TRUST IN
GERMAN
SICHERHEIT

G DATA SECURITYLABS MALWARE REPORT

HALBJAHRESBERICHT
JULI – DEZEMBER 2014

INHALT

AUF EINEN BLICK

- Die Zahl neuer Schadprogrammtypen ist im zweiten Halbjahr (H2) enorm gestiegen; es wurden 4.150.068 gezählt. In ersten Halbjahr 2014 waren es 1.848.617 und somit verzeichneten die Experten eine Steigerung der um knapp 125%.
- Insgesamt brachte das Jahr 2014 also insgesamt 5.998.685 neue Schadprogrammtypen hervor. Das sind im Vergleich zur Gesamtzahl von 2013 77% mehr.
- Statistisch wurde in H2 2014 alle 3,75 Sekunden ein neuer Schadprogrammtyp entdeckt.

- Die Kategorie Adware hat erneut die höchsten Zuwachsraten. Der Anteil an neuen Adware-Signaturvarianten lag in H2 bei 31,4 Prozent. Somit ist fast jede dritte neue Erkennung aus diesem Bereich.
- Die absoluten Zahlen der neuen Adware-Schadprogrammtypen haben die Kategorie Downloader sogar überflügelt und liegen jetzt auf Rang 2.
- Mit Hilfe der Malware Information Initiative (kurz MII) gelingt ein Blick auf die abgewehrten Angriffe auf Computernutzer: Adware liegt auch hier an der Spitze der Gefahren. Die Schädlinge der Familie Browsefox/Browserfox treten hier besonders in den Vordergrund.
- Die Zahl der neuen Signaturvarianten für Rootkits nahm wieder zu. Sie werden häufig verwendet wenn Angreifer Zombie-PCs in ihre Botnetze integrieren, damit Komponenten der Malware auf dem PC verborgen bleiben.

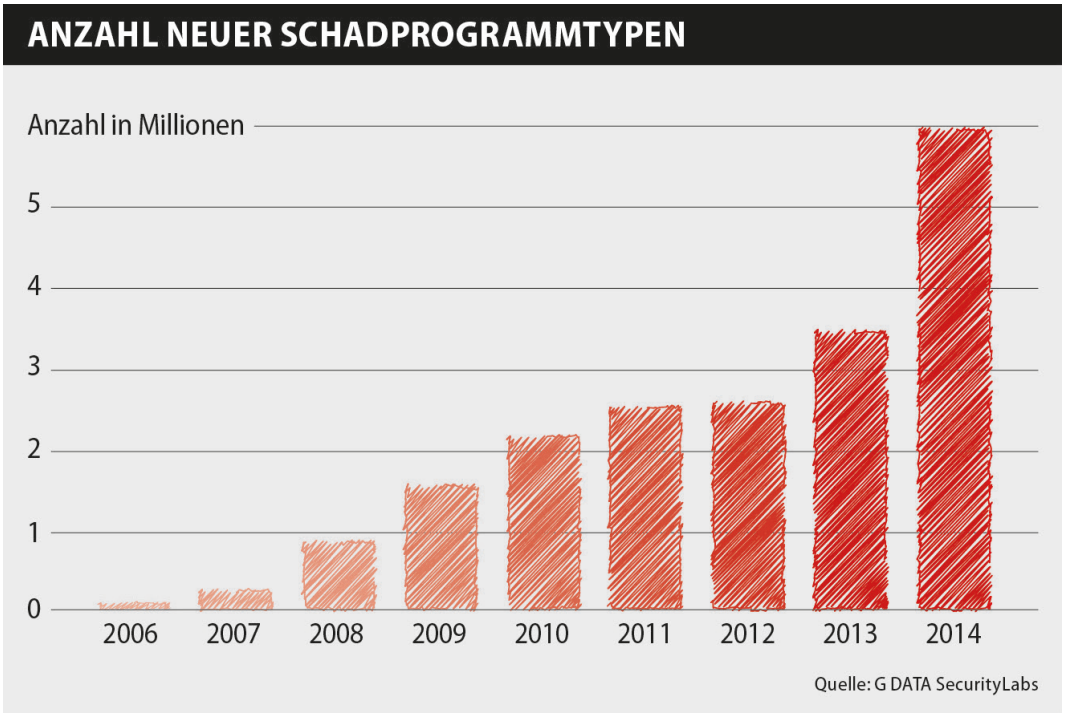
- Der Banking-Trojaner Vawtrak bleibt weiterhin ein sehr aktiver Schädling und behauptet sich seit dem Frühjahr 2014.
- Die Hürden für Cyberkriminelle werden durch neue Sicherheitsmaßnahmen der Banken und Bezahldienstleister immer höher gelegt und auch das Risiko, durch Strafverfolgungsbehörden erwischt zu werden, steigt.
- In H2 2014 wurden wenige Neuerungen im Bereich der Banking-Trojaner verzeichnet, die bestehende Gefahr ist deswegen aber nicht geringer einzustufen: Die Zahl der abgewehrten Angriffe stieg um 44,5 Prozent an! Das spricht eher für eine Konsolidierung des Marktes für Banking-Schädlinge.
- Die erneute Untersuchung der häufigsten Angriffsziele von Banking-Trojanern zeigte im zweiten Halbjahr sieben neue Ziele in den Top25, unter anderem in diesem Halbjahr auch eine Bank aus Frankreich.
- Dienstleister aus dem anglophonen Sprachraum stehen dabei weiterhin im Mittelpunkt: 36 Prozent der Ziele stammen aus den USA, 24% aus dem Vereinigten Königreich und 12% aus Kanada.

Prognosen und Trends

- Die Experten gehen davon aus, dass Angreifer in Zukunft aus reinen Phishing-Attacken multiple Angriffe machen, die auch Malware einbeziehen. Dann würden potentielle Phishing-Opfer auf den Phishing-Seiten nicht nur durch Social Engineering behelligt, sondern möglicherweise auch durch Exploit-Kits angegriffen.

SCHADPROGRAMM-STATISTIKEN

Die zweite Jahreshälfte 2014 hat erneut alle bisherigen Rekorde gebrochen und übertrifft die Vorhersagen der Experten um Längen. Die G DATA SecurityLabs verzeichneten in diesen sechs Monaten 4.150.068 neue Schadprogrammtypen[1]! Das ist fast das 2,3-fache des Ergebnisses aus dem ersten Halbjahr und sogar mehr als die Gesamtzahl 2013. Insgesamt wurden in 2014 knapp sechs Millionen neue Schadprogrammtypen registriert (5.998.685).



Kategorien

Ein Schädling wird aufgrund von registrierten schädlichen Aktionen auf einem System in eine Kategorie eingeordnet. Der Blick darauf lässt eine Einschätzung darüber zu, in welche Art von Angriffen aktuell besonders massiv von den Cyber-Angreifern investiert wird.

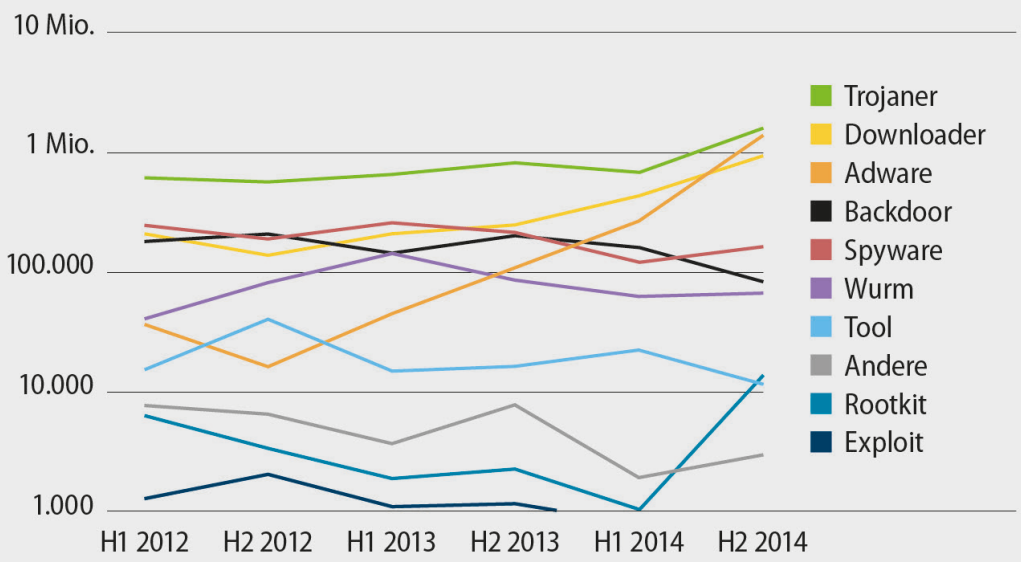
In diesem vergangenen Halbjahr wurde in nahezu allen Kategorien ein Anstieg der neuen Signaturvarianten verzeichnet, insofern ist nicht eine alleine für den rapiden Anstieg verantwortlich. Jedoch sind einige der Bereiche deutlich mehr angestiegen als andere.

Vor allem **Adware** hat zugelegt. Ihr Anteil an allen Kategorien betrug in H2 2014 31,4 Prozent, gegenüber 14,1 Prozent in H1 2014, und ihre Anzahl hat sich sogar verfünffacht. Adware hat die Downloader in dieser Untersuchung überholt und belegt nun hinter den Trojanischen Pferden Platz 2 in der Auswertung.

Ein Trend, der sich weiterhin fortsetzt und sogar noch Fahrt aufnimmt, ist das Verpacken (Bundling) von legitimer Software mit potentiell unerwünschten Programmen (PUP) von Drittanbietern. Auch in den Statistiken der von G DATA abgewehrten Angriffe liegen die Adware-Schädlinge weiter deutlich vorne, wie im Kapitel Gefahren-Monitor zu lesen ist.

[1] Die Zahlen in diesem Report basieren auf der Erkennung von Malware anhand von Virensignaturen. Sie basieren auf Ähnlichkeiten im Code von Schaddateien. Viele Schadcodes ähneln sich und werden dann in Familien zusammengefasst, in denen kleinere Abweichungen als Variationen erfasst werden. Grundlegend unterschiedliche Dateien begründen eigene Familien. Die Zählung basiert auf neuen Signaturvarianten, auch Schadprogrammtypen genannt, die im zweiten Halbjahr 2014 erstellt wurden.

ENTWICKLUNG VON SCHADCODEKATEGORIEN



Quelle: G DATA SecurityLabs

Einen Anstieg gab es auch bei **Rootkits**[2] fallen ebenfalls durch hohe Zahlen auf: die Experten zählten 18 Mal mehr neue Signaturvarianten als im ersten Halbjahr 2014 und ihr Anteil stieg auch deutlich, bleibt jedoch trotzdem bei nur 0,45% aller ausgewerteten Kategorien stehen. Die Zahlen der **Trojaner** und auch der **Downloader**, in den bisherigen Untersuchungen lange auf Platz 1 und 2 in der Übersicht, haben sich jeweils etwa verdoppelt, ihre Anteile blieben jedoch nahezu gleich. Wollen Angreifer neue Rechner zur späteren Nutzung in ihre Botnetze[3] integrieren, dann sind diese drei zuletzt genannten Kategorien sind sehr häufig als die Komponenten einer solchen Attacke involviert.

Das passiert bei einer Infektion mit Botnetz-Malware:
Angreifer verleiten einen Anwender dazu, ein Schadprogramm auszuführen, z.B. durch Social Engineering. Dazu verpacken sie z.B. ihren Schadcode in eine legitim aussehende Datei und verteilen dieses sogenannte **Trojanische Pferd** an möglichst viele Nutzer – per E-Mail, als angeblich interessantes Video/Programm, brandneues und peinliches Foto von Freunden, als angebliche Rechnung oder ähnliches.
Der verpackte Schadcode kann dabei alles Mögliche sein, vom Banking-Trojaner über Spam-Bots bis hin zu Backdoors, Spyware und Co. Häufig verpacken die Angreifer **Downloader**, als zweite Stufe ihres Angriffs. Downloader haben die Aufgabe, einen oder mehrere Server zu kontaktieren und von ihnen dann dort hinterlegte Informationen und/oder Dateien abzuholen. Der Vorteil für den Angreifer: Er kann die Dateien auf den Servern flexibel austauschen und muss sein Trojanisches Pferd nicht für jede Angriffswelle verändern.
Auch **Rootkits** sind häufig Teil des verpackten Schadcodes oder des nachgeladenen Codes. Sie werden dazu genutzt, den Schädling langfristig auf dem PC einzunisten und so gut wie möglich vor Scannern und Wächtern zu verstecken.

Im Jahr 2014 stieg die Zahl der mit Botnetz-Malware infizierten Systeme auf 40% an (33% in 2013).[4] Dies ist eine mögliche Erklärung für die so stark gestiegenen Zahlen des zweiten Halbjahres. Gerade nach dem ausgelaufenen Support für Microsoft Windows XP im April 2014 können besonders die noch immer mit diesem Betriebssystem ausgestatteten Systeme ein Herd für Malware sein und als Zombies eingesetzt werden, da sie gegen Angriffe auf vorhandene, bzw. neu entdeckte Sicherheitslücken weitgehend schutzlos sind.

Außerdem erreichte auch die Zahl der registrierten Angriffe durch Banking-Trojaner in H2 2014 ein Hoch, was im Banking-Teil dieses Reports näher beleuchtet wird.

[2] https://www.gdata.de/securitylabs/was-ist-eigentlich/rootkits
[3] https://www.gdata.de/securitylabs/was-ist-eigentlich/botnetze
[4] https://www.eco.de/2015/pressemeldungen/botfrei-de-jahresstatistik-2014-wieder-mehr-zombierechner-am-netz.html

Plattformen – .NET-Entwicklungen weiter auf dem Vormarsch

Die Programmierung von Schadcode als .NET-Anwendung hat auch im vergangenen Halbjahr dafür gesorgt, dass der Anteil von Signaturvarianten zur Plattform MSIL weiter hoch bleibt. Insgesamt machen neue Schädlingsvarianten für die Windowsplattformen einen Anteil von 99,9% aus.

	Plattform	#2014 H2	Anteil	#2014 H1	Anteil	Differenz #2014 H2 #2014 H1	Differenz #2014 H2 #2013 H2
1	Win	3.868.902	93,2%	1.688.719	91,4%	+129,1%	+118,1%
2	MSIL	279.207	6,7%	158.127	8,5%	+76,6%	+185,8%
3	NSIS	757	<0,1%	399	<0,1%	+89,8%	+200,7%
4	Scripts[5]	562	<0,1%	551	<0,1%	+2,1%	-12,5%
5	WebScripts	464	<0,1%	598	<0,1%	-22,4%	-35,5%

Tabelle 1: Top 5 der Plattformen der letzten beiden Halbjahre

GEFAHREN-MONITOR

Der Gefahren-Monitor gibt die Top 10 der abgewehrten Angriffe gegen Computernutzer[6] mit G DATA Sicherheitslösungen[7] und aktiviertem Feedback[8] an. Nachfolgend werden die am häufigsten abgewehrten Attacken aus dem zweiten Halbjahr 2014 dargestellt. Die Aufstellung der einzelnen Monate ist immer aktuell auf der G DATA SecurityLabs Webseite[9] zu finden.

Rang	Name	Prozent
1	Gen:Variant.Adware.SwiftBrowse.1	26,9%
2	Win32.Adware.Browserfox.H	7,8%
3	Gen:Variant.Adware.Graftor.159320	6,3%
4	Adware.Mplug.AF	6,0%
5	Adware.BrowseFox.D	5,5%
6	Adware.BrowseFox.H	4,2%
7	Script.Adware.DealPly.G	3,6%
8	Gen:Variant.Adware.Graftor.159134	2,4%
9	Script.Application.Plush.D	1,7%
10	Adware.RelevantKnowledge.A	0,8%

Tabelle 2: Die Top 10 der an die MII gemeldeten Angriffe in H2 2014

[5] Scripts sind Batch- oder Shell-Skripte oder Programme, die z.B. in den Skriptsprachen VB, Perl, Python oder Ruby geschrieben wurden.

[6] Die Zählweise in diesem Kapitel unterscheidet sich von dem vorherigen Kapitel, 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 sie Familie wenige (neue) Varianten hervorbringt.

[7] Seit Januar 2014 beziehen sich diese Statistiken ausschließlich auf die Scanner-Kombination aus G DATA CloseGap und Bitdefender.

[8] 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 aktiviert haben. 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.

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

Auch im zweiten Halbjahr des Jahres 2014 dominieren „Potentiell Unerwünschte Programme“ (PUP) die Statistiken der häufigsten Angriffe. Zwar zeigen sich die oben aufgeführten Top 10 „nur“ für 65% verantwortlich, was ein Minus von 6,8% zum vorherigen Halbjahr bedeutet, jedoch schmälert das keinesfalls das deutliche Übergewicht dieser Angriffe. Die Gesamtzahl der Angriffe gegen Computernutzer ist jedoch deutlich gestiegen, was die sinkenden Anteile erklärt.

Gen:Variant.Adware.SwiftBrowse.1 ist ein Vertreter einer hochvariablen Schädlingsfamilie und hat mit Blick auf die absoluten Angriffszahlen im Vergleich zum vorherigen Halbjahr vergleichsweise geringe Minuswerte, büßte damit beim Anteil jedoch ein, von 55,8% auf 26,9% aller registrierten Angriffe. Er injiziert ein JavaScript in den Browser, um potentiell unerwünschte, zusätzliche Werbung, Banner, Coupon-Werbung, Vergleichsangebote anderer Web-Shops oder ähnliches anzuzeigen. Dabei sind die Anzeigen gemeinhin penetrant und belästigend. Weitere Details zu dieser Familie wurden bereits im G DATA Malware Report H1 2014 veröffentlicht.

Die absolute Zahl der Angriffe durch **Script.Application.Plush.D** ist innerhalb der letzten sechs Monate um knapp ein Drittel gestiegen, der Anteil bleibt gleich. Alle anderen Vertreter der aufgelisteten Top 10 sind Neueinsteiger.

Die Schädlinge der **Familie BrowseFox/Browserfox** stechen in diesem abgelaufenen Halbjahr hervor, mit drei Varianten unter den ersten sechs Rängen. Die Schädlinge installieren Plug-Ins in Microsofts Internet Explorer, Mozilla Firefox und Googles Chrome, welche die Browsereinstellungen verändern, um Angreifern Profite zu generieren. Die Plug-Ins verändern die Startseite, ebenso wie die vom Benutzer eingestellte Suchmaschine. Auch die Sicherheitseinstellungen des Browsers werden manipuliert, um Injektionen zu ermöglichen: Während der Browsernutzung, werden JavaScripts in aufgerufene Webseiten injiziert, um Werbungen anzuzeigen.

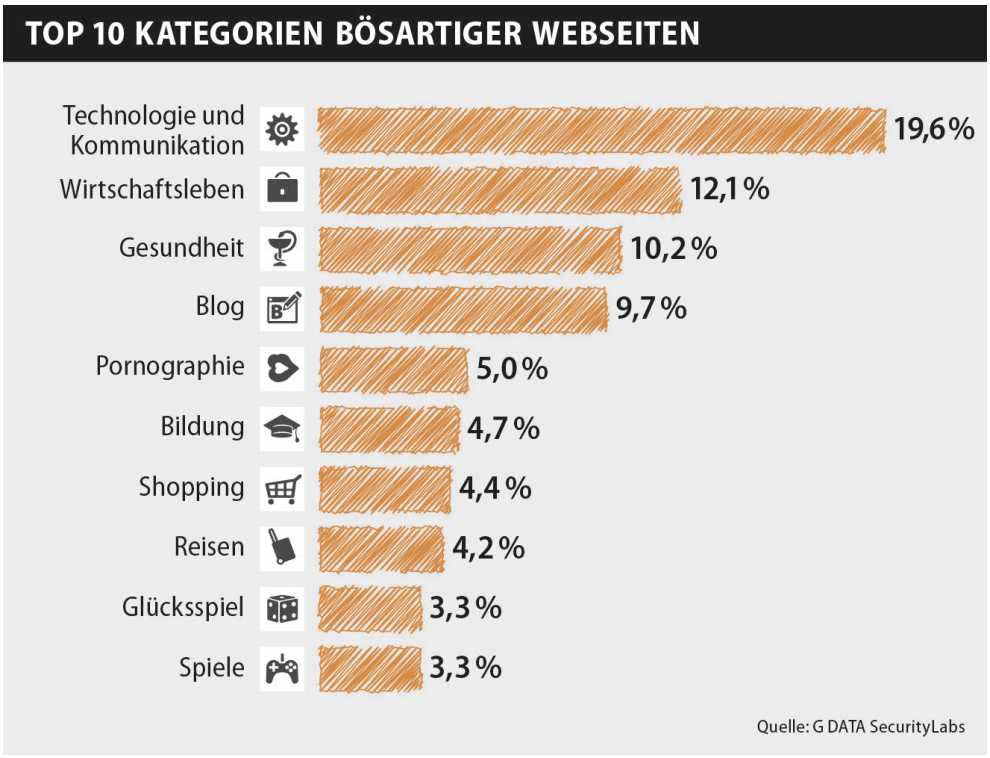
WEBSEITEN-ANALYSEN

Kategorisierung nach Themen

Im zweiten Halbjahr machen die Top 10 der als bösartig eingestuften Webseiten insgesamt 76,4% aus. Mehr als jede dritte bösartige Webseite stammt also in einer dieser nachfolgenden Themenbereiche.

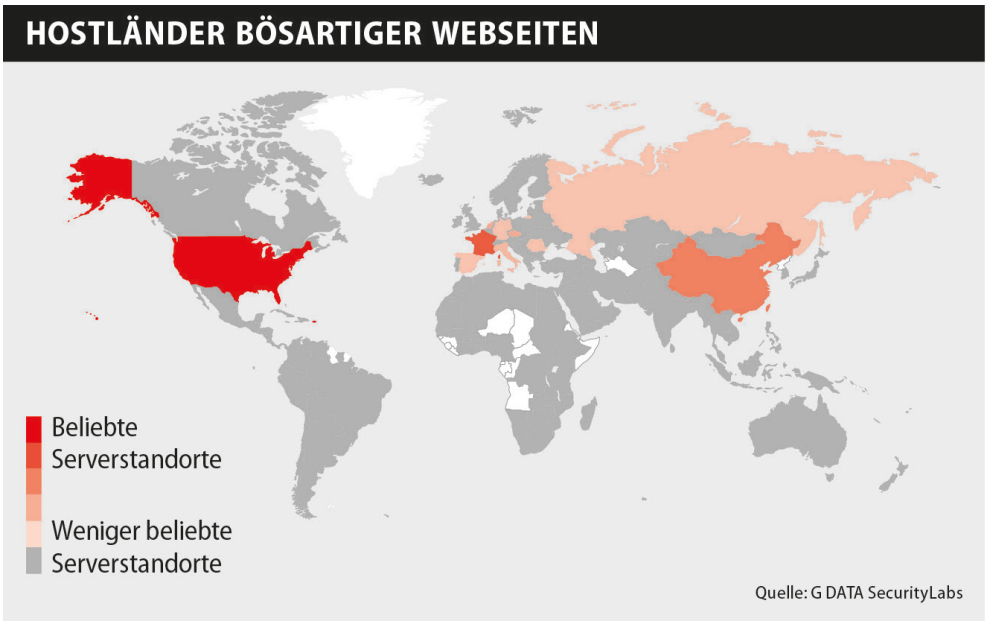
Insgesamt blieben die vertretenen Kategorien bestehen, mit einer Ausnahme: Auf **Rang 10** ist die Kategorie **Spiele** wieder eingestiegen und hat **Unterhaltung** verdrängt. Beide Kategorien liegen thematisch eng beieinander und

hatten schon im vorherigen Halbjahr die Plätze getauscht. Überraschend ist der starke Rückgang des Anteils der Seiten zum Thema **Glücksspiel**: von 24,3% und dem ersten Rang fielen sie nun im zweiten Halbjahr auf **Rang 9** mit nur noch **3,3%**.



Kategorisierung nach Server-Standort

Angreifer müssen ihre Angriffs-Webseiten auf Servern ablegen oder aber auch bestehende Seiten kapern und manipulieren. Die folgende Karte zeigt an, in welchen Ländern die Server mit den bösartigen Webseiten stehen. Phishing- und Malwareseiten werden an dieser Stelle beide als bösartig bezeichnet und es wird nicht zwischen speziell eingerichteten Domains oder einer legitimen Seite, die missbraucht wurde, unterschieden.



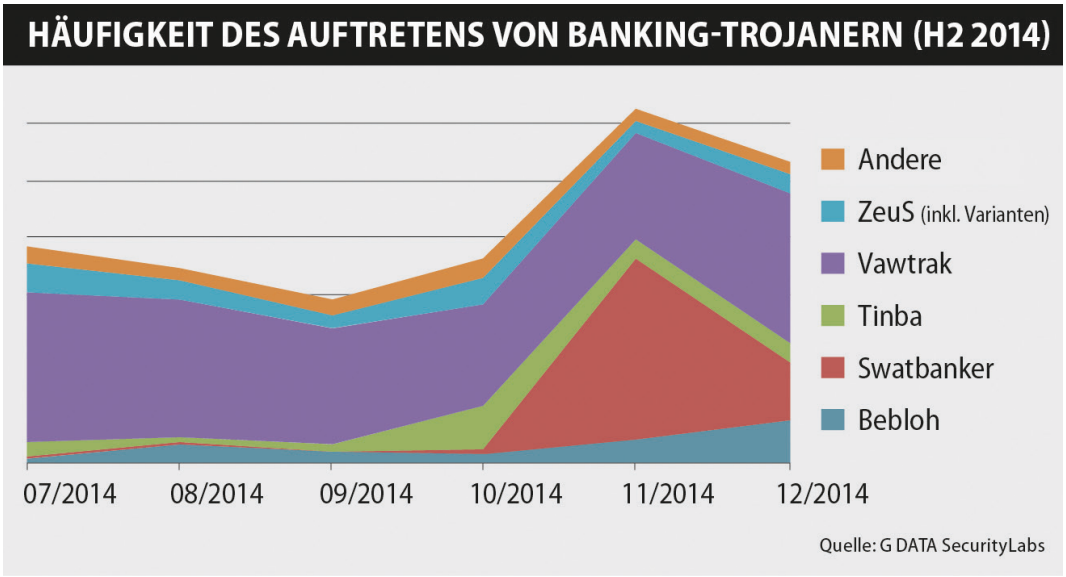
In der Untersuchung bösartiger Webseiten in H2 2014 wurden fast 45% der Seiten in den **USA** gehostet. Etwa jede zehnte Seite (10,6%) lag auf Servern in **Frankreich** und an dritter Stelle wird **China** als Host-Land gelistet, mit 6,1% aller Treffer. Deutschland liegt im aktuellen Vergleich auf Rang 7 (2,6%).

BANKING

Trends auf dem Trojaner-Markt

Im zweiten Halbjahr 2014 gab es auf dem Markt für Banking-Trojaner ein Novum: Es gab keinerlei signifikante Neuerungen im Vergleich zu den Vorjahren. Zuvor traten in diesem Feld über Jahre hinweg in kurzen Zeitabständen immer wieder neue Trojaner und neue Gruppierungen im Hintergrund mit neuen Angriffsmodellen auf. In den letzten Monaten gab es jedoch wenige Änderungen zu verzeichnen.

Die Infektionszahlen von **Tinba**, **Bebloh** sowie der verschiedenen Varianten aus der **ZeuS**-Familie blieben auf niedrigem, aber konstantem Niveau. Der seit dem Frühjahr 2014 stark verbreitete Trojaner **Vawtrak** konnte sein hohes Infektionsniveau halten. Auch die Gruppierung hinter **Swatbanker** aus der **Cridex**-Familie blieb ihrem Angriffsmuster treu. Bei diesem wird keine konstante Infektionsrate angestrebt, sondern es werden nadelstichartig Angriffswellen über einige Wochen durchgeführt, wobei die Infektionen über Spam-Mails erfolgen.



Es lässt sich also sagen, dass sich der Markt für Banking-Trojaner konsolidiert hat. Die Hintergründe hierbei dürften vielfältig sein.

Die häufigen Verhaftungen der Kriminellen in diesem Bereich spiegeln letztlich einen höheren Strafverfolgungsdruck wider. Zudem haben die Banken in den letzten Jahren nach teilweise ausufernden Schäden ihre Sicherheitsmaßnahmen im Bereich Online-Banking immer wieder erhöht.

Diese verschärften Sicherheitsmaßnahmen sind zum Teil unmittelbar sichtbar, z.B. eine Zwei-Faktor-Authentifizierung wie smsTAN oder chipTAN. Doch obwohl sie offensichtlich erkennbar sind, erfordern sie trotzdem einen höheren Aufwand zur Überwindung. Überwunden werden solche Methoden in der Regel durch **Social-Engineering**-Attacken, indem einem Kunden beispielsweise angezeigt wird, er müsse aus angeblichen Sicherheitsgründen eine „Testüberweisung“ durchführen, bei der kein Geld fließe, was tatsächlich doch der Fall ist. Auf solche Tricks dürften aber immer weniger Benutzer hereinfallen, was die Anzahl der erfolgreichen Angriffe senkt. Nichtsdestotrotz kann auch ein einziger erfolgreicher Angriff einen hohen Ertrag für die Angreifer bedeuten.

Andere Sicherheitsmethoden der Geldinstitute und Bezahldienstleister sind für die Angreifer unsichtbar, beispielsweise wenn die Banken Algorithmen zur **Anomalie-Erkennung** verwenden. Das kann bedeuten, dass Banken Transaktionen von hohen Geldbeträgen z.B. ins Ausland nicht ohne Rückfragen durchführen, wenn der

Kontoinhaber zuvor keine Transaktionen in das aktuell ausgewählte Zielland durchgeführt hat. Solche unsichtbaren Sicherheitsmaßnahmen schmälern die Zahl der erfolgreichen Angriffe ebenfalls.

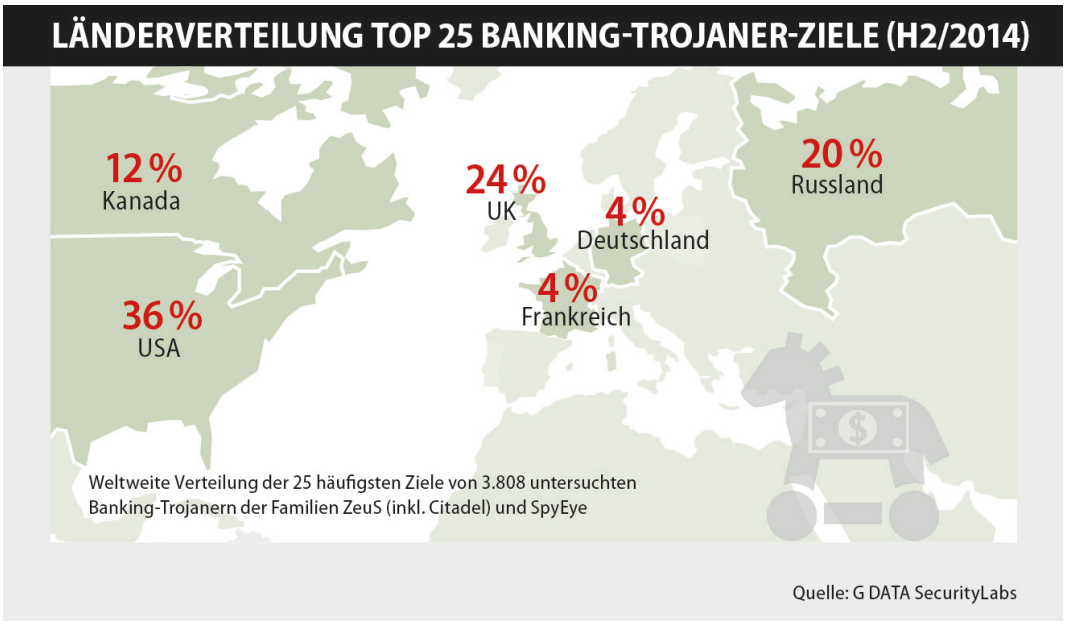
Zusammengefasst: Bei Attacken über Banking-Trojaner gibt es für die Kriminellen ein höheres Risiko bei höherem Aufwand und geringerem Ertrag. Der gefühlte Stillstand auf dem Markt dürfte also damit zu tun haben, dass die Kriminellen eine gewisse Expertise und eine gewisse Infrastruktur benötigen, damit sich diese Angriffe noch lohnen.

Bemerkenswerterweise heißt das aber keinesfalls, dass das Risiko für den Endkunden sinkt: Im Dezember 2014 war die Anzahl der abgewehrten Angriffe um 44,5% höher als noch im Januar.

Die Ziele von Banking-Trojanern

Neben der Verbreitung der Banking-Trojaner-Familien ist es ebenfalls interessant zu untersuchen, welche Ziele von diesen Trojanern angegriffen werden. Ein besonderer Fokus der Angreifer liegt, dem Schädlingstyp entsprechend, auf Banken und Finanzdienstleister.

Unter den 25 häufigsten Zielen der Banking-Trojaner waren wie auch schon im ersten Halbjahr 2014 vor allem Banken aus dem **anglophonen Sprachraum** zu finden, nämlich insgesamt 72% (36% **USA**, 24% **UK**, 12% **Kanada**). Wie zuvor befand sich eine **deutsche** Bank unter den Top 25. Insgesamt sind sieben neue Ziele in den Top25 zu finden, darunter eine **französische** Bank, zwei **russische** Banken, ein **russischer** Zahlungsdienstleister, zwei Banken aus **UK** und eine Bank aus **Kanada**.



Wie im vorherigen Halbjahr ist die Bank of America das am häufigsten ermittelte Ziel von Online-Banking-Trojanern. Die nächsten beiden Ziele in der Liste haben lediglich die Plätze getauscht: Auf Nummer zwei der Statistik landet nun die Citibank, PayPal auf Nummer drei.

TOP 25 DER ANGRIFFSZIELE VON BANKING-TROJANERN (H2/2014)

	Land	Rating Markenwert nach Brand Finance	Angriffshäufigkeit Relative Angriffshäufigkeit der Ziele von 3.808 untersuchten Banking-Trojanern der Familien ZeuS (inkl. Citadel) und SpyEye
Bank of America bankofamerica.com		3	5,88 %
Citi citibank.com		4	5,80 %
PayPal paypal.com		–	5,75 %
eBay ebay.com		–	4,83 %
USAA usaa.com		–	4,54 %
Barclays barclays.co.uk		13	3,81 %
Chase chase.com		5	3,73 %
Wells Fargo wellsfargo.com		1	3,73 %
Royal Bank of Canada royalbank.com		16	3,70 %
TSB Bank tsb.co.uk		53	3,65 %
Lloyds lloydstsb.co.uk		53	3,60 %
HSBC hsbc.co.uk		2	3,57 %
Canadian Imperial Bank of Commerce cibc.com		45	3,31 %
Capital One capitalone.com		24	3,28 %
Scotiabank scotiabank.com		30	3,10 %
Yorkshire Bank ybonline.co.uk		395	2,91 %
Postbank postbank.de		96	2,89 %
SunTrust suntrust.com		87	2,73 %
Yandex yandex.ru		–	2,68 %
WebMoney webmoney.ru		–	2,68 %
Uralsib Bank uralsibbank.ru		–	2,63 %
BNP Paribas bnpparibas.net		7	2,60 %
Shipbuilding Bank sbank.ru		–	2,57 %
RBK Money rbkmoney.ru		–	2,57 %
Clydesdale Bank cbonline.co.uk		393	2,49 %

Kategorie: = Bank = E-Payment = Auktion

Quelle: G DATA SecurityLabs

Methodik

Insgesamt wurden 3.808 Konfigurationsdateien aus Samples von Banking-Trojanern der Familien ZeuS und seines Klons Citadel sowie der SpyEye-Familie extrahiert. Mit diesen Schädlingen lässt sich traditionell ein guter Querschnitt über die Banking-Trojaner bilden. In den Konfigurationsdateien befindet sich eine Liste von Zielseiten (Webseiten von Banken, Bezahldienstleistern und Co.), die mit Webinjects angegriffen werden. Für diese aktuelle Auswertung wurden die Domänen aus den Zielseiten extrahiert und die DNS-Einträge dieser auf Gültigkeit überprüft. Schließlich wurde gezählt, welche Domänen in wie vielen Samples vorkommen. Dadurch konnte die relative Häufigkeit der Angriffe ermittelt werden. Die Domänen werden also letztlich als Angriffsziele begriffen. Den Top 25 der Domänen wurden zudem Herkunftsländer zugeordnet, wobei dazu die firmeneigenen Angaben auf den jeweiligen Seiten genutzt wurden.