G Data

MalwareReport

Halbjahresbericht Juli – Dezember 2011

G Data SecurityLabs

Geschützt. Geschützter. **G Data.**

Inhalt

Auf einen Blick

- Es gab 2,575 Millionen neue Schädlinge in 2011. Im Vergleich zum Vorjahr stieg das Aufkommen um 23% an.
- Die Anzahl neuer Rootkits ist rückläufig, Spyware und Adware haben dagegen deutlich zugelegt.

- Die Anzahl von neuem Schadcode für Mobilgeräte hat sich in einem Jahr verzehnfacht.
- Außerdem verbreitete sich Android-Schadcode nun auch weltweit und wurde durch Lokalisierungen damit auch rund um den Globus zur Gefahr.

- Das Hauptziel von Phishing war und bleibt Geld. Über 60% der Phishing-Seiten waren im Stil von Finanzinstituten aufgemacht.

- Torpig, SpyEye und ZeuS waren die aktivsten Banking-Trojaner.

Ereignisse

- Das Spionagewerkzeug DuQu tauchte auf. Es zielt darauf ab, möglichst viele Informationen zu sammeln und Angriffe, wie die von Stuxnet, vorzubereiten.
- Hacktivisten, wie Anonymous, starteten etliche gezielte Cyber-Angriffe gegen Firmen, Organisationen und Personen.

Ausblick für das erste Halbjahr 2012[1]

- Android Malware wird weiter zunehmen und bald auch technisch raffinierter sein.
- Es wird mehr gezielte Angriffe geben.
- Großereignisse, wie die Fußball Europameisterschaft, werden im Fokus von Cyber-Kriminellen liegen.
- Banking-Trojaner werden von Kriminellen weiterhin und vermehrt eingesetzt werden, um Online-Banking Kunden zu schädigen.

[1] Für weiterführende Informationen, siehe G Data Report "Trends 2012"

Malware: Zahlen und Daten

Malware-Millionäre

Die Anzahl neuer Schädlinge ist im zweiten Halbjahr 2011 um 6,8% gestiegen. In der zweiten Jahreshälfte zählten wir 1.330.146 neue Schadprogrammtypen.[2] Im Durchschnitt sind das täglich 7.229 Dateien. Für das gesamte Jahr 2011 wurde die erwartete Marke von mehr als 2,5 Millionen Schadprogrammen deutlich überschritten. Die Anzahl neuer Schädlinge stieg 2011 im Vergleich zu 2010 um 23,1%.

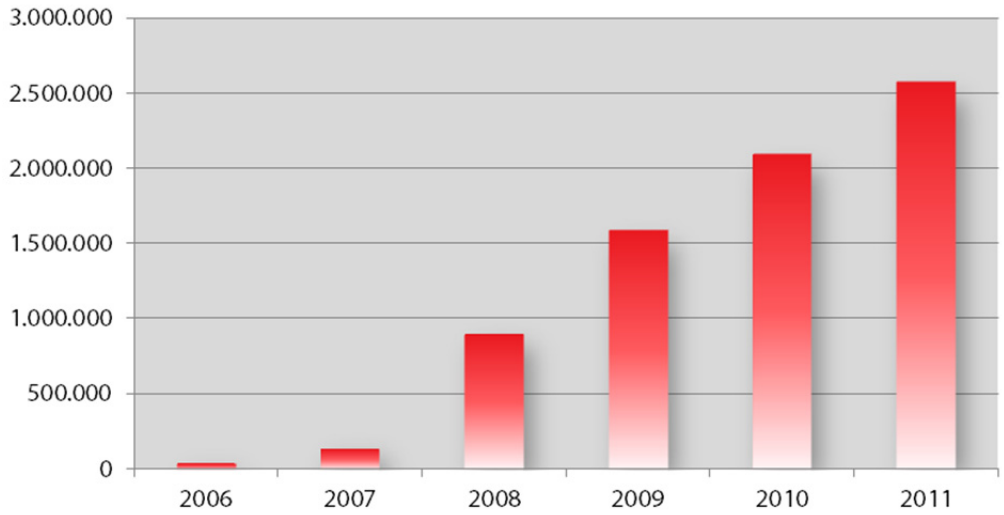


Abbildung 1: *Anzahl neuer Schadprogramme pro Jahr seit 2006*

Malware Kategorien

Schadprogramme können anhand ihrer Aktivitäten in Kategorien gruppiert werden. In Abbildung 2 sind die wichtigsten Kategorien und deren Entwicklung in den letzten vier Halbjahren dargestellt. Den größten Anstieg verzeichneten wir bei den Spionageprogrammen (**Spyware**). Ihre Anzahl ist in den letzten sechs Monaten um 52% gestiegen. Innerhalb der letzten zwei Jahre ist das Aufkommen um 20% angewachsen. Im gleichen Zeitraum ist auch die Gruppe der **Trojanischen Pferde** um 40% gewachsen, wobei der Anstieg im letzten Halbjahr etwas an Fahrt verloren hat und auf 6% zurückgegangen ist. Der Anteil an Software, die unautorisiert Werbeeinblendungen vornimmt (**Adware**) hat in den letzten Jahren ständig zugenommen. Auch im letzten Halbjahr ist ihre Anzahl um 18,5% angewachsen; von 2010 bis 2011 sind es sogar 25,4%.[3] Rückläufig ist hingegen die Anzahl der **Rootkits**. Sie dienen dazu, Schadprogramme wie Hintertüren (**Backdoors**) und Spionageprogramme auf dem Rechner so zu verstecken, dass Systemtools und Virenschutz-Software sie nicht finden. Im letzten Halbjahr haben sie 10% verloren. Im Jahresvergleich 2010 - 2011 ist die Anzahl sogar um 43% gesunken. Auch wenn die Anzahl neuer **Rootkit-Varianten**

[2]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, die im ersten Halbjahr 2011 erstellt wurden.

[3] Für Informationen zu abgewehrten Adware-Angriffen, siehe Kapitel Gefahren-Monitor

abgenommen hat, sind sie immer noch ein wichtiger Baustein in der Selbstverteidigungsstrategie von Schadprogrammen. Ebenfalls rückläufig ist die Anzahl der **Downloader**. Sie ging im letzten Halbjahr um 18% zurück (9% in den letzten beiden Jahren). Die Tatsache, dass die Anzahl neuer **Exploit-Schädlinge** sinkt, lässt sich dadurch erklären, dass Software immer besser abgesichert wird. Vorhandene Lücken werden im Idealfall schnell geschlossen, schon beim Programmieren vermieden oder durch Qualitätssicherung ausgemerzt, noch bevor ein Produkt auf den Markt kommt. Die Angriffsmöglichkeiten werden also minimiert. Außerdem reicht Angreifern ja eine einzige Sicherheitslücke, um auf einem Rechner Schaden anzurichten. Eine der Sicherheitslücken, die noch immer sehr populär ist und attackiert wird, ist in CVE-2010-0840 beschrieben.[4]

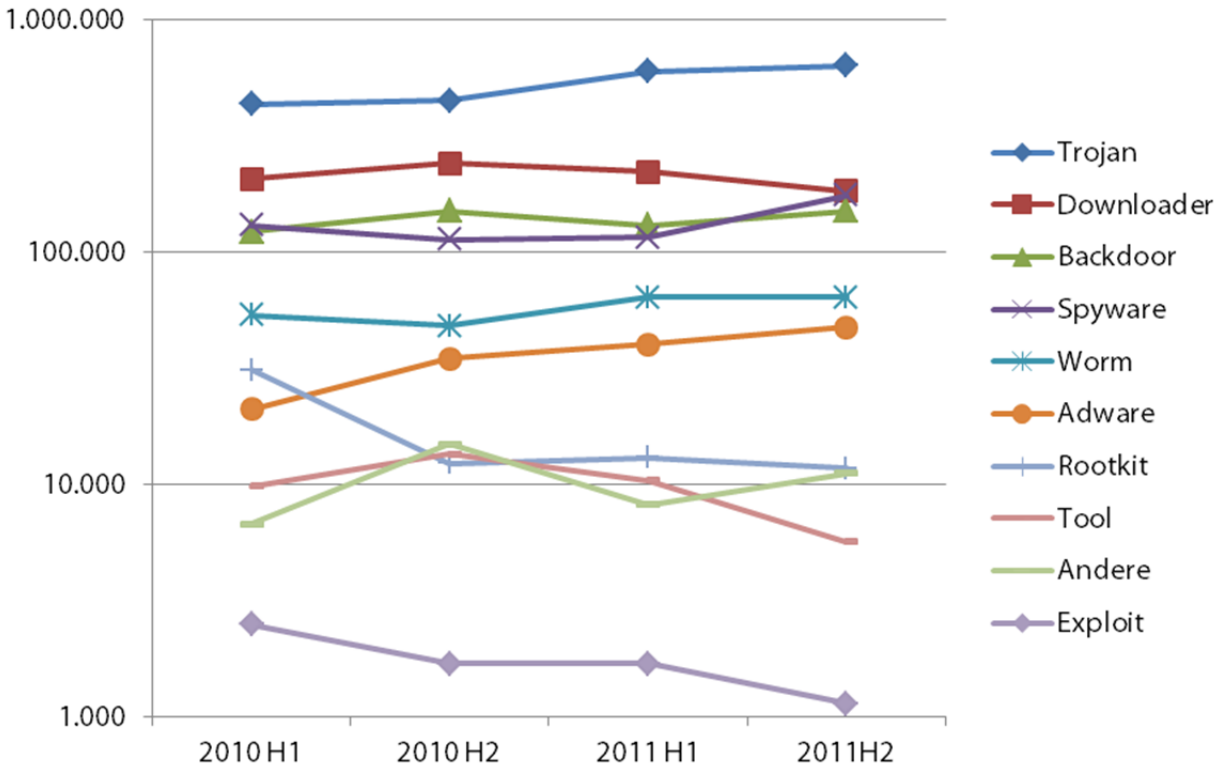


Abbildung 2: *Anzahl neuer Schädlinge pro Malwarekategorie in den letzten vier Halbjahren*

Malware Familien

Anhand ihrer Eigenschaften und Aktivitäten werden Schadprogramme in Familien unterteilt. Die Anzahl der unterschiedlichen Malware-Familien ist im zweiten Halbjahr um 2% auf 2.616 leicht zurückgegangen. 2011 waren es insgesamt 3.569 Familien. Das sind im Vergleich zum Vorjahr 7,7 Prozent mehr. Einige Familien sind sehr produktiv und es entstehen ständig neue Varianten - im Verlauf des Jahres 2011 waren es fast 2,6 Millionen.[5] Die 10 produktivsten Familien sind in der folgenden Tabelle beschrieben, für sie wurden die meisten neuen Virensignaturen erstellt.

[4] Siehe Kapitel Gefahren-Monitor
[5] Siehe Abbildung 1

Rang	Familie	Kategorie	Anteil	Diff. zu H1 2011
1	**Genome**	Trojanisches Pferd	8,5%	±0
	Die Trojanischen Pferde der Genome-Familie konnten ihre Spitzenposition mit weitem Abstand verteidigen. Sie vereinen Funktionalitäten wie Downloader, Keylogger und Dateiverschlüsselung.			
2	**VBKrypt**	Trojanisches Pferd	3,7%	+1
	VBKrypt ist ein Tool, das zur Tarnung von Schaddateien eingesetzt wird. Die Tarnroutinen sind in Visual Basic geschrieben. Der Inhalt der getarnten Dateien ist weit gefächert und reicht von Downloadern über Backdoors bis hin zu Spyware und Würmern. Diese Familie hat zwar gegenüber dem letzten Halbjahr 0,9% Anteil verloren, konnte aber einen Platz gut machen.			
3	**Diple**	Trojanisches Pferd	3,5%	+14
	Die Varianten der Diple-Familie steigerten ihren Anteil im zweiten Halbjahr 2011 um 2,4%. Diple-Varianten ermöglichen es den Rechner fernzusteuern und Steuer-Server zu kontaktieren. Auf diese Weise lassen sich beliebige Schadprogramme nachladen, z.B. Spyware und FakeAV			
4	**Menti**	Trojanisches Pferd	2,7%	+5
	Das Trojanische Pferd Menti nistet sich im betroffenen System ein und verbindet sich regelmäßig mit einem Server. Damit wird der Rechner Bestandteil eines Botnetzes. Mit 1,2% mehr konnte Menti um 5 Plätze steigen.			
5	**OnLineGames**	Spyware	2,4%	+2
	Die Mitglieder der OnLineGames-Familie stehlen vorrangig die Zugangsdaten von Online-Spielen. Dazu werden bestimmte Dateien und Registry-Einträge durchsucht und/oder ein Keylogger installiert. Im letzteren Fall werden dann nicht nur die Daten von Spielen gestohlen. Die meisten Angriffe zielen auf Spiele, die in Asien populär sind. Ihr Anteil ist im letzten Halbjahr um 0,7% gestiegen, was dazu führte, dass diese Familie im Ranking um zwei Plätze gestiegen ist.			
6	**Buzus**	Trojanisches Pferd	2,0%	±0
	Trojanische Pferde der Buzus-Familie durchsuchen infizierte Systeme ihrer Opfer nach persönlichen Daten (Kreditkarten, Online-Banking, E-Mail- und FTP-Zugänge), die an den Angreifer übertragen werden. Darüber hinaus wird versucht, Sicherheitseinstellungen des Computers herabzusetzen und das System des Opfers so zusätzlich verwundbar zu machen.			
7	**FakeAV**	Trojanisches Pferd	2,0%	-5
	Dieses Trojanische Pferd gibt sich als Antivirus-Software oder als ein anderes sicherheitsrelevantes Programm aus. Es simuliert die Entdeckung von mehreren Sicherheitsrisiken oder schädlichen Infektionen auf dem System des Benutzers. Dadurch soll der Nutzer ausgetrickst werden und für eine Software zur Entfernung der gefälschten Alarme Geld bezahlen. Der Anteil neuer Varianten dieser Familie ist um 3,3% zurückgegangen. Ein Abstieg von Platz 2 auf Platz 7 ist die Folge.			
8	**Llac**	Trojanisches Pferd	1,8%	+19
	Das Trojanische Pferd Llac ermöglicht es, unautorisiert auf einen Rechner von außen zuzugreifen und beliebige Software etwa zum Stehlen von Daten oder Senden von Spam auszuführen. Die Anzahl der Varianten ist um 1,0% gestiegen, was den Rang dieser Familie um 20 Plätze verbesserte.			
9	**Adload**	Downloader	1,7%	+17
	Die Varianten der Adload-Familie laden Dateien von einem externen Server nach (z.B. dollarrevenue.com) und führen sie aus. Da die Schaddateien auf dem externen Server liegen, kann ihre Schadfunktion variieren. In den meisten Fällen handelt es sich um Adware oder Spyware. Die Anzahl der Adload-Varianten ist um 0,9% gestiegen. Damit zieht Adload in die Top 10 ein.			
10	**Shiz**	Backdoor	1,6%	+67
	Shiz-Varianten sind neu in den Top 10. Sie injizieren sich in den Systemprozess services.exe. Damit laufen sie im Kontext von Systemdiensten und sind mit Standard-Tools kaum noch aufzuspüren. Sie öffnen eine Hintertür zum PC, über die Spyware und andere Malware nachgeladen werden kann.			

Plattformen: Hauptziel Windows, Mobile im Kommen

Schadprogramme werden - mit wenigen Ausnahmen - für spezielle Plattformen entwickelt. Seit Jahren wird die überwiegende Anzahl von Schadprogrammen für **Windows** geschrieben. Auch in diesem Halbjahr ist das nicht anders. Zwei Plattformen aus Tabelle 1 sind für Windows-Betriebssysteme ausgelegt: **Win** umfasst Schadcode, der auf 32-bit und 64-bit Varianten von Windows läuft. **MSIL** ist die Zwischenstufe für .NET Schadcode, die neben Windows-Systemen prinzipiell auch noch auf anderen Plattformen lauffähig ist. Dieses Potenzial wird in der Praxis selten ausgeschöpft. Zählt man diese beiden Gruppen zusammen, kommt man auf einen Anteil von 99,6% für Windows, was ein Plus von 0,1% gegenüber dem ersten Halbjahr 2011 bedeutet. Den größten Anteil an den restlichen 0,4% haben **WebScripts** mit 0,2%, obwohl deren Anzahl um 23,1% gesunken ist. **WebScripts** bilden die Grundlage für die Auslieferung von Schadcode über Webseiten. Aus der geringeren Produktivität kann man aber nicht auf eine nachlassende Nutzung von Schadcode in Webseiten schließen.

Einen Platz gut gemacht hat Schadcode für Smartphones (**Mobile**). Insbesondere die Anzahl der Schädlinge für Android basierte Geräte ist um mehr als das Achtfache angestiegen, während andere mobile Plattformen wie J2ME, SymbianOS und WinCE deutlich seltener geworden sind. Insgesamt ist die Zahl der Malware für Mobilgeräte um das 2,5-fache angestiegen. Vergleicht man 2010 mit 2011, dann hat sich die neue Malware für mobile Plattformen mehr als verzehnfacht (+949%).

Andere Plattformen wie **Unix-Derivate** (Linux, BSD etc.), Java und Malware, die in Skriptsprachen geschrieben wurde, ist im letzten Halbjahr seltener geworden. Die einzelnen Werte stehen in Tabelle 1.

	Plattform	#2011 H2	Anteil	#2011 H1	Anteil	Diff. #2011H2 #2011H1
1	Win	1.305.755	98,2%	1.218.138	97,8%	+7,2%
2	MSIL	18.948	1,4%	21.736	1,7%	-12,8%
3	WebScripts	2.402	0,2%	3.123	0,3%	-23,1%
4	Mobile	1.998	0,2%	803	0,1%	+148,8%
5	Scripts[6]	626	<0,1%	832	0,1%	-24,8%
6	Java	244	<0,1%	313	<0,1%	-22,0%
7	*ix[7]	34	<0,1%	233	<0,1%	-85,4%
8	NSIS[8]	62	<0,1%	131	<0,1%	-52,7%

Tabelle 1: *Top 8 Plattformen in den letzten zwei Halbjahren*

[6] "Scripts" sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden
[7] *ix bezeichnet alle Unix-Derivate, wie z.B. Linux, FreeBSD, Solaris etc.
[8] NSIS ist die Installationsplattform, die u.a. dazu genutzt wird den Mediaplayer Winamp zu installieren

Gefahren-Monitor

Nicht nur die Anzahl der neuen Schadprogramme erreichte 2011 ein Rekordhoch, auch die Masse der von G Data Sicherheitslösungen abgewehrten Angriffe ist von Monat zu Monat gestiegen. In der Rangliste der Angriffe gegen Computernutzer mit aktivierter MII[9] zeigt sich im zweiten Halbjahr folgende Verteilung:

Rang	Name	Prozent
1	Exploit.CplLnk.Gen	1,08%
2	Trojan.Wimad.Gen.1	0,91%
3	Java.Exploit.CVE-2010-0840.E	0,90%
4	Worm.Autorun.VHG	0,87%
5	Trojan.AutorunINF.Gen	0,82%
6	Generic.Adware.Adseo.7722145B	0,69%
7	Gen:Variant.Adware.Hotbar.1	0,54%
8	Java.Trojan.Downloader.OpenConnection.AI	0,46%
9	Java.Trojan.Exploit.Bytverify.Q	0,36%
10	Adware.Agent.NGZ	0,35%

Exploit.CplLnk.Gen ist ein Exploit, der schon im Zusammenhang mit Stuxnet benutzt wurde[10] und von Cyber-Kriminellen noch immer aktiv genutzt wird, um Rechner anzugreifen. Da dieser Angriff unabhängig von der Version des Windows-Betriebssystems funktioniert und nicht etwa eine bestimmte Software sondern eben das Betriebssystem als Ziel hat, ist die potentielle Opferzahl natürlich deutlich höher und damit ein lohnendes Ziel für die Angreifer. Es ist daher wenig verwunderlich, dass dieser Angriff **Platz eins** der Halbjahrescharts der abgewehrten Gefahren belegt.

Schädlinge, die versuchen, die Autostart-Funktion auf Windows PCs für ihre Zwecke zu nutzen, sind in den Halbjahrescharts auf **Rang 4 und 5** zu finden: „Die Hauptaufgabe von Autorun besteht darin, auf Hardwareaktionen, die auf einem Computer gestartet werden, softwareseitig zu reagieren“,[11] beschreibt Microsoft auf seiner Webseite. Eine weit verbreitete Verwendung ist z.B. das Einstecken eines USB-Sticks in einen Computer, wobei der USB-Stick dann automatisch geladen wird und eventuelle Programmroutinen darauf dann automatisch ausgeführt werden. Um Schadcode daran zu hindern, diese automatische Ausführung auszunutzen, sollte diese Funktion standardmäßig im Betriebssystem ausgeschaltet sein.

An der Halbjahresübersicht ist außerdem auffällig, dass drei der zehn Ränge mit **Adware** belegt sind. Der Anteil der eindeutig identifizierbaren Attacken durch Adware-Schädlinge schwankte im zweiten Halbjahr stark.[12] Trotzdem hat es für drei Top-Platzierungen gereicht, da vor allem im August, September und Oktober sehr viele Angriffe detektiert wurden. Die Anzahl der neu erstellten,

[9] 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.
[10] http://blog.gdatasoftware.com/blog/article/the-microsoft-lnk-usb-worm-rootkit-issue-could-kill-win-xp-sp2-and-win2000-earlier.html
[11] http://support.microsoft.com/kb/967715/de
[12] Siehe Abbildung 3

Adware-Schädlinge stieg im zweiten Halbjahr 2011 dagegen kontinuierlich an.[13] Das alles deutet darauf hin, dass sich dieses Geschäftsmodel für Cyber-Bösewichte auch weiterhin lohnt und sie mit diesen Praktiken genügend Geld verdienen.

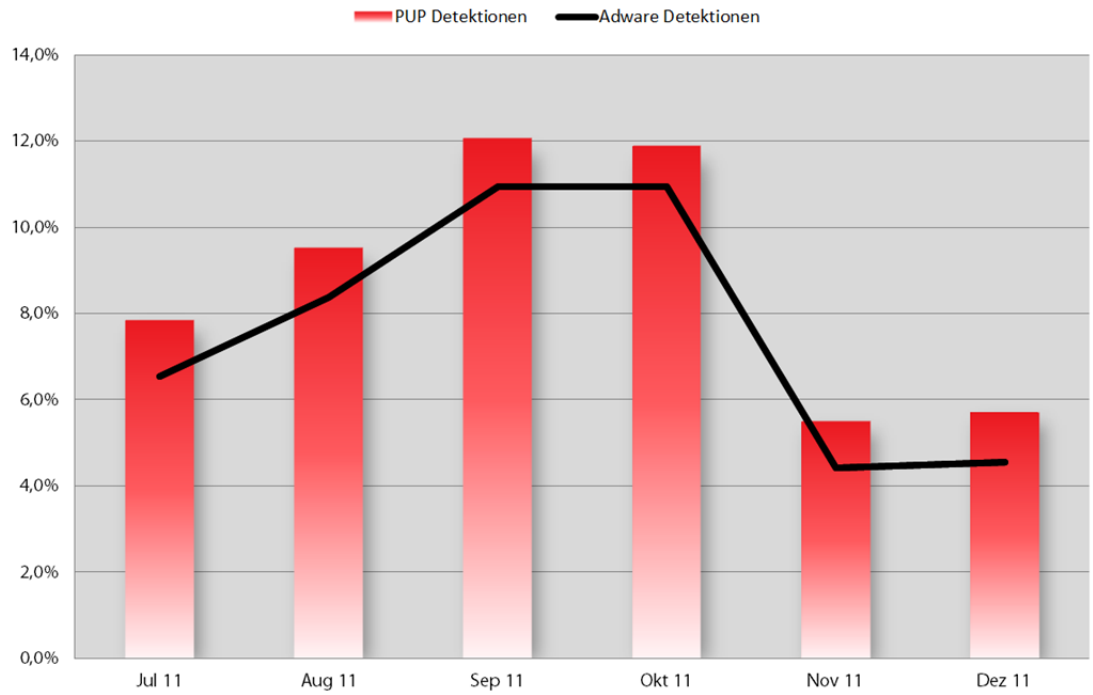


Abbildung 3: *Anteil der detektierten Potentially Unwanted Programs der Malware Information Initiative mit Anzeige des Adware-Anteils*

Ein Angriff auf eine bestimmte Sicherheitslücke hält sich ebenfalls seit langer Zeit in den Top-Plätzen der detektierten Angriffe: **CVE-2010-0840** ist weiterhin eine Sicherheitslücke, die stark attackiert wird. In der Halbjahresübersicht finden sich zwei Plätze, die mit diesem Angriff in Verbindung stehen: **Java.Exploit.CVE-2010-0840.E** und **Java.Trojan.Downloader.OpenConnection.AI**. Die Angreifer attackieren die in **CVE-2010-0840** beschriebene Sicherheitslücke noch immer,[14] denn das nachlässige Updateverhalten vieler Computerbenutzer bietet ihnen weiterhin die Möglichkeit, Schaden anzurichten. Viele Nutzer kümmern sich nicht um Updates oder wissen nicht um spezielle Anforderungen bestimmter Programm-Updates.[15] Oracle hat diese genannte Sicherheitslücke in Java bereits im März 2010 geschlossen.

[13] Siehe Abbildung 2
[14] http://blog.gdatasoftware.com/blog/article/various-money-related-spams-serve-as-versatile-attack-vector-to-spread-zeus.html
[15] http://blog.gdatasoftware.com/blog/article/the-top-10-threats-in-june-2011.html

Webseiten-Analysen

Das Haupteinfallstor für Schadcode und die Verbreitung von Phishing-Betrug ist das Internet und die Bedeutung dieses Mediums für die Gesellschaft wächst kontinuierlich: Es dient nicht nur zur Informationsbeschaffung, zum Spielen oder der Nutzung von E-Mail Diensten und sozialen Netzwerken, Weblogs oder Videoportalen, sondern wird selbstverständlich auch im Geschäftsbereich sowie in administrativen Angelegenheiten täglich eingesetzt.
Dies ist Grund genug, sich einmal mehr damit auseinanderzusetzen, welche thematischen Bereiche des so beliebten Mediums in den vergangenen sechs Monaten hauptsächlich durch Attacken aufgefallen sind.

Kategorisierung nach Themen

Eine Einordnung von detektierten bösartigen Webseiten[16] aus dem zweiten Halbjahr 2011 in Themenfelder zeigt, dass Domains mit bestimmten Inhalten häufiger in Angriffe verwickelt sind, als andere. Bei der Zählung wird nicht zwischen speziell eingerichteten Domains oder einer legitimen Seite, die missbraucht wurde unterschieden.

Die ersten fünf Plätze dieser Rangliste für das zweite Halbjahr 2011 machen zusammen mehr als die Hälfte aller klassifizierten Domains aus!
Der Spitzenreiter, **Technologie & Telekommunikation**, beinhaltet Webseiten, der die Themen Computer, Internet und Telekommunikation beinhaltet.
Rang 3, **Pornographie**, ist ein Themengebiet, das im Allgemeinen einen fragwürdigen Ruf hat. Schon frühere G Data Untersuchungen haben jedoch erläutert, dass es keinesfalls einen zwangsläufigen Zusammenhang zwischen Webseiten mit pornographischem Inhalt und Schadcode-Infektionen gibt und dies auch im Bewusstsein

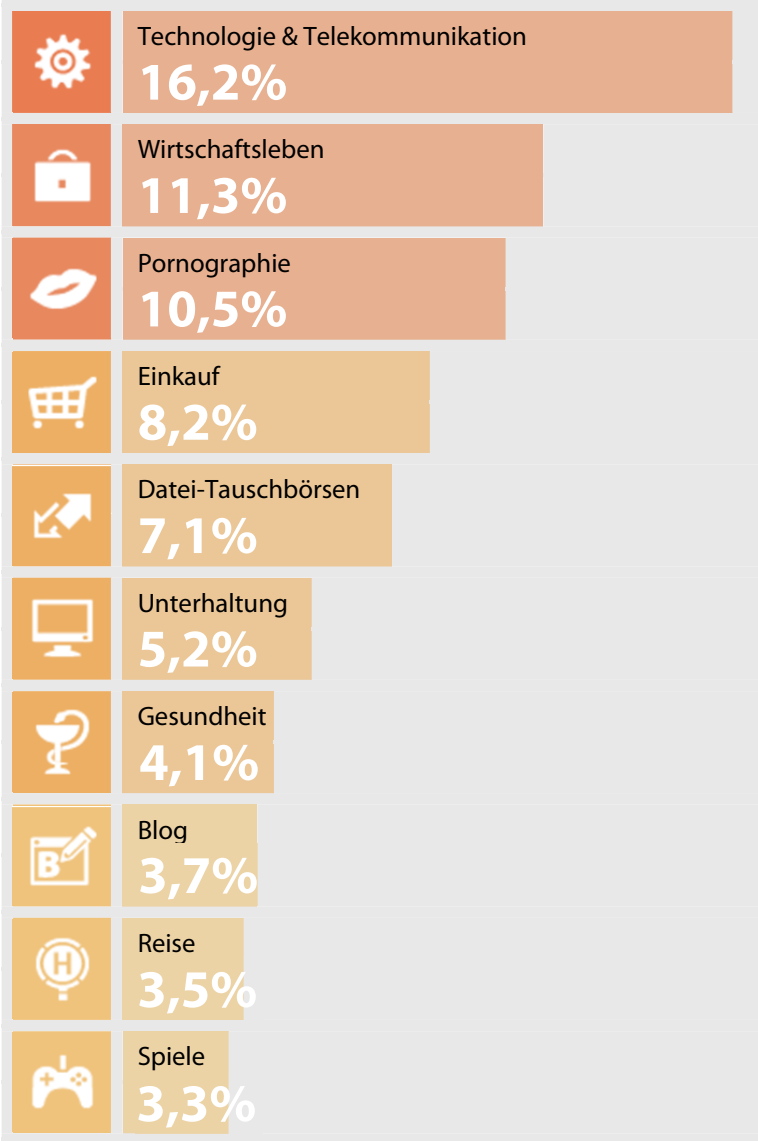


Abbildung 4: *Thematische Einordnung von bösartigen Webseiten in Kategorien, H2 2011*

[16] Als bösartige Webseiten werden in diesem Zusammenhang sowohl Phishing-Seiten als auch Malware-Seiten gezählt

einiger Internetnutzer ankommt.[17]

Webseiten, die in Verbindung mit **File Sharing** und **Peer-2-Peer Netzwerken** stehen, sind aus der Erfahrung heraus keineswegs unerwartet auf so einem hohen Rang anzutreffen. Ein großer Anteil von Schadcode wird mit Hilfe der häufig illegalen Verbreitung von urheberrechtlich geschützten Mediendateien verbreitet. Die Kategorie **Unterhaltung**, auf **Rang 6**, steht dabei, vielleicht nicht ganz zufällig, im engen Zusammenhang zu **Platz 5**, denn hier geht es um Unterhaltungsportale zu Musik, Film, Konzerten sowie Neuigkeiten rund um Stars und Sternchen des Show-Business.

Die Kategorie **Blogs**, **Rang 8**, beinhaltet Web Logs jeglicher Art – Foto Blogs, Audio-Blogs, reine Textblogs, etc. Da diese spezielle Art von Webseiten ein sehr hohes Maß an nutzerbasierten Inhalten hat, bieten sie sich als Missbrauchsziel für Täter besonders an. Die Verwaltungsbereiche privater Blogs sind unter Umständen nicht einwandfrei abgesichert und technisch nicht auf dem aktuellen Stand, was Angreifern die Möglichkeit bietet, ihren eigenen, schädlichen Inhalte sichtbar oder unsichtbar einzubinden und so Besucher des Blogs zu schädigen.

Fazit

Die Gefahr lauert immer und überall, es kann jeden treffen!
Cyberkriminelle achten nicht primär auf das Thema einer Webseite, sondern lediglich darauf, wie sie mit möglichst geringem Aufwand möglichst vielen Webseitenbesuchern schaden können. Es kommt also ganz auf den Eigenschutz der jeweiligen Webseite/des jeweiligen Webservers an und erlaubt keine Pauschalisierung in dem Sinne, dass ein Thema ganz besonders gefährdet ist und andere gar nicht. Findet sich z.B. eine Sicherheitslücke in einem weit verbreiteten Content Management System, Plug-In oder Programm, dann ist jeder damit bestückte Webserver potentiell gefährdet, egal welchen thematischen Inhalt die Webseite hat. Eine Massenattacke und Verbreitung von schädlichen Web Exploit Toolkits ist dann möglich und leider häufig die Folge, wie z.B. bei der sogenannten Lizamoon Attacke[18] oder der TimThumb Attacke in 2011.[19] Abgesehen davon ist selbstverständlich ein populäres Thema durch eine potentiell höhere Besucherzahl ein attraktiveres Ziel.

[17] vgl.: G Data Security Studie 2011. Wie schätzen Nutzer die Gefahren im Internet ein?
[18] http://blog.gdatasoftware.com/blog/article/it-never-stays-quiet-on-the-internet-the-lizamoon-attack-the-update-problem.html
[19] http://blog.sucuri.net/2011/08/mass-infection-of-wordpress-sites-counter-wordpress-com.html

Kategorisierung nach Server-Standort

Es ist außerdem interessant, einen Blick auf die lokale Verteilung der bösartigen Webseiten zu werfen. Die globale Choroplethenkarte (Flächenkartogramm) in Abbildung 5 zeigt an, wie hoch die Zahl der gehosteten, bösartigen Webseiten in einem Land ist.

Dabei zeigt sich, dass besonders die Länder stark involviert sind, die einerseits kostengünstige Hosting-Möglichkeiten und andererseits eine gut ausgebaute digitale Infrastruktur bieten. Wenig verwunderlich ist es also, dass in großen Teilen Afrikas keinerlei oder nur sehr wenige bösartige Domains auf den lokalen Servern liegen. Großflächige Länder, wie z.B. Russland kompensieren sogar die enorm große Fläche ohne Bevölkerung durch die Digital-Kapazitäten in den Metropolen und Großstädten.

Außerdem darf nicht außer Acht gelassen werden, dass in den verschiedenen Ländern auch unterschiedliche Gesetzgebungen im Bereich Internet herrschen. Daher werden einige Länder für Cyber-Kriminelle und Betrüger interessanter als andere. Eine potentielle Straftat wird in einem Land als illegal geahndet, in einem anderen als legal geduldet.
Nicht selten wurde schon darüber debattiert, dass das Internet mit Sicherheit kein rechtsfreier Raum ist und sein kann – eine globale und einheitliche Umsetzung von Gesetzen ist jedoch (noch) nicht gegeben. Die unterschiedlichen Staatsgewalten haben ihre Zuständigkeiten und eine länderübergreifende Zusammenarbeit ist aufwendig, nicht zuletzt durch die Schwierigkeit, zunächst einmal den „Tatort“ und damit auch eine Zuständigkeit zu ermitteln.

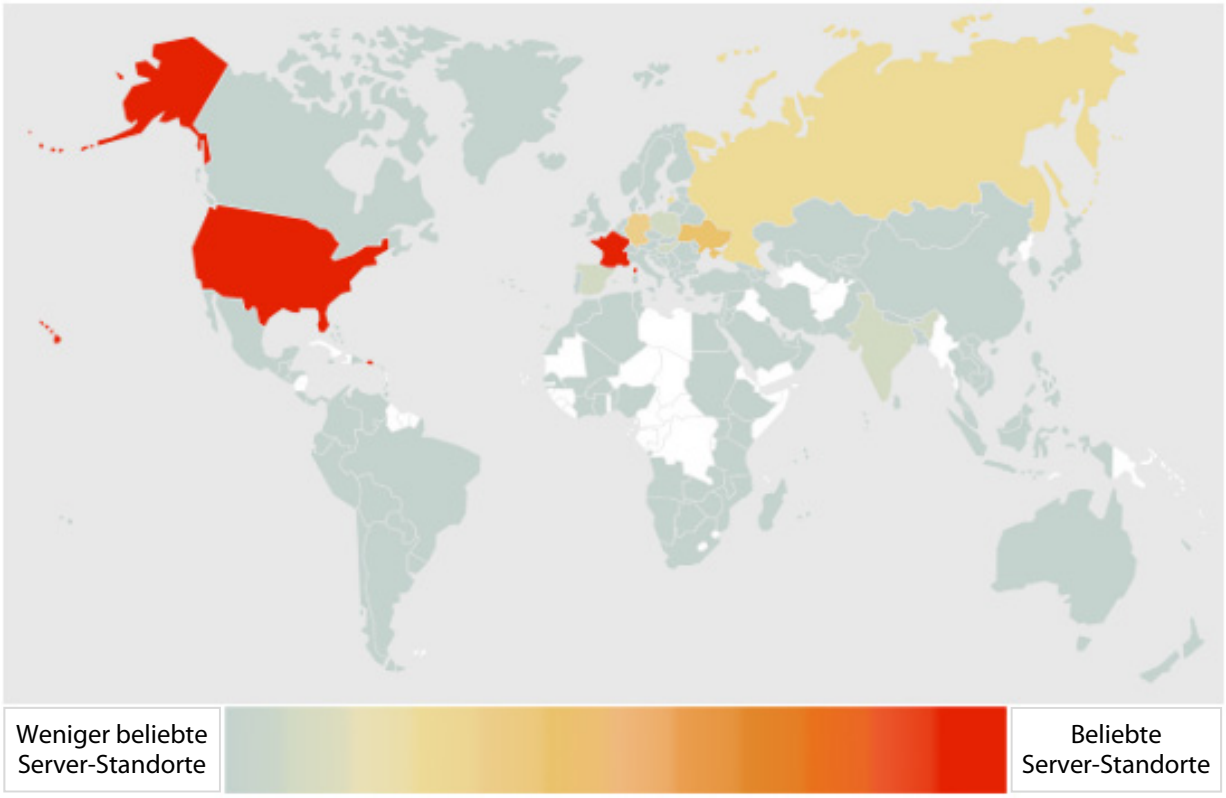


Abbildung 5: *Ein Flächenkartogramm, das zeigt, in welchem Land die meisten bösartigen Webseiten bereitgestellt werden*

Phishing-Webseiten

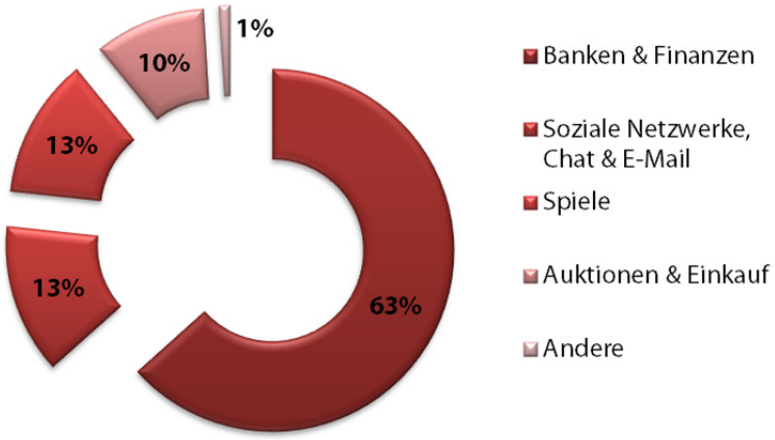


Abbildung 6: *Prozentuale Verteilung der Themen bei untersuchten Phishing-Webseiten*

Aus den Datenbanken der G Data SecurityLabs werden für diese folgende Analyse speziell Phishing-Webseiten und die dazugehörigen Seiten-informationen analysiert. Die Webseiten werden nach der Untersuchung ausgewählter Kriterien in Themenfelder einsortiert. Für das Jahr 2011 ergibt sich nebenstehende Themenaufteilung.

Ein Beispielszenario: Betrüger bauen sich die Original Login-Webseite einer Bank, eines Spiels oder einem sozialen Netzwerk, nach und stellen sie auf ihrem eigenen Server online. Die URL wird häufig so gewählt, dass sie typographisch oft kaum von den Originalen zu unterscheiden ist. So greifen Täter dann die Login-Daten ab, sobald ein Opfer sie auf dieser gefälschten Seite eingibt.

Bankgeschäfte & Finanzen belegen im zweiten Halbjahr 2011 mit Abstand den **ersten Platz**. Mehr als 60% aller untersuchten Phishing-Webseiten gehören zu diesem Thema. Besonders häufig wurden dabei gefälschte Login-Webseiten von PayPal und Santander als Falle ausgelegt. Das Ziel der Täter: Sie möchten die Zugangsdaten erbeuten (Name und Passwort) und benutzen diese erbeuteten Daten dann für Geld-Diebstahl und allerlei weitere Betrügereien.

Platz zwei und **Platz drei** teilen sich die Kategorien **Soziale Netzwerke, Chat & Mail** sowie **Spiele** mit gleichem Anteil. Die Login-Daten beider Kategorien sind bestens geeignet, um auf dem Untergrundmarkt verkauft zu werden. Die Accounts zu Onlinespielen, wie zum Beispiel World of Warcraft, haben je nach Level und Ausrüstung des Spiel-Charakters unterschiedliche Werte. Aber auch die Ausrüstungsgegenstände, ebenso wie die virtuellen Währungen werden verkauft.

Screenshot 1: *Der aktuell teuerste WoW-Account steht auf einer mehr oder weniger legalen Plattform zum Verkauf.*

Durch diese Zahlen wird noch eindrucksvoller deutlich, warum Gamer in der Schusslinie der Cyberkriminellen stehen – Es geht schon lange nicht mehr nur um Spaß, Pixel und virtuelle Goldmünzen, sondern um nicht zu unterschätzende reale Geldwerte!

Neben dem Verkauf der Zugangsdaten zu sozialen Netzwerken öffnen sich die Täter aber auch selbst Tür und Tor zu hochwertigen Verbreitungskanälen für Spam und Schadcode. Der Vorteil liegt

für sie eindeutig darin, dass Nutzer von sozialen Netzwerken Pinnwand-Einträgen und persönlichen Nachrichten von Freunden häufiger vertrauen und sie teilweise auch anklicken.

Rang 4, **Auktionen & Einkauf**, hat mit einem Anteil von 10 Prozent nur knapp das Treppchen verpasst. In dieser Kategorie befinden sich zum Beispiel Phishing-Seiten, die es auf Accounts von eBay-Kunden abgesehen haben. Erbeuten die Phisher die Daten, ändern sie im gekaperten Account z.B. die Bankdaten für den Geldeingang von verkauften Artikeln in ihre Bankdaten und schon erhalten sie die Überweisungen. Dies ist besonders bitter für gewerbliche Anbieter, die oft hunderte Artikel gleichzeitig verkaufen.

Online-Banking

Online-Banking ist ein beliebter Service, den immer mehr Menschen nutzen. Mit steigender Popularität und Akzeptanz der Nutzer, werden, wie schon so häufig, auch Cyberkriminelle auf den Plan gerufen, die versuchen, das weit verbreitete System auszunutzen und Profit daraus zu schlagen. So, wie die Nutzerzahlen steigen, so steigen auch die „Intensitäten der kriminellen Aktivitäten im Bereich Cyber-Crime [und damit auch] das für jeden Internetnutzer bestehende Gefährdungspotenzial“, [20] wie es das BKA in seinem Bundeslagebild 2010 ausdrückt. Auch wenn z.B. die Einführung des iTAN-Verfahrens im Online-Banking vor einigen Jahren zu sinkenden polizeilichen Fallzahlen (1.779 Fälle in 2008) geführt hatte, so wächst die Zahl seitdem stark (5.331 Fälle in 2010). Es ist jedoch außerdem von einer großen Dunkelziffer auszugehen, da dem BKA „lediglich ungefähr 40% der tatsächlichen Fälle bekannt werden.“ [21] Doch alleine die gemeldeten Fälle summieren sich bei einer durchschnittlichen Schadenssumme von rund 4.000€ pro Fall im Jahr 2010 zu 21,2 Mio. € in Deutschland, fast doppelt so viel wie im Jahr 2009 (11,7 Mio. €)![22]

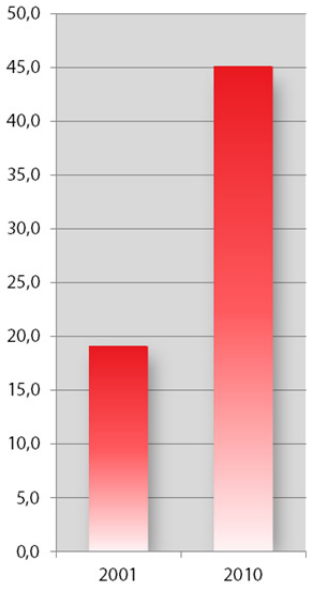


Abbildung 7: *Zahl der Online-Girokonten in Deutschland in Mio. (Quelle: Bundesverband deutscher Banken)*

Früher reichten den Bösewichten Phishing-Attacken aus, um die nötigen Zugangsdaten mit Hilfe raffinierter, täuschend echt aussehender Phishing E-Mails und Phishing-Webseiten zu erbeuten. Nach der Einführung von TANs als zusätzliche Sicherheitsstufe beim Online-Banking, mussten die Täter ihre Angriffe neu ausrichten und auch die TANs mit ergattern. Sie nutzen dazu einerseits neue Phishing-Methoden oder aber auch neue technische Verfahren – das Prinzip Man-in-the-Middle. Mit der nächsten von Banken eingesetzten Sicherheitsstufe, der SSL-Verschlüsselung des Datenverkehrs, mussten die Datendiebe im Kampf um die Daten erneut nachziehen:

inzwischen sind technisch ausgefeilte Schadprogramme die nötige und bevorzugte digitale Waffe. Mit speziellen Banking-Trojanern werden Man-in-the-Browser Angriffe durchgeführt, wodurch auch verschlüsselte Kommunikation von und zu einer Webseite manipuliert werden kann. In einfachen

[20] http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf
[21] Ebd.
[22] Ebd.

Fällen blendet der Trojaner dabei ein echt aussehendes Infofenster ein, mit einer Abfrage nach der vollständigen TAN-Liste des Online-Banking-Nutzers. Es gibt allerdings gleichermaßen ausgefeiltere Angriffe, die für den Benutzer sogar völlig unsichtbar ablaufen können.
Der Blick in die jüngste Vergangenheit zeigt, dass der nächste Schritt der Angreifer auf die Mobiltelefone abzielt, denn der Gebrauch von mTANs wird von Banken immer weiter verbreitet. Der Schädling **Android.Trojan.Spitmo.A** ist dabei der Erste, der aktiv Android-Mobilgeräte angreift, um die mTANs abzugreifen. Zuvor gab es solche Angriffe schon auf Mobiltelefone mit dem Symbian Betriebssystem, mit dem Schädling **ZitMo** (Abkürzung für **ZeuS in the Mobile**).

Charakteristisch für Banking-Trojaner ist nach wie vor das zu Grunde liegende Geschäftsmodell. Es gibt nur relativ wenige Familien von Banking-Trojanern, die von den Programmierern nicht selbst eingesetzt, sondern an andere Kriminelle verkauft werden (Malware as a service). Viele Banking-Trojaner nutzen zudem spezielle Methoden, um von AV-Software nicht erkannt zu werden. Die Käufer erwerben meist zusätzlich spezielle Verschlüsselungssoftware für Binärdateien (Crypter), um diese verändern zu können. Die Antivirenhersteller werden so zu häufigen Signaturupdates gezwungen. Die durchschnittliche Lebensdauer der Binärdateien dieser speziellen Art von

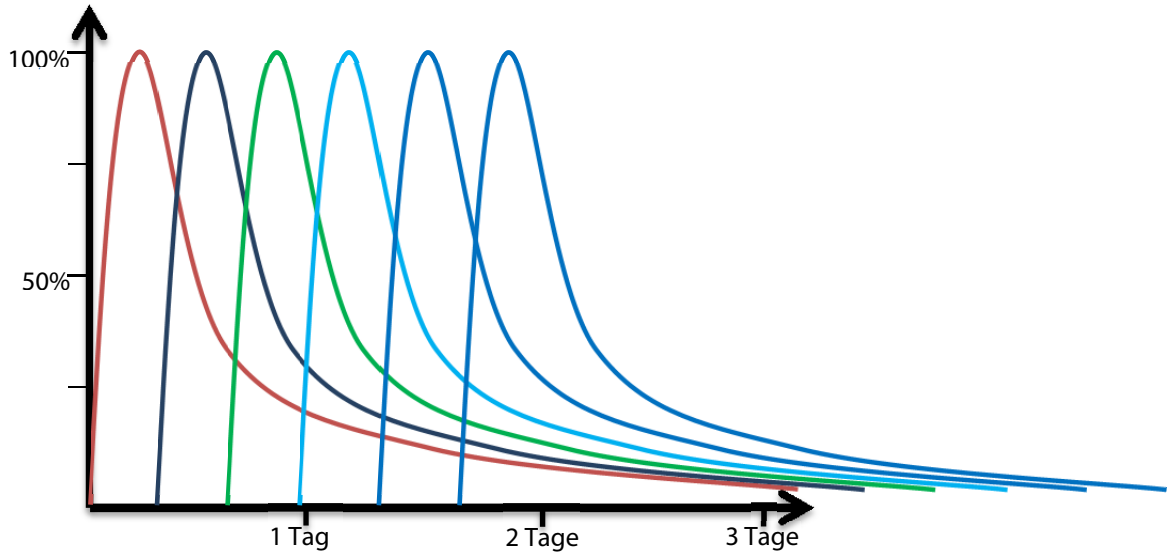


Abbildung 8: *Lebenszyklus von Banking-Trojanern*

Schadsoftware betrug zuletzt durchschnittlich allerdings nur rund 27 Stunden und sehr selten länger als 72 Stunden.[23] Da Herstellern von AV-Software bei Banking-Trojanern nur selten ein Signaturupdate in diesem Zeitfenster gelingt,[24] stellen Banking-Trojaner eine ernstzunehmende Gefahr für Computernutzer dar.

Wie auch viele andere Malware werden Banking-Trojaner häufig über sogenannte Exploits verbreitet. Dabei werden Schwachstellen bei Computer-Systemen der Internet-Benutzern ausgenutzt, um unbemerkt Malware auf den Rechner des Opfers herunterzuladen (Drive-by-Download) und zu installieren. Um nicht selbst bezüglich aktueller Schwachstellen auf dem laufenden Stand bleiben zu müssen, erwerben die Betreiber von Botnetzen üblicherweise fertige Exploit Kits im Untergrundmarkt.

[23] Siehe Abbildung 8
[24] Buescher, Armin / Leder, Felix / Siebert, Thomas: Banksafe. Information Stealer Detection Inside the Web Browser. RAID 2011, Springer Lecture Notes in Computer Science (Vol. 6961) / September 2011

Letztlich heißt das, dass Kriminelle für die Durchführung eines Online-Banking-Angriffs nur wenig Fachwissen benötigen.

Hervorzuheben für die Periode von Ende 2010 und 2011 ist insbesondere die Entwicklung um den wohl bekanntesten Banking-Trojaners **ZeuS**. Ende 2010 verkündete der Macher von **ZeuS** den Rückzug aus dem Markt und stellte den Verkauf seines Trojaners ein. **ZeuS** ist der Banking-Trojaner, der die Web Injects populär gemacht hat. Gleichzeitig wurde bekannt, dass der Quellcode an den Macher von **SpyEye** übergeben wurde. Seitdem wurden einige Funktionen von **ZeuS** in **SpyEye** integriert und **SpyEye** vermarktet sich als legitimer **ZeuS**-Nachfolger. Die Erkennungsraten von G Data BankGuard von **ZeuS** sowie **SpyEye** in 2011 bestätigen diese Entwicklung.

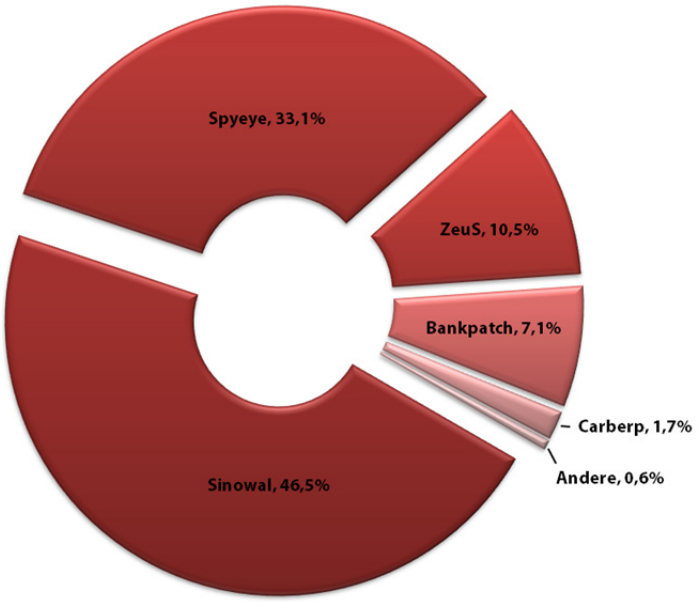


Abbildung 9: *Anteil der durch G Data BankGuard detektierten Banking-Trojaner Familien in H2 2011*

Anfang 2011 wurde der Quellcode von **ZeuS** in Untergrundforen von Unbekannten für einen Preis von 100.000 US$ zum Verkauf angeboten. Im Mai 2011 wurde der Quellcode schließlich auf ebenfalls unbekannten Wegen veröffentlicht.
Dies stellt die erste Veröffentlichung des Quellcodes eines Banking-Trojaners überhaupt dar. Im Verlauf des Jahres tauchten nach der Veröffentlichung des Quellcodes die ersten **ZeuS-Derivate** (z.B. **LICAT** und **IceIX**) auf, wodurch die Zahl der **ZeuS**-Detektionen insbesondere in Q4/2011 sprunghaft anstieg. Weitere **ZeuS-Derivate** im Verlauf des Jahres 2012 sind wahrscheinlich.

Der Trojaner mit der höchsten Detektionsrate in 2011 war **Sinowal**. **Sinowal** zeichnet sich insbesondere durch häufige Wechsel der Infektionsmechanismen sowie der verwendeten Rootkits aus. So wurde früher das MBR-Rootkit **Mebroot** verwendet, mittlerweile aber mal durch das MBR-Rootkit **TDSS**, mal durch eine selbstgeschriebene Rootkit-Komponente ausgetauscht.

Im letzten Quartal von 2011 konnte außerdem ein bemerkenswerter Anstieg von Detektionen des Banking-Trojaners **Carberp** verzeichnet werden. Der neuerliche Erfolg des Trojaners ist offenbar auf die Integration eines Bootkits in einer neuen Version zurückzuführen.

Gozi, **Silentbanker** und **Bebloh** spielen keine tragende Rolle, obwohl **Bebloh** immer wieder durch besonders ausgefeilte Angriffstaktiken auffällt, z.B. durch den sogenannten Retouren-Angriff. Dabei teilt die – durch den Trojaner manipulierte – Online-Banking-Seite dem Kunden mit, dass eine fehlgeleitete Überweisung das Konto erreicht habe und bittet um Rücküberweisung. Auch im Kontosaldo wird der zusätzliche Geldbetrag ausgewiesen. Überweist der Kunde den Betrag an das schon angegebene Konto zurück, ist dieser für ihn verloren: Tatsächlich war das zusätzliche Geld nie vorhanden. Bemerkenswert an diesem Angriff ist, dass dieser unabhängig vom verwendeten Authentifizierungsverfahren funktioniert – Egal ob iTAN, chipTAN oder mobileTAN: Arglose Benutzer führen die Überweisung selbst aus, so dass diese Autorisierungsverfahren effektiv ausgehebelt werden.

Mobile Malware

Der Zuwachs mobiler Malware, die von Schadsoftware-Autoren für Android OS entwickelt wird, steigt mit der zunehmenden Verbreitung von mobilen Android-Geräten. Waren es im Dezember 2010 täglich noch 300.000 aktivierte Android OS-Geräte, konnten ein halbes Jahr später, im Juni 2011, bereits 500.000 Aktivierungen pro Tag registriert werden. Gegen Ende 2011 verzeichnete man ca. 700.000 pro Tag, am 24./25. Dezember kurzfristig sogar 3,7 Mio. Aktivierungen, zwitscherte Andy Rubin, Mitgründer und Entwicklungsleiter der Android Inc. beim Micro-Blogging Dienst Twitter.[25]

Screenshot 2: *Andy Rubins Tweets zu Aktivierungen von Android-Geräten, Ende 2011 (Quelle: http://twitter.com/ARUBIN)*

Die Attraktivität der mobilen Geräte für Schadsoftware-Autoren steigt mit dieser Entwicklung, wie auch mit der Anzahl verfügbarer Apps im Android Market, auf Webseiten und in Märkten von Drittanbietern. Im Dezember 2011 verkündete Google, dass die Zahl der Downloads aus dem Android Market die Marke von 10 Milliarden geknackt hat.[26]

Die organisatorischen Hürden, die Android-Schadsoftware-Autoren überwinden müssen, sind auch weiterhin gering. Sie müssen lediglich 25 US$ für einen Google Entwickler-Account bezahlen, um für den offiziellen Market zu entwickeln. Kein Betrag, der Bösewichte abschreckt. Wird ein Entwickler-Account von Google gelöscht, erstellen die Schadsoftware-Autoren einfach einen neuen Account, unter dem sie die Malware erneut verbreiten. Einfacher ist jedoch die Veröffentlichung von Mobile Malware auf Webseiten oder in Märkten von Drittanbietern. Wird Schadcode im offiziellen Android Market entdeckt und entfernt, bleiben auf diesen anderen Vertriebswegen schadhafte Apps weiterhin im Umlauf.

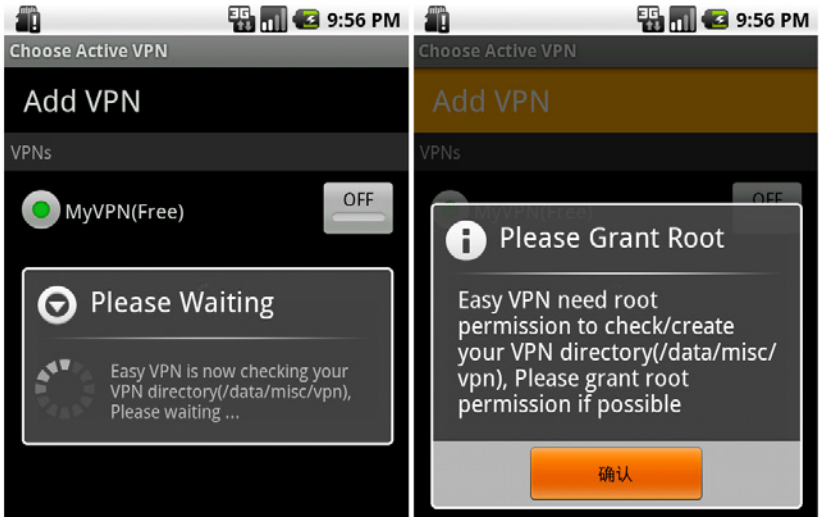
Die Anzahl neuer Schadprogramme für die Plattform Mobile ist 1.998.[27] Der Hauptgrund für diese Entwicklung liegt nicht in einer Anhäufung potentiell neuen Schädlingen, sondern rührt daher, dass viele Varianten von schon vorhandenen, sich gleichenden, einfacheren Schadprogrammen in Umlauf gebracht werden. Zum Beispiel handelt es sich dabei um Programme, die Hintergrundbilder anbieten, oder eine einfache Handhabung nützlicher Dienste, wie zum Beispiel den Zugriff auf Video-On-Demand Services. Alleine die Zahl der neuen Schadprogrammeder Kategorie Backdoor im Bereich Mobile hat von H1 2011 zu H2 2011 um 285% zugenommen.

Im Fall des Trojaners **Android.Trojan.FakeNetflix.A**, kurz **Fake NetFlix**, handelt es sich um ein simples Schadprogramm, das die NetFlix[28] Zugangsdaten abfragt. Die vom Trojaner gesammelten Daten überträgt dieser an einen vorgegebenen Server. Der Login-Versuch muss zwar aktiv vom Benutzer durchgeführt werden, eine anschließende Inkompatibilitätsmeldung jedoch versucht keinen Verdacht beim Benutzer auf ungefragte Aktivitäten aufkommen zu lassen.

[25] http://twitter.com/ARUBIN
[26] http://googleblog.blogspot.com/2011/12/10-billion-android-market-downloads-and.html
[27] Siehe Tabelle 1
[28] NetFlix ist ein amerikanisches Unternehmen, das in ausgewählten Ländern DVDs und Blu-rays per Post verleiht sowie auch Video-on-Demand anbietet.

Nach wie vor wird Android-Schadsoftware hauptsächlich dadurch verbreitet, dass bereits bekannte, gutartige Anwendungen kopiert, manipuliert und neu veröffentlicht werden. Diese trojanisierten Versionen wurden überwiegend in den Marktplätzen von Drittanbietern zum Herunterladen angeboten, fanden sich allerdings oftmals auch im offiziellen Android Market.

So, wie etwa **Android.Backdoor.LeNa.A**, kurz **LeNa** (Legacy Native). Es ist eine Backdoor, die sich selbst in Systemverzeichnisse kopiert, um so bei jedem Systemstart mit starten zu können. Gelingt dies, verbindet sich **LeNa** etwa einmal pro Stunde mit einem externen Server und überträgt Daten, die das Gerät eindeutig identifizierbar machen. Aufgrund ihres dynamischen Aufbaus ist eine Backdoor, wie **LeNa**, außerdem in der Lage, Software ohne Zutun des Benutzers nachzuladen und zur Installation anzubieten und öffnet somit Angreifern Tür und Tor zum Android Smartphone. Damit die Backdoor jedoch aktiv werden kann, benötigt sie entsprechende Berechtigungen,[29] die voraussetzen, dass das Mobilgerät gerootet sein muss. Ist dies nicht der Fall, bietet **LeNa** dem Benutzer Links zu Anleitungen und Tools an, die das Rooten des Gerätes für den Benutzer erklärt. Bleibt das Mobilgerät ohne Rootrechte, bleibt die Backdoor wirkungslos. Dabei zeigt sich einmal mehr, dass das Rooten eines Mobilgerätes nicht empfehlenswert ist.



Screenshot 3: *Screenshots einer App, die Mobilgeräte mit Android.Backdoor.LeNa.A infiziert*

Beim Blick auf die Funktionalitäten der gefundenen Malware finden sich im zweiten Halbjahr vor allem Schädlinge, die es auf Datendiebstahl und das Versenden kostenpflichtiger SMS abgesehen hatten. Bemerkenswert war die Entwicklung dahingehend, dass das Ausspähen von Daten nun mitunter innerhalb weniger Sekunden realisiert werden kann und die App, wie im Falle des Trojaners **Android.Trojan.GoneSixty.A** oder **Fake NetFlix** anschließend sogar selbst die Deinstallation initiierte und damit alle Spuren der Attacke verwischen will, denn der Benutzer spürt keinerlei Veränderung oder sieht eine App, die ihn misstrauisch machen könnte.

Weitgreifendere Schadfunktionen waren das Registrieren von Smartphones für kostenpflichtige Dienste, ohne das Wissen des Benutzers, und auch das Rooten des Android Geräts, das den Schadsoftware-Autoren die volle Kontrolle über sämtliche Funktionen des Smartphones einräumt. Hierbei wurde, bis zur Android Version 2.2, auf den bekannten Exploit Rage Against the Cage zurückgegriffen. Ab Version 2.3 wurde GingerBreak präferiert, da die bekannte Sicherheitslücke auf die sich der Exploit Rage Against the Cage stützte, ausgebessert wurde.

[29] Siehe Screenshot 3, rechts

Eine neue Form von Angriffen war das Verhöhnen des Benutzers, wie z.B. im Falle des Trojaners **Android.Trojan.Walkinwat.A**, kurz **Walkinwat**. Er zählt zu den ersten einer Art von Schädlingen, die Benutzer bloßstellen, die eine App illegal auf einer unautorisierten Internetseite heruntergeladen haben. Die Schadsoftware verschickt SMS an alle Kontakte aus dem Adressbuch. Der Text der SMS lautet: „Hey,just downlaoded a pirated App off the Internet, Walk and Text for Android. Im stupid and cheap,it costed only 1 buck. Don't steal like I did!" (deutsch; "Hey, ich habe gerade eine raubkopierte App aus dem Internet geladen, Walk and Text für Android. Ich bin blöd und geizig, sie kostete nur einen Dollar. Stiel nicht, wie ich es gemacht habe!"

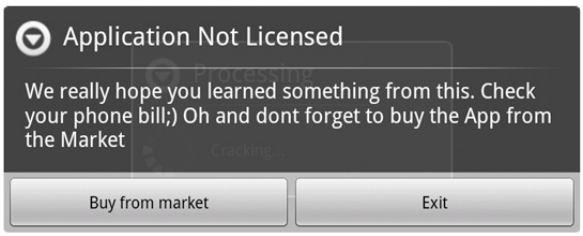
Ebenfalls diffamiert wurden Benutzer, die ein Spiel namens Dog Wars herunterluden. In diesem Fall handelt es sich um ein Spiel, bei dem man einen virtuellen Kampfhund trainiert, um ihn hinterher gegen virtuelle Hunde anderer Spieler antreten zu lassen. Bei dieser App wurden jedoch ungewollt auch SMS an alle gespeicherten Kontakte mit folgendem Text versendet: „I take pleasure in hurting small animals, just thought you should know that" (deutsch: „Ich habe Spaß daran, kleine Tiere zu quälen und dachte, das solltest Du wissen").

Screenshot 4: *App DogWars, die mobile Geräte mit Android.Trojan.DogoWar.A infiziert*

Beschränkte sich die Wirkung vieler Schadprogramme bis dato auf den asiatischen Raum, kam im November 2011 der erste Trojaner in Umlauf, der Rufnummern zu kostenpflichtigen Diensten nach Land sortiert gespeichert hat und so in Frankreich, Belgien, der Schweiz, Luxemburg, Deutschland, Spanien und England erfolgreich zur Ausführung kommen konnte. **Android.Trojan.SuiConFo.A**, kurz **SuiConFo**, tarnt sich u.a. als Kostenverwaltungs-App. Nach der Installation durch den Benutzer kommt, ähnlich wie beim Trojaner **Fake NetFlix**, eine Fehlermeldung über eine angebliche Inkompatibilität der App mit dem Gerät. Scheinbar passiert nun weiter nichts. Im Hintergrund jedoch versendet **SuiConFo** mehrere teure SMS an Premiumdienste. Kommt eine Bestätigungs-SMS an das Smartphone zurück, fängt der Trojaner diese ab, so dass die Folgen für den Benutzer bis zum Blick auf die Rechnung verborgen bleiben.

Trojaner, die mitunter kostenintensive SMS versenden, bieten nach wie vor die einfachste Möglichkeit, um schnell an Geld zu kommen. Diese Malware-Variante ist mittlerweile auf der ganzen Welt verbreitet. Malware-Hersteller erstellen spezielle Listen für die verschiedenen Ziel-Länder, um je nach Land die passende Premium-Nummer zu verwenden, so dass der Trojaner auch tatsächlich zur erfolgreichen Ausführung kommen kann.

Gegen Ende des Jahres zeigten sich weitere neue Absichten bei den Schadsoftware-Herstellern. Der 2011 bereits manigfaltig gebrauchte Begriff „Hacktivism", der ein u.a. politisches Engagement in Cyber-Attacken mit einbezieht, breitete sich auch auf das Feld der Mobile Malware aus. Der Trojaner **Android.Trojan.Arspam.A**, der am 19. Dezember erstmals entdeckt wurde, verbreitet politisch motivierte Inhalte. Nach der Installation des Trojaners durch den Benutzer, bei der u.a. Berechtigungen für den Zugriff auf sämtliche Daten und Statistiken, sowie das Versenden von



Screenshot 5: *Screenshot einer App, die Mobilgeräte mit Android.Trojan.Walkinwat.A infiziert*

SMS-Nachrichten gefordert werden, ist das Smartphone mit dem Trojaner **Arspam** infiziert und versendet anschließend SMS-Nachrichten an alle Kontakte aus dem Adressbuch, ohne, dass der Benutzer dies mitbekommt. Die im Dezember entdeckte Version des Trojaners installiert hierzu einen Dienst, der einen zufällig ausgewählten Link aus einem von 18 Forenbeiträgen zum Thema Naher Osten an alle Kontakte im Adressbuch des infizierten Smartphones verschickt. Befindet sich das infizierte Smartphone zudem noch in Bahrain, wird versucht, eine PDF Datei herunter zu laden, die weitere politische Inhalte beinhaltet.

Screenshot 6: *App, die den Trojaner Android.Trojan.Arspam.A verbreitet*

Die Anpassungsfähigkeiten der Malware haben bereits gegen Ende des Jahres 2011 für Aufmerksamkeit gesorgt und bieten für das Jahr 2012 einen düsteren Ausblick. Angriffe werden nicht mehr auf Asien begrenzt sein, sondern durch geringfügige Anpassungen eine weltweite Verbreitung erfahren. Smartphones sind nun weltweit bedroht. So werden z.B. simple Kombinationen aus Ländernamen und den dazu gehörigen Premium-Nummern dafür sorgen, dass die Malware eben nicht mehr nur im Entwicklerland zur Ausführung kommen kann. Das erhöht die finanziellen Schäden für die Opfer und gleichzeitig auch den möglichen Profit für die Täter.

Mobile Geräte werden auch 2012 immer weiter in den Fokus der digitalen Kriminellen rücken, da hier das Verhältnis zwischen Arbeitsaufwand und Profit noch sehr attraktiv ist. Solange Apps vor dem Einstellen in den offiziellen Android Market nicht eingehender kontrolliert werden, werden auch nach wie vor Schadprogramme erst nach einer längeren Zeitspanne auffallen und entfernt werden. Bis dahin haben sich jedoch bereits Mobilgeräte infiziert. Auch durch die steigenden Absatzzahlen der Android-Geräte wird der Android Market für den Untergrund immer interessanter.

Da außerdem die Nutzungsmöglichkeiten für Smartphones noch lange nicht ausgeschöpft sind, werden immer neue Technologien auch immer neue Angriffspunkte mit sich bringen – ein Beispiel für die nahe Zukunft wäre die Bezahlung mit dem Smartphone per NFC (in Android implementiert seit Version 2.3). Auch automatisierte Angriffe werden zukünftig für Unruhe sorgen – entsprechende Machbarkeitsstudien existieren bereits – und es ist nur eine Frage der Zeit, bis Angriffe gegen Benutzer gefahren werden, bei denen sie nicht aktiv beteiligt sein müssen. Und wenn es soweit ist, dass diese Angriffe in freier Wildbahn stattfinden, dann ergibt sich ein völlig neues Bedrohungsszenario.