TRUST IN GERMAN SICHERHEIT

G DATA SECURITYLABS MALWARE REPORT

HALBJAHRESBERICHT JANUAR – JUNI 2014

INHALT

AUF EINEN BLICK

- Die Zahl neuer Schadprogrammtypen bleibt auf dem gleichen Niveau wie zuvor: Das erste Halbjahr brachte 1.848.617 neue Signaturvarianten hervor.
- Seit 2006 verzeichneten die G DATA SecurityLabs bisher 15.197.308 neue Schadprogrammtypen.
- Statistisch wurde alle 8,6 Sekunden ein neuer Schadprogrammtyp entdeckt.

- Die Anzahl neuer Schädlinge der Kategorie Adware stieg weiterhin stark an. Angreifer verdienen mit der Anzeige von unerwünschter Werbung und Co. viel Geld mit wenig Aufwand.
- Auch in der Auswertung der registrierten Angriffe auf PC-Benutzer lagen Schädlinge der Kategorie Adware weit vorn. Die Familie Swiftbrowse sticht dabei negativ hervor und war mit 34 Varianten für fast zwei Drittel aller MII-Rückmeldungen des Halbjahres verantwortlich.
- Die Zahl der neuen Rootkits sank dagegen erneut. Dieser anhaltende Trend ist unter anderem auf verbesserte Abwehrmaßnahmen in 64-Bit Systemen zurückzuführen.

- Ein Newcomer im Bereich Banking, namens Vawtrak, hielt seit Anfang März den Spitzenplatz unter den am häufigsten erkannten Banking-Trojanern
- Auch die Schädlinge der Familien Cridex, mit ihrem Abkömmling namens Swatbanker, sind im vergangenen Halbjahr auffällig aktiv gewesen.
- Im Mai 2014 wurde ein neues Allzeithoch bei den Detektionszahlen der Banking-Trojaner verzeichnet.
- Die Bank of America war nach einer Erhebung von G DATA das am häufigsten angegriffene Ziel von Banking-Trojanern, gefolgt von PayPal und der Citibank.
- Insgesamt wurden mindestens 825 verschiedene Ziele von Banking-Trojanern angegriffen.
- Die Banking-Trojaner hatten vor allem Banken und Bezahldienstleister aus dem anglophonen Sprachraum im Visier. Die 25 am häufigsten angegriffenen Ziele stammten zu 48% aus den USA, zu 24% aus dem Vereinigten Königreich und zu 16% aus Kanada.
- 40% der 25 häufigsten Ziele waren mit den obligatorischen Sicherheitsmaßnahmen des Ziels anfällig für klassische Keylogger; 80% waren anfällig für Banking-Trojaner, die unbemerkt vom Benutzer Transaktionen manipulieren können.

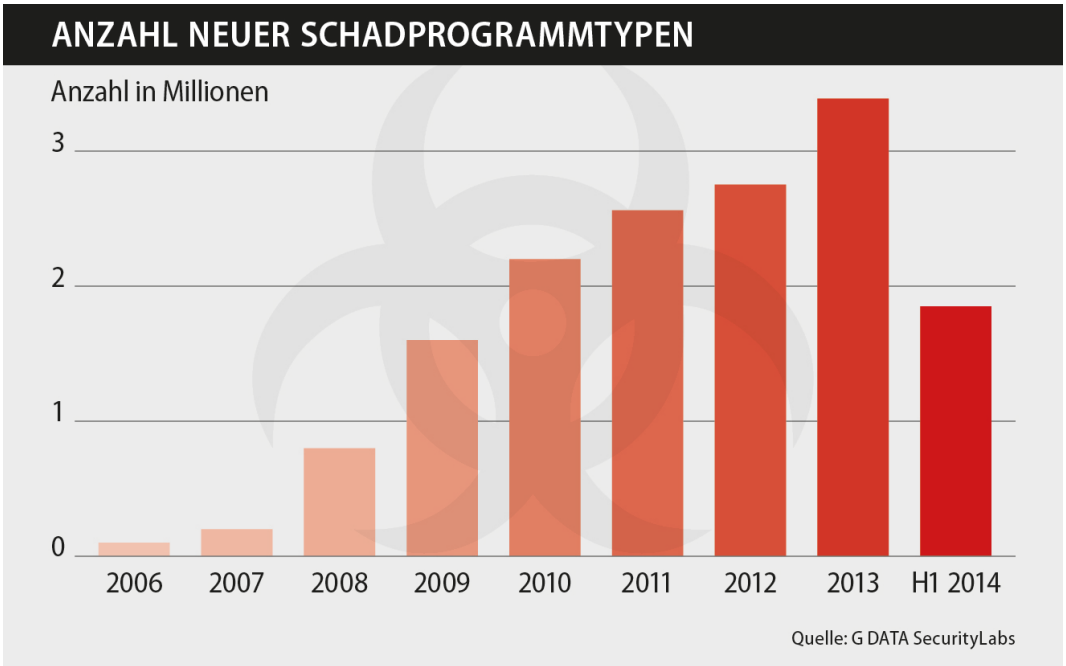
Prognosen und Trends

- Die Zeichen stehen auch weiterhin auf Wachstum: Nach Abschluss des Jahres 2014 wird die Marke von 3,5 Millionen neuen Schadprogrammtypen innerhalb eines Jahres überschritten.
- Der Bereich Adware hat sich bei Angreifern sehr etabliert und seine Schädlinge werden Computernutzer auch in Zukunft mit unerwünschten Einblendungen plagen.
- Banking-Trojaner sind ein höchst lukratives Geschäft und eine feste Größe in der Untergrundökonomie. Daher wird die Entwicklung der Banking-Trojaner auch im zweiten Halbjahr sehr dynamisch sein.

SCHADPROGRAMM-STATISTIKEN

Innerhalb der ersten sechs Monate des Jahres 2014 verzeichneten die G DATA SecurityLabs 1.848.617 neue Schadprogrammtypen[1]. Damit bleibt der Wert zwar nahezu konstant zum vorherigen Halbjahr (1.874.141), mit minimalem Minus von 1,38%, bedeutet aber insgesamt natürlich trotzdem eine deutliche Erhöhung des Angriffspotentials gegen Computernutzer.

Eine Betrachtung der Zahlen seit 2006 zeigt, dass die letzten 8,5 Jahre mehr als 15 Millionen neue Schadprogrammtypen hervorgebracht haben. Rein statistisch wurde in dieser gesamten Zeit alle 20 Sekunden ein neuer Schädling registriert! Die Schlagzahl hat sich jedoch deutlich erhöht, die nachfolgende Abbildung zeigt: Im ersten Halbjahr 2014 allein sinkt die statistische Zahl auf nur noch 8,6 Sekunden für eine Neuentdeckung. Das macht über 10.000 neue Malware-Typen pro Tag (10.327)!



Kategorien

Die Schadprogramme werden anhand der schädlichen Aktionen, die sie auf einem infizierten System ausführen, klassifiziert. Ein Blick auf diese Kategorien erlaubt eine Einschätzung zur aktuellen Angriffs-Ausrichtung von Cyber-Kriminellen. Die wichtigsten Kategorien sind in der Abbildung auf Seite 4 dargestellt. Prinzipiell ist jedoch zu beachten, dass eine hohe Anzahl neuer Schadprogrammtypen nicht zwingend einhergeht mit großer Gefahr oder Qualität, wie man am Beispiel **Adware** sieht. Ebenso wenig lässt eine niedrige Zahl neuer Signaturvarianten auf eine geringe Qualität oder mangelnde Gefährdung schließen, wie **Rootkits** und **Exploits** zeigen. Die Zahl der neuen Signaturvarianten der **Rootkits** und **Exploits** sank im vergangenen Halbjahr auf jeweils unter 1.000.

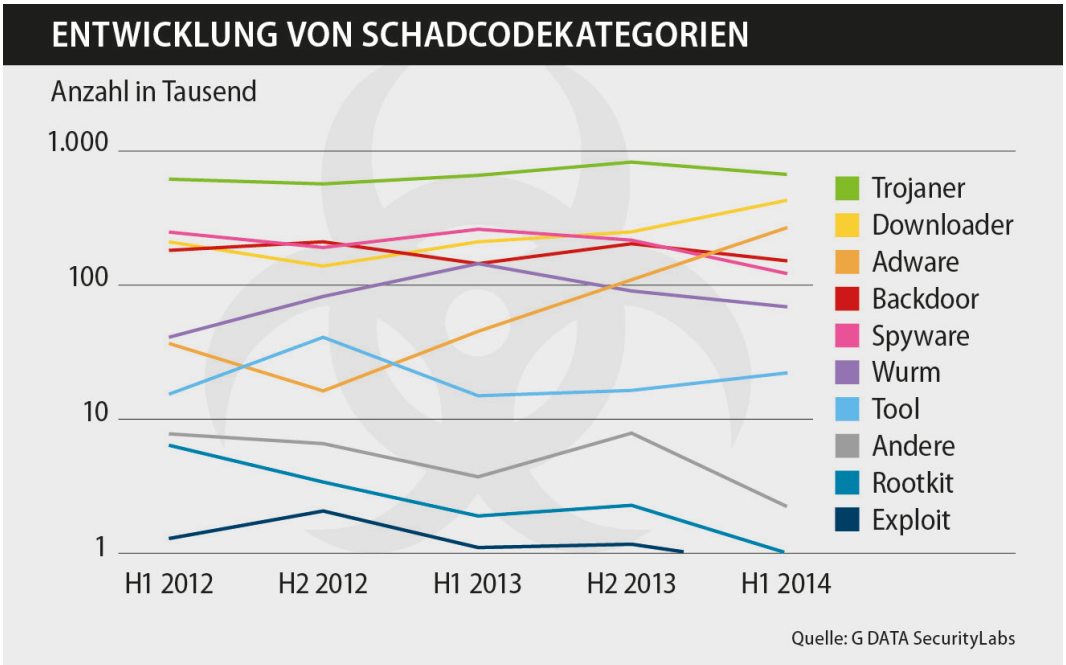
Speziell der Einsatz von **Rootkits** hat sich innerhalb der letzten Jahre deutlich gewandelt, denn mit dem Umstieg auf 64-bit Betriebssysteme sind die Angriffe für die Versteckkünstler deutlich schwieriger geworden. Eine der Schutzmaßnahmen, die mit neuen Windows OS-Generationen eingeführt wurde, ist der Kernel-Patch-Schutz.[2]

[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 2014 erstellt wurden.

[2] http://technet.microsoft.com/en-us/library/cc759759%28v=ws.10%29.aspx

Eine Umgehung dessen ist auch für Malware-Autoren sehr lange Zeit keine einfache Aufgabe gewesen. Ein Beispiel für die Aushebelung genau dieses Schutzes[3] wurde im Zuge der Analyse des **Uroburos-Rootkits**[4] entdeckt, einer hochkomplexen Spionagesoftware. Es gibt kaum einen Zweifel daran, dass die Zahl der neuen **Rootkits** auch wieder steigen wird.

Ganz im Gegensatz dazu setzt gerade die Kategorie **Adware** ihren Höhenflug weiter fort. Seit dem zweiten Halbjahr 2012 stiegen die Zahlen neuer Schadprogrammtypen dieser Kategorie rasant, um das 16-fache. 14% aller neuen Signaturvarianten fallen aktuell in die Kategorie **Adware**. Diese massive Steigerung zeigt sich, wie im vergangenen Halbjahr, auch in den abgewehrten Angriffen durch G DATA Produkte, ausgewertet im Kapitel GEFAHREN-MONITOR.



Plattformen – .NET-Entwicklungen auf dem Vormarsch

Zum wiederholten Mal konnte ein deutlicher Anstieg des Anteils von .NET-Entwicklungen (MSIL) verzeichnet werden. Ihr Anteil ist inzwischen sogar auf 8,5% gestiegen. An der Dominanz der Schadcodetypen, die auf Windows abzielen, hat sich auch im vergangenen Halbjahr nichts geändert – weiterhin liegt der Prozentsatz bei über 99,9%.

	Plattform	#2014 H1	Anteil	#2013 H2	Anteil	Differenz #2014 H1 #2013 H2	Differenz #2014 H1 #2013 H1
1	Win	1.688.719	91,4%	1.774.287	94,7%	-4,82%	+15,47%
2	MSIL	158.127	8,5%	97.686	5,2%	+61,87%	+240,44%
3	WebScripts	598	<0,1%	720	<0,1%	-16,95%	+10,70%
4	Scripts[5]	551	<0,1%	642	<0,1%	-14,26%	+277,19%
5	NSIS	399	<0,1%	252	<0,1%	+58,44%	+1561,91%

Tabelle 1: Top 5 der Plattformen der letzten beiden Halbjahre

[3] https://blog.gdata.de/artikel/uroburos-detaillierte-einblicke-in-die-umgehung-des-kernelschutzes/
[4] https://blog.gdata.de/artikel/uroburos-hochkomplexe-spionagesoftware-mit-russischen-wurzeln/
[5] Scripts sind Batch- oder Shell-Skripte oder Programme, die z.B. in den Skriptsprachen VB, Perl, Python oder Ruby geschrieben wurden.

GEFAHREN-MONITOR

Der Gefahren-Monitor gibt die Top 10 der abgewehrten Angriffe gegen Computernutzer[6] mit G DATA Sicherheitslösungen[7] und aktiviertem Benutzer-Feedback[8] an. Nachfolgend werden die am häufigsten abgewehrten Attacken aus dem ersten 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	55,8%
2	Adware.SwiftBrowse.B	4,0%
3	Adware.SwiftBrowse.P	2,5%
4	Adware.Relevant.CC	2,4%
5	Script.Application.Plush.D	2,2%
6	Script.Application.ResultsAlpha.D	1,8%
7	Win32.Application.Linkury.A	1,3%
8	Script.Application.JSLoadBrowserAddon.A	1,0%
9	Gen:Variant.Adware.Graftor.125313	0,5%
10	Win32.Application.SearchProtect.O	0,3%

Tabelle 2: Die Top 10 der an die MII gemeldeten Angriffe in H1 2014

Der beobachtete Trend, der rapide Anstieg von **Adware-Detektionen**, setzte sich auch in H1 2014 weiter fort. Die gesamten ersten Ränge der Auswertung sind fest in der Hand von Schädlingen aus der Kategorie **Adware**, die zur Gruppe der **„Potentiell Unerwünschten Programme" (PUP)** gehört. Insgesamt ging, statistisch gesehen, fast ¾ der Detektion auf das Konto der Schädlingsvarianten der Top 10 (71,8%).

Neue Hauptakteure sind allerdings nicht mehr die Schädlinge der Familie **Bprotect**, sondern die der Familie **Swiftbrowse**. Diese Familie belegt in den Halbjahres-Top-10 gleich drei Plätze und zeichnet sich allein mit diesen Plätzen für 62,4% aller Attacken dieses Halbjahres verantwortlich. Alle 34 in H1 aufgetretenen **Swiftbrowse-Varianten** addieren ihre Anteile sogar zu knapp 65%.
Schädlinge der Familie **Swiftbrowse** sind hochvariabel, ein Grund mehr für die hohe Anzahl an Detektionen. Der Plagegeist benutzt über 80 verschiedene Kampagnen-Decknamen, wie zum Beispiel: WebGet, BetterBrowse, EnhanceTonic, ... 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.
Die extrem hohen Detektionszahlen resultieren unter anderem daraus, dass die Installation von **Swiftbrowse** serverseitig gesteuert wird. Das bedeutet, dass das Browser Plug-In bei jeder Öffnung des Browsers versucht, sich zu dem zur Kampagne gehörigen Server zu verbinden und von dort schädlichen Code nachzuladen. Dieser Versuch wird von den Scannern erkannt und geblockt.

---

[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

Jede **Swiftbrowse-Kampagne** hat ihren eigenen Webauftritt und ihre eigene zugehörige Domain. Alle sind jedoch im selben Stil gestaltet und alle sind registriert auf Yontoo LLC, gegründet im Jahr 2011. Yontoo LLC ist eine von mehreren Tochterfirmen von Sambreel Holdings. Schon in der Vergangenheit gab es negative Medienberichte über die Firma Sambreel als sie unerlaubt Werbungen auf Google, Facebook, der New York Times Webseite und weiteren kaperte und damit sogar juristische Mühlen in Gang brachte.[10] Auch der Videodienst YouTube und seine Nutzer wurden von Sambreel belästigt, mit Malvertizing.[11] Die Drahtzieher hinter diesen beobachteten und massiven Kampagnen sind also keineswegs Unbekannte und ein Ende der Belästigungen ist nach aktuellem Stand nicht abzusehen.

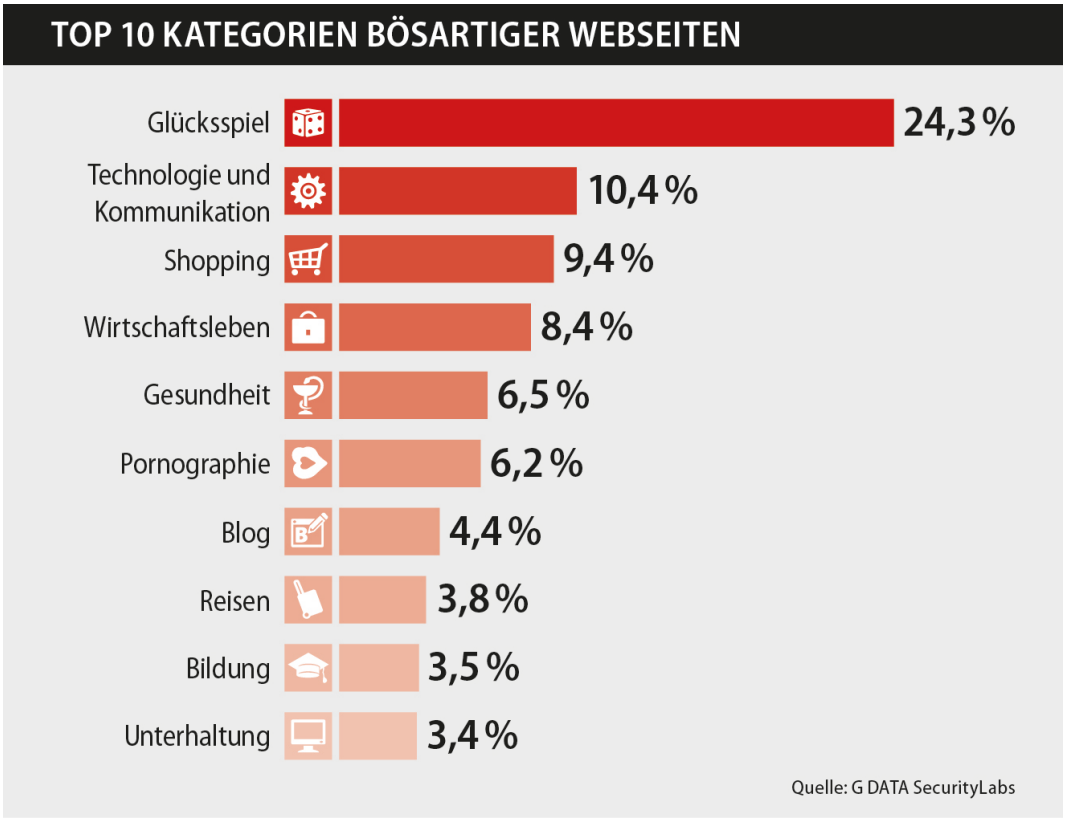
Das massive Auftreten der **PUP-Schädlinge** wirft gerade bei Kunden immer häufiger Fragen auf. Tech-Foren sind gefüllt mit Beschwerden zum Thema **„Potentiell Unerwünschte Programme"**. Die Nutzer klagen, dass „ein Virus ihren Browser infiziert hat" oder sich „eine Toolbar in den PC gehackt hat" und sie empfinden dies zu Recht als unglaublich störend. Von Malware im klassischen Sinne kann hier jedoch nicht gesprochen werden und die allermeisten dieser „Infektionen" ließen sich sogar vermeiden. Die Experten der G DATA SecurityLabs haben sich deshalb in einem Blogeintrag explizit mit diesem Thema beschäftigt, um aufzuklären.[12]
PUP sind in den meisten Fällen Programme, die Browser-Einstellungen verändert, Werbung einblendet und unerwünschte Angebote anzeigt – damit belästigen sie den Nutzer und erwirtschaften für den Verteiler Geld. Dabei gelangen diese Programme in aller Regel nicht etwa durch das Ausnutzen von Sicherheitslücken auf den Rechner, sondern werden häufig, vom Nutzer unbemerkt, als ungewünschtes Extra mitinstalliert. Angreifer verpacken diese Zusätze gerne mit populären Freeware-Programmen und verteilen sie im Internet. Daher ist es ratsam, sich Programme nur direkt von den Herstellerseiten herunterzuladen oder von vertrauenswürdigen Drittanbietern zu beziehen. Außerdem sollten die Installationsdialoge aufmerksam gelesen werden und dabei jedes Options-Feld, vor allem die bereits mit einem Haken versehenen, überprüft werden.

[10] http://www.zdnet.de/41558662/pagerage-bringt-facebook-in-rage/
http://www.nzz.ch/aktuell/digital/sambreel-hertz-facebook-1.17708909
http://www.thewire.com/technology/2012/10/meet-company-hijacking-new-york-times-ad-revenue/58147/
[11] http://www.spider.io/blog/2013/08/sambreel-is-still-injecting-ads-video-advertisers-beware/
[12] https://blog.gdata.de/artikel/potentiell-unerwuenschte-programme-viel-mehr-als-nur-nervig/

WEBSEITEN-ANALYSEN

Kategorisierung nach Themen

Die nachfolgende Grafik stellt dar, wie die als bösartig eingestuften Webseiten[13] im ersten Halbjahr 2014 nach Themen kategorisiert werden können. Insgesamt machen die Top 10 einen Anteil von 80,3% aller eingeordneten Webseiten aus und damit deutliche 8,3% mehr als noch im Halbjahr zuvor. Die Top 5 alleine sind für 59,0% verantwortlich.



Wiedereinsteiger in diesem ersten Halbjahr ist die Kategorie **Bildung** – sie hatte es in H2 2013 knapp nicht in die Top 10 geschafft, steigt nun aber wieder neu auf Rang 9 ein, mit 3,5%, und verdrängte die Kategorie **Spiele**.

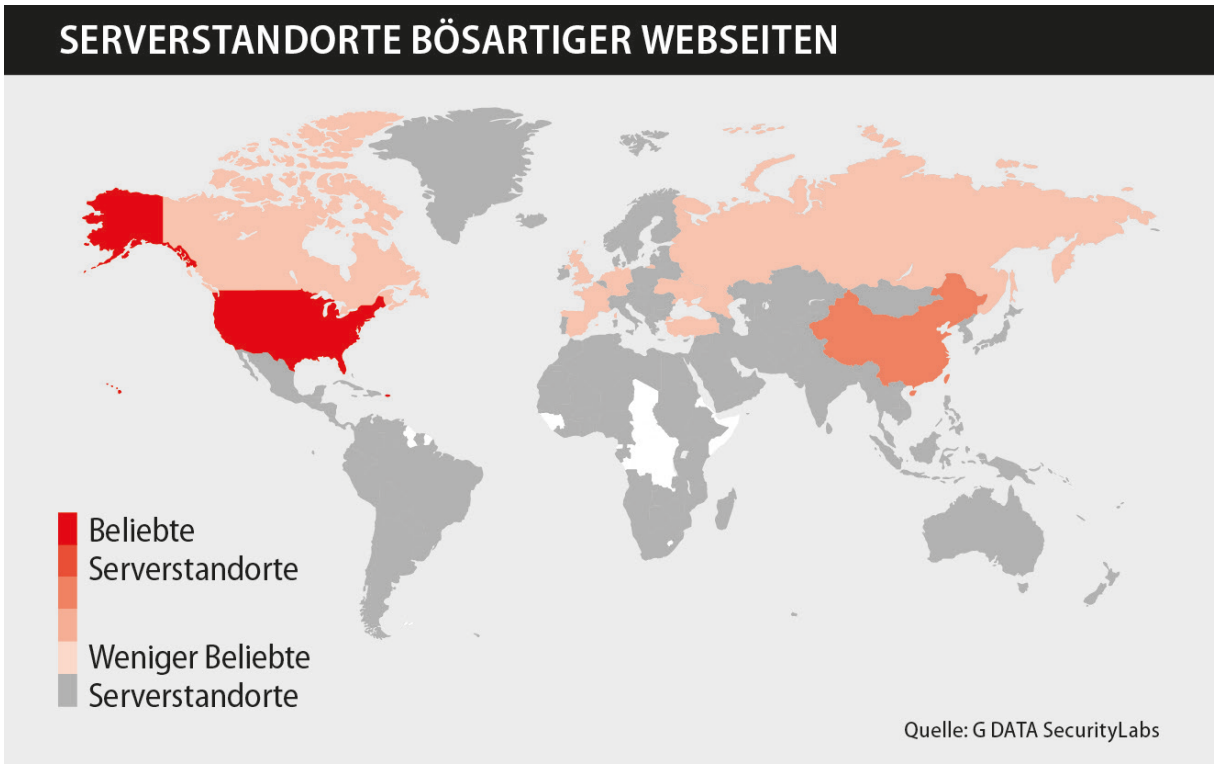
Im zweiten Halbjahr 2013 trat die Kategorie **Glücksspiel** als neues Thema auf Platz 9 hervor und belegt nun sogar Rang 1 der Auswertung von H1 2014. Jede vierte bösartige Webseite lag demnach im Bereich der **Glücksspiele**. Den Untersuchungen nach handelte es sich bei den attackierten Glücksspielseiten in erster Linie um kleine und weniger populäre Seiten. Angreifer verschaffen sich unerlaubt Zugriff auf den Webspace der Casinos und hinterlegen zum Beispiel Phishing-Seiten für populäre Bezahldienstleister, Banken, Webmailer und vieles mehr. Die Links zu diesen Phishing-Seiten verbreiten sie dann unter anderem in Spam E-Mails und locken Opfer unter dem Vorwand von drohenden Kontosperrungen oder ähnlich bedrohlichen Szenarien auf die Seiten.
Wird auf den angegriffenen Webseiten Schadcode hinterlegt, handelt es sich dabei häufig um Exploit-Kits. Skripte überprüfen den Rechner auf Schwachstellen und anschließend wird gegebenenfalls ein passender Angriff auf den Rechner gestartet. Infiziert werden die Rechner dann mit beispielsweise Banking-Trojanern, Spyware oder Malware, die sie in einen Zombie-Rechner verwandelt.

[13] 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.

Der Glücksspielmarkt im Internet boomt und viele neue Anbieter drängen auf den Markt. Angreifer sehen hier eine Chance, ihre Trefferquote der Angriffe zu erhöhen, indem sie Trends folgen. Mit der Aussicht auf schnellen Profit leiden jedoch auf Anbieterseite viel zu häufig die Qualität der eingerichteten Webseiten und damit auch ihre Absicherung. Dies machen sich Angreifer zunutze. Sie finden eine große Zahl möglicher anzugreifender Seiten und eine große Zahl potentieller Opfer, die diese Seiten besuchen.

Kategorisierung nach Server-Standort

Bei dieser Auswertung werden bösartige Webseiten lokalisiert. Egal ob es sich um eine Phishing-Seite oder um eine Webseite mit Schadcodebefall handelt, alle werden auf ihren Serverstandort hin überprüft. Die nachfolgende Weltkarte stellt dar, welche Länder bei den Angreifern besonders beliebt sind.



Auffällig ist, dass es in **Europa** keine deutlichen Unterschiede in der Beliebtheit der Serverstandorte mehr gibt. Hatte **Deutschland** in den vergangenen Halbjahren noch einen höheren Anteil an den bösartigen Seiten, liegen die europäischen Länder nun alle auf einem Niveau. Auch der Anteil der auf **russischen Servern** hinterlegten Seiten ist gesunken.

Im Gegensatz dazu findet sich jedoch **Kanada** nun ebenfalls auf Stufe zwei der beliebtesten Standorte, wenn auch noch weit hinter den **USA**.

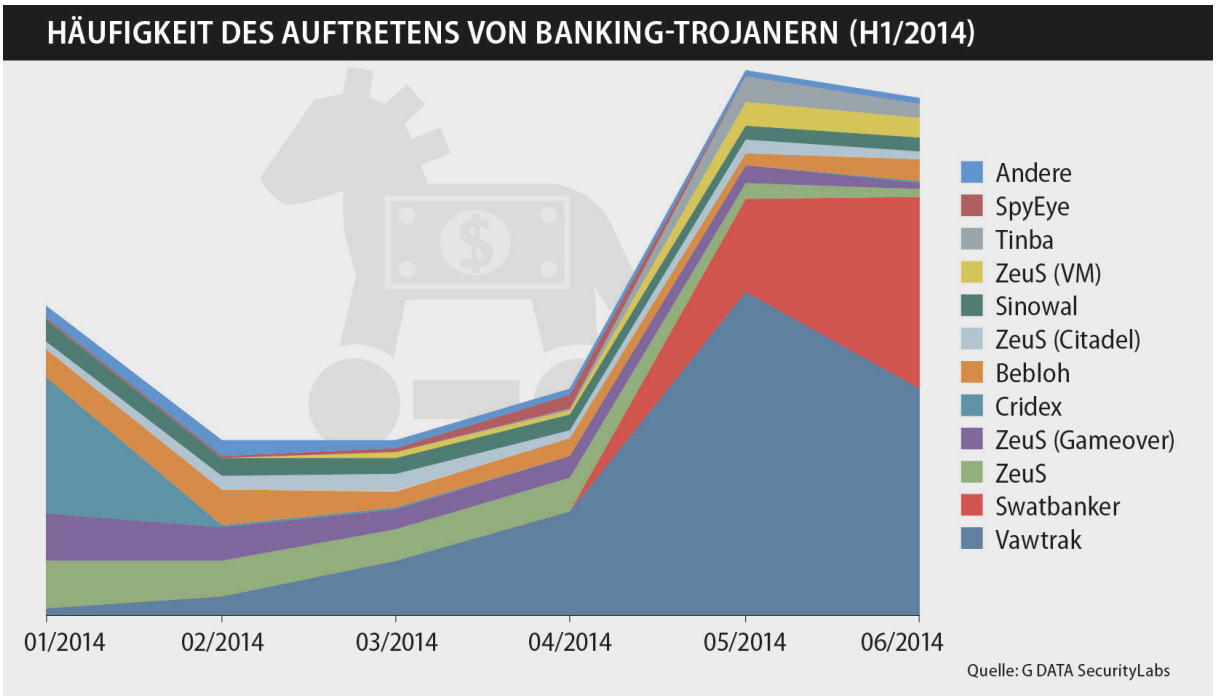
Die „weißen Flecken“ in **Afrika**, also die Länder, in denen laut unseren Kenntnissen im letzten Halbjahr keine bösartigen Webseiten hinterlegt waren, sind wieder etwas vergrößert, jedoch nicht überraschend verändert. **Zentralafrika** ist und bleibt eine Region mit nicht optimalen Bedingungen für Cyber-Attacken.

BANKING

Trends auf dem Trojaner-Markt

Das Bild auf dem Markt für Banking-Trojaner hat sich im ersten Halbjahr 2014 stark gewandelt. Ehemals dominante Schädlinge wurden von neuerer Malware verdrängt und zuvor scheinbar kleine oder auch gar komplett neue Trojaner-Familien haben den Platz der etablierten Alten übernommen und die Detektionszahlen zeitweise auf Rekordwerte getrieben.

Auch die Angriffsvektoren haben sich zum Jahr 2014 hin gewandelt und sind den Detektionszahlen zufolge besorgniserregend erfolgreich. Einerseits waren nach wie vor Exploit-Kits aktiv. Andererseits infizierten die Kriminellen hinter den Banking-Trojanern in der letzten Zeit jedoch zusätzlich eine große Anzahl an Computern mit massiven Spam-Wellen als Ausgangspunkt.
Anfang des Jahres konnte bei einer solchen Welle festgestellt werden, wie der bis dahin eher unauffällige Banking-Trojaner **Cridex**, auch als **Feodo** bekannt, in einer leicht modifizierten Variante massenhaft verteilt wurde. Er versteckte sich hinter Hyperlinks in E-Mails, die angeblich zu Rechnungen zeigten.[14] Diese Angriffswelle flachte zum Februar hin stark ab und verebbte kurze Zeit später vollständig. Nach zweimonatiger Pause kamen die, vermutlich, gleichen Angreifer mit derselben Masche zurück und verteilten in dieser Welle massenhaft Schädlinge der Familie **Swatbanker**/**Geodo**, einen bisher unbekannten und vermutlich ausschließlich für diese Angriffe programmierten Banking-Trojaner. In einigen Belangen weist dieser eindeutige Parallelen zu **Cridex** auf und kann daher als dessen Nachfolger betrachtet werden.[15]



Parallel zu **Cridex** und **Swatbanker** etablierte sich ein weiterer Schädling und seine Detektionszahlen überstiegen innerhalb weniger Monate alle der in den letzten Jahren beobachteten Banking-Trojaner. **Vawtrak**, dessen erstes Erscheinen kaum ein Jahr[16] her ist, hatte sich im Verlauf von 2013 stark unter dem Radar gehalten, im ersten Halbjahr 2014 stiegen seine Detektionswerte in den Statistiken dann aber wegen der Verbreitung in sowohl

[14] https://blog.gdata.de/artikel/cridex-banking-trojaner-auf-dem-vormarsch/
[15] https://blog.gdata.de/artikel/massive-spam-kampagne-kehrt-zurueck-cridex-nachfolger-swatbanker-wird-verbreitet/
[16] http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/Vawtrak.A

Exploit-Kits als auch über Spam steil nach oben. Seit Anfang März hält **Vawtrak** den Spitzenplatz unter den am häufigsten erkannten Banking-Trojanern.

Der parallel verlaufende, starke Anstieg von **Cridex**/**Swatbanker** und **Vawtrak** hat die insgesamt relativ niedrigen Infektionszahlen über Februar und März im Mai auf mehr als das Dreifache ansteigen lassen und damit ein neues Allzeithoch erreicht, was gegen Ende des ersten Halbjahres nur leicht zurück ging.

Der starke Rückgang der erhobenen Zahlen zur **ZeuS-Familie**, die die Varianten **Citadel**, **Gameover** und **VM** hervorgebracht hat, lässt sich nur teilweise erklären: Für **Gameover** gab es im Laufe des Halbjahres zwei wichtige Ereignisse. Zum einen wurde durch eine neue Variante von **Gameover** im März das **Kernelmode Rootkit Necurs** mitgeliefert.[17] Der einzige Zweck dieses Rootkits bestand darin, die Entfernung von **Gameover** zu verhindern, oder zumindest schwieriger zu gestalten. Dass dieser Plan misslang, sieht man an den stark sinkenden Detektionszahlen der darauf folgenden Monate. Die Erklärung hierfür liegt jedoch relativ nahe: Während die Angreifer hinter **Gameover** viel Aufwand betreiben, um die ausführbare Datei mit **Gameover** vor Antivirensoftware zu verstecken, ist das Rootkit **Necurs** jedoch relativ alt und wird von den meisten AV-Produkten zuverlässig erkannt. Die Kopplung der beiden Dateien hat demnach zu einer höheren Erkennung geführt, was wiederum die Infektionszahlen senkt.
Einen schweren Schlag erhielt **Gameover** außerdem im Juni, als das gesamte Botnet von amerikanischen Behörden übernommen und damit lahmgelegt wurde.[18]

Die **ZeuS Variante VM**, auch **KINS** genannt, hat dagegen stark zugelegt. War sie in den vorherigen Jahren kaum vertreten, hat sie mit einer neuen Version seit Februar etliche Infektionen vorzuweisen und ebenfalls im Mai ihren Höhepunkt erreicht.

Eine weitere, aus dem letzten Halbjahr des vergangenen Jahres absehbare, Entwicklung hat sich bestätigt. Die Erkennungszahlen der Trojaner-Familien **Tatanga** und **Bankpatch** sind stark zurückgegangen und fast nicht mehr sichtbar. Ebenso zeigt sich für **Sinowal** weiterhin eine starke Abwärtstendenz und bei gleichbleibender Entwicklung werden diese Familien in den kommenden Monaten fast vollständig von der Bildfläche verschwunden sein.

Eine kleinere Wiederbelebung hat der Banking-Trojaner **Tinba** erfahren, der seit Mai wieder deutlich verstärkt auftrat, was möglicherweise auf den Verkauf und die Verbesserung des Quellcodes zurückzuführen ist.[19]

Der Bereich der Banking-Trojaner ist nach wie vor einer der lukrativsten in der Untergrundökonomie. Dort wird viel Geld verdient, das unter anderem in die Verbesserung bestehender und Entwicklung neuer Banking-Trojaner investiert wird. Auch im zweiten Halbjahr von 2014 erwarten wir viel Bewegung im Bereich der Banking-Trojaner.

[17] http://stopmalvertising.com/rootkits/analysis-of-zeus-gameover-with-necurs.html
[18] http://blogs.microsoft.com/blog/2014/06/02/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup/
[19] https://www.csis.dk/en/csis/news/4303/

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 Schädlingstypen entsprechend, auf Banken und Finanzdienstleister.

Funktionsweise der Angriffe

Bei den Angriffen von Banking-Trojanern, muss im Prinzip zwischen zwei Formen unterschieden werden: es gibt unsichtbare Attacken und Attacken aus dem Bereich **Social Engineering**.

Bei unsichtbaren Attacken meldet sich der Nutzer beispielsweise bei seiner Bank an, führt eventuell eine Überweisung aus und ihm wird Geld gestohlen, ohne dass er irgendetwas davon bemerkt hätte.

Bei Angriffen über **Social Engineering** ist eine Interaktion des Schädlings mit dem Angreifer nötig, wobei der Kunde den Angreifer letztlich für seine Bank hält. Damit können z.B. auf Online-Banking-Portalen Popups angezeigt werden, die dem Benutzer suggerieren, er müsse aus angeblichen Sicherheitsgründen eine Testüberweisung durchführen, die tatsächlich aber eine echte Überweisung ist.

Angriffe über Social Engineering sind für Banken wie auch Benutzer bisweilen sehr schwierig zu erkennen. Schützen kann vor allem der sprichwörtliche menschliche Sachverstand des Benutzers, wobei auch hier die Erkennungschance von der Qualität des Angriffs und dem Wissen des Benutzers über die entsprechenden Protokolle abhängt. Eine Forderung nach einer Testüberweisung mit vielen sprachlichen Fehlern ohne weitere plausible Gründe mag bei vielen Benutzern einen Verdacht aufkommen lassen. Ist die Meldung aber sprachlich korrekt und es gibt mehr oder weniger plausible Gründe, wie z.B. eine angebliche Synchronisierung des TAN-Generators, wird die Erkennung für nicht fachkundige Benutzer sehr schwer.

Technisch realisieren Banking-Trojaner ihre Angriffe mit sogenannten **Webinjects**. Dabei handelt es sich um Codeschnipsel, die ein Banking-Trojaner in Webseiten einfügen kann, während ein infizierter PC eine Zielseite öffnet. Mit **Webinjects** kann dann z.B. im Verlauf einer Online-Banking-Session auch Code eingeschleust werden, der u.a. durch Manipulation der Liste von Überweisungen oder des Kontostandes verhindert, dass einem Benutzer im Online-Banking betrügerische Transaktionen auf seinem Konto auffallen. Dadurch soll verhindert werden, dass das Opfer seine Bank kontaktiert und diese die betrügerische Transaktion stoppen kann.

Sicherheitsmaßnahmen

Banken versuchen, Angriffen durch eigens implementierte Maßnahmen entgegenzutreten. Grundsätzlich muss unterschieden werden, ob die Maßnahmen obligatorisch (für den Kunden verpflichtend) oder optional sind. Einige häufig vorkommende Sicherheitsmaßnahmen sollen hier kurz vorgestellt werden. Da alle Sicherheitsmaßnahmen bei verschiedenen Banken unterschiedlich stark entwickelt sind, beziffert die im Folgenden vorgestellte Auswertung nur die relative Angriffshäufigkeit, sagt aber nichts darüber aus, ob diese Angriffe auch erfolgreich sind.

Einwegpasswörter

Die am häufigsten genutzte Sicherheitsmaßnahme sind Einwegpasswörter. Diese funktionieren, dem Namen entsprechend, nur für einen einzigen Vorgang. Manchmal entspricht ein Vorgang dabei einer Anmeldesitzung, manchmal auch einer einzelnen Finanztransaktion. Im Kontext der Transaktion wird ein Passwort oft als TAN, Kurzform für Transaktions-Nummer, bezeichnet.

Einwegpasswörter stellen sicher, dass ein Angreifer durch das reine Wissen des Einwegpassworts noch keinen Angriff durchführen kann, denn das Passwort wurde ja schon vom Opfer verbraucht. Mit dieser Methode lassen sich Angriffe durch einfache Keylogger effektiv verhindern.

Für die Generierung von Einwegpasswörtern gibt es verschiedene Verfahren:
Der Einsatz von Listen mit Passwörtern zum Abstreichen, sogenannten TAN-Listen, ist häufig. Oft werden Transaktionsnummern aber auch über einen zweiten Kanal zum Kunden versendet – entweder über das Mobilfunknetz („mTAN" oder „smsTAN"), oder aber über ein anderes zusätzliches Gerät (z.B. „chipTAN"). Wenn die Transaktionsdaten auf dem zweiten Kanal nochmals überprüft werden können, z.B. durch die Anzeige des Zielkontos und des Betrags auf dem Handydisplay in der SMS mit der TAN, können heimliche Transaktionsänderungen verhindert werden. Solche Transaktionsänderungen können ansonsten durch Online-Banking-Trojaner vorgenommen werden.
Ein Beispiel: Das Opfer will an ein bestimmtes Zielkonto 100€ überweisen. Der Banking-Trojaner ändert, für den Kunden unsichtbar, die Zielkontonummer in eine von ihm kontrollierte und den Betrag auf 1.000€. Wird die eingegebene TAN einfach von einer Liste abgestrichen, bemerkt das Opfer die Manipulation auf seinem Rechner nicht oder zumindest nicht rechtzeitig. Werden die Transaktionsdaten aber vor der Durchführung z.B. nochmals auf einem Mobiltelefon in der SMS mit einer TAN angezeigt, kann das Opfer die Manipulation rechtzeitig entdecken und die Transaktion unterbrechen.

Mehrwegpasswörter und persönliche Fragen

Zwischen Einwegpasswörtern und Dauerpasswörtern wird oft ein Zwischenweg eingesetzt. Es kann zum Beispiel ein neunstelliges Passwort geben, von dem bei jedem Login drei vom System zufällig ausgewählte Stellen eingegeben werden müssen. Oder der Benutzer wird bei seiner ersten Anmeldung aufgefordert, einige Sicherheitsfragen zu beantworten, z.B. nach dem Mädchennamen der Mutter, der eigenen Lieblingsfarbe, dem ersten Auto, etc. Einige Dienste erlauben auch das Erstellen gänzlich eigener Fragen mit dazugehörigen Antworten. Im weiteren Verlauf werden dann bei jedem Log-In-Vorgang eine oder mehrere dieser Fragen gestellt.

Diesen Verfahren ist gemein, dass dadurch ein gewisser Schutz gegen **Keylogger** besteht. Ein Angreifer kann sich nur mit aufgezeichneten Anmeldeinformationen einloggen. Da aber nicht immer alle Sicherheitsfragen gestellt werden, ist ungewiss, ob der Angreifer die Sicherheitsfragen gestellt bekommt, die er auch beim Opfer aufzeichnen konnte. Eine Rolle spielt hier natürlich auch die konkrete Implementierung der Bank, also z.B. ob der Angreifer bei einem zweiten Log-In-Versuch eine andere Frage gestellt bekommt, die er im Gegensatz zur ersten Frage vielleicht aufgezeichnet hat.

Man muss zwar feststellen, dass die Schutzwirkung dieser Sicherheitsmaßnahme begrenzt ist, trotzdem wurde in der folgenden Evaluation von einem Schutz gegen **Keylogger** ausgegangen, sofern die Maßnahmen implementiert wurden.

Plausibilitätsprüfung

Einige Banken beziehen weitere, eher unsichtbare, Sicherheitsmaßnahmen mit ein. Häufig wird von Fingerabdrücken der angemeldeten Benutzerrechner sowie von Plausibilitätsprüfungen geredet.

Ein Beispiel: Ein Benutzer meldet sich, seinem üblichen Profil nach, immer aus Großbritannien an und verfügt ausschließlich inländische Überweisungen. Wenige Minuten nach seiner letzten Abmeldung aus dem Service, wie üblich aus Großbritannien, meldet er sich vermeintlich von einem in Russland stationierten PC aus an und verfügt eine Überweisung nach Russland. Es ist offensichtlich, dass diese Transaktion nicht plausibel ist. Die Bank könnte in diesem Fall also die Transaktion blocken bzw. nur auf explizite Bestätigung des Kunden hin durchführen. Im Prinzip kann man sich solche Prüfungen als eine Adaptierung des menschlichen Sachverstands vorstellen, die zu einer automatischen Prüfung auf Bankenseite wird. Da die Funktionsweise dieser Prüfungen in der Regel aus

Sicherheitsgründen nicht transparent ist, werden diese bei der folgenden Evaluierung nur dann weiter betrachtet, wenn es explizit bekannte Sicherungen gibt, z.B. wenn eine Überweisung an einen bisher unbekannten Empfänger weitere Sicherheitsmaßnahmen auslöst.

Phishingschutz durch Personalisierung

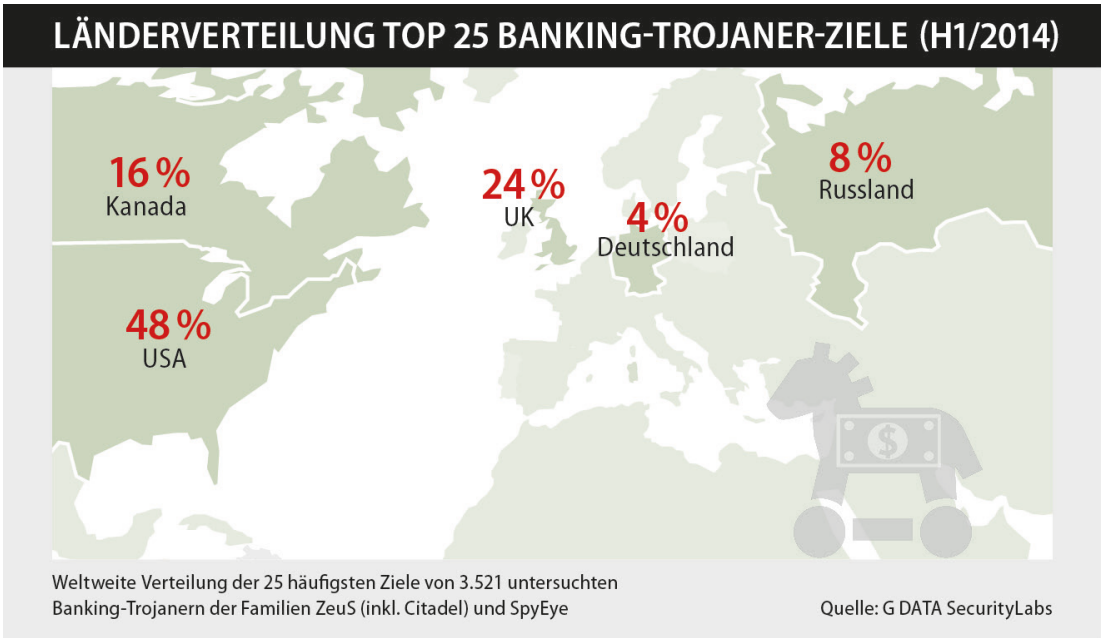
Eine weitere, oft verwendete Sicherheitsmaßnahme ist die Personalisierung des Anmeldevorgangs. Am häufigsten kann dabei ein persönliches Bild gewählt werden. Dieses wird vom Kunden bei seiner ersten Anmeldung an der Webseite der Bank frei gewählt. Dieses Bild wird dem Kunden vor dem letzten Schritt des Anmeldevorgangs gezeigt. Wenn dem Kunden das selbst gewählte Bild nicht angezeigt wird, kann er davon ausgehen, gerade Ziel eines **Phishing-Angriffs** geworden zu sein und er sollte den Anmeldevorgang umgehend abbrechen. Da nur der Betreiber der Webseite und der Kunde von diesem Bild wissen, kann der Angreifer die Webseite nicht vollständig fälschen.

Das persönliche Bild ist jedoch lediglich ein Schutz gegen **Phishing**. Angriffe durch Banking-Trojaner sind hiervon nicht berührt, da diese im Kontext der legitimen Bankseite agieren und daher die Oberfläche für den Benutzer legitim erscheint. In der folgenden Evaluierung wurden Maßnahmen dieser Art in der Regel nicht weiter beachtet.

Ergebnisse

Eine tabellarische Auswertung der Ergebnisse wird auf Seite 15 gegeben. Insgesamt wurden durch die untersuchten Banking-Trojaner 825 verschiedene Ziele angegriffen. Häufigstes Ziel war dieser Studie nach die Bank of America unter „bankofamerica.com“, die in 12,98% der untersuchten Banking-Trojaner-Konfigurationen als Angriffsziel eingebettet war.

Die ermittelten Top 25-Ziele wurden im Mittel von 8,68% der untersuchten Banking-Trojaner angegriffen, die Top 100-Ziele im Mittel von 4,69%, und alle 825 Ziele von 0,83%. Es liegt also keine Gleichverteilung vor, sondern die kriminellen Hintermänner bevorzugen offenkundig bestimmte Banken. Es ist anzunehmen, dass sich die Angreifer bei der Auswahl ihrer Ziele am erwarteten Erfolg orientieren. Dafür dürften Faktoren wie die Kundenzahl, der durchschnittlich erwartete Profit sowie die Sicherheitsmaßnahmen der Bank eine tragende Rolle spielen. Unter den Top 25 der angegriffenen Ziele stammten zwölf aus den **USA**, sechs aus dem **Vereinigten Königreich** und vier aus **Kanada**. Damit waren 88% der Angriffsziele im anglophonen Sprachraum zu finden. Zwei Zahlungsdienstleister stammten aus **Russland**. Aus **Deutschland** war nur eine Bank in der Topliste.



Die von Brand Finance Plc ausgewiesenen weltweit wertvollsten Banken in 2013 befinden sich ebenfalls unter den untersuchten Top 25 und haben allesamt Hauptsitze im anglophonen Sprachraum.[20]

Fast die Hälfte (40%) der Top 25-Ziele waren mit den obligatorischen Sicherheitsmaßnahmen anfällig für klassische **Keylogger**. Wenn vom Kunden sämtliche optionale Sicherheitsmaßnahmen in Anspruch genommen wurden, waren es immer noch 12%.
Vier von fünf Zielen (80%) waren anfällig für Banking-Trojaner, die unbemerkt vom Benutzer Transaktionen manipulieren können, wenn der Kunde nur obligatorische Sicherheitsmaßnahmen in Anspruch nimmt. Bei der Inanspruchnahme von zusätzlichen Sicherheitsmaßnahmen waren es immer noch mehr als drei Viertel (76%).

Vor Banking-Trojanern, die Techniken aus dem Bereich des **Social Engineering** benutzen, sind sowohl Banken als auch die anderen Betreiber der attackierten Webseiten relativ machtlos. Hier helfen nur clientseitige Schutzsysteme. Ein solches clientseitiges Schutzsystem zum Schutz vor Angriffen durch Online-Banking-Trojaner ist G DATA BankGuard. In der neuen Produktgeneration 2015 ist zudem die Keylogger Protection als neues Feature enthalten, das Angriffe per **Keylogger** unterbindet.

[20] Markenwert nach http://www.brandfinance.com/images/upload/the_banker_brand_finance_banking_500_full_results.pdf

TOP 25 DER ANGRIFFSZIELE VON BANKING-TROJANERN (H1/2014)

	Land	Rating Markenwert nach Brand Finance	Schutz gegen stille Banking-Trojaner verpflichtend	 optional	Schutz gegen Keylogger verpflichtend	 optional	Angriffshäufigkeit Relative Angriffshäufigkeit der Ziele von 3.521 untersuchten Banking-Trojanern der Familien ZeuS (inkl. Citadel) und SpyEye
Bank of America bankofamerica.com		4	✗	✗	✓	✓	12,98 %
PayPal paypal.com		–	✗	✗	✗	✓	12,92 %
Citi citibank.com		5	✗	✗	✓	✓	12,78 %
Lloyds lloydstsb.co.uk		60	✓	✓	✓	✓	10,91 %
TSB Bank tsb.co.uk		60	✓	✓	✓	✓	10,91 %
HSBC hsbc.co.uk		3	✓	✓	✓	✓	10,88 %
USAA usaa.com		–	✗	✗	✗	✓	10,25 %
Barclays barclays.co.uk		17	✓	✓	✓	✓	10,11 %
Wells Fargo wellsfargo.com		1	✗	✗	✓	✓	8,92 %
SunTrust suntrust.com		79	✗	✗	✓	✓	8,26 %
US Bancorp usbank.com		35	✗	✗	✗	✗	8,09 %
Chase chase.com		2	✗	✗	✗	✗	8,01 %
Royal Bank of Canada royalbank.com		21	✗	✗	✗	✓	7,87 %
Canadian Imperial Bank of Commerce cibc.com		47	✗	✗	✓	✓	7,75 %
TD Bank tdbank.com		20	✗	✗	✓	✓	7,36 %
eBay ebay.com		–	✗	✗	✗	✓	7,10 %
Postbank postbank.de		92	✓	✓	✓	✓	6,84 %
PNC Financial Services pnc.com		50	✗	✗	✓	✓	6,79 %
Halifax halifax-online.co.uk		78	✗	✗	✓	✓	6,76 %
Bank of Montreal bmo.com		36	✗	✗	✗	✗	6,59 %
Yandex yandex.ru		–	✗	✗	✗	✓	6,59 %
Skrill moneybookers.com		–	✗	✗	✗	✓	6,56 %
WebMoney webmoney.ru		–	✗	✓	✗	✓	6,53 %
Capital One capitalone.com		27	✗	✗	✓	✓	6,50 %
TDBG td.com		20	✗	✗	✓	✓	6,33 %

Kategorie: = Bank = E-Payment = Auktion

Quelle: G DATA SecurityLabs

Methodik

Insgesamt wurden 3.521 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-Landschaft 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 der Domänen auf Gültigkeit überprüft. Schließlich wurde gezählt, welche Domänen in wie vielen Samples vorkommen. Dadurch konnte die relative Häufigkeit der Angriffe auf Domänen 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. Außerdem wurden für diese die Sicherheitsmaßnamen der Seite evaluiert. Bei den Sicherheitsmaßnahmen wurden die zum Zeitpunkt der Untersuchung auf öffentlichen Webseiten zugänglichen Informationen zu Grunde gelegt, so dass für die tatsächliche Korrektheit keine Gewähr übernommen werden kann.

Zusätzlich wurde die Art der durch die häufigsten **Webinjects** durchgeführten Angriffe analysiert.

Sicherheitsmaßnahmen der Top 25 im Einzelnen

Da **Social Engineering-Attacken** über Banking-Trojaner (z.B. Testüberweisungen) von Banken nur über bankenseitige Heuristiken erkennbar sind, die hier nicht weiter betrachtet werden können, ist hier bei jeder Bank implizit die Anfälligkeit für diese Angriffe gegeben.
Da die Funktionsweise dieser Prüfungen in der Regel aus Sicherheitsgründen nicht transparent ist, werden diese bei der folgenden Evaluierung nur dann weiter betrachtet, wenn es bekannte Muster gibt (z.B. wenn eine Überweisung an einen bisher unbekannten Empfänger weitere Sicherheitsmaßnahmen auslöst).

Rang 1: Bank of America (bankofamerica.com)

Die Bank, die die vorangestellten Analyseergebnisse anführt, verwendet zwei Sicherheitsmaßnahmen mit den Namen SiteKey und SafePass.

SiteKey bezeichnet eine verpflichtende Sicherheitsmaßnahme. Dabei wird während des Log-in-Vorgangs ein Bild angezeigt, das beim ersten Anmeldevorgang vom Benutzer gewählt wurde. Zudem müssen drei vom Benutzer ebenfalls initial selbst gewählte Fragen beantwortet werden, wenn er sich von einem der Bank bisher unbekanntem Gerät aus anmelden will. Dieses System kann lediglich vor klassischem Phishing (v.a. über Spam-Mails) und vor Keyloggern schützen, aber nicht vor Banking-Trojanern.

Bei SafePass handelt es sich um Transaktions-Einwegpasswörter, die dem User über ein Mobiltelefon oder ein Zusatzgerät in Kartenform angezeigt werden. Es handelt sich allerdings um ein optionales Schutzverfahren. Nur um Transaktionen oberhalb eines bestimmten Limits durchzuführen, muss SafePass benutzt werden. Außerdem werden keine Details zur Verifikation der Transaktion angegeben, wodurch eine Manipulation möglich ist.

Quellen: https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/safepass.go
https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/sitekey.go

Rang 2: PayPal (paypal.com)

Der bekannte Zahlungsdienstleister PayPal ist das erste Angriffsziel in dieser Liste, das nicht dem klassischen Bankgeschäft zuzuordnen ist. In der Standardkonfiguration gibt es bei PayPal keinen Schutz vor Keyloggern oder Banking-Trojanern. PayPal besitzt allerdings ein optionales Schutzsystem über Login-Einwegpasswörter per Mobiltelefon oder Zusatzgerät in Kartenform namens „Security Key“. Das Schutzsystem kann gleichzeitig für Anmeldungen bei eBay mitgenutzt werden. Da die Transaktionsdaten (Zielkonto, Betrag) dem Benutzer nicht übermittelt werden, kann dieser diese nicht überprüfen. Ein Angreifer kann so mittels eines Banking-Trojaners bei einer Transaktion unbemerkt Betrag und Zielkonto austauschen; Social Engineering ist nicht nötig.

Quelle: https://www.paypal.com/securitykey

Rang 3: Citibank (citibank.com)

Die Citibank führte zum Ende des Jahres 2013 obligatorische Transaktions-Einwegpasswörter per Mobiltelefon ein. Allerdings enthalten die ans Mobiltelefon gesendeten Nachrichten dabei keine Transaktionsdaten, so dass diese nicht verifiziert werden können. Deshalb besteht vor Keyloggern, aber nicht vor Online-Banking-Trojanern Schutz.

Quelle: https://online.citibank.com/JRS/pands/detail.do?ID=SecurityCenter

Rang 4: Lloyds (lloydstsb.co.uk)

Die Lloyds Bank taucht gleich mit zwei verschiedenen Domänen in der Top 25-Liste auf, auf Rang 4 und Rang 5. Beim Log-In muss der Kunde jedes Mal drei zufällige Stellen aus einem längeren Passwort eingeben. Dies ist zwar prinzipiell ein Einwegpasswort, allerdings mit sehr eingeschränkter Anzahl an Möglichkeiten. Zudem ist diese Methodik sehr anfällig für Social Engineering-Angriffe, da dem Kunden lediglich suggeriert werden muss, er müsse aus angeblichen Sicherheitsgründen sein komplettes Passwort eingeben.

Allerdings erfolgt bei bisher unbekannten Zahlungsempfängern zudem eine automatisierte telefonische Rückfrage, in deren Zuge der Benutzer sich selbst identifizieren und die aktuelle Transaktion verifizieren muss. Hier erfolgt also eine Authentifizierung der Transaktion über einen zweiten Kanal.

Dadurch besteht vor Keyloggern und Online-Banking-Trojanern, die nicht über Social Engineering angreifen, Schutz. Ausnahme wäre hier der Grenzfall, bei dem ein Angreifer Geld zu einem bereits bekannten Konto transferieren möchte. Dies entspricht aber nicht den üblichen Angriffsmustern der Cyberkriminellen.

Quelle: http://www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp

Rang 5: Lloyds (tsb.co.uk)

Die Schutzmaßnahmen der Lloyds Bank sind in der Auswertung zu Rang 4 beschrieben. Die Maßnahmen der beiden Domänen unterscheiden sich nicht voneinander.

Quelle: http://www.lloydsbank.com/help-guidance/security/what-we-are-doing.asp

Rang 6: HSBC (hsbc.co.uk)

Bei der „Hongkong & Shanghai Banking Corporation“ (HSBC) kommt seit einigen Jahren ein Schutzsystem über ein Zusatzgerät zum Einsatz. Jede Anmeldung sowie jede Transaktionen an bisher unbekannte Empfänger müssen über Einwegpasswörter bestätigt werden. Dieses System bietet nicht nur vor Keyloggern Schutz. Transaktionsdetails werden auf dem Gerät verifiziert, indem Teile der Kontonummer des Empfängers zur Generierung einer Secure Key PIN benutzt werden. Prinzipiell besteht hier also Schutz vor Online-Banking-Trojanern, die unbemerkt Transaktionsdaten modifizieren. Wie auch bei der Lloyds Bank ist der Grenzfall hier, dass der Angreifer Geld zu einem bereits bekannten Konto transferieren möchte, was allerdings nicht den üblichen

Angriffsmustern der Angreifer entspricht. Zudem ist die Gefahr für Social-Engineering-Attacken besonders groß, da auf dem Secure Key-Gerät die Transaktion nicht explizit angezeigt wird und bestätigt werden muss, sondern das Zielkonto nur implizit durch die Eingabe der letzten vier Stellen der Kontonummer bestätigt wird.

Quelle: https://www.hsbc.co.uk/1/2/customer-support/online-banking-security/secure-key

Rang 7: USAA Bank (usaa.com)

Die USAA-Bank verwendet ein optionales Verfahren für Einwegpasswörter über Mobiltelefone zum Log-In, womit ein Schutz vor Keyloggern besteht. Transaktionen werden aber nicht authentifiziert, wodurch Kunden für Online-Banking-Trojaner anfällig sind, die unbemerkt Betrag und Zielkonto einer Überweisung austauschen.

Quelle: https://www.usaa.com/inet/pages/security_token_logon_options

Rang 8: Barclays (barclays.co.uk)

Barclays sichert mit dem Schutzsystem PINsentry sowohl Logins als auch Transaktionen über Einwegpasswörter. Diese können über Mobiltelefone oder ein Zusatzgerät generiert werden. Ohne Schutz durch PINsentry können nur Transfers zu bereits gespeicherten Empfängern oder zu bestimmten durch die Bank verifizierten Empfängern (insb. Firmen) durchgeführt werden. Als Legitimation hierfür reichen ein Passcode und ein sogenanntes memorable word. Die Details zur Verifizierung der Überweisung werden auf dem Mobilgerät oder dem Kartenleser eingegeben, jedoch nur im Falle eines neuen Empfängers. Somit ist eine Manipulation durch Banking-Trojaner nicht gänzlich auszuschließen, denn es besteht Gefahr in dem Grenzfall, in dem in betrügerischer Absicht Geld zu einem bekannten oder durch die Bank verifizierten Empfänger Geld transferiert werden soll.

Quellen: http://ask.barclays.co.uk/help/online_banking/register
http://www.barclays.co.uk/Helpsupport/HowtousePINsentry/P1242560253457
http://ask.barclays.co.uk/help/online_banking/memorable_word_passcode
Barclays PINsentry User Guide Leaflet (Item reference: 9907259)

Rang 9: Wells Fargo (wellsfargo.com)

Für Kunden, die die Dienste Direct Pay oder Foreign Exchange Online nutzen, wird beim Log-In ein per Zusatzgerät generiertes Einwegpasswort verlangt. Die anderen Kunden müssen eine von drei vordefinierten Sicherheitsfragen korrekt beantworten. Da jedoch nur der Log-In und nicht die Transaktion gesichert wird, können durch Banking-Trojaner unbemerkt Betrag und Zielkonto einer Überweisung geändert werden.

Quellen: https://www.wellsfargo.com/privacy-security/online/protect/
https://www.wellsfargo.com/biz/jump/securid

Rang 10: Suntrust (suntrust.com)

Neben dem klassischen Login über User-ID und Passwort schützt Suntrust mit Sicherheitsfragen vor Keyloggern. Allerdings besteht Anfälligkeit für Online-Banking-Trojaner.

Quelle: https://www.suntrust.com/FraudAndSecurity/FraudProtection/HowWeProtectYou

Rang 11: U.S. Bank (usbank.com)

Es konnten keine Informationen über Sicherungssysteme gefunden werden, die über ein einfaches Passwort hinausgehen. Demnach besteht sehr wahrscheinlich Anfälligkeit für Keylogger und Online-Banking-Trojaner.

Quelle: https://www.usbank.com/online-security/index.html

Rang 12: Chase (chase.com)

Es konnten keine Informationen über Sicherungssysteme gefunden werden, die über ein einfaches Passwort hinausgehen. Demnach besteht sehr wahrscheinlich Anfälligkeit für Keylogger und Online-Banking-Trojaner.

Quelle: https://www.chase.com/resources/privacy-security

Rang 13: Royal Bank of Canada (royalbank.com)

Die Royal Bank of Canada sichert den Log-In für zu seiner Sign-In Protection sowie die Vergabe von neuen Passwörtern zusätzlich zu Benutzer-ID und Passwort mit einer von drei vordefinierten persönlichen Fragen ab, was Schutz gegen Keylogger bedeutet. Hierbei wird lediglich der Log-In geschützt, jedoch nicht einzelne Überweisungen, weswegen Banking-Trojaner unbemerkt Betrag und Zielkonto einer Überweisung ändern können.

Quelle: https://www.rbcroyalbank.com/onlinebanking/bankingusertips/security/features.html#1

Rang 14: Canadian Imperial Bank of Commerce (cibc.com)

Im ersten Halbjahr 2014 schützte die Canadian Imperial Bank of Commerce ihre Kunden neben einem klassischen Log-In über Kartennummer und Passwort über persönliche Fragen. Somit besteht Schutz vor Keyloggern, aber nicht vor Online-Banking-Trojanern. Seit Juli 2014 ist eine Umstellung im Gange, nach der auch Transaktionen über Einwegpasswörter abgesichert werden. Diese außerhalb des Berichtszeitraums liegende Umstellung wurde in der Evaluation aber nicht weiter berücksichtigt.

Quellen: https://www.cibc.com/ca/legal/identity-fraud.html
https://www.cibc.com/ca/features/banking-enhancements.html?WT.mc_id-Int-ANCH-NGA-ComingSoon-E

Rang 15: TD Group (tdbank.com)

Die Toronto Dominion Bank ist mit zwei Domains in den Top 25 vertreten. Für beide gelten die gleichen Sicherheitsfunktionen. Der Benutzer muss beim Log-In von neuen Geräten eine von fünf vordefinierten Sicherheitsfragen beantworten. Damit ist der Log-In vor simplen Keyloggern geschützt. Jedoch werden einzelne Transaktionen nicht extra abgesichert, was eine Anfälligkeit gegenüber Online-Banking-Trojanern impliziert.

Quellen: http://www.tdbank.com/bank/securitycommitment.html
http://www.td.com/privacy-and-security/privacy-and-security/how-we-protect-you/online-security/idplus.jsp

Rang 16: eBay (ebay.com)

eBay besitzt ein optionales Schutzsystem über Log-In-Einwegpasswörter per Mobiltelefon oder Zusatzgerät in Kartenform. Das Schutzsystem kann gleichzeitig für Anmeldungen bei PayPal mitgenutzt werden. Prinzipiell ist auch hier problematisch, dass nur der Log-In und nicht auch die Transaktion (hier vor allem: der Kauf) geprüft wird. Klassische Online-Banking-Trojaner können das Transaktionsziel ändern, ohne dass der Benutzer davon Notiz nimmt.

Quelle: http://pages.ebay.com/securitykey/faq.html

Rang 17: Postbank (postbank.de)

Die Deutsche Postbank stellt laut der aktuellen Analyse das am meisten angegriffene Ziel mit Sitz außerhalb des angelsächsischen Raums dar. Es existieren mehrere Verfahren zur Authentifizierung von Transaktionen über Mobilfunk- und Zusatzgeräte, wodurch vor Keyloggern und Online-Banking-Trojanern, die nicht über Social Engineering angreifen, Schutz besteht.

Quelle: https://www.postbank.de/privatkunden/pk_sicherheit_tanverfahren.html

Rang 18: PNC Financial Services (pnc.com)

Mit den obligatorischen Sicherheitsmaßnahmen werden persönliche Bilder zum Phishing-Schutz angezeigt. Außerdem werden bei Anmeldung von unbekannten Endgeräten persönliche Fragen gestellt, wodurch ein Schutz vor Keyloggern besteht. Für Kunden, die das PINACLE-Portal für Firmenkunden nutzen, wird stattdessen ein Einwegpasswortgenerator verwendet. Dieser sichert allerdings nur den Login und keine Transaktionen ab. Schutz vor Online-Banking-Trojanern besteht deshalb in keinem Fall.

Quelle: https://www.pnc.com/webapp/unsec/ProductsAndService.do?siteArea=/pnccorp/PNC/PNC+Security+Center/Enhanced+Authentication+Landing+Page

Rang 19: Halifax (Halifax-online.co.uk)

Im Online-Banking Portal der Halifax Bank ist ein Schutz gegen Keylogger eingebaut, der darauf basiert, dass beim Log-In zusätzlich zu Benutzername und Passwort drei Buchstaben eines vordefinierten privaten Wortes ausgewählt werden müssen. Einzelne Transaktionen sind jedoch nicht weiter abgesichert, weswegen Banking-Trojaner unbemerkt Betrag und Zielkonto einer Überweisung ändern können.

Quelle: http://www.halifax.co.uk/aboutonline/security/protecting-you/

Rang 20: Bank Of Montreal (bmo.com)

Es konnten keine Informationen über Sicherungssysteme gefunden werden, die über ein einfaches Passwort hinausgehen. Demnach besteht wahrscheinlich Anfälligkeit für Keylogger und Online-Banking-Trojaner.

Quelle: http://www.bmo.com/home/about/banking/privacy-security/how-we-protect-you

Rang 21: Yandex (yandex.ru)

Yandex bietet ein mit Google vergleichbares Angebot mit Fokus auf den russischen Markt. Ziel der Angriffe war in allen untersuchten Fällen der Service Yandex Money, ein mit PayPal vergleichbarer Bezahldienst. Yandex bietet zur Transaktionssicherung optional Einwegpasswörter über Abstreichlisten sowie per SMS an. Bei den Einwegpasswörtern über SMS gibt es keinen Hinweis darauf, dass die Textnachrichten eine Authentifizierung des Transaktionsziels ermöglichen. Insofern ist davon auszugehen, dass nur der Login, nicht aber die Transaktionen gesichert werden. Deshalb besteht zwar Schutz vor Keyloggern, aber kein Schutz vor Banking-Trojanern. Ohne Einwegpasswörter besteht auch kein Schutz vor Keyloggern.

Quelle: https://money.yandex.ru/doc.xml?id=524852

Rang 22: Skrill (skrill.com)

Seit 2009 verteilte der Zahlungsdienstleister Skrill, damals noch unter dem Namen moneybookers, optionale Zusatzgeräte zur Generierung von Einwegpasswörtern zwecks Log-In-Sicherung. Dieses Verfahren schützt vor Keyloggern, aber nicht vor Online-Banking-Trojanern.
2011 wurde ein Rebranding-Prozess von moneybookers zu Skrill eingeleitet. Im letzten Quartal 2013 wurde skrill.com zur Hauptseite, während moneybookers.com nur noch eine Weiterleitung darstellt. Trotzdem greifen sämtliche betrachteten Samples moneybookers.com an und keines skrill.com, so dass die gefundenen Webinjects zum Zeitpunkt der Untersuchung nicht funktionieren. Hier zeigt sich eine gewisse Trägheit auf diesem Markt.

Quellen: https://www.skrill.com/en/personal/security/
https://www.skrill.com/en/vip/moneybackguarantee/

Rang 23: Webmoney (webmoney.com)

Für die Anmeldung beim Zahlungsdienstleister Webmoney können die proprietäre Clientsoftware WM Keeper WinPro (Classic) oder der Login über einen Browser via WM Keeper WebPro (Light) verwendet werden. Die Anmeldung über den Browser ist über drei Wege möglich: ein Clientzertifikat oder über Einwegpasswörter via Mobiltelefon (E-Num) oder aber über klassischen Log-In und Passwort. Damit ist, bei Nutzung der optionalen Einwahlmöglichkeiten, Schutz gegen Keylogger gegeben. Die untersuchten Webinjects griffen ausschließlich die Variante WM Keeper WebPro (Light) an. Der Benutzer kann aus einer Reihe von Verifikationsmaßnahmen für Überweisungen wählen und kann mit der richtigen Wahl auch Vorkehrungen gegen die Manipulation von Transaktionen durch Banking-Trojaner treffen.

Quellen: https://wiki.wmtransfer.com/projects/webmoney/wiki/Transaction_confirmation_in_WM_Keeper_WebPro
https://wiki.wmtransfer.com/projects/webmoney/wiki/WM_Keeper_WebPro
http://security.wmtransfer.com
http://www.e-num.com

Rang 24: Capital One (capitalone.com)

Die Capital One sichert den Log-In zum Online-Banking mit einer von fünf vorausgewählten Sicherheitsfragen ab. Diese Methode bietet Schutz vor Keyloggern. Einzelne Transaktionen werden nicht extra verifiziert, wodurch Banking-Trojaner unbemerkt Betrag und Zielkonto einer Überweisung ändern können.

Quelle: http://www.capitalone.com/online-banking-faq/?Log=1&EventType=Link&ComponentType=T&LOB=MTS%3A%3ALCTMJBE8Z&PageName=Contact+Us+FAQ&PortletLocation=4%3B4-12-col%3B2-2-3-1-1&ComponentName=FAQ+olb+small+business+home+LOANs%3B18&ContentElement=1%3BCredit+Cards&TargetLob=MTS%3A%3ALCTMJBE8Z&TargetPageName=Online+Banking+FAQ

Rang 25: TD Group (td.com)

Die Schutzmaßnahmen der TD Group sind in der Auswertung zu Rang 15 ausführlich beschrieben. Die Maßnahmen der beiden Domänen unterscheiden sich nicht voneinander.

Quellen: http://www.tdbank.com/bank/securitycommitment.html
http://www.td.com/privacy-and-security/privacy-and-security/how-we-protect-you/online-security/idplus.jsp