G Data

PC MalwareReport

Halbjahresbericht
Januar – Juni 2013

G Data SecurityLabs

G Data. Security Made in Germany.

Inhalt

Auf einen Blick

- Im ersten Halbjahr 2013 betrug die Gesamtzahl neuer Malware 1.509.934.
- Im Vergleich zum zweiten Halbjahr 2012 ist das eine Steigerung um fast 20%.
- Durchschnittlich entstanden in H1 2013 täglich 8.342 neue Schadprogrammtypen.
- Wir erwarten, dass Ende 2013 eine neue Rekordmarke von drei Millionen neuen Schadprogrammtypen in einem Jahr aufgestellt wird.

- Die Anzahl der neuen Schadprogrammtypen in der Kategorie Würmer hat im vergangenen Halbjahr erneut deutlich zugelegt.
- Auch in der Kategorie Adware konnte ein steiler Anstieg der Zahlen verzeichnet werden, nachdem es in 2012 etwas ruhiger war auf diesem Gebiet.

- Windows steht noch stärker im Fokus der Malware-Autoren. Insgesamt zielten in H1 2013 mehr als 99,9% der neuen Schadprogrammtypen auf Windows ab!

- Ein Blick auf die abgewehrten Angriffe gegen G Data Kunden zeigt im Gefahren-Monitor, dass das letzte Halbjahr im Zeichen von monetären Gewinnen durch Klickbetrug und Pay-per-Install stand.
- Die Schädlingsfamilie Sirefef, oder auch ZeroAccess genannt, dominiert weiter die Top 10.

- Bei bösartigen Webseiten ist das Thema Pornographie in den Vordergrund gerückt und hat seinen Anteil fast verdoppelt – nun zu finden auf Rang 2.
- Auch der Anteil von gefährlichen Webseiten mit dem Kontext Shopping hat sich deutlich erhöht und dieses Thema von Platz 9 auf Rang 4 katapultiert.
- Schädliche Webseiten verteilen sich verstärkt auf mehrere Kategorien. Der Anteil der Top 10 Ränge beträgt nur noch 74,6% und büßte damit ganze 14% gegenüber dem zweiten Halbjahr 2012 ein.

- Weiterhin wurden bösartige Webseiten bevorzugt in Ländern mit gut ausgebauter Infrastruktur gehostet.

- Die Infektionszahlen der Banking-Trojaner blieben im vergangenen Halbjahr auf einem vergleichsweise niedrigen Niveau. Im Juni waren die Zahlen jedoch zuletzt etwa ein Viertel höher als noch im Dezember 2012.
- Cridex ist als neue Familie hinzugekommen und machte sofort mit hohen Infektionszahlen auf sich aufmerksam.
- Ende Mai/Anfang Juni wurde ein Großteil des Citadel Botnetzes durch eine Kooperation zwischen Microsoft und Behörden zerschlagen.
- Der Quellcode des Trojanischen Pferds Carberp wurde im Internet veröffentlicht und ist nun frei verfügbar. Wir erwarten, dass Teile des Codes in neuen Schadprogrammen auftauchen.
- Ermittlungsbehörden werden zunehmend Schwierigkeiten bei der Strafverfolgung haben, da auf dem Markt der Banking-Trojaner eine zunehmende Diversifizierung stattfindet.
- Außerdem arbeiten die Angreifer immer weiter an der Dezentralisierung der Botnetz-Kommunikation und es werden auch hier neue Entwicklungen erwartet.

Schadprogramm-Statistiken

Im ersten Halbjahr 2013 betrug die Gesamtzahl neuer Schadprogrammtypen[1] 1.509.934. Damit verzeichnen die Experten der G Data SecurityLabs einen erneuten Anstieg und sogar eine neue Höchstmarke im Vergleich zu den vorangegangenen Halbjahren. Die Prognosen des letzten Halbjahresberichts hatten ein zu H2 2012 ähnlich hohes Niveau vorausgesehen, doch die aktuellen Zahlen lassen für das Ende des Jahres 2013 sogar einen neuen Rekord erwarten.

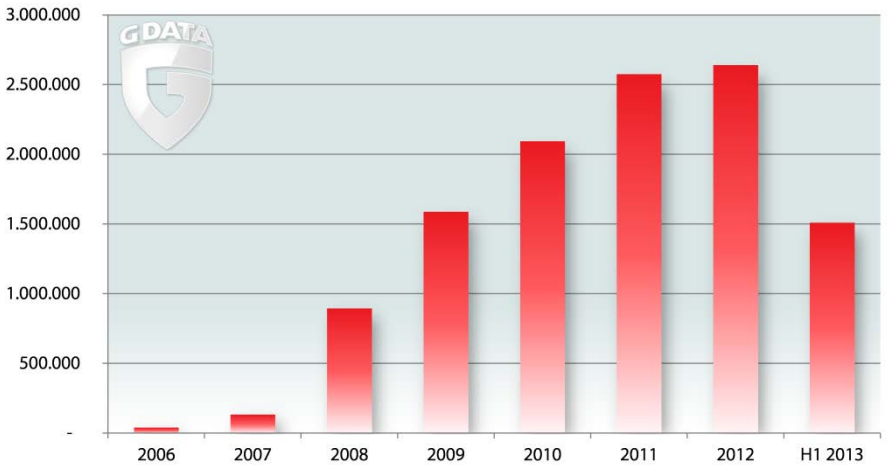

Abbildung 1: *Anzahl neuer Schadprogrammtypen seit 2006*

Im Gegensatz zu H2 2012 stieg die Zahl neu registrierter Schadprogrammtypen um 251.455 und damit um fast 20%. Verglichen mit H1 2012 ist es eine Steigerung um 127.967 und somit um etwas mehr als 9%. Tendenziell wurden jedoch in der Vergangenheit in den zweiten Jahreshälften mehr neue Schadprogrammtypen registriert und somit wird erwartet, dass am Ende des Jahres 2013 die Marke von drei Millionen neuen Schadprogrammtypen durchbrochen wird. Auch schon bei gleichbleibendem Durchschnittswert von 8.342 neuen bösartigen Programmen pro Tag wäre dies erreicht. Rechnerisch entstanden in H1 2013 pro Minute fast 6 neue Schadprogrammtypen!

Kategorien

Ein Blick auf die Kategorien der neuen Schadprogrammtypen zeigt an, in welche Richtung sich die Interessen der Cyberkriminellen orientieren. Die Schadprogramme werden anhand der schädlichen Aktionen, die sie auf einem infizierten System ausführen, klassifiziert. Die wichtigsten Kategorien sind in Abbildung 2 dargestellt.

Bei den dominierenden Kategorien, **Trojanische Pferde**, **Spyware**, **Downloader** und auch **Backdoors** gibt es keine großen Veränderungen oder Überraschungen. Auf gewohnt hohem Niveau sind auch im ersten Halbjahr 2013 wieder neue Schadprogramme hinzugekommen.

Bemerkenswert ist der steile Anstieg der Kategorie **Wurm**. Die Zahl der neuen Wurm-Schädlingsvarianten ist weiterhin auf dem Vormarsch und erreicht die Zahl der neuen Backdoor-Varianten, bleibt damit weiterhin auf Rang 5.

[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 ersten Halbjahr 2013 erstellt wurden.

Rang 6 wird belegt von **Adware** – nach einem Einbruch im zweiten Halbjahr 2012 ist die Zahl neuer Adware-Varianten nun wieder auf Vorjahresniveau und spiegelt damit auch die Tendenz wieder, die sich in den registrierten Angriffen gegen Computernutzer in H 1 2013 gezeigt hat. Nähere Informationen dazu finden sich im Kapitel „Gefahren-Monitor“.

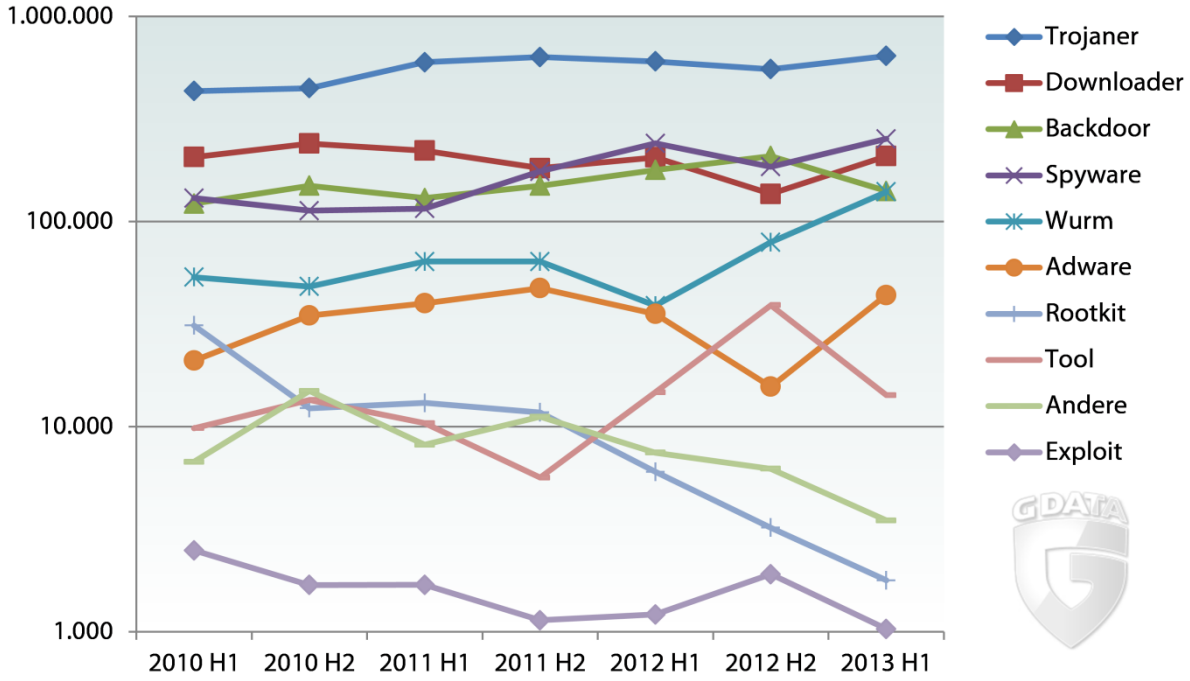

Abbildung 2: *Anzahl neuer Schädlinge pro Malwarekategorie in den letzten sieben Halbjahren*

Den wohl bemerkenswertesten Abwärtstrend hat die Kategorie **Exploits** hinter sich. Schon immer auf relativ niedrigem Niveau angesiedelt, fiel die Zahl der neuen Varianten jedoch noch einmal um 46%. Dass es weniger neue Detektionen für Exploit-Varianten gibt, bedeutet nicht zwangsläufig, dass die Gefahr durch das Ausnutzen von Sicherheitslücken geringer wird. Schon lange beobachten die Experten der G Data SecurityLabs, dass auch alte Schwachstellen immer wieder erfolgreich ausgenutzt werden, da Computernutzer es versäumt haben Updates und Patches einzuspielen. Somit öffnen sie Cyberangreifern Tür und Tor. Eine einzige (!) Sicherheitslücke auf einem PC reicht aus, um den PC und damit möglicherweise auch das gesamte Netzwerk zu infizieren. Studien zufolge wurden im Jahr 2012 insgesamt 9.776 Sicherheitslücken entdeckt, was einen Anstieg um 15% auf die letzten fünf Jahre bezogen und einen Anstieg um 5% gegenüber 2011 bedeutet.[2]

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft **Exploits** seit langem in seinem „Register aktueller Cyber-Gefährdungen und –Angriffsformen“[3] als besonders bedrohlich und relevante Gefährdung ein. Man kann also keinesfalls Entwarnung geben!

[2] Secunia Vulnerability Review 2013
[3] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Content_Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html

Plattformen – massive Konzentration auf Windows

Ein Blick auf die Zielplattformen der neuen Schadprogrammtypen zeigt wenige Überraschungen. Schadcode, der auf die Windows-Plattform abzielt, ist und bleibt die Nummer eins. Der Anteil der **.NET Entwicklungen** (MSIL) ist im Vergleich zum Vorjahreshalbjahr jedoch erneut angestiegen und hat seinen Anteil nun seit H2 2011 (1,4%) mehr als verdoppelt. Zusätzlich steigt auch die Anzahl der neuen .NET Entwicklungen – im Vergleich von H1 2012 zu H1 2013 ist ein Plus von mehr als 150% zu verzeichnen.

Insgesamt zielen in H1 2013 mehr als 99,9% der neuen Schadprogrammtypen auf **Windows**[4] ab. Das ist eine erneute Steigerung des Anteils!

	Plattform	#2013 H1	Anteil	#2012 H2	Anteil	Differenz #2013 H1 #2012 H2	Differenz #2013 H1 #2012 H1
1	Win	1.462.527	96,9%	1.223.419	97,2%	+19,54%	+7,52%
2	MSIL	46.448	3,1%	33.020	2,6%	+40,67%	+150,25%
3	WebScripts	540	<0,1%	1.087	0,1%	-50,32%	-67,70%
4	Java	163	<0,1%	426	<0,1%	-61,74%	-75,58%
5	Scripts[5]	146	<0,1%	392	<0,1%	-62,76%	-69,77%

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

Die Zahl der neuen Signaturen für **WebScripts** verringert sich auch weiterhin, da diese Bedrohung nach wie vor meist durch generische Signaturen erkannt werden kann und daher nicht viele neue Ansätze notwendig sind. Sie behaupten weiterhin Platz Nummer drei.

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[6] mit G Data Sicherheitslösungen und aktivierter MII[7] an. Im vergangenen Halbjahr standen die Zeichen klar auf Schadroutinen wie Klickbetrug und Pay-per-Install – die Jagd nach dem vermeintlich schnellen Geld!

Die Dominanz der Schädlingsfamilie **Sirefef**, oder auch **ZeroAccess** genannt, aus dem zweiten Halbjahr 2012 ist in der Bilanz des vergangenen Halbjahres weiterhin vorhanden. Es gab erneut zahlreiche neue Varianten der Familie, und einige davon waren so verbreitet, dass sie erneut die Topliste überspülten. Das Hauptmotiv der vielfältigen Malwarefamilie ist monetärer Gewinn durch z.B. manipulierte Suchmaschinenergebnisse (Klickbetrug). Gepaart mit verschiedenen

[4] 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.

[5] "Scripts" sind Batch- oder Shell-Skripte oder Programme, die z.B. in den Skriptsprachen VBS, 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 (Beispiel: Trojan.Wimad.Gen.1)

[7] 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.

ausgeklügelten Rootkit-Funktionalitäten entsteht eine sehr aggressive und mächtige Malware.

Rang	Name	Prozent
1	Win32:DNSChanger-VJ [Trj]	7,28%
2	Win64:Sirefef-A [Trj]	1,61%
3	Adware.BHO.BProtector.A	1,41%
4	Win32:ZAccess-PB [Trj]	1,20%
5	Exploit.CVE-2011-3402.Gen	0,78%
6	Generic.JS.Crypt1.C14787EE	0,77%
7	Trojan.Sirefef.XL	0,57%
8	Trojan.Sirefef.RG	0,53%
9	Gen:Variant.Kazy.138843	0,52%
10	Trojan.Wimad.Gen.1	0,48%

Tabelle 2: *Die Top 10 der durch die MII registrierten Angriffe in H1 2013*

Mit **Win64:Sirefef-A [Trj]**, **Win32:ZAccess-PB [Trj]**, **Trojan.Sirefef.XL** und auch **Trojan.Sirefef.RG** vier Plätze in der Hand dieser Multikomponentenfamilie und rund jeder 25. registrierte Angriff ging auf ihr Konto. Diese Zahl wird sogar noch energischer, zählt man **Win32:DNSChanger-VJ [Trj]** noch zum Dunstkreis der Sirefef-Schädlinge. Der DNSChanger wird sehr häufig als Payload der Sirefef-Familie ausgeliefert und ist deshalb auch weiterhin auf Rang eins der Statistik wiederzufinden. Zählt man seine Angriffe hinzu, ist sogar jede neunte Attacke auf die aggressive Schädlings-Kombination zurückzuführen.

Auch der Schädling **Gen:Variant.Kazy.138843** gehört in die Kategorie Klickbetrug. Der Schadcode überwacht den Internet Datenverkehr und übernimmt die Browser-Sitzung, sobald eine der im Code vordefinierten URLs aufgerufen wird. Außerdem steht auch **Generic.JS.Crypt1.C14787EE** im Verdacht, seine Funktionen für die künstliche Generierung von Klicks mit Hilfe von per JavaScript nachgeladenen Bildern zu nutzen.

Adware.BHO.BProtector.A, eine Detektion für potentiell unerwünschte Browser-Toolbars, erwirtschaftet für die Angreifer Geld nach dem Pay-per-Install Prinzip und komplettiert damit die Halbjahres Top 10, die geprägt ist von der Jagd auf direkte monetäre Profite, ohne Umwege über Datenklau und dem anschließenden Verkauf oder ähnlichen Szenarien.

Die „Ausnahmen" dieses Trends des ersten Halbjahres bilden **Exploit.CVE-2011-3402.Gen** und der Dauerbrenner **Trojan.Wimad.Gen.1**. Der Exploit ist einer, den schon Stuxnet und Duqu benutzten, um ihre Angriffe auf Computernutzer durchzuführen. Dass dieser Exploit noch heute in den Top 10 der Angriffe zu finden ist, zeigt, dass es eine solche spezielle Entwicklung nach einiger Zeit sogar in die Massen-Malware geschafft hat. In diesem Fall wurde der Exploit als Teil des Cool Exploit Kits und wenig später auch als Teil des Blackhole Exploit Kits verbreitet.[8]

[8] http://krebsonsecurity.com/tag/cve-2011-3402/

Webseiten-Analysen

Kategorisierung nach Themen

In den ersten sechs Monaten des Jahres haben sich einige Neuerungen in den Top 10 der Kategorien bösartiger Webseiten ergeben.[9]

Aufsummiert ergeben die Top 10 einen Anteil von 74,6% und büßen damit ganze 14% gegenüber dem zweiten Halbjahr 2012 ein. Insgesamt verteilen sich die Angriffe also vermehrt auf die vorhandenen Kategorien. Die restlichen 25,4% teilen sich auf 68 weitere Kategorien auf, was immer noch eine deutliche Fokussierung auf die Top 10 zeigt oder sogar auf die Top 5, denn alleine die ersten fünf Kategorien decken zusammen schon 55,3% aller als bösartig erkannten Webseiten ab.

Neu wieder eingestiegen, gegenüber H2 2012 sind die Kategorien **Gesundheit** und **Spiele**. Dafür haben **Sport** und **Forum** die Top 10 verlassen müssen – sie finden sich nach dem H1 2013 auf Rang 12 und 23 wieder.

Die Kategorie **Technologie & Telekommunikation** behält **Rang 1** sicher, verliert jedoch fast 10% gegenüber H2 2012. Eventuell haben die Seiten für Technik-begeisterte in ihren Sicherheitskonzepten nachgebessert und sind weniger angreifbar. Dafür hat sich das Themengebiet **Pornographie** auf **Rang 2** vorgeschoben und von 7,5% (damals Rang 5) auf 13,4% zugelegt.

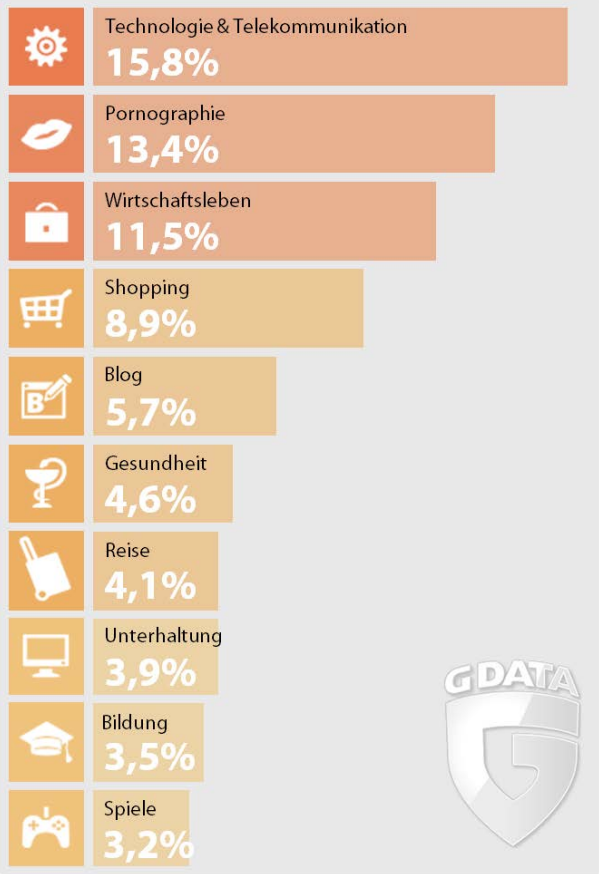

Abbildung 3: *Die Top 10 der Themen bösartiger Webseiten in H1 2013*

Die Situation der Schadseiten im Bereich **Blogs** hat sich nicht signifikant verändert – damals Rang 7 mit 5,1% und heute **Rang 5** mit 5,7%.

Auffallend ist jedoch der Abfall der Kategorie **Bildung**, die in H2 2012 noch Rang 2 mit 15,5% belegte und nun mit 3,5% fast aus den Top 10 verdrängt worden wäre. Dagegen hat sich **Shopping** von Rang 9 mit 3,1% auf **Rang 4** mit 8,9% vorgeschoben.

Die Verteilung auf 78 verschiedene Themenkategorien bestätigt weiterhin die Aussage, dass überall im Internet Angriffe durchgeführt werden. Es gibt sehr wohl Themengebiete, bei denen die Infektionsgefahr höher sein kann, jedoch ist kein Themengebiet per se böse oder per se harmlos. Angreifer orientieren sich an aktuellen Themen[10], setzen aber ansonsten auf ungerichtete, schnell auszuführende Angriffe, beispielsweise durch massenhafte Infektion von mit Sicherheitslücken versehen Webseiten. Das sichert Ihnen einen hohen Ertrag bei geringem Aufwand.

[9] 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.
[10] Beispiel: http://blog.gdata.de/artikel/explosionen-bei-boston-marathon-rufen-cyber-angreifer-auf-den-plan/

Kategorisierung nach Server-Standort

Bösartige Webseiten liegen auf den Host-Servern weltweit. Die unten stehende Karte, Abbildung 4, zeigt die Häufigkeitsverteilung der als bösartig gekennzeichneten Webseiten. In dieser Darstellung wird nicht zwischen Seiten mit Schadcode und Phishingseiten unterschieden.

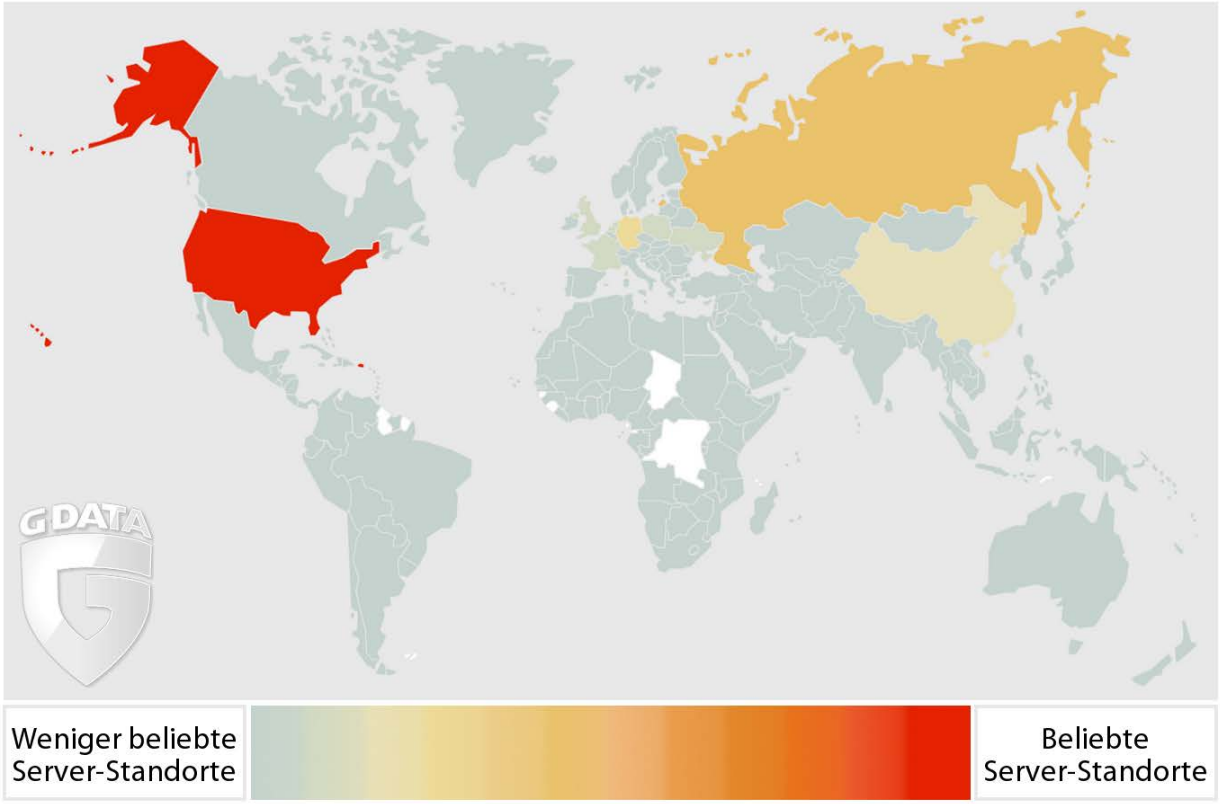

Abbildung 4: *Flächenkartogramm mit Informationen zur Häufigkeit der gehosteten, bösartigen Webseiten in den Ländern*

Die hochentwickelten Länder mit besonders guten infrastrukturellen Gegebenheiten in der Sparte Telekommunikation bleiben auch weiterhin die favorisierten Hosting-Länder für Angreifer. Dazu zählen die **USA**, **Russland**, die **Länder Mitteleuropas** (hier aktuell vor allem **Deutschland**) und auch **China**. Im Verhältnis haben Russland und Deutschland gegenüber früheren Auswertungen zugelegt.

Die in H2 2012 registrierten weißen Flecken auf dem afrikanischen Kontinent sind kleiner geworden. Auch hier fanden sich also zu Beginn des Jahres 2013 bösartige Webseiten, wenn auch nur wenige. Damit setzt sich der wahrgenommene Trend fort, dass die Zahl der gänzlich unbeteiligten Länder weiterhin abnimmt.

Online-Banking

Nachdem die Anzahl der Infektionen im zweiten Halbjahr 2012 kontinuierlich sank, konnte dieser Trend aufgehalten und teilweise umgekehrt werden. Im Juni 2013 waren die Infektionszahlen etwa ein Viertel höher als noch im Dezember 2012, nachdem die Infektionszahlen von Juli 2012 bis Dezember 2012 um zwei Drittel abgesunken waren.

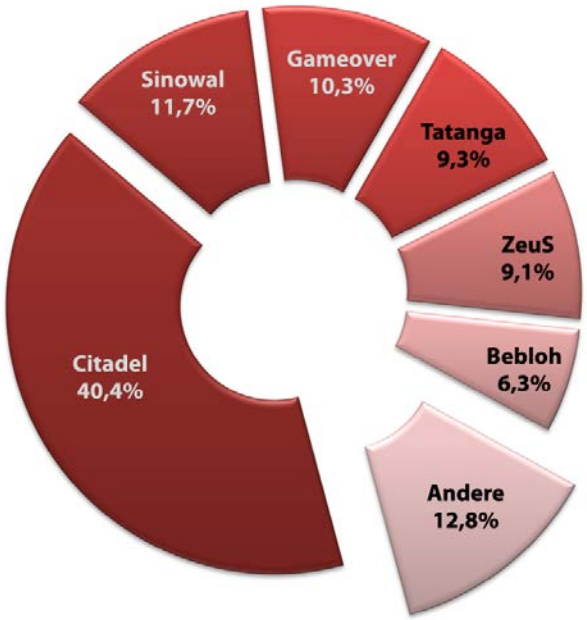

Abbildung 5: *Anteil der von BankGuard detektierten Banking-Trojaner Familien in H1 2013*

Q1 2013	
Citadel	34,7%
Gameover	14,8%
Sinowal	11,7%
Tatanga	11,2%
ZeuS	8,1%
Andere	19,5%

Q2 2013	
Citadel	42,4%
Sinowal	13,5%
ZeuS	9,1%
Tatanga	8,5%
Gameover	7,8%
Andere	18,7%

Tabelle 3: *Anteil der durch BankGuard detektierten Banking-Trojaner Familien in Q1 und Q2 2013*

Für die höheren Infektionszahlen ist weniger ein einzelner Trojaner, sondern eine ganze Reihe von Vorgängen verantwortlich. Die Chronologie des ersten Halbjahres 2013:

Im März und April konnten **Bankpatch** und **Tatanga** erhöhte Infektionszahlen vorweisen. Bei **Bankpatch** konnten diese durch die Verteilung einer neuen Version des Trojaners erzielt werden. Diese Version bedient sich zur Kommunikation des Jabber-Protokolls.

Mit **Cridex** konnte sich ein neuer Trojaner auf dem Markt positionieren. Insbesondere im April und Mai wies **Cridex** signifikante Infektionszahlen vor. Im Mai erreichte er sogar den dritten Platz in der Rangliste der häufigsten Banking-Trojaner.

Ende April wurde eine neue Version der **ZeuS-Variante Citadel** bekannt, nachdem der Autor zuvor als untergetaucht galt. Mit der Veröffentlichung dieser Variante gingen stark erhöhte Infektionszahlen einher. Der rapide Abfall der Infektionen im Juni hängt mit der organisierten Abschaltung (Takedown) von **Citadel** Command&Control-Servern durch Microsoft und verschiedene Behörden zusammen. Es wurde „gleichzeitig die Kommunikation zwischen 1.462 Citadel Botnetzen und den Millionen von infizierten Computern unter ihrer Kontrolle“ gekappt.[11]

Citadels deutliche Stärke im Mai bewirkte, dass in diesem Monat im Vergleich zum Januar doppelt so viele Infektionen festgestellt wurden. Auch wenn die Infektionszahlen von **Citadel** im Juni wieder auf ein durchschnittliches Niveau sanken, so lag die Gesamtzahl der Infektionen mit Banking-

[11] http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx

Trojanern immer noch um ein Viertel höher als im Januar. Daran hatten besonders **Bebloh** und auch **ZeuS** ihren Anteil:

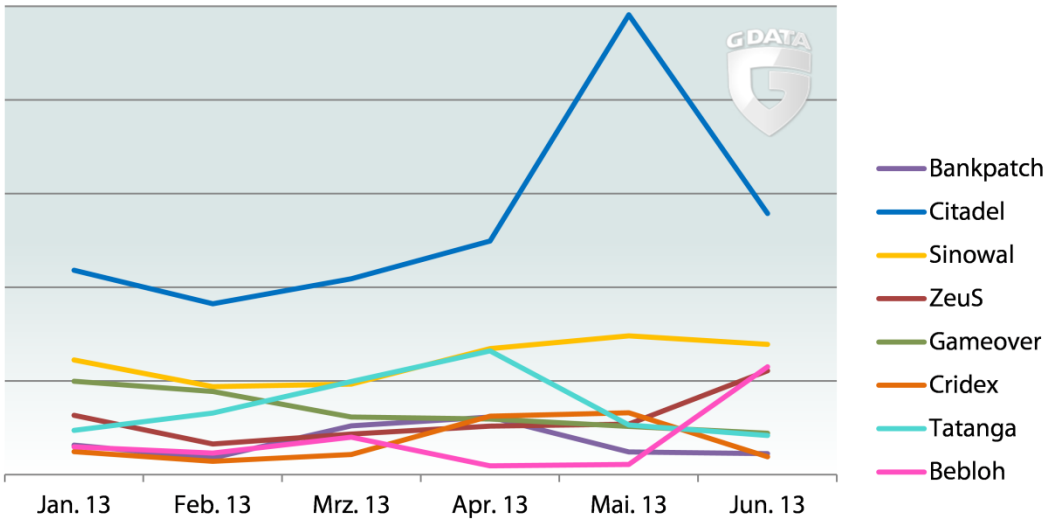

Abbildung 6: *Entwicklung der Infektionszahlen der auffälligsten Banking-Trojaner aus H1 2013*

Der Trojaner **Bebloh** (auch URLzone genannt) legte im letzten Halbjahr eine bemerkenswerte Entwicklung an den Tag. Dieser Trojaner ist zwar bereits seit längerer Zeit als sehr innovativ bekannt – z.B. durch die Vortäuschung von Retouren-Überweisungen – hatte aber trotzdem niemals besonders hohe Infektionszahlen. Im Juni hingegen konnte **Bebloh** sogar Platz drei in der Rangliste der häufigsten Banking-Trojaner erreichen.

Im Juni konnten außerdem stark erhöhte Infektionszahlen des **klassischen ZeuS-Trojaners** festgestellt werden. Diese könnten durch eine neue Gruppierung hervorgerufen worden sein, die sich des im Internet kursierenden Quellcodes bedient. Außerdem wurde ZeuS als Schadcode über Facebookseiten verbreitet und erlebte dadurch binnen kurzer Zeit eine regelrechte Wiederbelebung.[12] Die Angreifer erstellten für diese Masche Facebookseiten als Fälschungen von populären Sportvereinen und auch Sportartikelherstellern sowie Lederwarenherstellern und Sonnenbrillen-Labels, um die Opfer auf infizierte Seiten zu locken.

Bemerkenswert ist auch, dass nach **ZeuS** im Juni nun auch der Quellcode des Trojaners **Carberp** in Untergrundforen veröffentlicht wurde. Dieser Trojaner wurde von Sicherheitsforschern in der Vergangenheit oft als technisch besonders hochwertig beschrieben. Die Infektionszahlen von **Carberp** erreichten allerdings bisher nie besonders signifikantes Niveau.

Erste Analysen von G Data können die besondere technische Qualität auch nur teilweise bestätigen. Der Großteil des Quellcodes stellt aus Sicht von G Data keine signifikante Neuigkeit dar und ist dem Quellcode von **ZeuS** qualitativ eher unterlegen. Das beinhaltete Bootkit allerdings ist technisch hochwertig und könnte Cyberkriminelle motivieren, zukünftig zumindest diesen Teil des Trojaners mitzuverwenden.

[12] http://www.ibtimes.com/facebook-virus-hackers-exploiting-facebook-api-send-malware-nfl-nba-real-madrid-fc-fans-1314701

Fazit und Ausblick

Wie bereits im vorherigen MalwareReport prognostiziert, hat sich der Trend zu geringeren Infektionszahlen nicht fortgesetzt und teilweise sogar umgekehrt.

Mehr und mehr ist auf dem Markt der Trojanischen Pferde eine gewisse Diversifizierung erkennbar. Während früher einzelne Banking-Trojaner den Markt dominierten, ist ein klarer Trend zu mehreren gleichwertig auftretenden Trojanern erkennbar.

Dies dürfte den Strafverfolgungsbehörden die Arbeit erschweren: Während man sich zuvor auf einzelne Trojaner-Autoren fokussieren konnte, scheinen nun nach Ermittlungserfolgen und Festnahmen postwendend andere Autoren in die Bresche zu springen. Je nach Erfolg der Strafverfolgungsbehörden ist eine Fortsetzung dieses Trends zu erwarten. Nachdem im Jahr 2011 der **ZeuS**-Quellcode veröffentlicht wurde, findet sich nun auch der Quellcode von **Carberp** im Internet zugänglich, was die Entwicklung eigener Klone zudem leichter macht.

Wie prognostiziert, wurde an der Dezentralisierung der Botnetz-Kommunikation gearbeitet. **Bankpatch** hat hier mit der Kommunikation über den Chat-Dienst Jabber eine Vorreiterrolle eingenommen. Weitere Entwicklungen in diesem Bereich sind wahrscheinlich. Nach wie vor erscheint die Einführung der Kommunikation über Tor als eine sinnvolle Variante aus Sicht der Cyberkriminellen.