kits übernommen. Damit werden Nutzer, die ihre Systeme nicht auf dem neuesten Stand halten, zu leichten Opfern. Exploit Kits werden von Angreifern benutzt, um Rechner unbemerkt und unerlaubt auf viele Schwachstellen abzuklopfen und dann zu kapern, zum Beispiel bei einem Besuch einer Webseite (Drive-by-Infektion).
- Die Sicherheitslücken in Adobe Flash wurden am häufigsten dazu genutzt, Rechner automatisiert und unbemerkt anzugreifen. Sicherheitslücken in Java werden inzwischen aufgrund der "Click-to-Play"-Voreinstellungen im Browser kaum noch genutzt.
- Am 21. Januar wurde im Angler Exploit Kit eine bis dahin unbekannte und nicht geschlossene Sicherheitslücke in Adobe Flash integriert (CVE-2015-0311). In den folgenden Wochen maßen die Spezialisten der G DATA SecurityLabs Rekordzahlen für die Abwehr von Exploits.
- Ebenfalls sehr effektiv war die Integration des Nuclear Exploit Kits in Werbebanner eines Zulieferers für Google AdSense. Die Angreifer planten so Millionen von Nutzern mit Malware infizieren.

MALWARE-STATISTIKEN

Die Zahl der neuen Schadprogrammtypen aus dem ersten Halbjahr 2015 ist signifikant geringer als die Zahl des vorherigen Halbjahres und reiht sich damit eher wieder in die Regionen vor dem vermeintlichen Ausreißer in H2 2014 ein: insgesamt wurden 3.045.722 neue Signaturvarianten registriert.

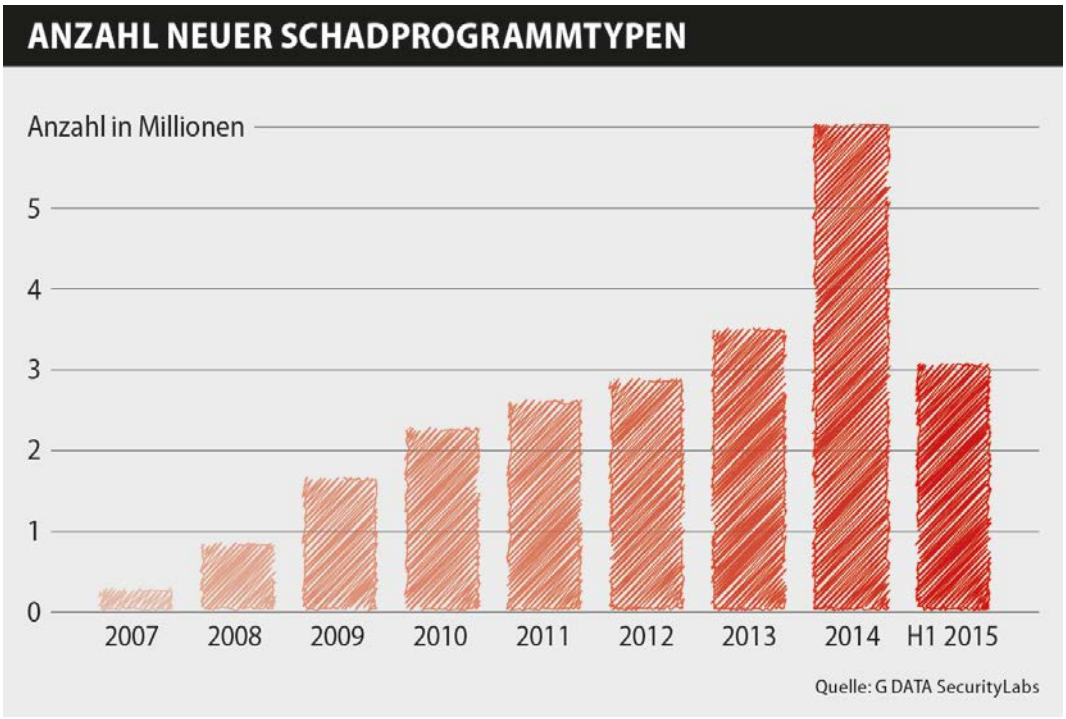

Abbildung 1: Anzahl neuer Schadprogrammtypen

Diese Zahl liegt zwar um etwas mehr als ein Viertel (26,6%) unter dem Rekordwert des letzten Halbjahrs. Es liegt aber knapp zwei Drittel (+64,8%) über dem Ergebnis des Vorjahreszeitraums. Im Durchschnitt entdecken die G DATA Sicherheitsexperten 12 neue Schädlinge pro Minute. Die Gesamtzahl aller Schädlinge seit 2006 liegt nun bei 22.393.098.

Gefahren-Monitor

Der Gefahren-Monitor gibt die Top 10 der abgewehrten Angriffe gegen Computernutzer mit G DATA Sicherheitslösungen und aktiviertem Feedback[1] an. Nachfolgend werden die am häufigsten abgewehrten Attacken aus dem ersten Halbjahr 2015 dargestellt. Eine Aufstellung für die einzelnen Monate ist immer aktuell auf der G DATA SecurityLabs Webseite[2] zu finden.

Die Zählweise in diesem Bereich unterscheidet sich von der für die Gesamtzahl der Schädlinge, da hier die Zahlen tatsächlicher Angriffe ausgewertet werden 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.

[1] 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.

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

Bemerkenswert ist, dass die Top10 in diesem Halbjahr nur 43,5% aller Meldungen ausmachen und somit 21,5% weniger Meldungen abdecken als im vorherigen Halbjahr. Dies deutet auf eine stärkere Varianz der Schädlinge hin welche dem Fokus auf einzelne Schädlinge entgegenwirkt.

Rang	Name	Prozent
1	Script.Adware.DealPly.G	16,2%
2	Adware.BrowseFox.BU	8,0%
3	Script.Application.Plush.D	5,3%
4	Gen:Variant.Adware.Graftor.173090	3,2%
5	Gen:Variant.Adware.Graftor.159320	3,1%
6	Gen:Variant.Adware.Graftor.159134	2,1%
7	Adware.RelevantKnowledge.A	1,6%
8	Win32.Application.OpenCandy.G	1,6%
9	Win32.Adware.IObit.A	1,5%
10	Win32.Application.Dealply.H	0,9%

Tabelle 1: Die Top 10 der an die MII gemeldeten Angriffe

In diesem Halbjahr wird der Trend zu den „Potentiell unerwünschten Programmen“ (PUP) weiter bestätigt. Die massive Verbreitung von Schadprogrammen dieser Kategorie schließt lückenlos an die Zahlen aus 2014 an. Während im letzten Report **Gen:Varient.Adware.SwiftBrowse.1** mit 26,9% die Rangliste anführte ist dieses Halbjahr Platz 1 durch **Script.Adware.DealPly.G** belegt. Dieser lag vorher auf Platz 7 und seine Verbreitung hat um 12,6% zugenommen.

Weiterhin auffällig ist die starke Präsenz von **Gen:Variant.Adware.Graftor** Schädlingen, welche der Gruppe der **BrowseFox** Adware zugeordnet werden können. Typischerweise wird dieser Schädling zusammen mit unterschiedlichster Freeware ausgeliefert und mehr oder weniger freiwillig installiert. Einmal auf dem System eingenistet werden sowohl Manipulationen an den installierten Browsern durchgeführt, als auch Systemdienste und Treiber installiert, welche unter anderem als lokaler Proxy genutzt werden. Eine der am häufigsten durchgeführten Manipulationen besteht im Austausch der Startseite und Standardsuchseite der Browser. Außerdem wird durch die Adware an verschiedenen Stellen Werbung eingebunden und unter anderem durch PopUps angezeigt.

WEBSEITEN-ANALYSEN

Kategorien bösartiger Webseiten

Die letzten Halbjahre hielten bei dieser Untersuchung relativ wenige Überraschungen bereit – fokussierten sich die Angreifer anscheinend auf die Ausnutzung von Webseiten mit technischen Themen oder auch Glücksspielen. Die Auswertung des ersten Halbjahres 2015 zeigt jedoch ein neues Bild:

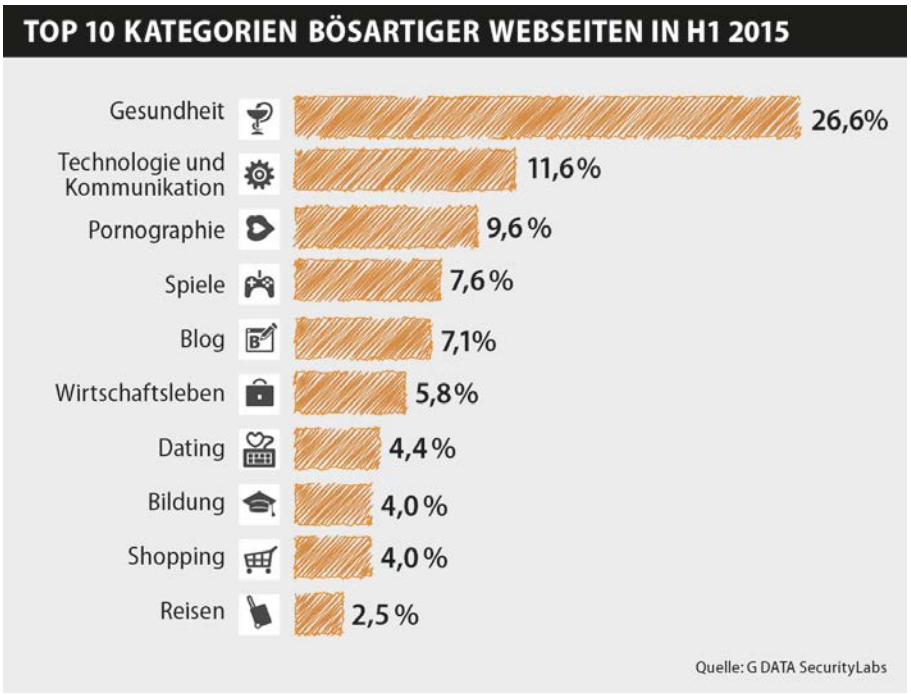

Abbildung 2: Top 10 Kategorien bösartiger Webseiten

Die statistischen Eckdaten zeigen, dass die aktuellen Top 10 Kategorien einen Anteil von 83,1% an allen klassifizierten Webseiten haben. Das ist ein Plus von 4,7% gegenüber dem zweiten Halbjahr 2014 und bezeichnet seit dem Beginn der Untersuchung sogar den zweithöchsten Wert nach dem H2 2012 (88,6%). Die restlichen 16,9% verteilen sich auf 63 weitere Themen.

Platz 1 belegt aktuell die Kategorie **Gesundheit**, mit einem Anteil von 26,6%. Das heißt: mehr als jede vierte bösartige Webseite stammt aus dieser Kategorie. Eine Kampagne, die wir innerhalb dieser Kategorie identifizieren konnten, ist eine so genannte Money Rain Kampagne. Dabei werden auf Webseiten Methoden versprochen, die angeblich ganz einfach einen Geldregen für den Leser bedeuten können. Die Aufmachungen dieser Seiten wechseln in unregelmäßigen Abständen, der Tenor bleibt jedoch immer gleich.

Screenshot 1: Eine Money Rain Kampagne von Beginn 2015

Angreifer nutzen für diese Art des Betrugs nicht nur Webseiten der Kategorie Gesundheit aus, aber 37% der Webseiten, die eindeutig mit Money Rain in Verbindung stehen, fallen in diese Kategorie.
Screenshot 1 zeigt eine Seite mit einer der Wellen dieser Masche, wobei organisatorische Ähnlichkeiten zu älteren Kampagnen bestehen, wie zum Beispiel die Nutzung des gleichen E-Mail Dienstes[3]. Die Kampagnen richten sich an Personen, die von zuhause aus arbeiten möchten und die mit mehr oder weniger seriösen Geldsegen-Versprechen gelockt werden.

In einer der dubiosen Geld-Kampagnen versuchen die Initiatoren sogar durch ein eigens erstelltes YouTube-Video dem ganzen Vorhaben einen seriöseren Ton zu verleihen. Im Stile einer Nachrichtensendung wird die „Breaking News" des angeblich schnellen Geldregens angepriesen, wie Screenshot 2 zeigt.

Eine weitere Überraschung ist das Themenfeld der Kategorie **Persönliche Werbung und Dating**, eine bisher noch nicht in Erscheinung getretene Kategorie. Hinter dieser Bezeichnung verbergen sich Webseiten, auf denen romantische oder sexuelle Kontakte geknüpft werden können, sowie gezielte Werbung zu kostenpflichtigen Services; wie etwa Premium-Rufnummern zu lokalen Diensten. In Verbindung mit Rang drei der aktuellen Auswertung, Pornographie, bedient sie das Klischee, dass Webseiten mit Inhalten für Erwachsene gefährlicher sind als andere. Diesen Mythos haben die Experten der G DATA SecurityLabs jedoch widerlegt.[4]
Gefährliche Webseiten lauern überall.

Screenshot 2: Das Video zeigt als „Breaking News", wie einfach das Geldverdienen angeblich ist

[3] G DATA SecurityBlog: https://blog.gdata.de/artikel/dubiose-casino-tipps-durch-spam-mails-verbreitet/
[4] G DATA SecurityBlog: https://blog.gdata.de/artikel/zwei-grosse-mythen-zur-it-sicherheit-entlarvt/

Kategorisierung nach Server-Standort

Wenn Angreifer Webseiten dafür nutzen, um bei Computernutzern Schaden durch Malware- oder Phishing-Attacken anzurichten, dann haben sie dafür vielfältige Möglichkeiten, denen aber immer eine von zwei Situationen zu Grunde liegt:

1) Die Angreifer haben eine legitime Webseite übernommen und attackieren die oft zahlreichen Besucher der Webseite. Sie schaden aber auch dem eigentlichen Betreiber – durch den Angriff auf die Infrastruktur, durch Reputationsverlust und evtl. auch finanziell durch erhöhten Traffic auf der Webseite.
2) Die Angreifer haben für ihren Zweck eine eigene Webseite aufgesetzt. Hierbei tragen sie die Kosten der Infrastruktur selbst und schaden in der Regel nur den potentiellen Opfern, die auf die Webseite gelockt oder geleitet werden. Im Untergrund bieten dubiose Dienstleister an, Besucher auf eine Webseite zu bringen. Das kostet für Tausende von Besuchern nur wenige Euro.

In die Kategorie 1 fallen dabei auch die sogenannten Malvertisement Kampagnen. Dieses Kunstwort setzt sich aus „Malware“ (= Schadsoftware) und „Advertisement“(=Werbung) zusammen und beschreibt das Verteilen von Malware über Werbenetzwerke. Im ersten Halbjahr 2015 ist dabei speziell der Missbrauch des **Google Adsense** Netzwerkes[5] ins Auge gefallen. Durch die weite Verbreitung dieses Werbedienstleisters wurden Seitenbesucher auch auf prominenten Seiten der Infektion durch das **Nuclear Exploit Kit** ausgesetzt. Dieser Fall unterstreicht erneut, dass Werbung nicht nur lästig ist, sondern auch gefährlich sein kann.

Die folgende Auswertung zeigt, wo auf der Welt die Mehrzahl der bösartigen Webseiten liegen, die in den G DATA SecurityLabs im ersten Halbjahr als schädlich oder betrügerisch gemeldet wurden. Die Lage der Webseite wird aus dem Standort der Server der Webseite ermittelt[6].

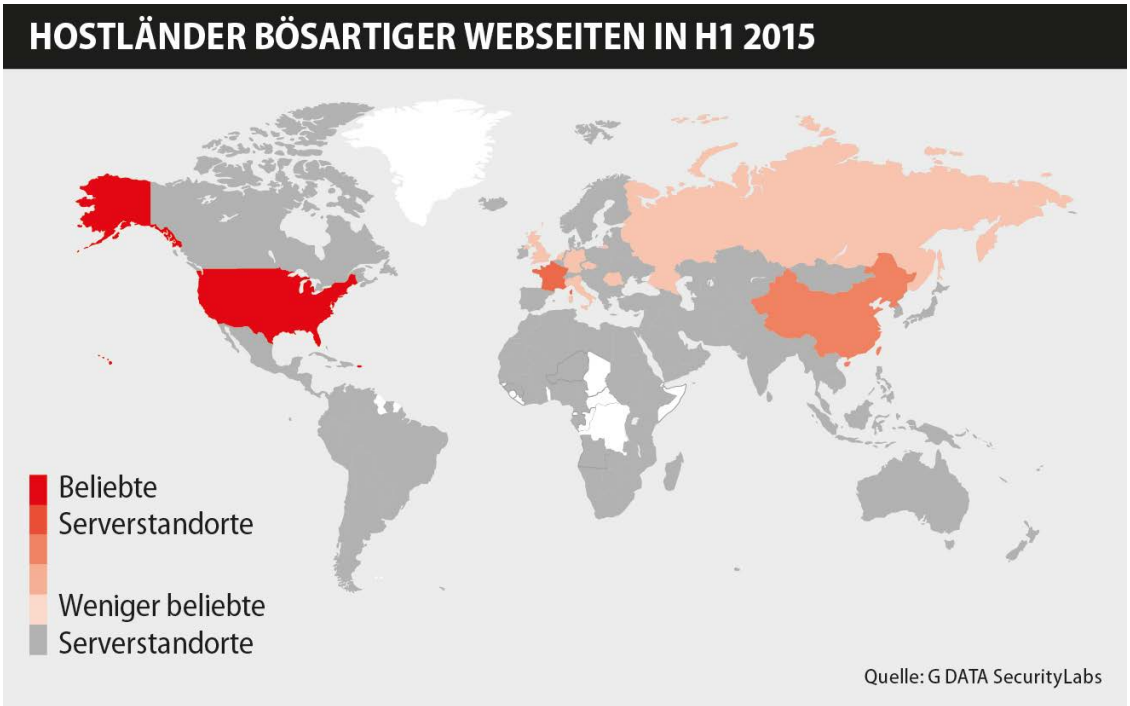

Abbildung 3: Hostländer bösartiger Webseiten

[5] G DATA SecurityBlog: https://blog.gdata.de/artikel/augen-auf-beim-bannerkauf-googles-werbedienst-zur-malwareverbreitung-missbraucht/
[6] Die Top-Level-Domain (z.B. „.de“ oder „.fr“) bezeichnet, wo der Domainname registriert wurde und wird hier nicht berücksichtigt. Es wird außerdem nicht unterschieden, ob es sich im eine gekaperte Seite oder eine speziell für einen Angriff angelegte handelt.

Einige Länder sind für Cyberkriminelle ein besonders attraktives Ziel, da dort sowohl die Infrastruktur als auch die Preise für Webspace sehr günstig sind. Auch die jeweils nationalen Gesetze in Bezug auf Cyberkriminalität und Dinge in diesem Zusammenhang spielen für Kriminelle und ihre Wahl eine Rolle. 43,3% aller bösartigen Webseiten lagen auf Servern in den **USA**. Dieser Wert ist damit quasi auf dem Stand des letzten Halbjahres. **China** wurde als Host-Land attraktiver und belegt nun Rang 2, mit 9,5%. **Frankreich** hingegen ist auf Platz 3 abgerutscht (8,2%). Insgesamt hat sich somit an den Top Platzierungen ebenso wenig geändert wie an den oben genannten Konditionen.

Interessant ist jedoch der vierte Platz. Die Experten der G DATA SecurityLabs konnten einen Anstieg von bösartigen Webseiten auf Servern in der **Ukraine** verzeichnen. In H1 2015 lag der Anteil bei 5% und bedeutet damit Rang 4 in der Liste. In den Vorjahren spielte die Ukraine in dieser Auswertung hingegen keine nennenswerte Rolle. Ein Zusammenhang mit der anhaltenden politischen Brisanz im **Ukraine**-Konflikt und den zahlreichen Medienberichten über einen Cyber-Krieg zwischen der **Ukraine** und Russland ist nicht auszuschließen.

BANKING

Trends auf dem Trojaner-Markt

Der Marktanteil der verschiedenen Familien von Banking-Trojanern variierte auch im ersten Halbjahr 2015. Es begann so, wie 2014 aufgehört hatte: Mit einer relativ hohen Anzahl an Infektionen durch die **Vawtrak**-Familie. Das Infektionsniveau von **Vawtrak** hat sich dann ab Mitte Februar etwa halbiert. Ebenfalls sank ab März die Präsenz von **Bebloh**, um dann im Juni in der Auswertung der G DATA SecurityLabs fast gänzlich bedeutungslos zu werden. Auch **Tinba** verlor ab April deutlich an Bedeutung. Gleichzeitig war **Gozi** im ersten Halbjahr 2015 seit längerer Zeit erstmalig wieder sichtbar. **ZeuS** mit seinen Varianten blieb auf dem bisher üblichen Niveau, wobei es im Juni eine Spitze der Variante **ZeuS-VM** gab.

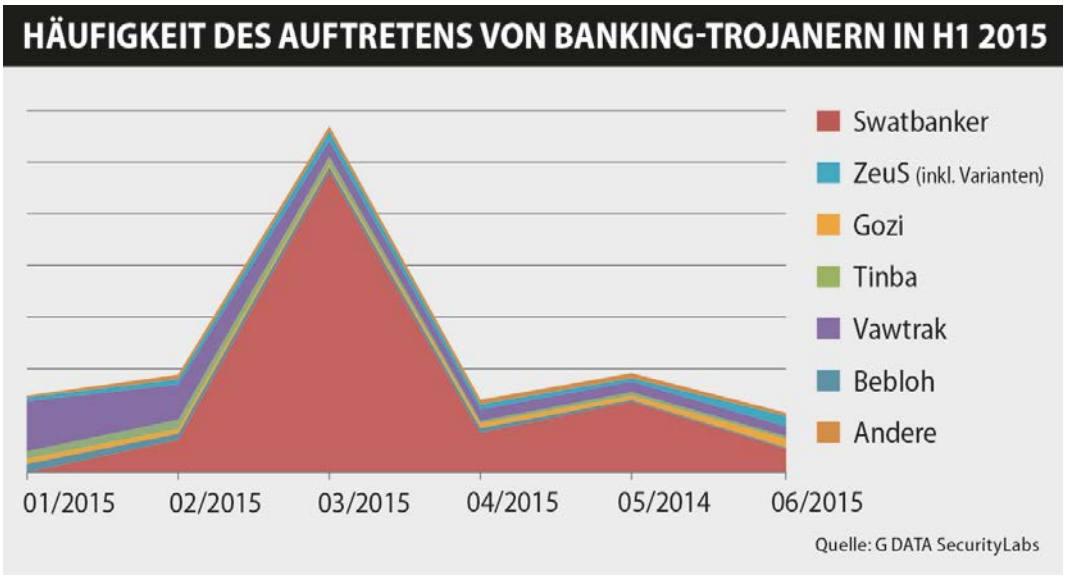

Abbildung 4: Häufigkeit von Banking-Trojanern

Die auffälligste Begebenheit im ersten Halbjahr 2015 begann ab Ende Februar, als eine neue Welle aus der Gruppe um **Swatbanker**, der **Cridex**-Gruppe, für Gefahr auf den PCs sorgte. Wellenartige Angriffe per E-Mail waren für diesen Trojaner bisher nicht ungewöhnlich, doch diese Welle war derart erfolgreich, dass im März 2015 die höchste Anzahl abgewehrter Angriffe von Banking-Trojanern seit Beginn der Aufzeichnungen gemessen wurde. Ungewöhnlich war auch, dass die Welle nicht wie üblich innerhalb einiger Wochen stoppte, sondern bis Mitte Juni anhielt. Kurz vor Ende der Angriffswelle gab es dabei außerdem noch einen weiteren ungewöhnlichen Vorfall: Die Angreifer hatten offenbar Rechner im **Intranet des Deutschen Bundestags** im Visier[7]. Ob ein Zusammenhang zum bereits zuvor bekannt gewordenen Angriff auf den **Bundestag**[8] besteht, ist nach wie vor unklar.

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.

[7] G DATA SecurityBlog: https://blog.gdata.de/artikel/banking-trojaner-hat-deutschen-bundestag-im-visier/
[8] https://de.wikipedia.org/wiki/Cyberattacken_auf_den_Deutschen_Bundestag

Wenn man die Anzahl der Vorfälle so normalisiert, dass alle Trojaner-Familien gleich häufig auftreten, ergibt sich ein ähnliches Bild wie im letzten Halbjahr. In diesem Falle stammen die 20 häufigsten Ziele mit der höchsten Angriffswahrscheinlichkeit – mit Ausnahme zweier spanischer Banken – ausschließlich aus dem anglophonen Sprachraum. Auf Platz 1 der Liste findet sich **Wells Fargo**. Neben Banken sind das Auktionsportal **eBay** und der Zahlungsdienstleister **PayPal** in der Liste vertreten (vgl. Tabelle 2).

Da das abgelaufene Halbjahr insgesamt von der oben beschriebenen **Swatbanker**-Welle dominiert wurde, entsprechen die 20 Ziele von **Swatbanker** exakt den 20 gefährdetsten Zielen insgesamt, wenn die von G DATA beobachtete Verteilung der Trojaner zugrunde gelegt wird. **Swatbanker** greift dabei ausschließlich Banken aus Deutschland, Österreich und Polen an. Das Angriffsziel mit der insgesamt höchsten Angriffswahrscheinlichkeit bei Infektion mit einem Banking-Trojaner war das Portal fiducia.de der Volksbanken, dicht gefolgt von den weiteren **Swatbanker**-Zielen (vgl. Tabelle 3).

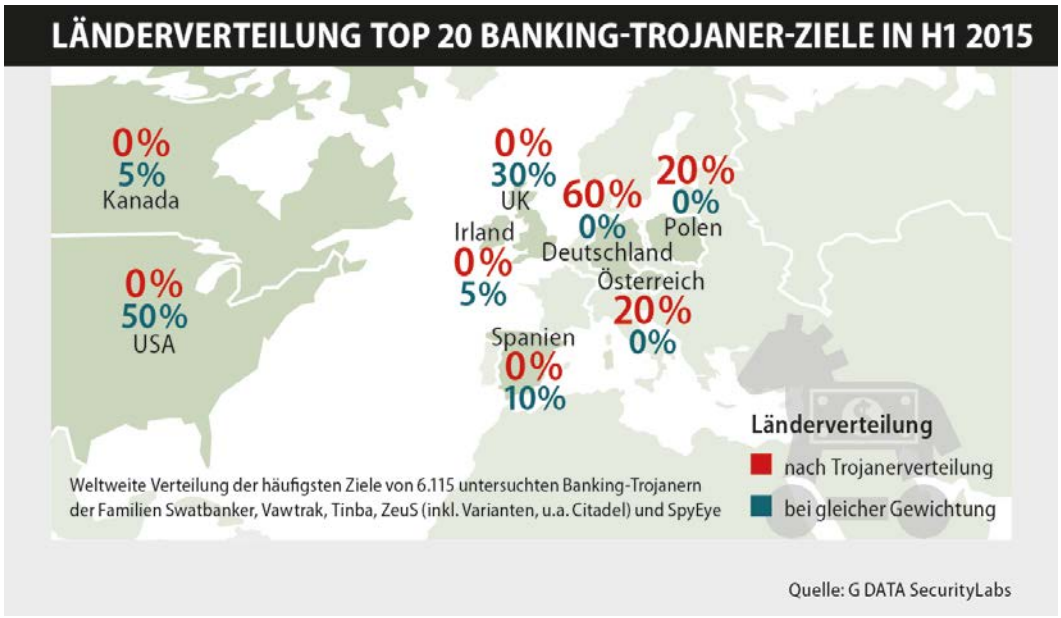

Abbildung 5: Länderverteilung der Top 20 Banking-Trojaner-Ziele

Methodik

Die Analyse-Methodik wurde für diesen Malware-Report aktualisiert. Die Liste der unterstützten Banking-Trojaner-Familien wurde auf folgende Familien erweitert: **Swatbanker**, **Vawtrak**, **Tinba**, **ZeuS** (inkl. Varianten, u.a. **Citadel**) und **SpyEye**. Insgesamt wurden 6.115 Konfigurationsdateien entschlüsselt und analysiert. In den Konfigurationsdateien befindet sich eine Liste von Zielseiten (d.h. Webseiten von Banken, Bezahldienstleistern etc.), die mit speziellem Schadcode (sog. Webinjects) angegriffen werden[9]. Einmal wurde dabei angenommen, dass alle Trojaner gleichverteilt auftreten (vgl. Tabelle 2). Für die Grafik nach Trojaner-Verteilung wurde auch der Verbreitungsgrad der jeweiligen Trojaner-Familie einbezogen (vgl.).

[9] 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.

Der errechnete prozentuale Wert entspricht der Wahrscheinlichkeit, dass ein Ziel bei Infektion mit einem Banking-Trojaner auch in der Liste der Angriffsziele steht. Den Top 20 wurden zudem Herkunftsländer zugeordnet (vgl. Abbildung 5)[10].

TOP 20 DER ANGRIFFSZIELE VON BANKING-TROJANERN IN H1 2015 (TROJANER GLEICH GEWICHTET)

	Land	Rating Markenwert nach Brand Finance	Angriffswahrscheinlichkeit Basierend auf der Analyse von 6.115 Banking-Trojanern der Familien Swatbanker, Vawtrak, Tinba, ZeuS (inkl. Varianten), SpyEye
Wells Fargo wellsfargo.com		1	35,28 %
HSBC hsbc.co.uk, hsbc.com, hsbc.com.hk, ...		3	34,07 %
Lloyds Banking Group lloydstsb.co.uk, halifax-online.co.uk, ...		35	32,13 %
Barclays barclays.co.uk		13	30,05 %
RBS Group (RBS, NatWest, Ulster) nwolb.com, rbsdigital.com, ...		60	27,92 %
PayPal paypal.com, paypal.co, paypal.com.mx		-	27,55 %
Bank of America bankofamerica.com		6	27,32 %
Chase chase.com, chasecanada.ca, chaseonline.com		7	27,08 %
Citi citibank.com, citibank.com.au, citibank.com.sg		5	25,98 %
TD Bank tdcanadatrust.com		18	24,18 %
U.S. Bancorp usbank.com		46	24,04 %
Citizens Bank citizensbankonline.com		264	23,20 %
smile smile.co.uk		-	22,60 %
Fifth Third Bank 53.com		111	22,11 %
The Co-operative bank co-operativebank.co.uk		114	22,02 %
BBVA bbvanetoffice.com, bbva.es, ...		28	21,47 %
SunTrust suntrust.com		93	20,61 %
eBay ebay.com, ebay.de, ebay.co.uk, ebay.ca, ...		-	20,10 %
Santander ES gruposantander.es		10	19,79 %
Allied Irish Banks aib.ie		181	19,77 %

Kategorie: = Bank = E-Payment = Auktion

Quelle: G DATA SecurityLabs

Tabelle 2: Top 20 Angriffsziele von Banking-Trojanern (Trojaner gleich gewichtet)

[10] 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 Brand zu Grunde gelegt.

TOP 20 DER ANGRIFFSZIELE VON BANKING-TROJANERN IN H1 2015 (NACH TROJANERVERTEILUNG)

	Land	Rating Markenwert nach Brand Finance	Angriffswahrscheinlichkeit Basierend auf der Analyse von 6.115 Banking-Trojanern der Familien Swatbanker, Vawtrak, Tinba, ZeuS (inkl. Varianten), SpyEye
Volksbanken (Fiducia) fiducia.de		42	71,91 %
Deutsche Bank Gruppe deutsche-bank.de, norisbank.de, ...		19	71,90 %
GE Capital gecapital.de		-	71,88 %
Targobank targobank.de		77	71,80 %
Flessabank flessabank.de		-	71,77 %
Bank1Saar bank1saar.de		42	71,77 %
Commerzbank commerzbanking.de, commerzbank.de, ...		75	71,77 %
Sparda-Banken sparda.de		42	71,77 %
PKO Bank ipko.pl		115	70,61 %
mBank mbank.pl		310	70,55 %
ING PL ingbank.pl		26	70,55%
Citi PL citibankonline.pl		5	70,55 %
DKB dkb.de		176	70,44 %
Sparkassen DE berliner-sparkasse.de, haspa.de, ...		174	69,84 %
Volksbanken (GAD) gad.de		42	69,77 %
comdirect comdirect.de		75	69,76 %
Bank Austria bankaustria.at		152	69,76 %
BAWAG PSK bawagpsk.com		322	69,76 %
Sparkasse AT sparkasse.at		78	69,76 %
Raiffeisen raiffeisen.at		110	59,99 %

Kategorie: = Bank = E-Payment = Auktion

Quelle: G DATA SecurityLabs

Tabelle 3: Top 20 Angriffsziele von Banking-Trojanern (nach Trojaner-Verteilung)

G DATA BankGuard verhindert Schäden von über 100 Millionen Euro

Gegen Banking-Trojaner werden Kunden von G DATA durch die seit April 2011 eingesetzte und mittlerweile patentierte[11] BankGuard-Technologie geschützt. Jedes Jahr wehrt BankGuard zehntausende Angriffsversuche ab. Bis zum Ende des ersten Halbjahres 2015 waren es insgesamt 182.457 vereitelte Angriffe.

In einer Studie von **Google** wurde für vergleichbare Angriffe eine durchschnittliche Erfolgswahrscheinlichkeit von 13,78% errechnet[12]. Gleichzeitig geht das **deutsche Bundeskriminalamt** von einer durchschnittlichen Schadenssumme von rund 4.000€ pro Fall aus.[13] Nimmt man diese Zahlen als Grundlage, übersteigt die Summe der durch BankGuard verhinderten Schäden nun die Marke von 100 Millionen Euro (100.570.298,40€).

In Abbildung 6 ist zu erkennen, dass die Fallzahlen bei Hochrechnung des bisherigen Halbjahres auf das gesamte Jahr erstmalig seit 2012 wieder steigen. Verantwortlich ist dabei allen voran **Swatbanker** aus der **Cridex**-Familie, der in immer neuen Wellen seit Januar Kunden von Banken in **Deutschland**, **Österreich** und **Polen** angreift. Deren Kunden müssen im Moment als besonders gefährdet angesehen werden. Danach folgen Banken aus dem **englischen Sprachraum** als Angriffsziel. Wichtigster Akteur ist hier **Vawtrak**.

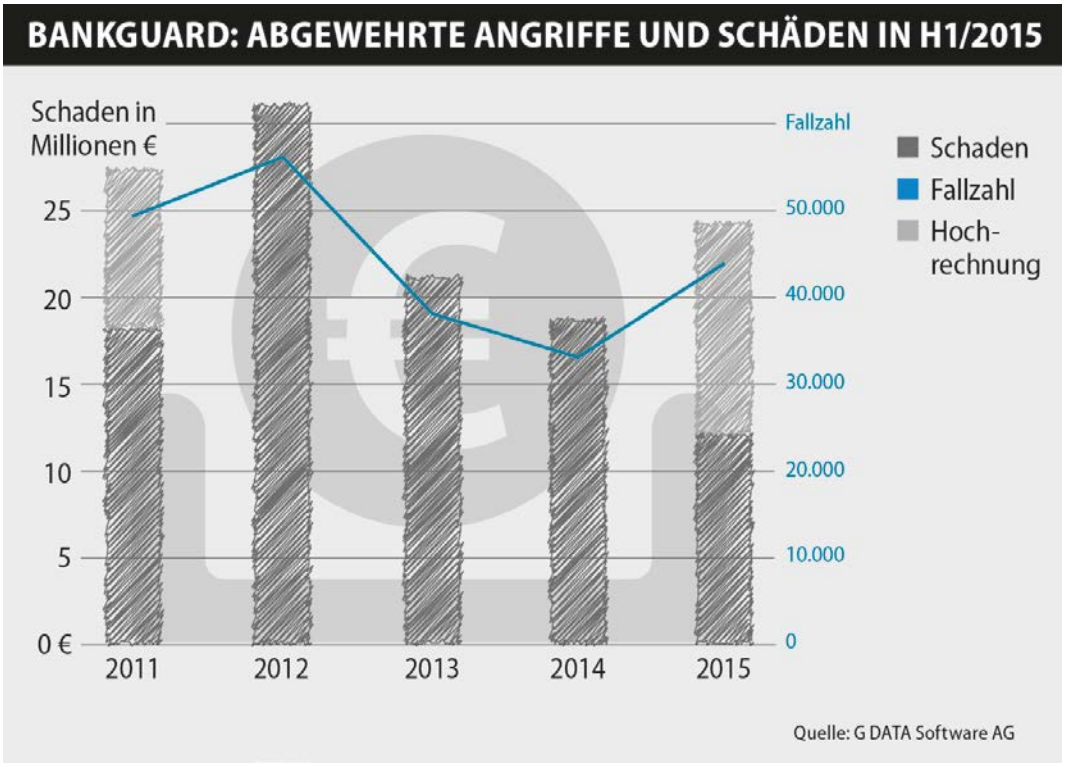

Abbildung 6: Abgewehrte Angriffe und Schäden

[11] Patent-Nr. US8898781
[12] http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf
[13] http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

EXPLOIT KITS

G Datas Exploit Protection bietet einen generischen Schutz gegen das automatisierte Ausnutzen von Sicherheitslücken. Solche Exploits werden in Untergrundforen in konkurrierenden Produktlinien – sogenannte Exploit Kits – zum Kauf angeboten. Die Analyse der abgewehrten Angriffe zeigt, dass im ersten Halbjahr 2015 drei Exploit Kits besonders dominant waren: Angler, Nuclear und Neutrino. Andere Exploit Kits, von denen Angriffsversuche registriert wurden, waren RIG, Sweet Orange, Magnitude, Niteris, Fiesta und Huanjuan.

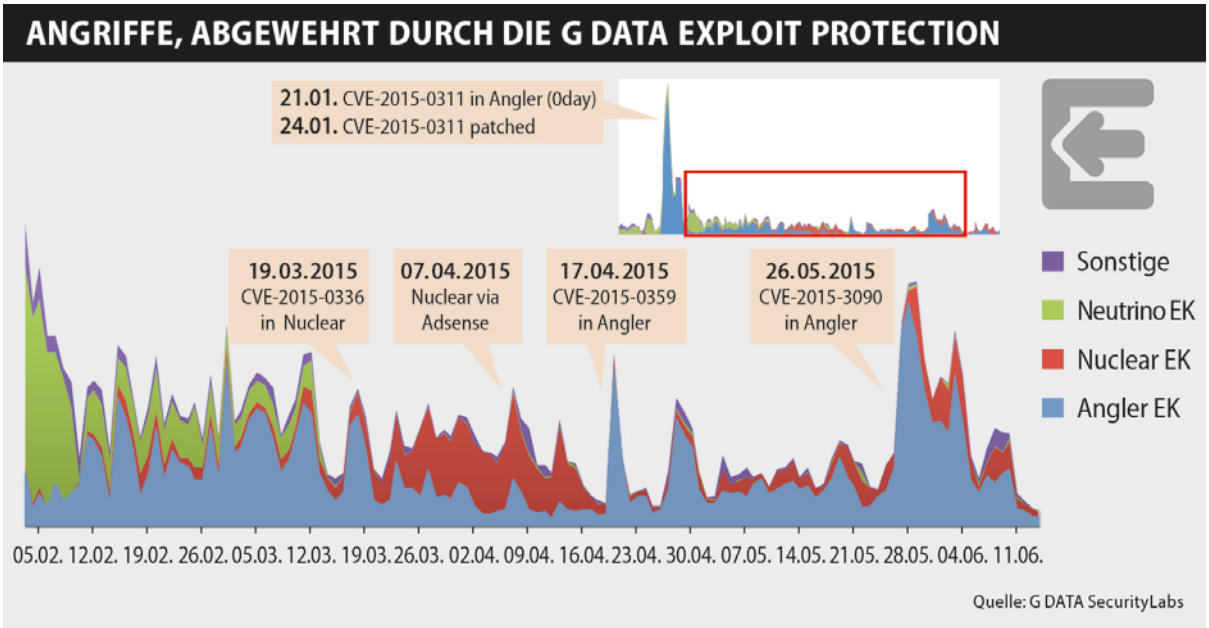

Abbildung 7: Durch die G DATA Exploit Protection abgewehrte Angriffe

Im Fokus der Angreifer stand in diesem Halbjahr durchgehend Adobe Flash. Das bedeutet, dass für diese Plattform besonders viele Exploits entwickelt wurden, da die Erfolgschancen auf eine PC-Infektion besonders hoch waren. Zuvor machte vor allem Java durch immer wieder neu auftauchende Sicherheitslücken von sich reden. Die Attraktivität von Java dürfte aber allein deshalb abgenommen haben, da die Browser hier immer mehr Schutzfunktionen eingebaut haben. So wird in Firefox seit der Version 26, die Ende 2013 erschien, standardmäßig „Click-to-Play" aktiviert[14]. Das bedeutet, dass Benutzer vor der Ausführung von Java-Applets bestätigen müssen, dass der Nutzer die Ausführung wirklich wünscht. Da Angreifer jedoch bei Exploit Kits darauf setzen, dass die Drive-By-Infection für den Benutzer unsichtbar im Hintergrund und ohne notwendige Nutzerinteraktion passieren, wird Java durch diese Neuerung für die Angreifer weniger attraktiv. Bei Google Chrome ist Click-to-Play für Java-Applets sogar schon länger der Standard. Seit Chrome Version 42 vom April 2015 wurde die Java-Unterstützung sogar komplett eingestellt.[15] Im Internet Explorer wurde zwar kein generelles Click-to-Play für Java implementiert, zumindest wird aber die Ausführung von veralteten Versionen seit August 2014 verhindert.[16]

Die Angreifer wechselten daraufhin zu Adobe Flash als bevorzugten Angriffsvektor. Hier gibt es in der Standardkonfiguration der Browser noch kein „Click-to-Play", dafür aber eine hinreichend große Zahl von Sicherheitslücken und Programmfehlern, sogenannte Bugs. Diese können ausgenutzt werden, um Rechner zu infizieren und übernehmen, was im Englischen als „to exploit" bezeichnet wird. Die benutzten Exploits können

[14] https://bugzilla.mozilla.org/show_bug.cgi?id=914690
[15] https://www.java.com/de/download/faq/chrome.xml
[16] http://blogs.msdn.com/b/ie/archive/2014/08/06/internet-explorer-begins-blocking-out-of-date-activex-controls.aspx

zudem sehr zuverlässig auch die Sicherheitsmaßnahmen aktueller Windows-Versionen wie DEP, ASLR und CFG umgehen[17]. Flash-Exploits sind dabei über die Browsergrenzen hinweg funktionsfähig.

Die deutlich größte Anzahl abgewehrter Angriffe im ersten Halbjahr geht auf eine Kampagne des **Angler Exploit Kits** im Januar zurück. Seit dem 21. Januar wurde eine bis dahin unbekannte und nicht geschlossene Flash-Schwachstelle mit der Bezeichnung **CVE-2015-0311**/APSB15-03[18] allen Nutzern des Kits verfügbar gemacht. Die Rekorde bei den abgewehrten Angriffen zeigen, wie gefährlich solche Zero-Day-Exploits sind. Am 24. Januar wurde von Adobe das passende Update 16.0.0.296 veröffentlicht, mit dem die Schwachstelle beseitigt wurde. Kurz danach, Anfang Februar, wurde der Exploit zu dieser inzwischen geschlossenen Lücke und auch einige ältere Flash-Exploits ins **Neutrino-Kit** aufgenommen. Selbst zu diesem Zeitpunkt wurden noch relativ hohe Infektionszahlen erreicht. Viele Computernutzer hatten ihre Version des Adobe-Produkts noch nicht auf den aktuellsten Stand gebracht und blieben so anfällig für diesen Angriff.

Ein weiterer Zero-Day-Angriff auf Flash erfolgte seit dem 13. Januar durch das **Exploit Kit Huanjuan** über die Schwachstelle **CVE-2015-0313**/APSB15-02[18]. Die Anzahl betroffener Nutzer war aber gering.

Bemerkenswert ist außerdem eine Kampagne des **Nuclear Exploit Kits**. Die bereits am 12. März durch Adobe gepatchte Sicherheitslücke wurde ab dem 19. März vom **Nuclear Exploit Kit** genutzt. Hier gelang es den Angreifern die Exploits über das **Google AdSense** Netzwerk zu verbreiten. Diese äußerst populäre Werbeplattform wird von vielen Anbietern populärer Webseiten genutzt. In diesem Fall führten die Werbeeinblendungen dazu, dass Webseitenbesucher angegriffen wurden. Dieser Coup zeigt sich in einem deutlichen Peak bei den abgewehrten Angriffen.[19]

Im weiteren Verlauf des Halbjahres wurden immer wieder Flash-Schwachstellen identifiziert. In Exploit Kits wurden diese allerdings immer erst kurz nach Veröffentlichung eines Patches zur Behebung durch Adobe veröffentlicht. Es waren also lediglich Benutzer ohne Patch betroffen, was erneut verdeutlicht, wie wichtig das zeitnahe Einspielen von offiziellen Updates und Patches für Computernutzer ist.

So wurde am 14. April die Schwachstelle **CVE-2015-0359**/APSB15-06[18] von Adobe behoben, jedoch nur drei Tage später, am 17. April in **Angler** und am 27. April in **Neutrino** integriert. Am 12. Mai wurde die Sicherheitslücke **CVE-2015-3090**/APSB15-09[18] geschlossen. Wieder integrierte zuerst **Angler** am 26. Mai einen Exploit, und wieder zog **Neutrino** wenig später, am 29. Mai nach. Als nächstes wurde unter anderem die Kombination aus **CVE-2015-3104** und **-3105**/APSB15-11[18] von Adobe behoben. Dem Patch vom 3. Juni folgte in diesem Fall die Integration in das **Magnitude Exploit Kit** am 16. Juni. Der letzte Patch des Halbjahres durch Adobe wurde am 23. Juni für **CVE-2015-3113**/APSB15-14[18] veröffentlicht. Die Erstintegration erfolgte vier Tage später am 27. Juni abermals durch das **Magnitude Exploit Kit**, zwei Tage später folgte **Angler**.

Fazit und Ausblick

Angriffe auf Adobe Flash stellten im ersten Halbjahr 2015 die größte Bedrohung für Nutzer des WWW dar. Besonders effektiv in der Ausnutzung zeigte sich dabei das **Angler Exploit Kit**, insbesondere beim herausragenden Angriff mittels Zero-Day-Exploit im Januar. Daneben spielte bis Mitte März **Neutrino** eine Rolle, wurde dann aber zunehmend von **Nuclear** abgelöst. Da die **Angler**-Hintermänner sehr effektiv vorgehen und ihr Exploit Kit in sehr kurzen Zyklen aktualisieren, ist auch im zweiten Halbjahr von einer tragenden Rolle auszugehen.

[17] https://blog.coresecurity.com/2015/03/04/exploiting-cve-2015-0311-a-use-after-free-in-adobe-flash-player/
[18] https://helpx.adobe.com/de/security/products/flash-player.html
[19] G DATA SecurityBlog: https://blog.gdata.de/artikel/augen-auf-beim-bannerkauf-googles-werbedienst-zur-malwareverbreitung-missbraucht/