G Data
Malware-Report

Halbjahresbericht Juli-Dezember 2009

Ralf Benzmüller & Sabrina Berkenkopf
G Data SecurityLabs

Geschützt. **Geschützter. G Data.**

Inhalt

Copyright © 2010 G Data Software AG

Auf einen Blick

Im zweiten Halbjahr 2009 wurden 924.053 neue Malwaretypen entdeckt. Das liegt 39% über dem Wert des ersten Halbjahrs und 60% über dem Vorjahreswert und ist somit neuer Rekord.

Im gesamten Jahr 2009 wurden 1.588.005 Malwaretypen gefunden - 78% mehr als 2008.

Der Anteil Trojanischer Pferde ist um 9,0% gestiegen. Sie haben mit 42,6% den größten Anteil an der Malware-Flut.

Überdurchschnittlich gestiegen sind die Schädlinge der Kategorien Wurm, Exploit und Virus.

Die Anzahl der Malwaretypen, die PDFs benutzen, hat sich fast verdreifacht.

Die Anzahl neuer Adware ist um 25% gesunken.

Über das gesamte Jahr sind 2.908 Familien aufgetreten, während es 2008 noch 3.069 waren. Das heißt, das neue Rekordergebnis geht auf weniger aktive Malware-Familien zurück.

Die produktivsten Malware-Familien sind „Genome“ (3), „PcClient“ (neu) und „Hupigon“ (1)[1].

Angriffsziel Nummer 1 bleibt Windows mit 99,0%. Der Rückgang um 0,3% zum ersten Halbjahr 2009 wird von .NET Malware (0,3%) kompensiert. Skriptsprachen für Webanwendungen halten ihren Anteil von 0,5%.

Ausblick

Downloader, Backdoors und Rootkits werden ihren Anteil behaupten. Sie haben einen festen Platz in der Untergrundökonomie.

Exploits werden auch im kommenden Jahr in Windeseile ausgenutzt.

Webanwendungen werden als Angriffsziele immer wichtiger.

Die Bedeutung von sozialen Netzwerken, wie MySpace, Facebook und Twitter, als Plattform für Werbung (Spam) und als Informationsquelle zur Vorbereitung und Durchführung von Straftaten wird steigen.

Der Diebstahl von Daten ist und bleibt ein lukratives Geschäft. Banking-Trojaner, Spyware und Keylogger werden ihren Anteil behaupten.

Ereignisse

„Koobface“ wird ein Jahr alt und ist aktiver denn je.

„Gumblar“ ist der Schädling, der die meisten Webseiten infiziert.

Zahlreiche Datenpannen und Datenschutzverletzungen erschüttern das Vertrauen der Verbraucher in die Vertrauenswürdigkeit von Unternehmen auch aus dem Umfeld von Kreditkarten und Banken.

1 Die Zahlen in Klammern beziehen sich auf die Platzierung im ersten Halbjahr 2009

Copyright © 2010 G Data Software AG

Malware: Zahlen und Daten

Grenzenloses Wachstum?

Seit Jahren wächst die Zahl neuer Malware kontinuierlich, wie Diagramm 1 zeigt. Auch im zweiten Halbjahr 2009 liegt die Anzahl mit 924.053 neuen Malwaretypen auf neuem Rekordniveau.

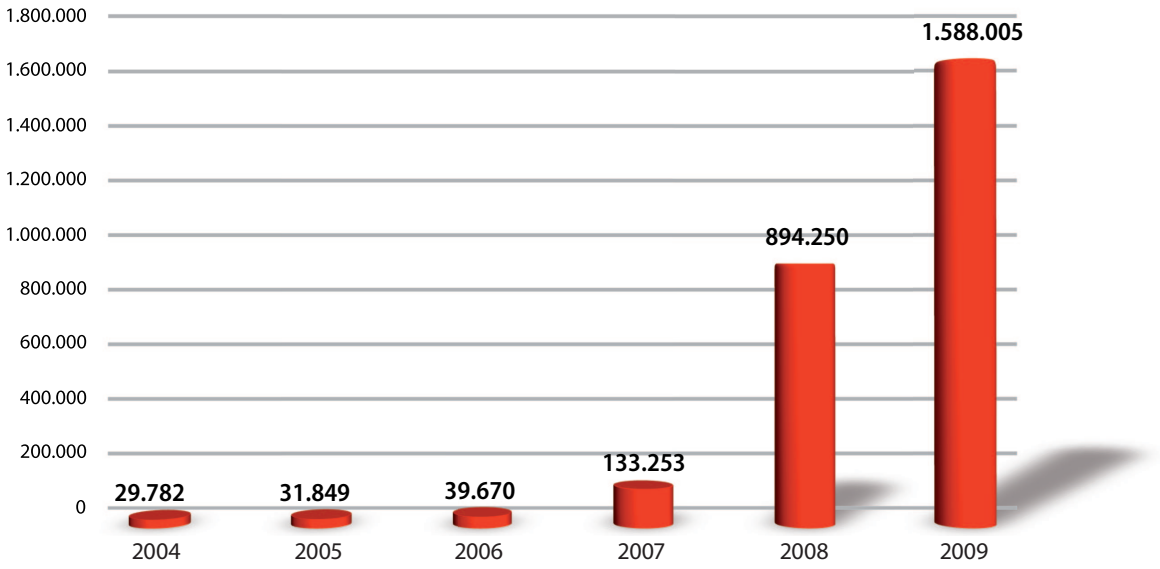


Diagramm 1: Anzahl neuer Malware pro Jahr seit 2004

Die Wachstumsrate liegt mit 39% gegenüber dem ersten Halbjahr 2009 und 60% im Vergleich zum Vorjahreszeitraum unter den Werten der vergangenen Jahre. Im gesamten Jahr 2009 wurden 1.588.005 Malwaretypen gefunden - 78% mehr als 2008. Die Anzahl neuer Malware aus dem Jahre 2004 wird aktuell in einer Woche übertroffen.

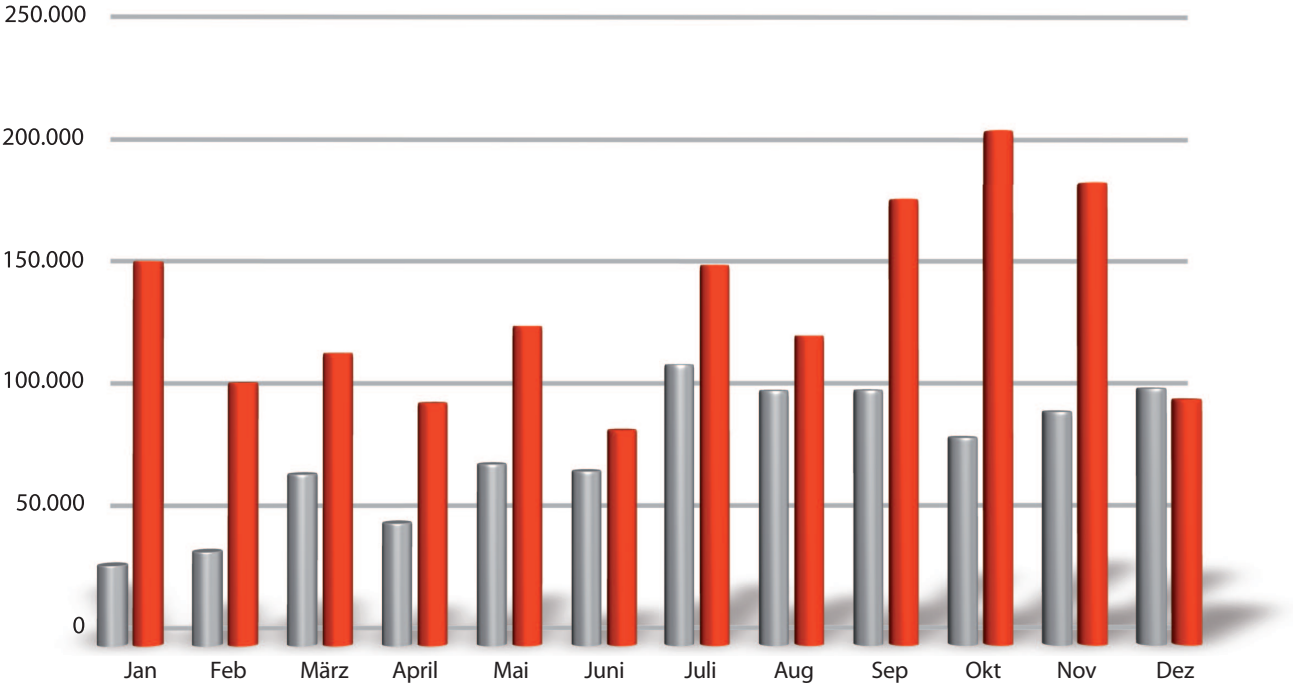


Diagramm 2: Anzahl neuer Malware pro Monat für 2008 und 2009

Copyright © 2010 G Data Software AG

Malware-Kategorien

Die Anzahl der Trojanischen Pferde ist in der zweiten Jahreshälfte deutlich angestiegen. Ihr Anteil liegt - wie Tabelle 1 zeigt bei 42,6% - 9,0% mehr als in der ersten Jahreshälfte. Damit sind sie mit weitem Abstand die häufigste Malware-Kategorie. Die Anzahl der Downloader, Backdoors und Tools steigt ebenfalls. Die Zahlen liegen etwas unter dem durchschnittlichen Anstieg von 39% zum ersten Halbjahr und 60% zum Vorjahreszeitraum. Aber diese Kategorien stellen die wichtigsten Komponenten der Malware-Schattenwirtschaft dar. Die Downloader sorgen für die Verbreitung, Backdoors machen die Rechner fernsteuerbar (Botnetze) und die Tools sind notwendig, um Einsteigern den Zugang zur Malware-Szene zu gewähren und Profis die tägliche Arbeit zu erleichtern.

Einen überdurchschnittlichen Anstieg konnten auch die Würmer verbuchen. Ihre Anzahl hat sich gegenüber dem ersten Halbjahr fast verdoppelt und gegenüber dem gleichen Zeitraum im Vorjahr ungefähr verdreifacht. Mit dazu beigetragen haben die Familien „Basun“, die es als erster Wurm seit Jahren wieder in die Top 10 geschafft hat und „Autorun“, der Spitzenreiter bei den Würmern aus dem ersten Halbjahr.

Überdurchschnittlich zugenommen hat die Anzahl der Exploits. Das steht im Gegensatz zur deutlich gesunkenen Zahl der bei CVE gemeldeten Sicherheitslücken. Sie lag 2009 mit 4.594 gemeldeten Schwachstellen deutlich unter dem Rekordergebnis von 2008, als 7.250 Schwachstellen verzeichnet wurden. Die Anzahl bekannt gewordener Sicherheitslücken besagt also nur unzureichend, wie viele Schwachstellen auch in Malware genutzt werden. Und diese Zahl ist deutlich gestiegen. Immer öfter werden Sicherheitslücken in weit verbreiteter Software ausgenutzt, um Rechner vorwiegend aus dem Internet zu attackieren. Rechner mit veralteter Software sind dann leichte Beute für Cyberkriminelle.

Den stärksten Zuwachs hat aber eine bereits totgeglaubte Kategorie verzeichnet - die Viren. In diese Kategorie fallen die klassischen Dateiinfektoren, die ausführbare Dateien befallen. Mit der gestiegenen Nutzung von USB-Sticks und anderen Wechseldatenträgern lohnt sich der Einsatz von solchen Verfahren wieder. Mit einem Anteil von 0,1% hält sich die Verbreitung allerdings in Grenzen.

Kategorie	# 2009 H2	Anteil	# 2009 H1	Anteil	Diff. 2009H2 2009H1	# 2008 H2	Anteil	Diff. 2009H2 2008H2
Trojan. Pferde	393.421	42,6%	221.610	33,6%	+78	155.167	26,9%	+154
Downloader/ Dropper	187.958	20,3%	147.942	22,1%	+27	115.358	20,0%	+63
Backdoors	137.484	14,9%	104.224	15,7%	+32	125.086	21,7%	+10
Spyware	86.410	9,4%	97.011	14,6%	-11	96.081	16,7%	-10
Würmer	51.965	5,6%	26.542	4,0%	+96	17.504	3,0%	+197
Adware	30.572	3,3%	34.813	5,3%	-12	40.680	7,1%	-25
Tools	14.516	1,6%	11.413	1,6%	+27	7.727	1,3%	+88
Rootkits	11.720	1,3%	12.229	1,9%	-4	6.959	1,2%	+68
Exploits	3.412	0,4%	2.279	0,3%	+50	1.841	0,3%	+85
Viren	637	0,1%	143	0,0%	+345	167	0,0%	+281
Dialer	415	0,0%	1.153	0,2%	-64	1013	0,2%	-59
Sonstige	5.543	0,5%	4.593	0,7%	+21	8.419	1,5%	-34
Gesamt	924.053	100,0%	663.952	100,0%	+39	576.002	100,0%	+60

Tabelle 1: Anzahl und Anteil neuer Malwarekategorien im ersten und zweiten Halbjahr 2009 sowie deren Veränderung

Copyright © 2010 G Data Software AG

Abgenommen hat hingegen die Anzahl neuer Spyware. Deren Anteil ist auf 9,4% gesunken, das sind 5,2% weniger als im ersten Halbjahr 2009 und 7,3% weniger als ein Jahr zuvor. Das bedeutet allerdings nicht, dass keine Daten mehr ausspioniert werden. Im Gegenteil. Die Spionagefunktionen sind aber häufiger in umfangreichere Pakete integriert, die als Trojanische Pferde klassifiziert werden.

Rootkits sind eine wichtige Komponente, um Spyware und Backdoors zu verstecken. Ihre Anzahl hat im 1. Halbjahr 2009 deutlich zugenommen und ihre Verwendung in Malware ist mittlerweile etabliert. Dennoch hat die Anzahl neuer Rootkits leicht abgenommen.

Im Bereich der Adware hingegen ist eine Entspannung zu verzeichnen. Die Anzahl neuer Werbeschädlinge liegt 25% unter den Zahlen des Vorjahres. Das geht hauptsächlich auf den Rückzug von „Monder" zurück. Im letzten Halbjahr war „Monder" die produktivste Malware-Familie. Im zweiten Halbjahr ist deren Produktivität deutlich gesunken.

Variantenreiche Familien

Die Funktionen und Eigenschaften eines Computerschädlings ermöglichen die Zuordnung zu Familien. In den vergangenen Jahren nahm zwar die Zahl der Malware kontinuierlich zu, die Anzahl der Familien sank aber ebenso beständig. Im ersten Halbjahr 2008 waren es noch 2.395 und im zweiten 2.094. Im ersten Halbjahr 2009 wurden 1.948 verschiedene Vertreter von Virenfamilien gezählt. Im zweiten Halbjahr 2009 hat die Anzahl der Malware-Familien erstmals wieder zugenommen. Schädlinge aus 2.200 verschiedenen Familien waren in diesem Zeitraum aktiv. Über das gesamte Jahr 2009 waren es 2.908 Familien gegenüber 3.069 in 2008. Der Trend zur Konzentration hält also an. Nach wie vor wird die steigende Zahl an Computerschädlingen von immer weniger Familien hervorgebracht.

	# 2009 H2	Virenfamilie	# 2009 H1	Virenfamilie	# 2008 H2	Virenfamilie
1	67.249	Genome	34.829	Monder	45.407	Hupigon
2	38.854	PcClient	26.879	Hupigon	35.361	OnlineGames
3	37.026	Hupigon	18.576	Genome	20.708	Monder
4	35.115	Scar	16.719	Buzus	18.718	MonderB
5	24.164	Buzus	16.675	OnlineGames	15.937	Cinmus
6	20.581	Lipler	13.889	Fraudload	13.133	Buzus
7	19.848	Magania	13.104	Bifrose	13.104	Magania
8	18.645	Refroso	11.106	Inject	12.805	PcClient
9	16.271	Sasfis	10.322	Poison	11.530	Zlob
10	16.225	Basun	10.312	Magania	10.412	Virtumonde

Tabelle 2: Top 10 der aktivsten Virenfamilien 2009 und im zweiten Halbjahr 2008

In Tabelle 2 werden die Familien gezeigt, die in den letzten 18 Monaten die meisten Varianten hervorgebracht haben. Der aktuelle Spitzenreiter „Genome" bringt es auf durchschnittlich 184 neue Varianten pro Tag. Auch die Backdoors „PcClient" und „Hupigon" auf Platz 2 und 3 bringen es im Schnitt auf mehr als 100 Varianten pro Tag.

Genome

Die Trojaner der „Genome"-Familie vereinen Funktionalitäten wie Downloader, Keylogger, Dateiverschlüsselung.

Copyright © 2010 G Data Software AG

PcClient

Bei „PcClient“ handelt es sich um ein Hintertürprogramm (Backdoor), mit dem sich der Rechner fernsteuern lässt und Daten gestohlen werden können. Seine Dateien und Registry-Einträge versteckt er mit Rootkit-Techniken.

Hupigon

Die Backdoor „Hupigon“ ermöglicht dem Angreifer unter anderem die Fernsteuerung des Rechners, das Mitschneiden von Tastatureingaben, Zugriff auf das Dateisystem und das Einschalten der Webcam.

Scar

Dieses Trojanische Pferd lädt eine Textdatei, mit der weitere Downloads von Schadprogrammen wie Downloadern, Spyware, Bots etc. initiiert werden.

Buzus

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 dadurch zusätzlich verwundbar zu machen.

Lipler

Bei „Lipler“ handelt es sich um einen Downloader, der weitere Malware von einer Webseite nachlädt. Außerdem verändert er die Startseite des Browsers.

Magania

Trojanische Pferde der in Ostasien aktiven „Magania“-Familie haben sich auf den Diebstahl von Gaming-Accountdaten der taiwanesischen Softwareschmiede Gamania spezialisiert. In der Regel werden „Magania“-Exemplare per Mail verteilt, in der sich ein mehrfach gepacktes, verschachteltes RAR-Archiv befindet. Beim Ausführen der Schadsoftware wird zur Ablenkung zunächst ein Bild angezeigt, während im Hintergrund weitere Dateien im System hinterlegt werden. Zudem klinkt sich „Magania“ per DLL in den Internet Explorer ein und kann somit den Web-Verkehr mitlesen.

Refroso

Dieses Trojanische Pferd ist neu in der Top 10. Erste Exemplare wurden Ende Juni 2009 entdeckt. Es hat Backdoor-Funktionen und kann andere Rechner im Netzwerk attackieren.

Sasfis

Dieses Trojanische Pferd installiert eine Datei auf dem Rechner und versucht weitere aus dem Internet nachzuladen. Häufig werden diese Varianten als E-Mail Anhang verschickt.

Basun

Erstmals seit zwei Jahren hat es wieder ein Wurm in die Top 10 der produktivsten Malware-Familien geschafft. „Basun“ kopiert sich unter dem Namen des aktuellen Benutzers bzw. des Administrators auf den PC. Danach attackiert er andere Rechner im lokalen Netzwerk, um sich zu verbreiten.

Copyright © 2010 G Data Software AG

Angriffsziel Nr. 1: Windows

In den letzten Jahren zeichnet sich eine Konzentration der Malwareautoren auf die Windows-Plattform ab. Obwohl absolut gesehen immer mehr Malware entwickelt wird, steigt auch der Anteil an Schädlingen für Windows beständig. Im abgelaufenen Halbjahr liegt er mit 99,0% etwas unter den Ergebnissen der letzten beiden Halbjahre (vgl. Tabelle 3). Dieser leichte Rückgang wird aber durch die Malware für die dritthäufigste Plattform relativiert. Denn die Schädlinge, die in der Microsoft Intermediate Language erstellt werden, haben deutlich zugelegt und ihren Anteil auf 0,3% gesteigert. MSIL ist das Zwischenformat, in dem .NET-Anwendungen in ihrer plattform- und programmiersprachenunabhängigen Form repräsentiert werden. Auch Malwareautoren nutzen nun vermehrt die Vorzüge der .NET-Umgebung. Die meisten .NET-Anwendungen sind auf Windows ausgerichtet.

Skripte von Webseiten (z. B. JavaScript, PHP, HTML, ASP etc.) behaupten ihren Anteil von 0,5% beharrlich. Infizierte Webseiten werden als Infektionsweg immer wichtiger. Von den 4.371 Webskripten sind 3.295 JavaScript-Schädlinge. JavaScript wird dabei aber nicht nur in Webseiten eingesetzt. 1.624 Schädlinge setzen auf PDFs als Verbreitungsmedium. Waren es 2008 noch 780 PDF-basierte Schädlinge, so ist deren Anzahl 2009 auf 2.394 angestiegen - fast eine Verdreifachung.

	Plattform	# 2009 H2	Anteil	# 2009 H1	% 2009 H1	# 2008 H2	% 2008 H2
1	Win32	915.197	99,0%	659.009	99,3%	571.568	99,2%
2	WebScripts	4.371	0,5%	3.301	0,5%	2.961	0,5%
3	MSIL	2.732	0,3%	365	0,1%	318	0,1%
4	Scripts	1.124	0,1%	924	0,1%	1.062	0,2%
5	NSIS	229	0,0%	48	0,0%	58	0,0%
6	Mobile	120	0,0%	106	0,0%	70	0,0%

Tabelle 3: Top 5-Plattformen 2008 und 2009.
Unter WebScripts ist Malware zusammengefasst, die auf JavaScript, HTML, Flash/Shockwave, PHP oder ASP basiert und üblicherweise Schwachstellen per Browser nutzt. „Scripts" sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden. MSIL ist Malware, die im Zwischencode von .NET-Programmen vorliegt. NSIS ist die Installations-Plattform, die auch von Winamp genutzt wird. Unter Mobile ist Malware für J2ME, Symbian und Windows CE zusammengefasst.

Die Plattform NSIS hat mit einer deutlichen Zunahme die 120 Schädlinge für Mobile-Plattformen aus den Top 5 verdrängt. Trotz vereinzelter Vorfälle setzen sich Mobile-Schädlinge nicht durch. NSIS ist die Installationsplattform, die u. a. dazu genutzt wird, den Mediaplayer Winamp zu installieren. Die Beliebtheit von NSIS als Installationsplattform steigt nicht nur bei legalen Softwareentwicklern.

Für Unix-basierte Systeme erschienen 37 Schädlinge (im Vergleich zu 66 im ersten Halbjahr 2009) und für Apples OSX wurden 8 neue Schädlinge gefunden. Im Vergleich zur Masse an Schädlingen für Windows, sind Anteile anderer Plattformen verschwindend gering.

Copyright © 2010 G Data Software AG

Ausblick 2010

Die kommerzielle Nutzung von Malware hält an. Die immensen Umsätze in der Underground-Ökonomie erlauben es, die Entwicklung neuer Technologien zur Verbreitung, Nutzung und Tarnung von Malware voran zu treiben. Auch Investitionen in aufstrebende Nutzungsfelder wie soziale Netzwerke, mobile Endgeräte, Spielekonsolen und wenig genutzte Betriebssysteme lassen sich so realisieren. Sollten sich diese Versuche als lukrativ erweisen, werden die Cyberkriminellen sicher ihre Aktivitäten verlagern. Momentan gibt es dafür aber keine Anzeichen.

Darum wird auch im kommenden Jahr die Malware-Flut keineswegs verebben - eher dürfte das Gegenteil der Fall sein. Downloader, Backdoors, Tools und Rootkits sind fester Bestandteil dieser Schattenwirtschaft und werden mit immer raffinierteren Methoden ihren Aufgaben nachkommen.

Im Bereich der Exploits werden weiterhin Sicherheitslücken in populären Desktopanwendungen in Windeseile ausgenutzt. Die gesunkene Zahl der gemeldeten Sicherheitslücken und das gestiegene Sicherheitsbewusstsein von Softwareentwicklern könnten dazu führen, dass eine Verlagerung auf Webapplikationen vorgenommen wird. Je populärer die Miete von Software und deren Betrieb im Internet wird, desto lukrativer wird es für Cyberkriminelle, die gemietete Webanwendung zu kapern. Ähnliches gilt bei Angeboten für Mietrechner (Schlagwort: Cloud Computing). Es bleibt abzuwarten, ob die Entwickler von Webanwendungen die gleiche Sorgfalt bei der Umsetzung von Sicherheitsvorgaben an den Tag legen, wie sie für Desktop-Software mittlerweile etabliert sind.

Für das kommende Jahr sind neue Betriebssysteme und Rechnerplattformen angekündigt. Es bleibt abzuwarten, wie sich diese Märkte entwickeln. Auch der langsame Umstieg auf 64-bit Versionen von Windows 7 wird von den Malwareautoren eine Umstellung verlangen.

Prognosen

Kategorie	Trend
Trojanische Pferde	↗
Backdoors	→
Downloader/Dropper	→
Spyware	→
Adware	↘
Viren/Würmer	→
Tools	→
Rootkits	→
Exploits	↗
Win32	↗
WebScripts	↑
Scripts	→
MSIL	↗
Mobile	↗

Copyright © 2010 G Data Software AG

Web 2.0: Soziale Netzwerke

Das Internet hat sich im Laufe der Zeit von einem Medium mit wissenschaftlichem Grundton zum Alltagsmedium der breiten Masse entwickelt. Jeder vierte Mensch benutzt das Internet.[2] Diese Zahl allein ist schon beeindruckend. Schaut man aber zusätzlich noch auf die Nutzerstatistiken der weltweit größten Social Network Community, Facebook, so wird deutlich, welchen Anteil an der Internetnutzung die Online-Community inzwischen hat: Laut Angaben des Facebook-Gründers Mark Zuckerberg tummeln sich im Dezember 2009 schon mehr als 350 Millionen Menschen[3] bei Facebook – das bedeutet im Umkehrschluss, dass statistisch gesehen jeder 5. Internetnutzer bei dem amerikanischen Web 2.0-Anbieter ein Profil besitzt!

Es gibt aber nicht nur soziale Netzwerke in der Vielfalt der Web 2.0 Anwendungen: Google Docs, Google Maps, Picasa, Flickr, Identi.ca, Jaiku, usw. sind nur einige weitere Beispiele für das Mitmach-Web. So hilfreich und attraktiv die breite Palette an Web 2.0-Anwendungen auch ist, jeder Dienst birgt seine eigenen Gefahren. Diese ergeben sich einerseits dadurch, dass User viele, und oft zu viele, persönliche Informationen über sich auf den Community-Seiten preisgeben und andererseits durch die technische Struktur der Plattformen. Sind die Grundgerüste an sich schon durch Cyberkriminelle angreifbar, wie verschiedene Fälle immer wieder zeigen, implementieren die Netzwerke zudem immer mehr Applikationen, die ihrerseits eine eigene Angriffsfläche bieten.

Branchenprimus Facebook als Fallbeispiel

Am Beispiel der Community Facebook lassen sich eine Vielzahl von Angriffen und Unannehmlichkeiten für User exemplarisch darstellen. Abgesehen von den immer wieder kritisierten Privacy-Einstellungen des Netzwerks und des zu geringen Schutzes junger Menschen, lauerte die Gefahr für den Nutzer an verschiedenen Stellen:

Mitte November wurden mehr als 200 Facebook-Gruppen von einer Initiative namens „Control Your Info“ übernommen und umbenannt. Die Gruppe wollte mit dieser harmlos anmutenden Aktion auf eine Sicherheitslücke aufmerksam machen, die es möglich macht, Inhalte der Gruppen zu verändern und sie brauchte dafür noch nicht einmal Facebook zu hacken. Die Gruppe „Control Your Info“ musste sich lediglich als Administrator von Gruppen registrieren, aus denen der

2 Weltweit gibt es laut www.internetworldstats.com 1.733.933.741 Internetnutzer, was einem Anteil von etwa 25 Prozent der Weltbevölkerung entspricht.

3 Quelle: http://blog.facebook.com/blog.php?post=190423927130

Copyright © 2010 G Data Software AG

eigentliche Administrator ausgetreten war. Die Änderung des Gruppennamens und -inhalts sollte Aufmerksamkeit erzeugen, kann aber auch die Reputation des unwissenden Nutzers schädigen, wenn die Angreifer z. B. rechtswidrige Inhalte posten. Unter anderem können Administratoren von Gruppen Nachrichten an alle Mitglieder der Gruppe versenden und somit gezielt Spam verbreiten.

Spam aus dem eigenen Freundeskreis

Nachrichtenversand von Kontakten aus dem Facebook-Adressbuch oder aus einer Facebook-Gruppe wird von den meisten Nutzern als seriös eingestuft. Wird aber Spam aus einer entführten Gruppe versendet oder über den unerlaubt übernommenen Facebook-Account eines Freundes, ist Kontrolle besser als Vertrauen allein: Man erhält eine Nachricht, die ein lustiges Video, schockierende Fotos oder einfach nur brandneue und interessante Inhalte anpreist.
Anbei ein Link, der beim Anklicken den Rechner auf verschiedene Arten infizieren kann – ein unbemerkter Drive-by-Download oder gefälschter und infizierter Codec, um das lustige Video zu sehen, sind die beliebtesten Tricks. Was jahrelang als E-Mail-Masche funktionierte, verbreitet sich nun auch in sozialen Netzwerken. Facebook-Nutzer wurden schon häufig von genau diesem Pseudo-Seriositätstrick getroffen.

Koobface in Hülle und Fülle

Seit mehr als einem Jahr treibt der Wurm „Koobface" nun sein Unwesen in Web 2.0-Portalen und hielt auch 2009 die AV-Hersteller in Atem. Jüngstes Beispiel im Zusammenhang mit dem amerikanischen Facebook ist ein kursierendes Video namens „SantA". Der Klick auf das Video öffnet eine Webseite mit einem angeblich benötigten Codec. Die Installation des gefälschten Codecs bringt „Koobface" auf den Rechner des Opfers und dieser verbreitet sich dann in allen möglichen sozialen Netzwerken des Opfers.

Zuvor hatte „Koobface" in der zweiten Jahreshälfte schon zahlreiche andere neue Einfallstore in die Welt der Social Networks gefunden: Das Aushebeln der Captcha-Funktion bei Anmeldungen, die Registrierung eines neuen Users mit komplettem Profil, die Verbreitung von gefälschten Videocodecs zu immer neuen Videos, und vieles mehr – Immer auf der Suche nach neuen Daten, die der Wurm auslesen, abspeichern und verbreiten kann. Sobald der Wurm sich in den Freundeskreis eines Community-Mitglieds integriert hat, nimmt er emsig seine Arbeit als Sammler auf und verbreitet sich.

Eine Variante wurde dann bei Skype entdeckt. Der Trojaner verbreitet sich über infizierte Webseiten, stiehlt die Log-in Daten des Skype-Nutzers und liest Daten aus dem Skype-Adressbuch aus. Aber auch Nutzer anderer großer Social Networks (z. B. MySpace, Hi5) sind betroffen.

Auch Twitter bietet Angriffspotenzial

Der Micro-Blogging Dienst Twitter gehört zu den beliebtesten Webapplikationen, um seine Mitmenschen auf dem Laufenden zu halten. Durch den Wunsch, überall und jederzeit „zwitschern" zu können, ergeben sich jedoch auch immer neue Sicherheitslücken: So wurde im August ein Twitter-Account genutzt, um mit Base64-kodierten Kurznachrichten ein Botnetz zu steuern. Twitter sperrte den Account umgehend.

Copyright © 2010 G Data Software AG

Ein weiteres Infektionsrisiko geht besonders bei den „short message"-Blogdiensten von gekürzten URLs aus. User können den wahren Link hinter den Abkürzungen nicht sehen und werden so schnell zu Opfern infizierter Seiten. Bekannte URL-Verkürzungsdienste sind u. a. TinyURL, bit.ly, is.gd, tr.im oder auch twi.bz.
Man sollte sich nicht auf den gekürzten Link verlassen und auch das Vertrauen zu der Person, die ihn veröffentlicht hat, kann Nutzer in die Falle locken, wenn z. B. Twitter-Accounts gekapert werden. Nutzer sollten vor dem Klick auf eine Kurz-URL die von den Verkürzungsdiensten selbst zur Verfügung gestellten Sicherheitsmaßnahmen benutzen, um eine Gefahr möglicherweise zu erkennen. Hierzu kann man die diensteigenen Infoseiten zur jeweiligen Kurz-URL aufrufen.

Hier einige Beispiele von bekannten Diensten und ihre Infoadressen:

http://www.gdata.de/virenforschung/news.html

	Short URL	Aktion	Vorschauoption URL
TinyURL	http://tinyurl.com/yzuwcwd	preview. vor die URL	http://preview.tinyurl.com/yzuwcwd
bit.ly	http://bit.ly/7jH8xP	/info hinter bit.ly	http://bit.ly/info/7jH8xP
is.gd	http://is.gd/5yGtz	- hinter die URL	http://is.gd/5yGtz-
twi.bz	http://gdata.de.twi.bz/b	/e hinter die URL	http://gdata.de.twi.bz/b/e
tr.im	http://tr.im/lqpj	-	-

Tabelle 4: Ein Beispiel für Short-URLs und ihre Vorschauoptionen

Fazit

Die Zahl der Angriffe auf Web 2.0-Applikationen wird weiter zunehmen. Datensätze sind und bleiben eine hochinteressante und hochrentable Ware für Schwarzmarkt-Dealer und Identitätsdiebe. Die neuen Schädlingsvarianten, die 2009 hinzugekommen sind, werden sich weiter verbreiten und Malwareautoren werden sie verfeinern, um immer neue Schwachstellen in den Portalen und APIs auszunutzen.

Copyright © 2010 G Data Software AG

Problemfall: Datenschutz

Im zweiten Halbjahr 2009 sind überdurchschnittlich viele Probleme im Bereich Datenschutz aufgetreten. Die Bandbreite der erwähnten Probleme ist dabei vielfältig: Sie reicht von Datendiebstahl über Datenverkauf oder Datenmissbrauch bis zu illegaler Überwachung. Das Onlineportal „projekt-datenschutz.de“ zeigt alleine zwischen Anfang Juli und Ende Dezember 2009 75 Fälle von Datenschutzproblemen in Deutschland auf.

Beim Datendiebstahl muss unterschieden werden, ob die Daten verloren gehen, weil eine Sicherheitslücke in einem Computersystem oder anderen elektronischen System von externen Angreifern ausgenutzt wurde oder ob das Abgreifen von Daten mit Hilfe von Insidern geschieht.

Das größte Problem an Datenlücken ist, dass die Daten, wenn sie einmal in Umlauf sind, unkontrolliert weiterverbreitet werden können und nicht mehr zurück zu holen sind. Betroffene haben kaum eine Chance, sich gegen die Vervielfältigung zu wehren.

Soziale Netzwerke und Kreditkarten im Visier

In der zweiten Jahreshälfte sorgte ein Datenleck beim sozialen Netzwerk schülerVZ für Aufsehen. Nutzerdaten von mehr als einer Million Mitglieder der Community wurden mit Hilfe von automatisierten Datensammlern (Crawlern) über eine ungesicherte Schnittstelle ausgelesen und an die Betreiber der Webseite netzpolitik.org gemailt. Der daraufhin festgenommene 20-jährige Mann aus Erlangen beging zwei Wochen nach seiner Festnahme während der Untersuchungshaft in seiner Zelle Selbstmord. Das Mutterportal studiVZ wurde schon Anfang 2007 Opfer von Datendiebstahl. Böse Stimmen behaupteten, dass die Firma anscheinend aus den vergangenen Vorfällen nichts gelernt habe.

Ein weiteres Topthema im November 2009 war ein Datenleck bei einem spanischen Kreditkartendienstleister. Offenbar befand sich die Lücke bei einem spanischen Dienstleister für Kartenabrechnungen. In Folge dessen wurden über 100.000 Kreditkarten von überwiegend deutschen und britischen Kunden ausgetauscht. Auch wenn die Anzahl der ausgetauschten Karten im Vergleich zur Gesamtzahl nur einen geringen Prozentsatz darstellt, wurde durch diesen Vorfall die Angreifbarkeit deutlich. Kreditkartendaten können an vielen Stellen verloren gehen:

- Beim Bezahlen werden mit präparierten Lesegeräten die Daten von der Karte kopiert
- Die Daten werden von Keyloggern und anderen Spionageprogrammen vom PC ausspioniert, z. B. beim Online-Shopping
- Auf gefälschten Webseiten (Phishing) oder in betrügerischen Webshops mit Lockangeboten werden die Informationen in einem Formular erfragt und vom Opfer eingegeben
- Unzureichend gesicherte Datenbanken von Online-Shops, Bezahldiensten und Banken enthalten Transaktionsdaten. Sie sind immer wieder Ziel von Angriffsversuchen

Copyright © 2010 G Data Software AG

Die Inhaber von Kreditkarten haben nicht auf alle Aspekte der Datenverarbeitung einen Einfluss. Und immer öfter hört man, dass jemand Opfer von Kreditkartenbetrügern wurde. Viele Verbraucher sind daher verunsichert und erwägen auf die Kreditkarte zu verzichten. Das ist allerdings keine Alternative.

Kreditkartennutzer können sich aktiv gegen Gefahren durch Angreifer schützen:

- Betriebssystem und Browser auf dem neuesten Stand halten
- Einen zuverlässigen und umfassenden Virenschutz einsetzen und aktuell halten
- Bei der Eingabe von Daten in Formulare immer hinterfragen, ob der Betreiber der Seite die erfragten Informationen überhaupt braucht. PINs, TANs, Passwörter oder Sicherheitscodes von Kreditkarten (CCV) nur angeben, wenn man etwas bezahlt
- Sensible Daten nur per https, d. h. verschlüsselt versenden

Unüberlegtes Webseitenmanagement

Ende Oktober wurde bekannt, dass der Onlinebuchhandel und -Marktplatz Libri.de die Rechnungen seiner Kunden unverschlüsselt und für jedermann zugänglich gespeichert hat. Wer eine Rechnung erhielt, musste lediglich die fortlaufende Nummer in der Adresszeile des Browsers ändern: Libri.de versah jede Rechnung mit einer Rechnungsnummer, die auch im Namen des Dokuments gespeichert wurde. Beim Onlineabruf der Rechnung war diese Nummer als Adressbestandteil sichtbar und ließ sich einfach sequenziell verändern. Somit gewährte man findigen Leuten Zugriff auf fremde Rechnungen und Kundendaten. Mit einer ebenso eklatant einfachen Methode konnten auch Benutzernamen und Passwort - bestehend aus sequenziellen Nummern - von Händlern ausspioniert werden. Libri.de hat später seine Sicherheitsmaßnahmen überdacht und verbessert. Besonders brisant ist auch folgendes Detail: Das Unternehmen Libri.de schmückt sich mit einem TÜV Süd-Siegel, das für besonders sichere Onlineshops vergeben wird.

Auch technischer Rückstand wird ausgenutzt

Es ist bekannt, dass die Funknetze der Einsatzkräfte von Polizei, Feuerwehr und Rettungsdiensten in Deutschland größtenteils noch analog betrieben werden. Damit ist Deutschland in dieser Hinsicht quasi Schlusslicht in Europa. Die alte Technik gilt als störanfällig und vor allem als nicht abhörsicher. Eine Umrüstung auf digitale Technologie sollte schon zur FIFA Fußballweltmeisterschaft 2006 erfolgen, scheiterte jedoch. Zu hohe Kosten (rund 3,6 Milliarden Euro), technische Schwierigkeiten und politische Querelen verschoben eine Einführung immer wieder aufs Neue.

Ein Fall aus Österreich zeigt, welche Risiken die veraltete Technik mit sich bringt: Anfang September hat ein Mann aus Österreich den unverschlüsselten Datenverkehr zwischen einer Leitstelle und Einsatzkräften der Feuerwehren, Rettungsdienste und Krankentransporte protokolliert. Er bekam so Einsatzorte, Patientendaten und Einzelheiten zum jeweiligen Einsatz heraus und konnte sich daraus eine Datenbank mit detaillierten Informationen anlegen.

Der Feind von innen – Mitarbeiter spionieren Daten aus

Ein Datenabgriff ohne explizite technische Sicherheitslücke fand im November 2009 in Großbritannien statt. Ein Mitarbeiter des Londoner Telekom-Tochterunternehmens T-Mobile verkaufte Kundendaten an einen Wettbewerber. Durch die Weitergabe von tausenden Namen, Adressen

Copyright © 2010 G Data Software AG

und Vertragslaufzeiten war es dem Unternehmen möglich, den Kunden kurz vor Ablauf ihrer Vertragslaufzeit bei T-Mobile, gezielt Angebote für Neukunden zuzusenden. Dieses Datenleck entstand unter anderem durch die im Unternehmen gegebene Möglichkeit, interne Daten ohne großen Aufwand zu kopieren - leichtes Spiel für unkooperative Mitarbeiter.

Auch der Finanzdienstleister AWD muss eine Lücke innerhalb der eigenen Reihen befürchten. Im Oktober 2009 tauchten über 27.000 Datensätze bei NDR Info auf. Darunter Personendaten und unter anderem auch Laufzeiten und Betragsangaben von Lebensversicherungen. AWD bestätigte die Vorwürfe und ging auf Spurensuche. Laut eines Unternehmenssprechers muss es sich in diesem Fall bei dem Datendieb um hochrangige Mitarbeiter handeln, denn lokale Berater hätten keinen Zugriff auf eine solche Art und Menge an Daten.

Ähnliche Probleme gab es auch bei der Postbank, bei der im Oktober 2009 durch Recherche der Stiftung Warentest bekannt wurde, dass freie Finanzberater Zugriff auf die Girokontendaten von Postbankkunden hatten. Der Zugriff erfolgte, obwohl die Kontoinhaber einer Weitergabe ihrer Daten nicht ausdrücklich zugestimmt hatten. So hatten die Berater unter anderem Zugriff auf die Kontostände und Kontobewegungen von Prominenten. Die Postbank erklärte gegenüber der ARD, dass der „Zugriff auf die Kontodaten technisch durch ein Zugriffs- und Berechtigungskonzept geregelt“ sei.

Herausforderung für Datenschützer: Google Street View

Ein heikles Thema im Bezug auf Datenschutz ergab sich durch die nun auch in Deutschland durchgeführten Street View-Fahrten der Google Germany GmbH. Für die im Programm Google Maps integrierte Funktion fahren Google-Mitarbeiter in Autos mit montierten Kameras über Deutschlands Straßen und nehmen Bilder der Umgebung auf. Deutsche Datenschutzbehörden und Gegner der Aktion sehen die Privatsphäre deutscher Bürger in Gefahr. Google verpflichtet sich zur Einhaltung geltender Gesetze in den für Street View abgefahrenen Ländern. Aufnahmen von Gesichtern und Nummernschildern werden unkenntlich gemacht. Zusätzlich hat jeder Nutzer die Möglichkeit, anstößiges oder bedenkliches Material zu melden, welches dann gegebenenfalls nach Prüfung entfernt wird. Nutzer sollen künftig auch die Möglichkeit bekommen, bestimmte Örtlichkeiten, die sie nicht in Street View veröffentlicht sehen möchten, zu melden.

Copyright © 2010 G Data Software AG

Ereignisse und Trends des zweiten Halbjahres 2009

Auch das zweite Halbjahr 2009 stand stark unter dem Einfluss von Angriffen auf soziale Netzwerke. Egal ob Twitter, MySpace, Facebook oder andere, die Attraktivität für Phisher und Malwareverbreiter ist ungebrochen.

Juli 2009

1. 7 Der „**Month of Twitter Bugs**“ beginnt. Aviv Raff, der schon seit 2006 an „Month of Bugs“-Projekten teilgenommen hat, möchte die User und Programmierer für Schwachstellen des Web 2.0-Mediums sensibilisieren. Sein Fokus liegt dabei aktuell auf angreifbaren Twitter Browser APIs, Tiny-URL-Diensten und präparierten Bildern mit Wurm-Schadcode.

4. 7. Amerikanische und südkoreanische Rechner am **Independence Day** unter Beschuss. **Gezielte DDoS-Angriffe** beschäftigen die Sicherheitsexperten der beiden Regierungen. Ein Botnetz aus mehreren zehntausend Zombie-PCs attackiert Regierungs- und andere Webseiten, die wirtschaftliche Relevanz haben, z. B. die New Yorker Börse oder auch südkoreanische Banken. Die Geheimdienste vermuteten Nordkorea als Auslöser der Angriffe.

8. 7. Das **Exploit-Portal Milw0rm** kündigt seine Schließung an. Sie kann nach intensiven Diskussionen abgewendet werden. Auch wenn die Gründe nicht explizit genannt werden, gehen Experten davon aus, dass die Anzahl an einzupflegenden Exploits die Kapazitäten der Betreiber übersteigt. Das Portal ist Anlaufstelle für IT-Sicherheitsforscher sowohl aus dem weißen, als auch aus dem dunklen Lager.

9. 7. **Kurios:** Eine **südafrikanische Bank** initiiert **Skimming-Gegenmaßnahmen** an Geldautomaten. Bei einem Routinecheck durch einen Techniker löst das Abwehrsystem Alarm und damit eine **Pfeffersprayattacke** aus. Drei Techniker müssen im Krankenhaus behandelt werden.

23. 7. Eine bis dato **unbekannte Sicherheitslücke** in der Komponente authplay.dll im **Adobe Acrobat** oder **Adobe Flashplayer** wird in infizierten PDF-Dateien und manipulierten Webseiten per Drive-by-Download genutzt.

August 2009

„Koobface“ wird ein Jahr alt und hat in seiner Aggressivität nichts eingebüßt.

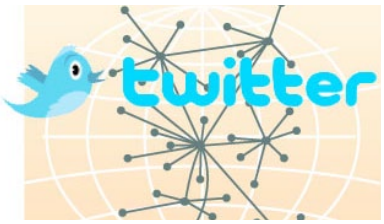
4. 8. Das **BSI** distanziert sich von einer angeblich von ihnen verschickten Mail, die Nutzer auf eine **Scareware**-Seite schickt. Hier werden unachtsame User in eine Abofalle gelockt, mit einem Zwei-Jahres-Vertrag und 192 Euro Kosten.

6. 8. Der Micro-Blogging Dienst **Twitter** ist für Stunden im **Time-out**. Sowohl die Hauptanwendung, als auch die API Clients sind betroffen. Die Ursache war wohl eine Vermischung aus **verteilten Überlastangriffen** (DDoS) und einer scheinbar gezielten Offensive gegen den

Copyright © 2010 G Data Software AG

Blogger namens „Cyxymu“ durch Extraklicks, die in Spam-Mails auf bestimmte Twitter-Seiten verwiesen.

13.8. Es wird bekannt, dass **Microsoft** eine kritische **Zero-Day-Lücke** schon seit zwei Jahren bekannt war und erst im Juli 2007 beim Patchday darauf reagiert wurde.



14.8. **Twitter** eventuell als **Botnetz-Kommunikator** missbraucht: Ein Arbor Security Researcher entdeckt verschlüsselte Twitter-Einträge eines Accounts, die möglicherweise Befehle für Botnetze enthalten.

24.8. Das Stockholmer Amtsgericht verurteilt den Internet Service Provider „**Black Internet**“ dazu, den Traffic der Webseite „**The Pirate Bay**“ zu stoppen, oder 500.000 Schwedische Kronen (rund 48.000 Euro) zu zahlen. Kurze Zeit später findet „The Pirate Bay“ einen anderen Provider.

27.8. Ein ehemaliger Mitarbeiter einer Sicherheitsfirma veröffentlicht Programmcode zum Einschleusen einer **Softwarewanze in Skype**. Die Wanze kann Gespräche unbemerkt mitschneiden und als MP3 an eine vordefinierte Adresse senden.

29.8. In **China** werden **vier Software-Piraten** zu Gefängnisstrafen und rund 1,6 Millionen US-Dollar Strafe verurteilt. Ihnen wird vorgeworfen, illegale Kopien von Windows XP und anderer Software verteilt zu haben.

September 2009

4.9. **T-Online Kunden** müssen mitunter tagelang auf ihre E-Mails warten. Einige PCs von Kunden hatten sich infiziert und arbeiteten, in ein **Botnetz** eingebunden, als Spam-Schleudern. Die Verlangsamung des E-Mail Dienstes wird beseitigt, indem die Zombie-Rechner vom Internet abgeklemmt werden.

8.9. **Kurios**: Ein findiger **Österreicher** hat den **unverschlüsselten Datenverkehr** zwischen Leitstelle und Einsatzkräften der Feuerwehren, Rettungsdiensten und Krankentransporten mit protokolliert. Er bekam so Informationen über Einsatzorte, Patientendaten und Einzelheiten zum jeweiligen Einsatz.

14.9. Besucher der **New York Times-Webseite** werden Opfer einer **Social Engineering Attacke**: Hacker haben Scareware-Werbebanner auf der Homepage geschaltet und ahnungslose Besucher zum Herunterladen von kostenpflichtiger und falscher Antivirensoftware gedrängt.

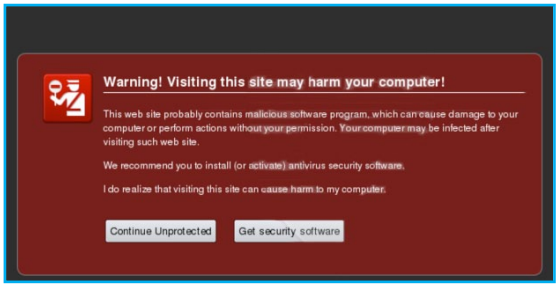
15.9. Najat M'jid Maalla, UN-Berichterstatterin, zeigt eine drastische **Zunahme von Kinderpornographie-Webseiten** auf. Sie erläutert, dass die Zahl der Seiten mit massiven Ausbeutungen sich von 2003 bis 2007 vervierfacht hat. Laut Schätzungen von UNICEF kursieren über vier Millionen solcher Webseiten.

16.9. **Kurios**: In den USA hat ein Mann seine **zwei gestohlenen Laptops** mit Hilfe eines **Remote Access**-Programms zurück bekommen. Der Mann kann den Delinquenten per RA-Zugang beim Surfen, Chatten, E-Mail Schreiben, Videochatten und Besuch von Erwachsenenseiten beobachten und die Aktionen per Videokamera filmen. Die **Polizei** hat dann leichtes Spiel.

Copyright © 2010 G Data Software AG

18.9. **Microsoft** verklagt Firmen, die sogenanntes **Malvertising** betreiben. Im wohl ersten Prozess dieser Art will Microsoft gegen die Verbreitung von unseriösen Werbebannern mit Schadcodeeinfluss vorgehen.

21.9. Mit dem **Trojanischen Pferd** „Trojan.FakeAlert.BFW" infizierte Systeme leiten den gesamten URL-Verkehr auf eine gefälschte Sicherheitswarnung. Diese Warnung imitiert die des Browsers Firefox und lockt User zur Installation der **Scareware** „Personal Antivirus".



Screenshot 1: Die gefälschte Sicherheitswarnung der Scareware „Personal Antivirus"

Oktober 2009

1.10. **Cracker** haben die **Captcha**-Sicherheitsabfrage von **Facebook** geknackt und sind in der Lage, Profile automatisiert zu erstellen. Die angelegten Profile locken Benutzer dann per Link auf ein angebliches Video und versuchen, den Benutzer zur Installation von falscher Antivirussoftware (Rogueware) zu überreden.

2.10. **Google** entfernt die Homepage der illegalen Tauschbörse „**The Pirate Bay**" und sieben weiterer Seiten, die zur BitTorrent Tracker-Webseite gehören aus ihren Suchergebnissen.

6.10. Eine Liste mit zehntausenden Usernamen und dazugehörigen Passwörtern von Microsofts Live Hotmail Accounts ist im Netz aufgetaucht. Die Daten wurden wohl durch **Phishing-Attacken** erbeutet und in der Liste zusammengefasst. Wenig später wird bekannt, dass auch Accounts von Yahoo, Gmail, Comcast und Earthlink betroffen sind.

7.10. **Kurios**: Der **FBI-Chef** Robert Mueller wird beinahe Opfer einer Bank **Phishing E-Mail**. Laut eigener Aussage sah die Mail verblüffend echt aus und er sei der Aufforderung zur „Verifizierung ihrer Daten" gefolgt, bis es bei ihm „Klick" gemacht hat. Seine Frau erteilt ihm daraufhin Onlinebanking-Verbot.

8.10. Die **FBI Operation „Phish Fry"** führt zur Anklage von 100 Personen, die im Zusammenhang mit Phishing-Attacken stehen. Das System der Phisher: Ägyptische Hacker spüren **persönliche Daten und Bankdaten** von Opfern auf, leiten diese an amerikanische „Kollegen" weiter und diese missbrauchen die Daten für illegale Geldgeschäfte.

8.10. Sechsmonatiges **De-Mail Pilotprojekt** in Berlin gestartet. Die De-Mail soll in Deutschland als verschlüsselte elektronische Versandeinheit den Austausch von rechtsgültigen Dokumenten ermöglichen.

9.10. **Zombie-Rechner**, die in das **Bahama Botnet** eingebunden sind, leiten Surfanfragen auf täuschend echt aussehende Klone um, anstatt die wahre Seite aufzurufen. Besonders betroffen sind dabei aktuell die Suchseiten von Google, Bing und Yahoo. Ziel der Aktion: Geld durch Klickbetrug verdienen.

17.10. Der Seite **netzpolitik.org** wird ein Datensatz mit persönlichen **Daten** von mehreren hunderttausend Usern des deutschen Portals **schülerVZ** zugespielt. Die Daten wurden mit Hilfe eines Datensammelprogramms (Crawler) abgegriffen.

Copyright © 2010 G Data Software AG

19.10 Ein schwedisches Gericht vertagt den **Prozess** zwischen Angehörigen der illegalen P2P Seite „**The Pirate Bay**“ und der Entertainment-Industrie auf den Sommer 2010. Zwei Richtern des Prozesses wird Befangenheit vorgeworfen. Der Prozess sollte ursprünglich am 13.11.2009 beginnen.

23.10. Die Firma Click Forensics veröffentlicht einen Bericht, aus dem hervorgeht, dass im dritten Quartal des Jahres 2009 42,6% von **betrügerischen Klicks (click fraud)** von Computern aus Botnetzen stammen - ein Anstieg von 5,7%.

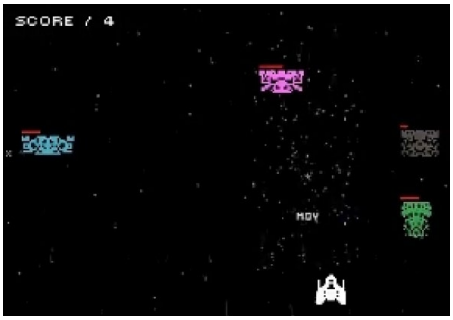
31.10. Der vor zwei Wochen verhaftete 20-jährige, der die Nutzerdaten aus der deutschsprachigen Online Community **schülerVZ** ausgelesen hat, begeht in seiner Zelle **Selbstmord**.

November 2009

1.11. Der **Conficker Wurm** hat diese Woche sein etwa **siebenmillionstes Opfer** infiziert. Seine Kombination aus Verbreitungs-, Tarn- und Schutzmechanismen macht ihn zum erfolgreichsten Schädling des Jahres.

3.11. In Manchester wird ein 20-jähriges Pärchen verhaftet. Die beiden sind die mutmaßlichen **Verbreiter** der **Spyware Zbot**. Sie stiehlt Onlinebanking-Informationen, Kreditkartendaten und Passwörter. Es ist der erste Arrest dieser Art in Europa.

5.11. **Kurios:** Macintosh-Computer durch einen „Schädling“ angreifbar. Der als Nachahmung des Spiels Space Invaders entwickelte Schädling löscht eine Datei aus dem Ordner „Dokumente“, sobald man im Spiel „**Lose/Lose**“ ein Alien abschießt. Der Entwickler weist die Spieler jedoch vor dem Spiel ausdrücklich darauf hin.



Screenshot 2: Spielszene aus „Lose/Lose“

10.11. Die Autoren von „**Koobface”** schaffen es zum ersten Mal, eine Variante zu programmieren, die sich im sozialen Netzwerk „Facebook” wie ein Mensch verhält: Der Schädling registriert Accounts, legt sich ein normal anmutendes Profil an, verschickt Freundschaftseinladungen und postet sogar Nachrichten auf den Pinnwänden anderer User.

17.11. Die britische Telekomtochter **T-Mobile** ist in einen Datenskandal verwickelt. Mitarbeiter haben Daten tausender Kunden an Zwischenhändler verkauft.

20.11. **Microsoft** unter Zugzwang. Cracker posten einen **Zero-Day Exploit** für die Webbrowser Internet Explorer 5, 6 und 7. Zwar ist der Code nicht in allen Fällen und auf allen Rechnern schädlich, jedoch arbeiten Cracker mit Hochdruck an einer Optimierung des Codes.

24.11. Schlag gegen die **Onlinekriminalität**. Über 200 Polizisten aus Deutschland und Österreich führen **Razzien** in 50 Wohnungen durch und nehmen vier Personen vorläufig fest. Die Durchsuchten stehen im Verdacht, mit gestohlenen Kreditkartendaten, Zugangsdaten, Kontodaten und Schadsoftware Tausch und Handel betrieben zu haben. Die „Elite Crew“ soll außerdem ein Botnetz mit mehr als 100.000 Computern unter ihrer Kontrolle haben.

Copyright © 2010 G Data Software AG

24.11. In den USA wird der selbsternannte „**Godfather of Spam**“, der 64-jährige Alan Ralsky, zu 51 Monaten Haft, fünf Jahren Bewährungsstrafe und 250.000 US-Dollar Geldstrafe **verurteilt**. Er hatte mit seinen Komplizen, die ebenfalls empfindliche Strafen hinnehmen müssen, E-Mail Spam in großem Stil vertrieben.

25.11. **Kurios**: Südkorea limitiert den SMS-Versand. **Südkoreas** Kampf gegen **Spam** hat Auswirkung auf den Mobilfunksektor. Pro Handy können nun nur noch 500 **SMS** am Tag versendet werden. Obwohl es in der Republik empfindliche Strafen auf die Verbreitung von unerwünschten Nachrichten gibt, ist die Flut von Spam extrem hoch. Statistisch gesehen besaßen im Oktober 98% der südkoreanischen Bevölkerung ein Mobiltelefon, was 47,7 Millionen Geräten entspricht.

27.11. Eine neue **Spamwelle** trifft besonders **World of Warcraft-Spieler**. Eine E-Mail mit Fotos von jungen, asiatischen Frauen lockt Empfänger zum Anklicken eines angehängten Videos, das sich als Trojanisches Pferd entpuppt und gezielt WoW-Accountdaten ausspioniert.

29.11. **Kurios**: Das englischsprachige „**Top Word 2009**“ ist „Twitter“, so die Betreiber der Webseite Global Language Monitor. „Twitter“ verweist die Wörter „Obama“, „H1N1“, „Stimulus“ und „Vampir“ auf die Plätze zwei bis fünf. Die Wörter der Dekade waren „Erderwärmung“, „9/11“ und „Obama“.

Dezember 2009

4.12. Die User der **virtuellen Hotelwelt „Habbo”** sehen sich einer länderübergreifenden Welle von **Phishing-Attacken** gegenüber. Onlinekriminelle versuchen mit Phishing-Seiten an Zugangsdaten und Kreditkartendaten der Spieler zu gelangen. Auch betrügerische Blog-Einträge häufen sich. Besonders brisant dabei: Das Onlinespiel richtet sich hauptsächlich an Kinder und Jugendliche.

Screenshot 3: User des virtuellen Habbo-Hotels werden von Betrügern in die Falle gelockt

6.12. Das deutsche **Kinderportal** haefft.de ist laut **Chaos Computer Club** völlig ungesichert gegenüber Datendieben. Der CCC berichtet, man hätte sich ohne Kenntnis eines Passworts und ganz ohne technische Manipulation als Teil der Community bewegen und so an Daten kommen können. Die Seite wird vom Netz genommen.

8.12. Dienstleistung „WLAN-Verschlüsselung knacken”: Eine US-amerikanische Firma bietet an, mit 400 Cloud-CPUs und **Wörterbuchangriff** die **WPA-Verschlüsselung** eines Funknetzes in 20 Minuten auszuhebeln. Kostenpunkt: 34 US-Dollar.

15.12. In den Programmen Adobe Reader und Adobe Acrobat 9.2 und älter wird eine **bis dahin unentdeckte Schwachstelle** in der Funktion „Doc.media.newPlayer“ bekannt. Diese Lücke ermöglicht dem Angreifer im schlimmsten Fall eine Übernahme des befallenen Systems. Adobe kündigt den Patch für den 12. Januar 2010 an.

Copyright © 2010 G Data Software AG

16.12. Der **Raubkopierer** des Films „X-Men Origins: Wolverine“ wird nach neunmonatiger Fahndung in New York verhaftet. Der 47-jährige hatte den unfertigen Film vor Kinostart in Filesharing-Netzwerken verbreitet, er sei jedoch nicht die eigentliche Quelle. Es gibt noch keine Informationen darüber, wer den Film ursprünglich entwendete.

17.12. Ein Angriff auf **Twitter** legt die Homepage durch **manipulierte DNS-Einträge** lahm und zeigt eine Seite der „Iranian Cyber Army“. Die Verantwortlichen von Twitter vermuten hinter dem Vorfall eine Attacke gegen Twitter als Anbieter und keinen Angriff auf User.
Es werden keine weiteren Schäden bekannt.

Copyright © 2010 G Data Software AG