



G Data

Malware-Report

Halbjahresbericht Januar-Juni 2010

Ralf Benzmüller & Sabrina Berkenkopf
G Data SecurityLabs

Geschützt. Geschützter. G Data.

Inhalt

Auf einen Blick	3
Malware: Zahlen und Daten	4
Malware-Füllhorn.....	4
Malware-Kategorien	5
Malware-Familien.....	6
Plattformen: .Net legt zu	8
Fazit und Trends 2010.....	9
Prognosen.....	9
Ereignisse und Trends des ersten Halbjahrs 2010.....	10
Januar 2010.....	10
Februar 2010	11
März 2010	13
April 2010	15
Mai 2010.....	17
Juni 2010	18

Auf einen Blick

- Mit 1.017.208 neuen Computerschädlingen wird auch im ersten Halbjahr 2010 ein neuer Rekord erreicht.
- Gegenüber dem vorhergehenden Halbjahr stieg die Zahl um 10 %, gegenüber dem Vorjahreszeitraum sogar um 50 %.
- Wir erwarten, dass im gesamten Jahr 2010 mehr als 2 Mio. neue Computerschädlinge erkannt werden.
- Mit 51 % Zuwachs ist Spyware die Malware-Kategorie, deren Anzahl am meisten gestiegen ist. Das gilt insbesondere für Keylogger und Banking-Trojaner.
- Die Anzahl neuer Adware ist um 40 % gesunken.
- Die beiden produktivsten Malware-Familien Genome und Hupigon erzeugten mehr Varianten als alle Schädlinge des Jahres 2007 zusammen.
- Schädlinge für Windows dominieren mit einem Anteil von 99,4 % weiterhin das Geschehen. Der Anteil von .NET-Schädlingen ist aber auf das 3,4fache angestiegen und macht nun 0,9 % aus. Auch Malware-Autoren nutzen die Vorzüge von .NET.
- Schadcode für Unix-Derivate und Java nimmt ebenfalls deutlich zu.

Trends

- Daten stehlen ist und bleibt eine Kernfunktion von Malware.
- Adware wird von Virenschutz-Imitaten (FakeAV) und Erpresser-Software abgelöst.
- Immer mehr Online-Dienste und Funktionen werden für schädliche Zwecke missbraucht.

Ereignisse

- Soziale Netzwerke schaffen es mit vielen Neuerungen aber auch einigen Datenpannen in die Ereignislisten – vorneweg: Twitter und Branchenprimus Facebook.
- Das Botnetz Mariposa wird lahm gelegt. Die spanische Polizei verhaftet die drei Betreiber.
- Auch das Waledac-Botnetz, eines der zehn größten in den USA, wird von Ermittlern hart getroffen und 277 .com-Domains werden vom Netz genommen.
- Die Deutsche Emissionshandelsstelle wird Opfer einer Phishing-Attacke, bei der die Täter mit Rechten im Wert von rund drei Millionen Euro handelten.
- PDF-Dateien geraten immer mehr in den Fokus der Malware-Autoren und damit häufen sich auch Berichte über Schwachstellen in PDF-Readern.

Malware: Zahlen und Daten

Malware-Füllhorn

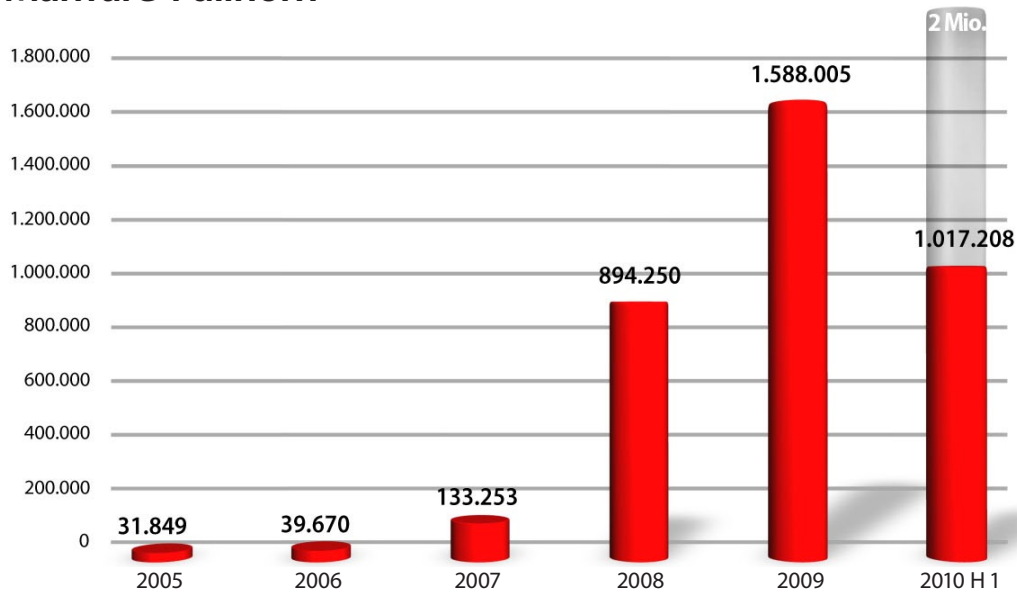


Diagramm 1: Anzahl neuer Malware pro Jahr seit 2005 und 1. Halbjahr 2010

Auch im ersten Halbjahr 2010 wurde mit 1.017.208 neuen Computerschädlingen¹ der Rekord aus dem letzten Halbjahr um ca. 10 % übertroffen. Gegenüber dem Vorjahreszeitraum stieg die Zahl um mehr als 50 %. Bereits im ersten Halbjahr 2010 sind mehr neue Schädlinge aufgetaucht als im gesamten Jahr 2008. Bis zum Ende des Jahres wird die Anzahl neuer Schädlinge voraussichtlich die zwei Millionen-Marke knacken.

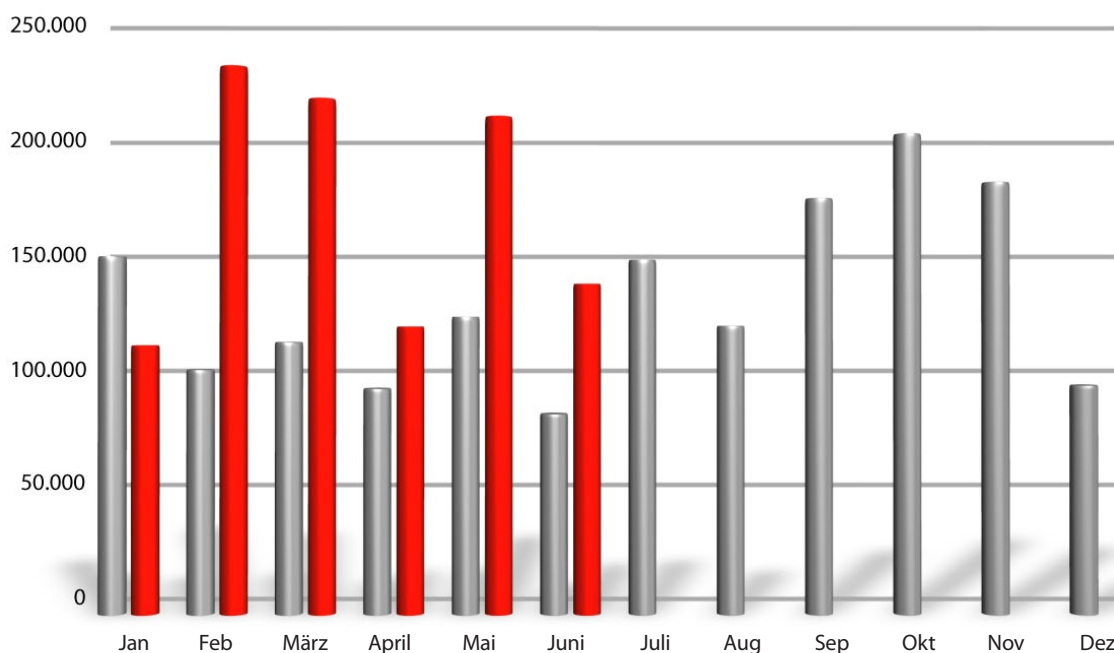


Diagramm 2: Anzahl neuer Malware pro Monat für 2009 und 2010

¹ Die Zahlen in diesem Report basieren auf der Erkennung von Malware anhand von Virensignaturen. Sie basieren auf Ähnlichkeiten im Code von Schaddateien. Viele Schadcodes ähneln sich und werden dann in Familien zusammengefasst, in denen kleinere Abweichungen als Variationen erfasst werden. Grundlegend unterschiedliche Dateien begründen eigene Familien. Die Zählung basiert auf neuen Signaturvarianten, die im ersten Halbjahr 2010 erstellt wurden.

Malware-Kategorien

Der Anteil von **Spyware** ist gegenüber dem 2. Halbjahr 2009 um 3,4 % angewachsen – Keine andere Kategorie konnte ihren Anteil so stark steigern. Damit ist der starke Rückgang, der im letzten G Data Malware-Report verzeichnet werden musste, gestoppt, auch wenn der Anteil gegenüber dem Vorjahreszeitraum nicht erreicht werden konnte. In absoluten Zahlen bedeutet das einen Zuwachs von 51 %. Besonders hohe Zuwachsraten in der Kategorie **Spyware** verzeichnen Keylogger² und Banking-Trojaner³.

Fortgesetzt hat sich hingegen der verstärkte Einsatz von **Rootkits**. Ihre Anzahl stieg im letzten Halbjahr erneut auf das 2,6fache. Würmer, die Shooting-Stars des letzten G Data Malware-Reports, konnten hingegen ihren Anstieg nicht fortsetzen, halten allerdings das Niveau.

Der Anteil an **Trojanischen Pferden** behauptet sich auf dem hohen Niveau des vorherigen Halbjahrs. In dieser Gruppe hat sich die Zahl der Ransomware (Erpressersoftware und manche FakeAV) gegenüber dem Vorjahreszeitraum etwa verzehnfacht!

Der Anteil an neuen Backdoors ist um 2,9 % gesunken und sie setzen damit den Abwärtstrend aus dem ersten Halbjahr 2009 fort. Auch die Anzahl der **Tools** nimmt um ca. ein Drittel ab, ihr Anteil sinkt auf 1,0 %. Am deutlichsten hat sich die Anzahl von **Adware** verringert. Gegenüber dem Vorjahr (H1 2009 zu H1 2010) sinkt deren Anzahl um 40 % und der Anteil sinkt von 5,3 % auf 2,1 %.

Kategorie	# 2010 H1	Anteil	# 2009 H2	Anteil	Diff. 2010 H1 2009 H2	# 2009 H1	Anteil	Diff. 2010 H1 2009 H1
Trojanische Pferde	433.367	42,6 %	393.421	42,6 %	+10 %	221.610	33,6 %	+96 %
Downloader/Dropper	206.298	20,3 %	187.958	20,3 %	+10 %	147.942	22,1 %	+39 %
Spyware	130.175	12,8 %	86.410	9,4 %	+51 %	97.011	14,6 %	+34 %
Backdoors	122.469	12,0 %	137.484	14,9 %	-11 %	104.224	15,7 %	+18 %
Würmer	53.609	5,3 %	51.965	5,6 %	+3 %	26.542	4,0 %	+102 %
Rootkits	31.160	3,1 %	11.720	1,3 %	+166 %	12.229	1,9 %	+155 %
Adware	21.035	2,1 %	30.572	3,3 %	-31 %	34.813	5,3 %	-40 %
Tools	9.849	1,0 %	14.516	1,6 %	-32 %	11.413	1,6 %	-14 %
Exploits	2.495	0,2 %	3.412	0,4 %	-27 %	2.279	0,3 %	+9 %
Sonstige	6.751	0,7 %	5.543	0,5 %	+22 %	4.593	0,7 %	+47 %
Gesamt	1.017.208	100,0 %	924.053	100,0 %	+10 %	663.952	100,0 %	+53 %

Tabelle 1: Anzahl und Anteil neuer Malwarekategorien 2009 und 2010 sowie deren Veränderung

² 2,5fach im Vergleich zum zweiten Halbjahr 2009

³ 2,2fach im Vergleich zum ersten Halbjahr 2009

Malware-Familien

Nach ihren Funktionen und Eigenschaften lassen sich Computerschädlinge in Familien zusammenfassen. Für einige dieser Familien werden ständig neue Varianten produziert. Während die Anzahl neuer Schädlinge in der Vergangenheit konstant angestiegen ist, war die Anzahl der Familien rückläufig. Dieser Trend wurde im letzten Halbjahr gestoppt. Im ersten Halbjahr 2010 waren 2.262 Malware-Familien aktiv. Das liegt ca. 3 % über dem Wert des letzten Halbjahrs und etwa ein Siebtel über dem des ersten Halbjahrs 2009.

	# 2010 H1	Virenfamilie	# 2009 H2	Virenfamilie	# 2009 H1	Virenfamilie
1	116.469	Genome	67.249	Genome	34.829	Monder
2	32.830	Hupigon	38.854	PcClient	26.879	Hupigon
3	30.055	Buzus	37.026	Hupigon	18.576	Genome
4	25.071	Refroso	35.115	Scar	16.719	Buzus
5	24.961	Scar	24.164	Buzus	16.675	OnlineGames
6	21.675	Lipler	20.581	Lipler	13.889	Fraudload
7	19.385	OnlineGames	19.848	Magania	13.104	Bifrose
8	17.542	Palevo	18.645	Refroso	11.106	Inject
9	16.543	Startpage	16.225	Basun	10.312	Magania
10	16.517	Magania	16.271	Sasfis	10.322	Poison

Tabelle 2: Top 10 der aktivsten Virenfamilien. Anzahl neuer Varianten 2009 und 2010

Tabelle 2 zeigt die Familien, die in den letzten eineinhalb Jahren am produktivsten waren. Spitzenreiter ist weiterhin **Genome**, seine Anzahl ist um 73 % angestiegen (H2 2009 zu H1 2010). Im Durchschnitt bringt es **Genome** damit täglich auf 640 neue Varianten. Die Anzahl der Varianten dieser Familie aus dem ersten Halbjahr 2010 liegt nur knapp unter der Zahl aller Schädlinge von 2007 (vgl. Tabelle 1). Der Zweitplatzierte aus dem letzten Halbjahr **PcClient** konnte sich nicht in den Top 10 behaupten. Auf den weiteren Rängen tummeln sich alte Bekannte (vgl. Kurzbeschreibung). **OnlineGames** schaffte es erneut in die Top 10. Die Familien des Wurms **Palevo** und des Browser Hijackers **Startpage** schafften es erstmals unter die ersten zehn.

Genome

Die Trojanischen Pferde der „Genome“-Familie vereinen Funktionalitäten wie Downloader, Keylogger, Dateiverschlüsselung.

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.

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.

Refroso

Dieses Trojanische Pferd tauchte Ende Juni 2009 erstmals auf. Es hat Backdoor-Funktionen und kann andere Rechner im Netzwerk attackieren.

Scar

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

Lipler

Bei „Lipler“ handelt es sich um eine Familie von Downloadern, die weitere Malware von einer Webseite nachlädt. Außerdem verändert er die Startseite des Browsers.

OnlineGames

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.

Palevo

Der Wurm „Palevo“ verbreitet sich über Wechseldatenträger (autorun.inf), kopiert sich unter verlockenden Namen in Freigaben von Peer-to-Peer-Tauschbörsenprogrammen wie Bearshare, Kazaa, Shareaza etc. Er verschickt auch per Instant Messages (vorwiegend MSN) Links auf schädliche Webseiten. Er injiziert Backdoor-Funktionen in den Explorer und sucht auf bestimmten Servern nach Befehlen.

Startpage

Diese Malware-Familie verändert die Startseite und häufig auch viele weitere Einstellungen des Browsers. Sie stellen die prominenteste Variante der Browser Hijacker dar.

Magania

Trojanische Pferde der aus China stammenden 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.

Plattformen: .Net legt zu

Nach wie vor wird das Gros der Malware für Windows geschrieben. Der Anteil der ausführbaren Dateien unter den Windows-Schädlingen (Win32) ist auf 98,5 % gesunken, obwohl die Anzahl um 9 % gestiegen ist. Damit setzt sich ein Trend fort, über den wir im letzten Malware-Report berichtet haben. Aber erneut wird die geringere Anzahl an Windows-Malware durch eine auf das 3,4fache gestiegene Anzahl von Malware für die .NET-Plattform ausgeglichen. Auch Schadcode-Autoren nutzen die Vorzüge von .NET – insbesondere weil es bei neueren Betriebssystemen zum Lieferumfang gehört. Insgesamt liegt der Anteil an Windows-Schadprogrammen also bei ca. 99,4 %.

Von den verbleibenden 0,6 % belegen Schadcodes aus Webseiten (z.B. JavaScript, PHP, HTML, ASP etc.) etwa zwei Drittel (also 0,4 %). Hier ist ein leichter Rückgang bei der Anzahl neuer Varianten zu verzeichnen. Die vorhandenen Varianten sind allerdings sehr verbreitet.

	Plattform	# 2010 H1	Anteil	# 2009 H2	Anteil	Diff. 2010 H1 2009 H2	# 2009 H1	Anteil	Diff. 2010 H1 2009 H1
1	Win32	1.001.902	98,5 %	915.197	99,0 %	+9 %	659.009	99,3 %	+52 %
2	MSIL ⁴	9.383	0,9 %	2.732	0,3 %	+243 %	365	0,1 %	+2471 %
3	WebScripts	3.942	0,4 %	4.371	0,5 %	-10 %	3.301	0,5 %	+19 %
4	Scripts ⁵	922	0,1 %	1.124	0,1 %	-18 %	924	0,1 %	-0 %
5	NSIS ⁶	260	0,0 %	229	0,0 %	+14 %	48	0,0 %	+442 %
6	*ix ⁷	226	0,0 %	37	0,0 %	+511 %	66	0,0 %	+242 %
7	Java	225	0,0 %	31	0,0 %	+626 %	3	0,0 %	+7400 %
8	Mobile	212	0,0 %	120	0,0 %	+77 %	106	0,0 %	+100 %

Tabelle 3: Top 5 Plattformen 2009 und 2010.

Computerschädlinge für andere Plattformen gehen in dieser Masse unter. Erwähnenswert ist dennoch, dass sich die Anzahl der Malware für Unix-basierte Betriebssysteme mehr als versechsfacht hat und Malware für Java auf ca. das Siebenfache angestiegen ist (jeweils gegenüber dem 2. Halbjahr 2009).

4 MSIL ist das Zwischenformat, in dem .NET-Anwendungen in ihrer plattform- und programmiersprachenunabhängigen Form repräsentiert werden.
 5 „Scripts“ sind Batch- oder Shell-Skripte oder Programme, die in den Skriptsprachen VBS, Perl, Python oder Ruby geschrieben wurden
 6 NSIS ist die Installationsplattform, die u. a. dazu genutzt wird den Mediaplayer Winamp zu installieren.
 7 *ix bezeichnet alle Unix-Derivate, wie z.B. Linux, FreeBSD, Solaris etc.

Fazit und Trends 2010

Die Malware-Flut ebbt nicht ab. In einer florierenden Untergrund-Ökonomie haben Backdoors, Rootkits, Spyware und Konsorten einen festen Platz. Besonderes Augenmerk richten die Autoren von Schadprogrammen auf Spyware in den Bereichen Keylogging, Online-Banking und Online-Games. Daten stehlen ist und bleibt eine der Kernfunktionen von Malware. Deren Vermarktung ist in Untergrundforen fest etabliert.

Die Anzahl neuer Adware-Varianten sinkt deutlich. Möglicherweise hat das damit zu tun, dass mit aggressiveren „Werbemethoden“, Imitaten von Schutzprogrammen (Fake AV) oder Entschlüsselungs- und Schutz-Software (Ransomware), mehr Geld verdient werden kann.

Windows bleibt das wichtigste Angriffsziel. Aber die Malware-Autoren schauen sich verstärkt nach Alternativen um.

Prognosen

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

Ereignisse des ersten Halbjahrs 2010

Januar 2010

- 04.01. **Kurios:** Die Webpräsenz der spanischen **EU Ratspräsidentschaft** präsentiert sich im wahren Sinn des Wortes mit neuem Gesicht: Ein **Hacker** hat mit Hilfe eines Cross-Site-Scripting-Angriffs das Konterfei des spanischen Premierministers Zapatero durch ein Bild des fiktiven Comedy-Charakters Mr. Bean ersetzt.
- 06.01. **Kurios:** Ein 26-jähriger Brite setzt eine Wutnachricht per **Twitter** ab und wird eine Woche später dafür **verhaftet!** „You’ve got a week and a bit to get your s*** together, otherwise I’m blowing the airport sky high“, war seine „Drohung“ an den britischen Robin Hood Airport, weil er wegen des schlechten Wetters fürchtete, dass sein für den 15.1. geplanter Flug gestrichen werden könnte. Für diesen Tweet wurde er fast sieben Stunden verhört, verlor seinen Job und bekam lebenslanges Hausverbot im Flughafen Doncaster. Die Internetgemeinde tauft Paul Chambers liebevoll einen „**Twidiot**“. Chambers selbst kann den Rummel nicht nachvollziehen.
- 12.01. Die „**Iranian Cyber Army**“ kapert die größte chinesische Suchseite **Baidu** mit Hilfe von geänderten DNS-Einträgen und hinterlässt ein Bekennerbanner. Im Dezember 2009 hatten sie, ebenfalls durch geänderte DNS Einträge, den Micro-Blogging Dienst Twitter für einige Stunden lahm gelegt.
- 14.01. Die Betreiber der Internetseite **opendownload.de** verlieren vor dem Landgericht Mannheim in zweiter Instanz, ohne Chance auf Revision. Ein Nutzer hatte Anfang 2008 eine **Rechnung** von opendownload.de zugeschickt bekommen, obwohl eine Kostenpflicht „nicht so leicht erkennbar und gut wahrnehmbar ist, dass der Durchschnittsverbraucher über die entstehenden Kosten ohne weiteres informiert wird“, so das **Landgericht Mannheim** in seiner Entscheidung. Der Kunde verweigerte durch seinen Anwalt die Zahlung und klagte seinerseits die Anwaltskosten ein. Die Verbraucherzentrale Rheinland-Pfalz hatte schon Ende 2008 über die fragwürdigen Methoden der Seite berichtet.
- 14.01. Ein ehemaliger Administrator der **Untergrundwebseite DarkMarket** wurde zu zehn Jahren Haft verurteilt. Der 33jährige Mann aus London, Renukanth Subramaniam, hatte unweisend Seite an Seite mit einem verdeckt arbeitenden **FBI** Agenten die Webseite betreut. Die amerikanische Bundespolizei hatte die Seite erstellt und mit ihrer Hilfe Ermittlungen in den Kreisen der Cyberkriminellen durchgeführt.
- 19.01. Im Blog der Webseite **netzpolitik.org** wird veröffentlicht, dass der Firma Ruf-Jugendreisen durch einen **Cyberangriff** Daten gestohlen wurden. Die Täter gelangten an Daten von hauptsächlich jugendlichen Community-Mitgliedern des Reiseveranstalters. Die Firma Ruf habe laut netzpolitik.org schon vor drei Jahren Hinweise auf **Sicherheitslücken** erhalten, diese aber anscheinend ignoriert, heißt es am 21.1.
- 21.01. **Microsoft** veröffentlicht außerhalb des normalen Zyklus einen **Sicherheitspatch**. Der Notfall-Patch wurde zwingend notwendig, da der **Exploit**-Code, der im Dezember 2009 die

Angriffe auf Google und andere Firmen ermöglichte, Anfang der Woche im Internet veröffentlicht wurde. Der Patch behebt insgesamt acht Sicherheitslücken.

25.01. Die **Cyber-Angriffe auf Google** und weitere Firmen, die Anfang Januar heftige Wellen geschlagen hatten, wurden wohl unter anderem erst durch die Nutzung **sozialer Netzwerke** möglich. Experten haben zurückverfolgt, dass die Angreifer Personen in Schlüsselpositionen ausfindig gemacht, sie per Web 2.0 ausspioniert und dann Accounts von Freunden der Opfer kompromittiert haben. Als Freund getarnt, verschickten sie dann Nachrichten mit Links zu infizierten Webseiten und gelangten so in die Firmennetzwerke. Der Konzern erwägt den Ausstieg aus **Chinas** Wirtschaft und die Schließung von google.cn.



Illustration: G Data 2009

29.01. Die **Deutsche Emissionshandelsstelle** (DEHSt) äußert sich zu gestern erfolgten **Phishing-Angriffen**: Betrüger gaben ihre Betrugs-Mails als Mails der DEHSt aus und brachten die Empfänger dazu, sich auf einer gefälschten Webseite einzuloggen – ironischerweise, um sich vor angeblichen Hackerangriffen zu schützen. Die Täter übertrugen mit den gestohlenen Zugangsdaten Emissionsrechte, vor allem nach Dänemark und Großbritannien und erbeuteten vermutlich bis zu drei Millionen Euro. Man sieht: Gezielte Phishing-Angriffe können sehr lukrativ sein.

Februar 2010

02.02. **Twitter-Passwörter** zurückgesetzt: Verantwortliche beim Mikroblogging-Dienst Twitter haben Angriffe auf ihre User registriert, die mutmaßlich mit Hilfe von Torrent-Seiten durchgeführt worden sind – es handelt sich hauptsächlich um User, die **gleiche Anmeldedaten** auf mehreren Plattformen benutzt hatten und dadurch angreifbar wurden. Passwörter sollten für jeden Account unterschiedlich sein. Einfache Variationen zu einem Basispasswort reichen oft schon aus.

03.02. Die Webseiten populärer deutscher **Online-Newsportale** sind Opfer von so genanntem **Malvertising** geworden. Golem.de, Handelsblatt.com und auch Zeit.de lieferten zeitweise durch infizierte Werbebanner Schadcode an die Besucher ihrer Webseite aus. Die Gefahr einer Infektion ist nicht mehr auf die düsteren Seiten des Internets beschränkt. Ein zuverlässiger Virenschutz muss die Inhalte von Webseiten auf Schadcode prüfen.

03.02. Edwin Andrew Pena hat sich im Bezirksgericht von New Jersey für schuldig erklärt, zwischen 2004 und 2006 rund 1.000.000 US\$ mit dem **illegalen Verkauf von Voice over IP-Minuten** verdient zu haben. Pena schleuste die Datenpakete über Server von Telekommunikations-Dienstleistern, die ihre Server nur durch die voreingestellten **Standardpasswörter** „sicherten“.

- 09.02. Fünf Tage nach der Nachricht über zwei infizierte **Add-ons** muss **Mozilla** eingestehen, dass eins der beiden Zusatzprogramme zu Unrecht aussortiert wurde. Ein nachträglicher Scan hat das angeblich infizierte Tool als einen **False Positive** erkannt.
- 09.02. Ein Entfernungstool gegen ein Trojanisches Pferd bringt ein neues auf den Rechner: „**Kill Zeus**“ ist der Name des Programms aus dem „Spy Eye Toolkit“, dass zwar den „Zeus Trojaner“ von einem Rechner entfernt, aber selbst bössartige Absichten hat und seinerseits Nutzerdaten und Passwörter ausliest. Das **Zeus-Toolkit** kursiert seit Ende 2009 in Untergrundforen und wird für rund 500 US\$ gehandelt.
- 09.02. Eine **niederländische Scareware** taucht im Netz auf. Auch wenn die Benutzeroberfläche voll mit orthographischen Fehlern ist, wird die Existenz einer nicht-englischen Version als unmissverständliche Ausweitung auf Länder gesehen, die nicht englischsprachig sind. Insgesamt unterstützt diese Scareware **19 Sprachen**.
- 10.02. Die **australische Regierung** wird von gezielten **DDoS-Attacken** der Aktivistengruppe „Anonymous“ lahmgelegt. Die Angriffe werden als politisch motivierter Hactivismus bezeichnet und sowohl von Regierungsseite als auch Zensurgegnern stark verurteilt. Grund für die Aufregung: Australien plant die **Zensur** von ausgewählten pornografischen Onlineinhalten, wobei Zensurgegner eine unangemessene Filterung fürchten.

17.02. **Kurios:** Eine Gruppe junger **Niederländer** veröffentlicht die Seite **PleaseRobMe.com**, um die Gefahr von unbedachten Abwesenheitsnachrichten in sozialen Netzwerken ins Bewusstsein zu rufen. User sollten bedenken, dass ihre Tweets und Posts über ihren **Aufenthaltort** für alle verfügbar sind und meist nicht nur für Freunde. So wissen Diebe, wann man definitiv nicht zu Hause ist und nutzen unter Umständen die Gelegenheit. Gerüchten zufolge sollen Versicherungen einen Anstieg der Versicherungsprämie erwägen, wenn Klienten nachweislich Dienste zur **Geolokalisierung** nutzen.



Screenshot 1: Quelle: pleaserobme.com

17.02. **Microsoft** erläutert, dass das **Rootkit Alureon** Schuld an den **Bluescreen**-Abstürzen von vielen Windows XP- und einigen Windows 7-Rechnern ist. Die Bluescreens of Death (BSoD) häuften sich nach dem Systemupdate MS10-015 von letzter Woche. Betroffen sind Maschinen, die vor dem Update mit Alureon infiziert waren.

23.02. **Microsoft** gibt bekannt, dass es einen harten und bislang einzigartigen Schlag gegen eines der zehn größten Botnetze der USA, „**Waledac**“, ausgeführt habe. Es setze die richterliche Erlaubnis um, 277 .com Internetdomains vom Netz zu nehmen, bei denen ein Zusammenhang mit dem „Waledac“ Botnetz angenommen wird. So sollen die infizierten **Bot-Rechner** den Kontakt zu den steuernden Command&Control-Servern verlieren.



Illustration: G Data 2009

Das „Waledac“-Botnetz soll schätzungsweise mehr als **1,5 Milliarden Spam-E-Mails** pro Tag versendet haben.

März 2010

- 01.03. Zu den Vorfällen der so genannten „**Operation Aurora**“ gegen Google und wohl mehr als hundert weitere Firmen wird bekannt, dass die Angriffe möglicherweise auch durch **infi-zierte PDF-Dateien** getätigt wurden. Auf einigen Rechnern, die durch die Forensik untersucht wurden, fanden sich schädliche PDF-Dokumente, die durchaus im Zusammenhang mit dem Angriff stehen könnten. Die Dateien weisen wohl Ähnlichkeiten in Zeit, Herkunft und Art zu den bisher entdeckten Spuren auf. In diesem Zusammenhang gibt auch der Chiphersteller **Intel** in seinem Finanzbericht bekannt, dass man im Januar ebenfalls von einem „**ausgeklügelten Sicherheitsvorfall**“ betroffen war, jedoch gibt das Unternehmen keine Auskunft über das Ausmaß oder die Auswirkungen.
- 03.03. Die spanischen Behörden geben bekannt, dass sie **drei mutmaßliche Betreiber** des Botnetzes „**Mariposa**“ (spanisch; deutsch = Schmetterling) festgenommen haben. Die spanischen Männer im Alter zwischen 25 und 31 Jahren sollen mit Hilfe des Botnetzes vor allem Online-Banking- und Kreditkartendaten gestohlen haben. Schätzungen beziffern das Ausmaß des Netzes auf **mehr als 13 Millionen Computer** in 190 Ländern.
- 06.03. Eine große Anzahl von **Twitter-Accounts** wurde **gehackt** und zwitscherten Spam zu einer angeblichen Diät aus. „Check out this diet I tried, it works!“ und „I lost 20 lbs in 2 weeks“ waren die Lockrufe. Noch unbestätigt, aber denkbar, ist die Kompromittierung der Accounts durch **Brute Force-Angriffe** (Wörterbuchattacken) auf Twitter-Schnittstellen (APIs).
- 07.03. Eine Umfrage von GlobeScan für BBC World Service ergibt, dass fast **80 % der Bevölkerung** den Zugang zum **Internet als Grundrecht** einschätzen. Was in Ländern wie Finnland und Estland schon per Gesetz geregelt ist, wünscht sich die Mehrheit der rund 28.000 Befragten aus 26 Ländern, wobei 14.306 Befragte bereits selbst Internetnutzer sind.
- 09.03. **Twitter** startet eine neue Sicherheitsmaßnahme in Bezug auf gesendete Links. Alle Links, die zu Twitter geschickt werden, werden vor der Aussendung auf mögliche Schadwirkung (Phishing und andere Attacken) **geprüft**. So soll eine Verbreitung von schädlichen Verlinkungen über den Twitter-Service entdeckt, abgefangen und verhindert werden.
- 10.03. Nutzer der Browser **Internet Explorer 6 und 7** stehen im Fadenkreuz der Hacker. Microsoft veröffentlicht eine Sicherheitswarnung zu einem **0-Day Exploit**. Angreifer können unter bestimmten Umständen schädliche Befehle auf den angegriffenen PCs ausführen. Gerade der Internet Explorer 7 ist noch immer weit verbreitet und so vermuten Experten nach der Veröffentlichung des Exploit-Codes eine massenhafte Ausnutzung der Sicherheitslücke.
- 11.03. Die Anzahl der Steuerungsserver (Command&Control Server) des **Zeus Botnetzes** hat sich wieder erholt. Die schweizerische Initiative Zeus Tracker verzeichnete innerhalb der letzten zwei Tage ein massives Minus der C&C Serverzahlen (von 249 auf 104) und führt das auf die zeitweise Abschaltung des Upstream Providers Troyak-as zurück. Die **Zahl der Server** hat sich gegenüber heute wieder auf 191 erhöht.

- 12.03. Der offizielle Jahresbericht des **Internet Crime Complaint Centers** (kurz IC3) verzeichnet einen Anstieg von **Beschwerdemeldungen**. 2009 waren es 336.655 Vorfälle, was einen Anstieg von 22,3 % zu 2008 bedeutet. Der Großteil der Anzeigen wurde wegen Internetbetrugs in Verbindung mit finanziellem Schaden gemacht, wobei sich der monetäre Verlust hier auf **559,7 Millionen US\$** beläuft. Das IC3 ist ein Zusammenschluss aus FBI und dem National White Collar Crime Center und ist die zentrale Beschwerdestelle für Internetkriminalität in den Vereinigten Staaten.
- 16.03. Zwei **Gymnasiasten** aus dem niederländischen Heeswijk-Dinther wurden der Schule verwiesen, da sie sich mit Hilfe von **Keyloggern** Zugang zu **19 E-Mailkonten** von Lehrern verschafft hatten. Sie stahlen Prüfungsunterlagen und teilten die Informationen mit ihren Freunden.
- 19.03. Eine **kritische Sicherheitslücke** im Browser **Firefox 3.6** veranlasst das Bürger-CERT, ein Projekt des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), eine Nutzungswarnung auszugeben. User sollten die Version 3.6 vorerst nicht mehr nutzen. Mozilla reagiert schnell und bringt am 23.03. einen Sicherheitspatch auf den Weg, der die Sicherheitslücke **CVE-2010-1028** schließt.
- 22.03. Der Mobilfunkanbieter Vodafone gibt zu, insgesamt knapp 3.000 Geräte mit **infizierten Speicherkarten** ausgeliefert zu haben. Drei Wochen zuvor hatte Vodafone gemeldet, es handele sich um einen absoluten Einzelfall, nachdem ein Malware-Analyst den Schadcode nach dem Kauf eines **Smartphones** entdeckt hatte. Der Vorfall sei auf **Spanien** begrenzt. Die vermeintlich betroffenen Kunden werden angeschrieben und Tools zur Entfernung der Schadsoftware stehen zum Download bereit. Es lohnt sich, neue Gadgets auf Viren zu prüfen.
- 24.03. Die Organisation **Messaging Anti-Abuse Working Group** (MAAWG) veröffentlicht die Ergebnisse einer Studie zum Nutzerverhalten rund um das Thema **E-Mail-Sicherheit**. Die in Amerika und Westeuropa durchgeführte Studie zeigt: 43 % aller 3.716 Befragten öffneten Mails, die sie selbst als **Spam** einstufen, 11 % klickten sogar einen Link in einer dieser Mails. 8 % der Befragten schätzen ein, dass sie keinesfalls Opfer einer Bot-Infektion werden könnten
- 26.03. In den USA wurde **Albert Gonzalez** zu 20 Jahren Haftstrafe verurteilt. Der 28jährige gilt als Drahtzieher des wohl „größten und kostspieligsten Beispiels von Computer Hacking in der Geschichte der Vereinigten Staaten“, so der urteilende Richter. Gonzales soll mit zwei **rus-sischen Konspiratoren** über **130 Millionen Kreditkarten- und Bankkartendatensätze** gestohlen haben.
- 29.03. Sicherheits-Experte **Didier Stevens** nutzt eine **PDF-Funktion**, um beliebige Programme beim Öffnen eines PDF-Dokuments zu starten. Das Abschalten der Java-Script Funktion schützt in diesem Falle nicht. Der Foxit Reader führt bis zur Veröffentlichung eines Updates den Code ohne weitere Nachfrage aus, Adobes Reader zeigt eine Warnmeldung an. Der Text des angesprochenen Warnfensters lässt sich jedoch verändern und eröffnet Möglichkeiten zum **Social-Engineering**.

30.03. Eine **Facebook** Antivirus-Applikation verbreitet sich innerhalb des Social Networks – allerdings ist es ein Betrugsversuch, denn es gibt keine dedizierte Schutzapplikation für den Branchenprimus. Nach der Installation **der falschen App** fügt diese 20 Freundeskennezeichnungen in ein Bild, um weitere Freunde in die Falle zu locken.



Screenshot 2: „Fake Facebook Antivirus“
Quelle: SecurityWatch Blog

31.03. **Facebook** ist erneut in den Schlagzeilen: Der Netzwerk gigant hatte versehentlich **alle E-Mail Adressen** der rund 400 Millionen Nutzer für rund 30 Minuten **öffentlich** auf den Profilen angezeigt. Die Nutzer hatten keine Chance, die Adresse zu löschen oder zu verbessern.

31.03. Wie heute bekannt wird, verbreitete die Webseite des **deutschen Umweltbundesamtes** zwischen dem 19.3. und dem 22.3. einen **ZeuS-Trojaner**. Wie die Seite infiziert wurde, ist offiziell nicht bekannt.

April 2010

01.04. In **Belgien** entsteht ein neues **Experten-Zentrum zum Thema Cyberkriminalität**. Die Universität von Leuven wird dafür mit anderen akademischen Institutionen, der belgischen Regierung, der Europäischen Kommission und einigen privaten Firmen zusammenarbeiten. Ziel des Zentrums ist es, geeignete Schulungsmaßnahmen zu entwickeln und Wissen zu vermitteln.

15.04. Nachdem vor zwei Tagen Details über eine **Sicherheitslücke in Javas Development Toolkit** an die Öffentlichkeit gelangten, ist heute der Java 0-Day Exploit „in the wild“ gesichtet worden. Tavis Ormandy und Rubén Santamarta veröffentlichen detaillierte Informationen zur Sicherheitslücke. Sun entschied sich kurzfristig doch zu einem **außerzyklischen Update**, wohl nachdem sich die Vorhersagen einer **Infektionswelle** häuften. Version 6u20 steht seit heute zum Download bereit und schließt die Lücke.

15.04. Durch das Herunterladen von **gefälschten Hentai-Computerprogrammen** aus P2P-Netzwerken verbreitet sich ein **japanischer Computerschädling**. Er greift Informationen vom infizierten Computer ab und macht sie öffentlich auf einer Homepage zugänglich. Es handelt sich dabei Berichten zufolge um den Namen des Opfers, die Favoriten aus dem IE, die Browser-Historie etc. Die Opfer erhalten eine E-Mail und werden zu einer Zahlung von **1.500 Yen** aufgefordert, damit ihre Daten von der Webseite gelöscht werden.

15.04. Die **niederländische Bahngesellschaft**, Nederlandse Spoorwegen, kämpft gegen **Skimmer**. Die Gesellschaft wechselte seit August 2009 alle Kartenslots an den Ticket-Automaten aus, nachdem in 2009 insgesamt 467 Skimming-Apparaturen an Automaten entdeckt wurden. In 2010 wurde bis jetzt keine einzige Fremdapparatur registriert.



Illustration: G Data 2009

- 16.04. Ein Mitarbeiter der **Polizei Gwent** (UK) **verschickte** eine brisante Microsoft **Excel-Tabelle** mit persönlichen Daten und Informationen aus **dem polizeilichen Strafregister** von 10.006 Personen. Durch die eingeschaltete Funktion „automatisches Ausfüllen“ im E-Mail-Programm und Unachtsamkeit gelangte die **unverschlüsselte und ungesicherte** Liste in die Hände eines „The Register“-Journalisten. Die Liste wurde in Kooperation mit der Polizei vom System des Journalisten gelöscht und nicht veröffentlicht.
- 19.04. Der **niederländische Hacker „Woopie“**, der 22-jährige Kevin de J., wird verhaftet. Ihm wird der Hack der Webseiten CrimeClub und ExtremeClub und das Stehlen und Veröffentlichen von **Skripten** aus der Administratordatenbank vorgeworfen. Angeblich hat er diese Seiten mit **DDoS-Attacken** lahm gelegt. Seine eigene Webseite, woopie.nl, wurde von der Polizei-Spezialeinheit Team High Tech Crime konfisziert. Es ist wohl das erste Mal, dass eine Webseite in den Niederlanden beschlagnahmt wird.
- 21.04. Seit heute gibt es bei **Facebook** eine erneute, große Änderung der **Privatsphären-Einstellungen**. Die Funktion nennt sich „**Instant Personalization**“ und lässt Webseitenanbieter auf das öffentliche Profil von Nutzern zugreifen, damit die aufgerufene Webseite personalisiert werden kann. Die „Instant Personalization“-Funktion wurde als sogenanntes **opt-out** angelegt, das heißt, sie gilt generell für jeden User, es sei denn, er widerspricht. Diese Funktion ist ein weiterer Schritt auf dem Weg zum **gläsernen User** und kann sowohl für Marketingzwecke/gezielte Werbung ausgenutzt werden, als auch von **Identitätsdieben** zur Recherche benutzt werden.
- 22.04. **Kurios:** Im April 2010 wurden bereits knapp **900 .be-Domains gehackt**, betrachtet man die Statistiken von zone-h.org. Der Weblog Belsec erwähnt, dass die Zahl der Hacks in diesem Monat **ungewöhnlich hoch** sei. Als ein Grund wird das Benutzen von shared Hosting in Betracht gezogen – Also das Verwalten vieler Webseiten auf einem Webserver.
- 24.04. Eine Art Twitter für Online-Shoppingtouren, das ist „**Blippy**“. Getätigte **Einkäufe** werden dem Netzwerk als **Kurznachricht** angezeigt, inklusive Preisangaben und Beschreibung des gekauften Artikels. Fünf Mitglieder des Web 2.0-Services fanden jedoch auch ihre **Kreditkartendaten bei Google gepostet**. Laut „Blippy“ handelt es sich um „isolierte Vorfälle“, die aus der frühen Beta-Testphase des Services stammen.
- 27.04. Das Projekt **Google Street View** steht in Deutschland seit Tagen erneut in der Kritik. In seinem offiziellen Google Policy Europe Blog erläutert der Internetdienstleister Google Details über die von den Street View Autos gesammelten Daten. Zu den gesammelten WLAN-Daten gehören laut Angaben die SSID und die MAC-Adresse. Der deutsche Bundesdatenschutzbeauftragte Peter Schaar forderte die sofortige Löschung der Daten und einen Stopp der Datensammlung in der Zukunft. Google sagt, die Sammlung und Speicherung von Payload-Daten, gesendeten Datenpaketen, finde nicht statt. Diese Information wird am 14.05.2010 revidiert werden.
- 29.04. Ein **bulgarischer Skimmer** wird zu **vier Jahren Haft** verurteilt, nachdem er in Brügge, Antwerpen und Brüssel Skimming betrieben hat. Er wurde verurteilt wegen Unterbrechung des gültigen Bankverkehrs und wegen Mitgliedschaft in einer international organisierten **kriminellen Organisation**.

Mai 2010

- 04.05. Zwei der mutmaßlichen Köpfe hinter dem **Mariposa Botnet**, „Netkairo“ und „Ostiator“, versuchten, bei einer spanischen Firma **für Security Software eine Anstellung zu bekommen**. Der Firmenleiter sagte daraufhin: „Ich weiß nicht, was Sie sich gedacht haben, aber Mariposa als Visitenkarte zu benutzen ist nicht wirklich eine große Hilfe, eher im Gegenteil“. Als sich die Firma nicht an einer Anstellung interessiert zeigte, drohte einer der beiden mit der Aufdeckung von Sicherheitslücken in ihrer Software.
- 04.05. Das Internetportal **netzpolitik.org** berichtet erneut von massenhaftem Datenabgriff bei der deutschen Web 2.0-Plattform für Schüler: **SchülerVZ**. Obwohl die Betreiber der VZ-Portale wohl nach den letzten Vorfällen in die Datensicherheit investiert hatten und unter anderem auch ein **TÜV-Prüfzeichen für Datensicherheit und Funktionalität** erhielten, konnte ein Student die Daten von **mehr als zwei Millionen**, meist minderjährigen, Nutzern sammeln. Sein Crawler würde gleichermaßen für die Plattformen MeinVZ und StudiVZ funktionieren, doch dem Programmierer war es wichtig, das Augenmerk auf den Schutz der Daten von Minderjährigen zu legen. Das SchülerVZ hat nach eigenen Angaben im Mai 2010 über 5,8 Millionen Mitglieder.
- 05.05. Eine erneute **Sicherheitslücke bei Facebook** erregt Aufsehen: Die **Vorschauoption** des eigenen Profils, zu finden in den Privatsphäreneinstellungen, öffnet ungewollt Einblicke in die Live-Chats und Kontaktanfragen der Person, die als Vorschaubetrachter ausgewählt wurde. Facebook reagierte und nahm den Chatfunktion zunächst vom Netz.
- 14.05. Die Ende April gegebenen Informationen über den Umfang der gesammelten **WLAN-Daten durch Google Street View-Fahrzeuge** erweisen sich als falsch. In einem Blogbeitrag lenkt Google ein, dass „**irrtümlicherweise Proben** von Nutzdaten aus offenen (z.B. aus nicht durch Passwörter gesicherten) **WiFi-Netzwerken** gesammelt wurden“, schreibt Alan Eustace. „Weiterhin, in Anbetracht der aufgekommenen Bedenken, haben wir entschieden, dass es das Beste ist, das Sammeln von WiFi-Netzwerkdaten mit unseren Google Street View-Fahrzeugen vollkommen einzustellen.“
- 17.05. Rund 200 **Soldaten des israelischen Militärs** wurden offenbar von der **libanesischen Schiitenmiliz** im Social Network Facebook hinter das Licht geführt. Getarnt hinter dem israelischen Namen Reut Zukerman und einem Frauenfoto sollen sich die Drahtzieher hinter dem Profil Insider-Informationen der Militärs ergaunert haben. Die Militärs seien schon vor etwa einem Jahr gewarnt worden, dass Internetbekanntschaften riskant seien.
- 18.05. Das spanische Unternehmen UPCnet erstellt Hochrechnungen, nach denen **spanische öffentliche Einrichtungen** pro Jahr rund **5.400 Cyberattacken** ausgesetzt sind. Die Messungen wurden mit Hilfe des Programms SIGVI der Technischen Universität von Katalonien erstellt, das alleine für die Universität zwischen **12 und 15 Attacken pro Tag** registrierte.
- 19.05. Eines der größten **kriminellen Untergrundforen** wurde gehackt: „**Carders.cc**“, eine Platt-



Screenshot 3
Quelle: Facebook.com

form, die sich hauptsächlich mit Kreditkartenthemen befasst. Die mutmaßlichen Angreifer sollen die sein, die im November 2009 auch das Forum der „**1337 Crew**“ gehackt haben. Die Beute des aktuellen Hackangriffs: Eine **Datenbank mit E-Mail-Adressen, IP-Adressen und mehr**.

24.05. Aza Raski, ein Mitarbeiter der **Mozilla Labs**, veröffentlicht einen **Proof-of-Concept** zu dem von ihm getauften „**Tabnabbing**“. Mit Hilfe von Javascript werden das Favicon und der Seiteninhalt eines geöffneten Browsertabs nach einer bestimmten Zeit außerhalb des Fokus verändert. Die veränderte Seite kann dann eine beliebige **Log-In Seite nachahmen** und den User glauben machen, er hätte sie selbst aufgerufen. Gibt der Benutzer seine Log-In Daten ein, ist die **Phishing-Attacke** geglückt.

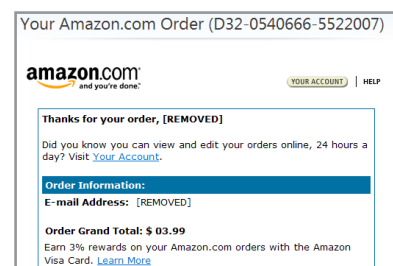
Juni 2010

04.06. **Adobe** berichtet auf seiner Webseite über eine betriebssystemübergreifende, **kritische Sicherheitslücke (CVE-2010-1297)** für Adobe Flash Player 9.0.277.0 und 10.x, Adobe Reader 9 und Acrobat 9 und 8. Mit speziell präparierten Flash-Dateien werden Rechner kompromittiert.

07.06. **Japanische Polizeikräfte** haben zwei Männer wegen Datenklau und Erpressung verhaftet, die im Zusammenhang mit der Verbreitung eines **Computerschädlings** durch **Hentaispiele** stehen. Der Schädling sammelte persönliche Informationen der Opfer von deren Rechnern und veröffentlichte sie auf einer Webseite. Die beiden sollen seit Ende 2009 zusammen arbeiten, **mindestens 5.000** Rechner infiziert und damit über **3,8 Mio. Yen** (ca. 34.000 Euro) ergaunert haben.

10.06. Microsoft berichtet auf seiner Webseite von einer **Sicherheitslücke im Microsoft Hilfe- und Supportcenter**, die auf einigen Versionen von Windows XP und Windows Server 2003 ausgenutzt werden kann, um **Schadcode zu verbreiten**. Das Aufrufen von Hilfedokumenten kann das Tor für Angreifer öffnen, die über die Sicherheitslücke dann Programme auf dem Rechner des Opfers starten oder Malware dorthin nachladen können.

25.06. Eine Welle von **gefälschten Amazon.com** und **Buy.com-Bestellbestätigungen** landet in den E-Mail-Postfächern. Die verlinkte Webseite enthält Schadcode und lädt aktuell eine **Fake AV-Software** auf den Rechner des Opfers herunter. Das Besondere an dieser **Scareware**: Sie kann gespeicherte **Passwörter** aus dem Internet Explorer 6 auslesen und anzeigen.



Screenshot 4: „Fake Amazon Order“

28.06. Laut einer repräsentativen Umfrage des deutschen **Bundesverbands Bitkom** verändern 41 Prozent der deutschen Bundesbürger ihre **Passwörter** für Online-Konten, E-Mail-Postfächer, etc. nicht aus eigener Initiative. Dabei seien Frauen noch weniger aktiv bei der Änderung der Log-in Daten: 45 % von ihnen ändern es nie, gegenüber 38 % der Männer. Als häufigster Grund für die **Aktualisierungs-Faulheit** wird die Angst vermutet, das Passwort zu vergessen. So haben **Datendiebe** leichtes Spiel.