TRUST IN
GERMAN
SICHERHEIT

G DATA SECURITYLABS MALWARE REPORT

HALBJAHRESBERICHT
JULI – DEZEMBER 2013

INHALT

AUF EINEN BLICK

- Im 2. Halbjahr 2013 ist die Anzahl neuer Malware um 24% auf 1.874.141 gestiegen.
- Die Anzahl der Malware stieg 2013 im Vergleich zu 2012 um 28%. Die prognostizierte Marke von 3 Millionen wurde mit 3.384.075 deutlich übertroffen. Im Jahresdurchschnitt wurden täglich 9.271 neue Malware-Typen identifiziert.
- Adware nimmt zu. Nicht nur die Anzahl der Schadprogrammtypen steigt. Exemplare von einzelnen Adware-Familien sind auch am weitesten verbreitet und bestimmen die Top 10 der häufigsten Malware.
- Exploits sind nicht sehr zahlreich. Aber sie spielen eine wichtige Rolle bei automatisierten Angriffen.
- 99,9% der Malware läuft unter Windows. Der Anteil von .NET Malware steigt auf 5,2%.

- Schädliche Webseiten sind nur geringfügig auf mehr Kategorien aufgeteilt als im letzten Halbjahr (2,6%).
- Neu in der Top 10 gefährlicher Webseiten ist die Kategorie Glücksspiele.
- Webseiten aus der Kategorie Bildung sind nicht mehr unter den Top 10.

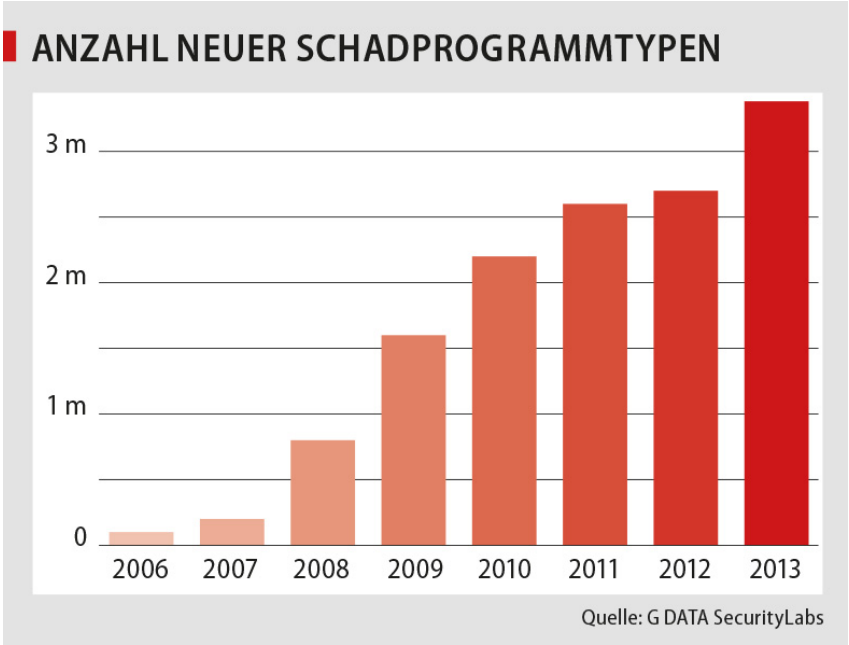
- Die Wirkung eines von Microsoft initiierten Botnetz-Server-Takedowns verpufft nach kurzer Zeit.
- Die Festnahme des Entwicklers des Blackhole Exploit Kits zeigt insbesondere beim Zeus-Klon Citadel mehr Wirkung.
- Die Bebloh-Familie der Banking-Trojaner behauptet ihren Marktanteil und baut ihn sogar aus. Die Familie BankPatch spielt keine Rolle mehr.
- Cridex (alias Feodo) erreicht über Spam-Kampagnen immense Infektionszahlen.

Prognosen und Trends

- Auch im kommenden Jahr wird die Anzahl neuer Malwarekategorien steigen. Wir erwarten, dass die Marke von täglich 10.000 neuen Malware-Typen übertroffen wird.
- Adware und Verschlüsselungstrojaner werden zunehmen.
- Hosting wird weiterhin in High-Tech-Ländern durchgeführt.
- Aufgrund von großen Sport-Events erwarten wir, dass Angriffe auf Webseiten zum Thema Gambling und Sport einen höheren Anteil einnehmen.
- Banking-Trojaner werden immer raffinierter.

SCHADPROGRAMM-STATISTIKEN

Das Jahr 2013 hat bezogen auf die Anzahl neuer Schadprogrammtypen[1] erneut alle vorherigen Rekorde gebrochen und schließt mit einer Gesamtzahl von 3.384.075. Im zweiten Halbjahr verzeichneten die Experten der G DATA SecurityLabs eine neue Höchstzahl mit 1.874.141 neu registrierten Schadprogrammtypen.



Das zweite Halbjahr erreichte damit ein Plus von 364.207 gegenüber der ersten Jahreshälfte, was einer Steigerung um 24% entspricht. Der Vergleich der Gesamtzahlen von 2012 und 2013 zeigt sogar ein Mehr von rund 28%. Der erwartete Durchbruch der Marke von drei Millionen neuen Schadprogrammtypen ist nicht nur erreicht, sondern deutlich übertroffen worden. Rechnerisch entstanden in H2 2013 pro Minute 7 und im Jahresdurchschnitt täglich 9.271 neue Schadprogrammtypen.

Auch im kommenden Jahr wird die Anzahl der neuen Malware-Typen weiter zunehmen. Es ist möglich, dass die Marke von 10.000 neuen Schadprogrammtypen pro Tag überschritten wird.

Kategorien

Anhand der Auswertung der Kategorien der neuen Schadprogrammtypen lassen sich einige Rückschlüsse auf die Ziele der Cyberkriminellen schließen. Die Schadprogramme werden anhand der schädlichen Aktionen, die sie auf einem infizierten System ausführen, klassifiziert. Die wichtigsten Kategorien sind in Abbildung 1 dargestellt.

Die dominanten Kategorien der letzten Jahre, **Trojanische Pferde**, **Downloader**, **Backdoors** und **Spyware** sind auch 2013 weiterhin an der Spitze der Auswertung zu finden.

[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 2013 erstellt wurden.

Downloader werden von Angreifern sehr häufig verwendet, um die eigentliche Schadsoftware auf das System zu spielen. Erst im zweiten Schritt wird bestimmt, wie der Opferrechner missbraucht wird. Das macht Angriffe gegen Computernutzer variabler. Nicht selten schleusen sie dann **Backdoors** auf den Systemen ein, um die Rechner fernzusteuern und sich den dauerhaften Zugriff auf den infizierten Rechner zu sichern. Die **Trojanischen Pferde** waren schon immer die beliebteste Waffe der Cyberkriminellen, die sie wegen ihrer Variabilität und der breiten Spanne an Schadfunktionen schätzen.

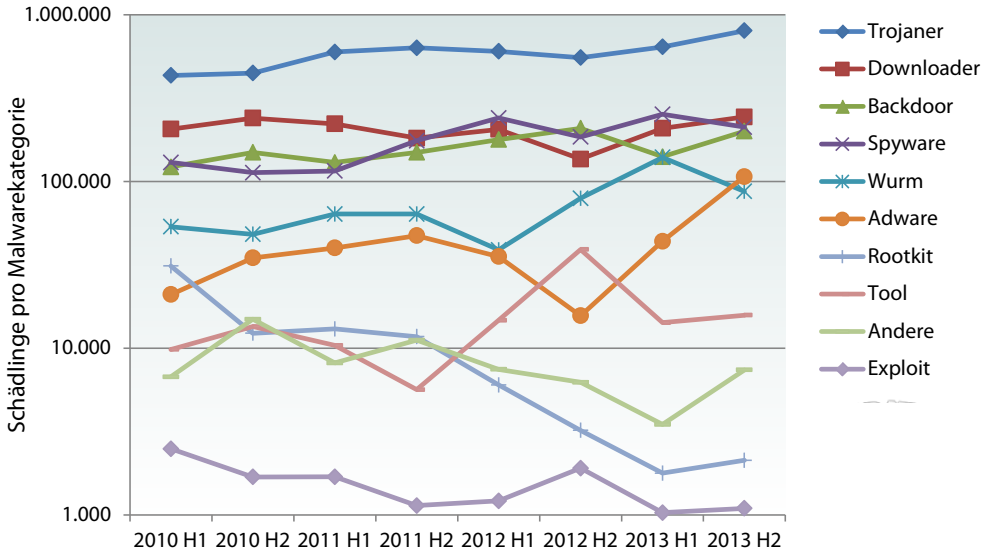


Abbildung 1: *Anzahl neuer Schädlinge pro Malwarekategorie in den letzten Halbjahren*

Bemerkenswert ist der erneut starke Anstieg der Zahl neuer Schadprogrammtypen der Kategorie **Adware**. Das Verbreiten von meist ungewollten Browser-Erweiterungen oder Programmzusätzen, die dem Nutzer dann unerwünschte Werbung oder Angebote anzeigen, ist ein sehr lukratives Geschäft für Angreifer. Aufwand und Ertrag stehen für sie in einem sehr guten Verhältnis und das spiegelt sich auch in den tatsächlich gemessenen abgewehrten Angriffen gegen Computernutzer wieder, wie im Kapitel „GEFAHREN-MONITOR“ berichtet wird.

Die Anzahl der Exploits ist zwar leicht gestiegen aber insgesamt weiterhin gering. Das bedeutet allerdings nicht, dass Exploits keine Gefahr sind. Sie sind ein zentraler Bestandteil von automatisierten Angriffen wie sie z.B. als Drive-By-Infektionen beim Besuch von Webseiten genutzt werden. Web Exploit Kits sind im Untergrund eine wichtige Ware, die es auch Laien ermöglichen Webseiten ohne spezielle Kenntnisse zum Verbreiten von Malware zu nutzen.

Plattformen – Windows weiterhin im Fokus

Die neuen Schadprogrammtypen sind weiterhin in der absoluten Mehrheit gegen Microsofts Betriebssystem Windows gerichtet. Der Anteil der **.NET-Entwicklungen** (**MSIL**) verzeichnet zum wiederholten Male in Folge einen deutlichen Anstieg und hat seinen Anteil nun auf 5,2% erhöht, was einer Verdoppelung des Anteils aus H2 2012 (2,6%) und einer Verdreifachung des Anteils von H2 2011 (1,4%) entspricht. Dabei steigt nicht nur der Anteil von **MSIL**, sondern auch die Anzahl der neuen Schadprogrammtypen hat sich im letzten Halbjahr mehr als verdoppelt und im letzten Jahr sogar fast verdreifacht.

Insgesamt zielen in H2 2013 mehr als 99,9% der neuen Schadprogrammtypen auf **Windows**[2] ab. Der Anteil hat sich zum vorherigen Halbjahr nicht verändert.

	Plattform	#2013 H2	Anteil	#2013 H1	Anteil	Differenz #2013 H2 #2013 H1	Differenz #2013 H2 #2012 H2
1	Win	1.774.287	94,7%	1.462.527	96,9%	+21,3%	+45,0%
2	MSIL	97.686	5,2%	46.448	3,1%	+110,3%	+195,8%
3	WebScripts	720	<0,1%	540	<0,1%	+33,3%	-33,8%
4	Java	154	<0,1%	163	<0,1%	-5,6%	-63,9%
5	Scripts[3]	642	<0,1%	146	<0,1%	+333,9%	+63,8%

Tabelle 1: *Top 5 der Plattformen der letzten beiden Halbjahre*

Ein Blick in das nachfolgende Kapitel GEFAHREN-MONITOR zeigt an, welche Attacken tatsächlich gegen die Computernutzer im vergangenen Halbjahr durchgeführt wurden, unabhängig von der Entwicklung der neuen Schadprogrammtypen.

GEFAHREN-MONITOR

Der Gefahren-Monitor gibt die Top 10 der abgewehrten Angriffe gegen Computernutzer[4] mit G DATA Sicherheitslösungen und aktivierter MII[5] an. Nachfolgend werden die am häufigsten abgewehrten Attacken aus dem zweiten Halbjahr 2013 dargestellt. Die Aufstellung der einzelnen Monate ist immer aktuell auf der G DATA SecurityLabs Webseite[6] zu finden.

Der beobachtete Trend, dass immer mehr neuer Schadcode zur Kategorie der **Adware** gezählt wird, spiegelt sich auch in den registrierten Angriffen auf die G DATA Nutzer wider. Die Top 10 sind gefüllt mit den Angriffen, die von den meisten Benutzern als sehr unangenehme, gar lästige Veränderung ihres Systems wahrgenommen wird. In den vorherigen zwei Halbjahren dominierte die Schädlingsfamilie **Sirefef**, auch **ZeroAccess** genannt, die Rangliste. Auch diese Familie hatte Komponenten für Klickbetrügereien parat, die weit verbreitet waren. Doch die aktuell beobachtete Entwicklung ist nicht mehr nur einer speziellen Schädlingsfamilie zuzuschreiben.

Adware.BHO.BProtector.A, eine Detektion für potentiell unerwünschte Browser-Toolbars, erwirtschaftet für die Angreifer Geld nach dem Pay-per-Install Prinzip. In diesem besonderen Fall geht es um die Babylon Toolbar. Auch wenn dieser Schädling in den aktuellen Top 10 nur auf Rang 10 zu finden ist, so ist er doch ein Indiz für den andauernden Trend, der geprägt ist von der Jagd auf direkte monetäre Profite, ohne Umwege über Datenklau oder ähnlichen Szenarien. **Gen:Variant.Adware.BHO.Bprotector.1**, auf Platz 1 der Halbjahreswertung, ist die Weiterentwicklung der eben genannten Erkennung. Mit ihr werden viele weitere Adware-Fälle in Verbindung mit der Babylon Toolbar generisch erfasst.

---

[2] Als Malware für Windows betrachten wir ausführbare Dateien im PE-Format, die dort für Windows deklariert werden, oder ausführbare Dateien, die in der Microsoft Intermediate Language (MSIL) erstellt wurden. MSIL ist das Zwischenformat, das im .NET-Umfeld verwendet wird. .NET-Anwendungen sind zwar weitestgehend plattformunabhängig, sie werden aber de facto fast ausschließlich auf Windows-Rechnern verwendet.

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

[4] 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 (Beispiel: Adware.BHO.BProtector.A)

[5] 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.

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

Auch die Schädlingsvarianten der **Familie Addlyrics** fallen in die Kategorie Adware. Wie der Familienname suggeriert, handelt es sich um Songtexte, die in gestreamten Videos eingeblendet werden können. Doch neben der offiziellen und erwünschten Funktion beinhalten die detektierten Varianten auch Funktionen für nicht gewollte Werbeeinblendungen.

DNSChanger ändern die Internet-Einstellungen eines Rechners. Der Kontakt ins Internet wird über Server hergestellt, die auf gefälschte Inhalte zeigen können. Auch hier wird häufig mit Werbung Geld verdient.

Rang	Name	Prozent
1	Gen:Variant.Adware.BHO.Bprotector.1	5,75%
2	JS:AddLyrics-B [Adw]	2,33%
3	Trojan.Downloader.JQAC	1,61%
4	Gen:Variant.Graftor.10487	1,50%
5	JS:AddLyrics-D [Adw]	0,92%
6	Gen:Adware.MPlug.1	0,86%
7	Win32:DNSChanger-VJ [Trj]	0,76%
8	Adware.DealPly.B	0,60%
9	Adware.WebCake.C	0,60%
10	Adware.BHO.BProtector.A	0,58%

Tabelle 2: *Die Top 10 der durch die MII registrierten Angriffe in H2 2013*

WEBSEITEN-ANALYSEN

Kategorisierung nach Themen

Im zweiten Halbjahr 2013 verzeichnen die Experten der G DATA SecurityLabs einen Neueinsteiger in den Top 10 Kategorien der bösartigen Webseiten.[7]

In der Summe ergeben die zehn gefährlichsten Kategorien exakt 72%. Das ist gegenüber H1 2013 zwar ein Minus von 2,6%, jedoch bleibt das Niveau hoch. Somit stammt weiterhin fast jede dritte gefährliche Webseite aus einem dieser Themenbereiche. Die Top 5 der Kategorien addieren sich zu fast 50% - das sind etwa 5% weniger als im ersten Halbjahr.

Glücksspiel ist das neue Themenfeld, das bisher noch nie in den Untersuchungen den Sprung in die Top 10 Ränge geschafft hat. Der Neueinsteiger steigt mit 3,8% auf **Platz 9** ein. Prominente Vertreter dieser Kategorie sind Online-Casinos und Online-Wettbüros sowie Lotterien.

Betrachtet man dazu die thematisch ähnlichen Kategorien **Spiele** und **Unterhaltung**, machen diese drei gemeinsam immerhin 12,6% aus.

Die Kategorie **Bildung** hat sich dafür aus den obersten Rängen verabschiedet und ist im zweiten Halbjahr nur noch auf Platz 11 gelandet.

[7] Als bösartige Webseiten werden in diesem Zusammenhang sowohl Phishing-Seiten als auch Malware-Seiten gezählt. Bei der Zählung wird außerdem nicht zwischen speziell eingerichteten Domains oder einer legitimen Seite, die missbraucht wurde, unterschieden.

Kategorisierung nach Server-Standort

Die lokale Verteilung bösartiger Webseiten zeigt auf, in welchen Ländern vorwiegend bösartige Webseiten gehosted werden, wobei auch in dieser Auswertung Seiten mit Schadcode und Phishing-Seiten zusammengefasst werden. Abbildung 2 zeigt, dass Cyberkriminelle bei der Auswahl der Hostländer deutlich auf die Länder setzen, in denen sie gute Infrastruktur und günstige Preise für das Bereitstellen von Webseiten vorfinden.

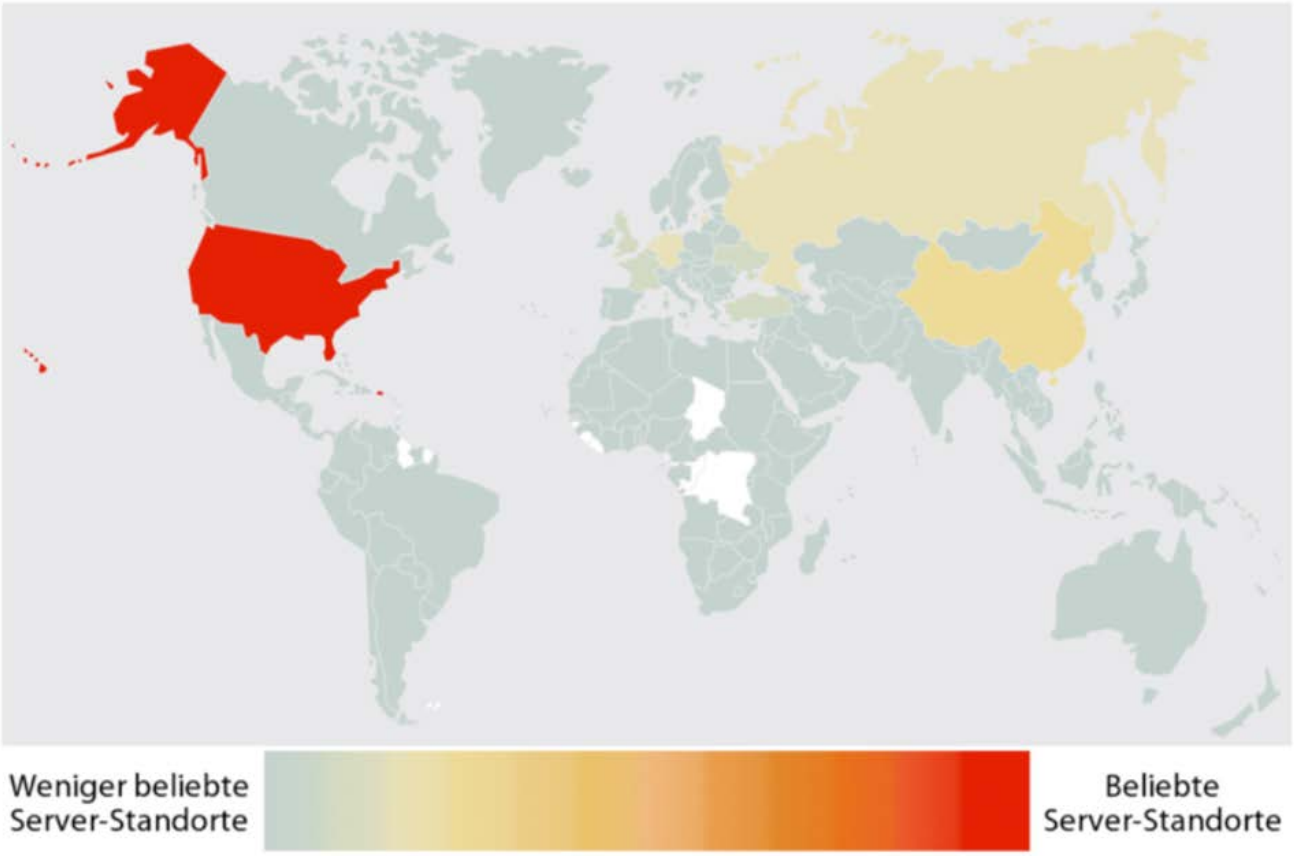


Abbildung 2: *Flächenkartogramm mit Informationen zur Häufigkeit der gehosteten, bösartigen Webseiten in den Ländern*

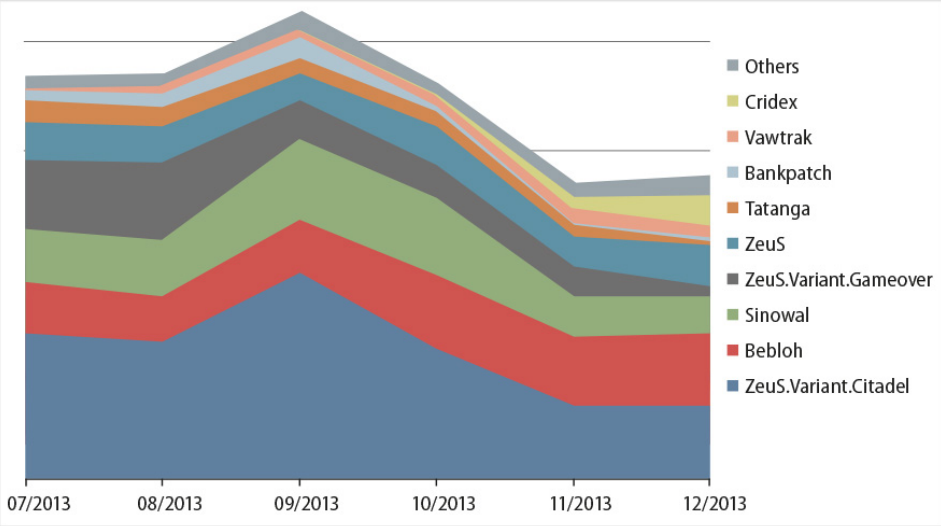
Im zweiten Halbjahr 2013 wurden im Gegensatz zum vorherigen Halbjahr mehr bösartige Webseiten in **China** gemessen. China hat damit seit H1 2012 Zuwachs in dieser Auswertung verzeichnet und ist nun in H2 2013 das Land mit den zweitmeisten schädlichen Webseiten, nach den **USA**. **Russland** hat diesen zweiten Platz abgegeben und liegt nun in der Liste der gezeigten Häufigkeitsverteilung auf einem Niveau mit **Deutschland**.

BANKING

Entwicklungen auf dem Trojanermarkt

Nachdem Microsoft Ende des ersten Halbjahres 2013 eine organisierte Abschaltung (Takedown) von Command&Control-Servern vornahm[8], blieb der gewünschte Effekt aus. Im September gab es die höchste Infektionsrate des zweiten Halbjahres, sie lag rund 16% höher als noch im Juli. Der Effekt der Abschaltung war offenkundig verpufft.

HÄUFIGKEIT DES AUFTRETENS VON BANKING-TROJANERN IM 2. HALBJAHR 2013



Quelle: G DATA Security Labs

Dann konnte allerdings ein weiterer Schlag gegen die Cyberkriminellen durchgeführt werden: Der Drahtzieher hinter dem „Blackhole Exploit Kit“ mit dem Pseudonym „Paunch“ konnte verhaftet werden.[9] Mittels Exploit Kits werden PCs massenhaft mit Schädlingen verseucht. Und insbesondere das Blackhole Exploit Kit war für die häufige Verbreitung von Banking-Trojanern berüchtigt. Der Abfall an Infektionen war insbesondere beim ZeuS-Klon Citadel spürbar. Bankpatch, der Trojaner, der im ersten Halbjahr 2013 eine innovative Technik zur Kontrolle über Jabber implementierte, verschwand fast völlig von der Bildfläche.
In der neuen Produktgeneration 2015 bietet G DATA mit seiner „Exploit Protection“ Schutz vor Angriffen durch Exploit Kits.

Zum Ende des Jahres pendelte sich die Infektionszahl bei etwa 3/4 des Volumens vom September ein.

Die nächste Welle rollte aber schon: Cridex (alias Feodo) konnte mit zahlreichen Infektionen über Spam-Mails erhebliche Infektionszahlen erreichen.[10]

Bereits zum Ende des letzten Halbjahres tauchte Bebloh – was die Infektionszahlen angeht – aus dem Nichts auf. Im zweiten Halbjahr wurde dieser Eindruck bestätigt und Bebloh konnte sich durchgehend unter den vier häufigsten Banking-Trojanern platzieren. Bebloh war zuvor zwar z.B. durch den „Retouren-Trick“ als innovativ bekannt, fiel aber nie durch besonders hohe Infektionszahlen auf.
Beim Retouren-Trick wird dem Benutzer durch den Trojaner vorgespielt, er hätte fälschlich eine Überweisung

[8] http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx
[9] http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/
http://www.bbc.co.uk/news/technology-24456988
[10] http://blog.gdata.de/artikel/cridex-banking-trojaner-auf-dem-vormarsch/

erhalten, die sich scheinbar auch im (durch den Trojaner manipulierten) Kontostand niederschlägt. Diese Social-Engineering-Methode führt dazu, dass viele ehrliche Opfer das Geld ungefragt zurücküberweisen wollen. In diesem Fall werden diese zu einem vorausgefüllten Formular für die Retour-Überweisung umgeleitet. Tatsächlich ist das Empfängerkonto ein Konto des Angreifers, dem das Opfer durch alle Authentifizierungsverfahren wie TAN hindurch quasi freiwillig die genannte Summe überweist. Eine fälschlich getätigte Überweisung hat es aber nie gegeben und die Überweisung geht zu Lasten des Infektionsopfers.

Banking-Trojaner Trends

Ein Trend ist der von G DATA lange antizipierte, verstärkte Einsatz der Anonymisierungstechnik Tor. Bereits im September 2012 entdeckte G DATA „Skynet“[11], den ersten Trojaner, der seine Kontrollfunktionen über Tor abwickelte. Später wurde eine Variante bekannt, in der auch ZeuS in einer Variante über das Tor-Netzwerk gesteuert wird.[12] Die Köpfe hinter Skynet konnten Ende 2013 verhaftet werden.[13] Fast zeitgleich wurde allerdings eine weitere ZeuS-Variante mit Tor-Funktionalität entdeckt.[14]

Als Trend lässt sich vor allem eine weitere Diversifizierung ausmachen. In den letzten Jahren gab es zuvor immer bestimmte Trojaner, die den Markt dominiert haben. Zum Ende 2013 hingegen war das Feld unter den Banking-Trojanern praktisch homogen. Das macht die Entdeckung und Verfolgung der Täter nicht einfacher.

[11] http://blog.gdatasoftware.com/blog/article/botnet-command-server-hidden-in-tor.html
[12] http://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit
[13] http://thehackernews.com/2013/12/alleged-skynet-botnet-creator-arrested.html
[14] http://www.heise.de/security/meldung/Baukasten-Trojaner-Zeus-jetzt-in-64-Bit-und-mit-TOR-2064515.html