



G Data

# Malware-rapport

## Halfjaarlijks rapport januari-juni 2010

Ralf Benzmüller & Sabrina Berkenkopf  
G Data SecurityLabs

Go safe. Go safer. **G Data.**

# Inhoud

<b>In één oogopslag</b> .....	<b>3</b>
<b>Malware: cijfers en informatie</b> .....	<b>4</b>
Malware-overvloed.....	4
Malwarecategorieën.....	5
Malware-families .....	6
Platforms: .NET neemt toe .....	8
<b>Besluit en trends 2010</b> .....	<b>9</b>
Prognoses.....	9
<b>Gebeurtenissen en trends in de eerste helft van 2010</b> .....	<b>10</b>
Januari 2010.....	10
Februari 2010 .....	11
Maart 2010 .....	13
April 2010.....	15
Mei 2010.....	17
Juni 2010.....	18

## In één oogopslag

- Met 1.017.208 nieuwe schadelijke computeritems werd ook in de eerste helft van 2010 een nieuw record behaald.
- In vergelijking met het voorgaande half jaar is dit aantal gestegen met 10% en in vergelijking met dezelfde periode in het voorgaande jaar, zelfs met 50%.
- Wij verwachten dat in het volledige jaar 2010 meer dan 2 miljoen nieuwe schadelijke computer-items zullen worden herkend.
- Met een toename van 51% is spyware de malwarecategorie die het meest gegroeid is. Dat geldt vooral voor keyloggers en Trojaanse paarden voor internetbankieren.
- De hoeveelheid nieuwe adware is met 40% gedaald.
- Genome en Hupigon, de twee meest productieve malwarefamilies, maakten samen meer varianten dan alle schadelijke items van 2007 samen.
- Schadelijke items voor Windows domineren nog steeds de gebeurtenissen met een aandeel van 99,4 %. Het aandeel van schadelijke .NET-items is echter 3 tot 4 keer gestegen en bedraagt nu 0,9 %. Ook malware-auteurs gebruiken de voordelen van .NET.
- Schadelijke codes voor Unix-afleidingen en Java nemen eveneens aanzienlijk toe.

## Trends

- Het stelen van gegevens is en blijft een kernfunctie van malware.
- Adware wordt vervangen door virusbeschermingsimitaties (FakeAV) en afpersingssoftware.
- Steeds meer online services en functies worden misbruikt voor schadelijke doeleinden.

## Gebeurtenissen

- Sociale netwerken worden volop misbruikt voor aanvallen. Twitter en Facebook lopen hierin voorop.
- Het botnet Mariposa werd platgelegd. De Spaanse politie heeft de drie beheerders gearresteerd.
- Ook het Waledac-botnet, een van de tien grootste van de V.S. werden hard getroffen door de speurders en maar liefst 277 .com-domeinen zijn van het net gehaald.
- De Duitse Emissionshandelsstelle (bestuur van emissieautoriteit) wordt het slachtoffer van een phishing-aanval waarbij de daders met rechten ter waarde van ongeveer drie miljoen euro handelden.
- PDF-bestanden worden steeds meer het doel van malware-auteurs, waardoor berichten ook toenemen via de zwakke punten in PDF-lezers.

# Malware: cijfers en informatie

## Malware-overvloed

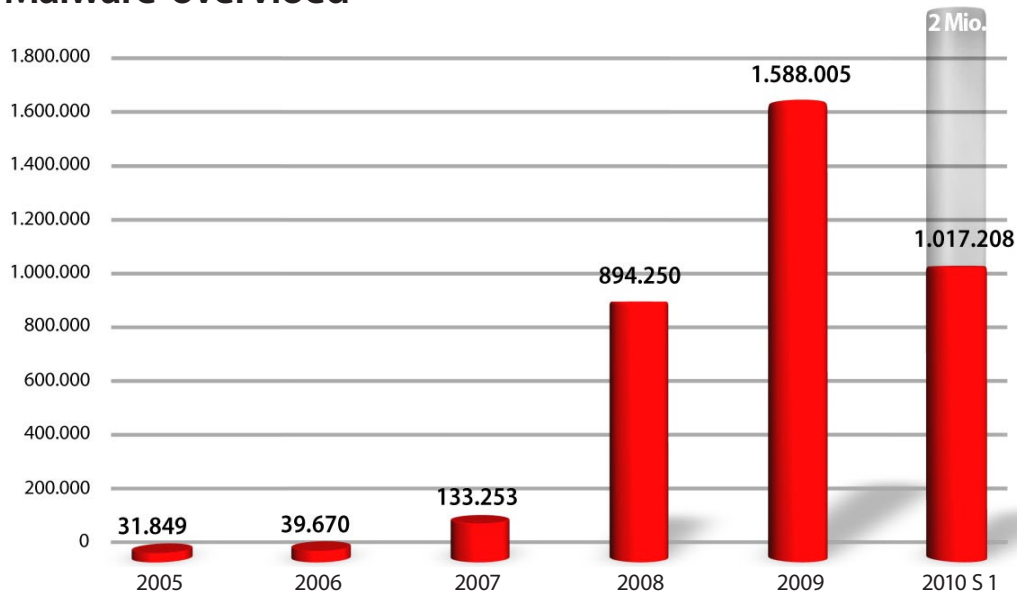


Diagram 1: aantal nieuwe malwareprogramma's per jaar sinds 2005 en tijdens de 1ste helft van 2010

Ook in de eerste helft van 2010 werd met maar liefst 1.017.208 nieuwe schadelijke computeritems<sup>1</sup> het record van het laatste semester met ongeveer 10% overschreden. In vergelijking met dezelfde periode vorig jaar nam het aantal toe met meer dan 50 %. In de eerste helft van 2010 zijn als meer nieuwe schadelijke items opgedoken dan in het volledige jaar 2008. Naar verwachting zal het aantal nieuwe schadelijke items tegen het einde van dit jaar wellicht de grens van twee miljoen overschrijden.

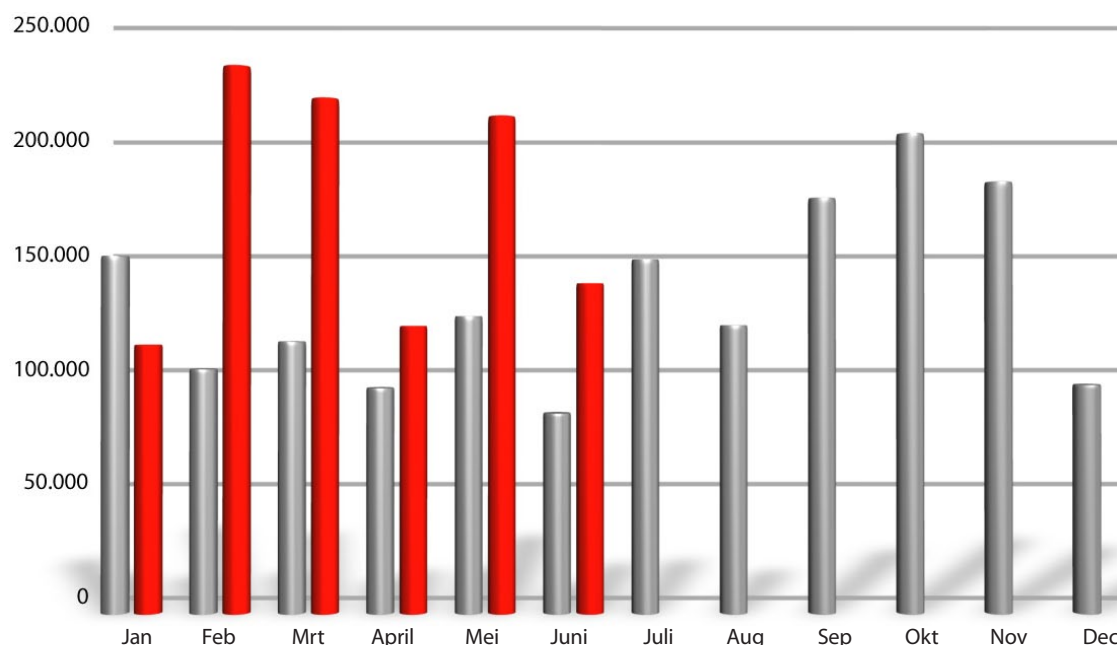


Diagram 2: aantal nieuwe malwaregevallen per maand voor 2009 en 2010

<sup>1</sup> De getallen in dit rapport zijn gebaseerd op de herkenning van malware aan de hand van virusdefinities. Zij zijn gebaseerd op overeenkomsten in de code van schadelijke bestanden. Veel schadelijke codes lijken op elkaar en worden dan in families ondergebracht waarin kleinere afwijkingen als variaties worden geregistreerd. Fundamenteel verschillende bestanden vormen eigen families. De telling baseert zich op nieuwe definitievarianten die in de eerste helft van 2010 werden ontwikkeld.

## Malwarecategorieën

Het aandeel van **spyware** is met 3,4% gestegen ten opzichte van de tweede helft van 2009 – in geen enkele andere categorie steeg het aandeel zo sterk. Hierdoor is de sterke achteruitgang gestopt, die in het laatste G Data Malware-rapport werd vermeld, al werd het aandeel van vorig jaar niet geëvenaard. In absolute cijfers betekent dit echter wel een groei van 51%. Bijzonder hoge groeipercentages in de categorie **spyware** zijn vooral te vinden in keyloggers<sup>2</sup> en Trojaanse paarden voor internetbankieren<sup>3</sup>.

De versterkte inzet van **rootkits** heeft zich wel voortgezet. Hun aantal werd in het laatste semester opnieuw 2,6 keer groter. Wormen, de rijzende sterren in het laatste G Data Malware-rapport, zijn niet verder toegenomen, maar ze blijven toch op hetzelfde niveau.

Het aantal **Trojaanse paarden** handhaaft zich op het hoge niveau van het voorgaande semester. In deze groep is het aantal ransomwareprogramma's (afpersingssoftware en vele FakeAV) nagenoeg vertienvoudigd ten opzichte van dezelfde periode vorig jaar.

Het aandeel nieuwe backdoors is gedaald met 2,9 %, wat betekent dat de neerwaartse trend van de eerste zes maanden van 2009 wordt voortgezet. Ook het aantal **tools** neemt met ongeveer 1/3 af, waardoor hun aandeel daalt tot 1,0%. Het aantal **adwareprogramma's** kent de opvallendste daling. Ten opzichte van vorige jaar (semester 1 2009 tot semester 1 2010) daalt het aantal met 40 % en neemt het aandeel af van 5,3 % naar 2,1 %.

Categorie	# 2010 S1	Aandeel	# 2009 S2	Aandeel	Vgl. 2010 S1 2009 S2	# 2009 S1	Aandeel	Vgl. 2010 S1 2009 S1
Trojaanse paarden	433.367	42,6 %	393.421	42,6 %	+10 %	221.610	33,6 %	+96 %
Downloaders/droppers	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 %
Wormen	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 %
Hulpprogramma's	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 %
Overige	6.751	0,7 %	5.543	0,5 %	+22 %	4.593	0,7 %	+47 %
<b>Totaal</b>	<b>1.017.208</b>	<b>100,0 %</b>	<b>924.053</b>	<b>100,0 %</b>	<b>+10 %</b>	<b>663.952</b>	<b>100,0 %</b>	<b>+53 %</b>

Tabel 1: Aantal en aandeel nieuwe malwarecategorieën 2009 en 2010 en hun wijziging

<sup>2</sup> 2,5 keer meer ten opzichte van de tweede helft van 2009

<sup>3</sup> 2,5 keer meer ten opzichte van de eerste helft van 2009

## Malware-families

Schadelijke computerprogramma's worden op basis van hun functies en eigenschappen in families ingedeeld. Voor enkele van deze families worden voortdurend nieuwe varianten geproduceerd. Terwijl het aantal nieuwe schadelijke items in het verleden voortdurend is gestegen, daalde het aantal families. Deze trend werd in de laatste zes maanden niet meer waargenomen. Tijdens de eerste helft van 2010 waren 2.262 malware-families actief. Dit is ongeveer 3 % meer dan de waarde van de laatste zes maanden en ongeveer een zevende van de eerste helft van 2009.

	# 2010 S1	Virusfamilie	# 2009 S2	Virusfamilie	# 2009 S1	Virusfamilie
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

Tabel 2: Top 10 van de actiefste virusfamilies. Aantal nieuwe varianten 2009 en 2010

Tabel 2 toont de families die het laatste anderhalf jaar het productiefst waren.

**Genome** is nog steeds de koploper. Het aantal van dit type is gestegen met 73 % (S2 2009 tot S1 2010). Gemiddeld brengt dit **Genome** dagelijks op 640 nieuwe varianten. Het aantal varianten van deze familie in de eerste helft van 2010 ligt net onder het totaal van alle schadelijke programma's van 2007 (vgl. tabel 1). **PcClient** die het vorige semester op de tweede plaats stond, is verdwenen uit de Top 10. De volgende plaatsen worden ingenomen door oude bekenden (vgl. korte beschrijving). **OnlineGames** kwamen opnieuw in de Top 10 terecht. De familie van de wormen **Palevo** en de **Startpage** van de browser-hijackers haalden voor het eerst een plaats in de eerste 10.

### Genome

De Trojaanse paarden van de familie "Genome" verenigen functies zoals downloaders, keyloggers en bestands codering.

### Hupigon

Met de backdoor "Hupigon" kunnen aanvallers onder andere de computer op afstand bedienen, de toetsenbord invoer opnemen, toegang krijgen tot het bestandssysteem en de webcam inschakelen.

### Buzus

Trojaanse paarden van de familie "Buzus" zoeken in geïnfecteerde systemen van hun slachtoffers naar persoonlijke gegevens (creditcards, online banking, toegang tot e-mail en FTP), die naar de aanvaller worden verstuurd. Bovendien wordt geprobeerd om de beveiligingsinstellingen van de computer te verzwakken en het systeem van het slachtoffer op die manier nog kwetsbaarder te maken.

## **Refroso**

Dit Trojaanse paard dook eind juni 2009 voor de eerste keer op. Het is uitgerust met backdoor-functies en kan andere computers in het netwerk aanvallen.

## **Scar**

Dit Trojaanse paard laadt een tekstbestand waarmee verdere downloads van schadelijke programma's, zoals downloaders, spyware, bots enz. in gang worden gezet.

## **Lipler**

Bij "Lipler" gaat het om een familie van downloaders die bijkomende malware van een website laadt. Bovendien wijzigt hij de startpagina van de browser.

## **OnlineGames**

De leden van de OnlineGames-familie stelen in eerste instantie de toegangsgegevens van online games. Hiervoor worden bepaalde bestanden en registergegevens doorzocht en/of een keylogger geïnstalleerd. In het laatste geval worden dan niet alleen de gegevens van de games gestolen. De meeste aanvallen zijn gericht op games die in Azië populair zijn.

## **Palevo**

De worm "Palevo" verspreidt zich via verwisselbare schijven (autorun.inf) en kopieert zich onder een verleidelijke naam in de vrijgave van peer-to-peer file-sharing-programma's, zoals Bearshare, Kazaa, Shareaza, enz. Hij verzendt ook koppelingen naar schadelijke websites via instant messaging (vooral MSN). Hij injecteert backdoor-functies in de Verkenner en zoekt op bepaalde servers naar opdrachten.

## **Startpage**

Deze malware-familie verandert de startpagina en in veel gevallen ook talrijke andere instellingen van de browser. Ze vormen de meest opvallende varianten van de browser-hijackers.

## **Magania**

Trojaanse paarden uit de Magania-familie, afkomstig uit China, zijn gespecialiseerd in de diefstal van gaming-accountgegevens van de Taiwanese softwarefabrikant Gamania. Doorgaans worden Magania-exemplaren verspreid via een e-mail, waarin een meervoudig gezippt, ingedeeld RAR-archief is opgenomen. Bij het uitvoeren van de schadelijke software wordt als afleiding eerst een afbeelding weergegeven, terwijl op de achtergrond extra bestanden in het systeem worden opgeslagen. Bovendien nestelt Magania zich per DLL in Internet Explorer en kan het op die manier alle webverkeer meelesen.

## Platforms: .NET neemt toe

Net als eerder wordt het grootste deel van de malware voor Windows geschreven. Het aandeel uitvoerbare bestanden onder de schadelijke items voor Windows (Win32) is gedaald naar 98,5 %, hoewel het aandeel met 9 % is gestegen. Hiermee wordt de trend die wij in het laatste malware-rapport hebben gemeld, voortgezet. Maar opnieuw wordt het lagere aantal Windows-malware-programma's gecompenseerd door een 3 tot 4 keer groter aantal malware voor het .NET-platform. Ook auteurs van schadelijke codes gebruiken de voordelen van .NET – vooral omdat deze bij de levering van nieuwe besturingssystemen horen. In totaal bedraagt het aandeel schadelijke Windows-programma's ongeveer 99,4 %.

Van de resterende 0,6 % nemen schadelijke codes uit websites (bijv. JavaScript, PHP, HTML, ASP, enz.) zowat een derde (dus 0,4 %) in beslag. Hier is een lichte terugval te melden bij het aantal nieuwe varianten. De beschikbare varianten zijn in elk geval op zeer grote schaal verspreid.

	Platform	# 2010 S1	Aandeel	# 2009 S2	Aandeel	Vgl. 2010 S1 2009 S2	# 2009 S1	Aandeel	Vgl. 2010 S1 2009 S1
1	Win32	1.001.902	98,5 %	915.197	99,0 %	+9 %	659.009	99,3 %	+52 %
2	MSIL <sup>4</sup>	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 <sup>5</sup>	922	0,1 %	1.124	0,1 %	-18 %	924	0,1 %	0 %
5	NSIS <sup>6</sup>	260	0,0 %	229	0,0 %	+14 %	48	0,0 %	+442 %
6	*ix <sup>7</sup>	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 %

Tabel 3: Top 5 platforms 2009 en 2010.

Schadelijke computeritems voor andere platforms gaan onder in deze massa. Het is echter het vermelden waard dat het aantal malwareprogramma's voor op Unix gebaseerde besturingssystemen meer dan zes keer groter is geworden en malware voor Java maar liefst zeven keer (telkens in vergelijking met de 2de helft van 2009).

4 MSIL is het tussenformaat waarin .NET-toepassingen in hun platform- en programmeertaalafhankelijke vorm worden vertegenwoordigd.  
 5 "Scripts" zijn batch- of Shell-scripts of programma's die in de programmeertalen VBS, Perl, Python of Ruby zijn geschreven.  
 6 NSIS is het installatieplatform dat onder andere wordt gebruikt om de mediaspeler Winamp te installeren.  
 7 \*ix duidt alle Unix-afleidingen aan, zoals Linux, FreeBSD, Solaris, enz.

## Besluit en trends 2010

De malware-vloed ebt niet weg. In een bloeiende ondergrondse economie hebben backdoors, rootkits, spyware en soortgelijke programma's een vaste plaats. De auteurs van schadelijke programma's richten zich vooral op spyware binnen het bereik van keyloggers, internetbankieren en online games. De diefstal van gegevens is en blijft een van de kernfuncties van malware. Hun commercialisering is vastgesteld in de ondergrondse fora.

Het aantal nieuwe adware-varianten neemt aanzienlijk af. Dit is mogelijk ook te wijten aan het feit dat meer geld kan worden verdiend met agressievere "reclamemethoden", imitaties van beveiligingsprogramma's (Fake AV) of decoderings- en beveiligingssoftware (ransomware).

Windows blijft het belangrijkste aanvalsdoel. Maar de malware-auteurs zijn steeds meer op zoek naar alternatieven.

### Prognoses

Categorie	Trend
Trojaanse paarden	→
Backdoors	→
Downloaders/droppers	→
Spyware	→
Adware	↘
Virussen/wormen	→
Hulpprogramma's	→
Rootkits	↗
Exploits	↘
Win32	↘
WebScripts	↗
MSIL	↗
Mobile	↗
*ix	↗

# Gebeurtenissen tijdens de eerste helft van 2010

## Januari 2010

- 04.01. **Opmerkelijk:** De webpresentatie van het Spaanse **EU-voorzitterschap** wordt in de werkelijke zin van het woord voorgesteld met een nieuw gezicht: een **hacker** had met de hulp van een cross-site-scripting-aanval de foto van de eerste minister Zapatero vervangen door een foto van het fictieve comedy-personage Mr. Bean.
- 06.01. **Opmerkelijk:** een 26-jarige Brit stuurt een woedebericht via **Twitter** en wordt een week later daarvoor **gearresteerd!** "You've got a week and a bit to get your s\*\*\* together, otherwise I'm blowing the airport sky high", was zijn "dreigement" aan de Britse luchthaven Robin Hood Airport, omdat hij vreesde dat zijn voor 15 januari geboekte vlucht zou worden geschrapt vanwege het slechte weer. Voor deze Tweet werd hij bijna zeven uur verhoord, verloor hij zijn baan en kreeg hij een levenslang toegangsverbod tot de luchthaven van Doncaster. De internetgemeenschap heeft Paul Chambers liefdevol gedoopt als "**Twidiot**". Chambers zelf begrijpt al deze commotie niet helemaal.
- 12.01. De "**Iranian Cyber Army**" kaapt de grootste Chinese zoekpagina **Baidu** met de hulp van gewijzigde DNS-gegevens en laat daar een banner met een boodschap achter. In december 2009 hadden ze, eveneens via gewijzigde DNS-gegevens, de micro-bloggingsservice Twitter enkele uren platgelegd.
- 14.01. De beheerders van de internetsite **opendownload.de** verliezen in beroep voor de arrondissementsrechtbank van Mannheim, zonder kans op herziening. Een gebruiker had begin 2008 een **rekening** van opendownload.de ontvangen, hoewel het verplicht betalen van onkosten "niet zo gemakkelijk herkenbaar of goed waarneembaar was, dat de gemiddelde verbruiker zonder meer wordt geïnformeerd of de ontstane kosten", aldus de **arrondissementsrechtbank van Mannheim** in haar vonnis. De klant weigerde de betaling via zijn advocaat en eiste op zijn beurt de betaling van zijn advocaatkosten. De consumentenorganisatie van Rheinland-Pfalz had al eind 2008 de bedenkelijke methoden van de site aangeklaagd.
- 14.01. De voormalige beheerder van de **ondergrondse website DarkMarket** werd veroordeeld tot een gevangenisstraf van tien jaar. Renukanth Subramaniam, de 33-jarige man uit Londen, had onbewust pagina na pagina toevertrouwd aan een undercover werkende **FBI**-agent. De Amerikaanse federale politie had de site opgemaakt en met behulp daarvan onderzoek uitgevoerd in de kringen van cybercriminelen.
- 21.01. **Microsoft** publiceert een **beveiligingspatch** buiten de normale cyclus om. De noodpatch was absoluut noodzakelijk omdat de **Exploit**-code die in december 2009 de aanval op Google en andere bedrijven mogelijk maakte, aan het begin van de week op het internet werd gepubliceerd. De patch lost in totaal acht beveiligingslekken op.
- 25.01. De **cyberaanvallen op Google** en andere bedrijven die begin januari een storm ontketenden, werden onder meer mogelijk door het gebruik van **sociale netwerken**. Bij een

onderzoek door experts werd vastgesteld dat de aanvallers personen in sleutelposities hadden opgespoord, ze via Web 2.0 hadden bespioneerd en vervolgens accounts van vrienden van het slachtoffer hadden besmet. Vermomd als vriend stuurden ze vervolgens berichten met links naar geïnfecteerde websites en raakten zo in de bedrijfsnetwerken binnen. Het concern overweegt de uitstap uit de **Chinese** economie en de sluiting van google.cn.



Illustratie: G Data 2009

- 29.01. De **Deutsche Emissionshandelsstelle** (DEHSt) geeft zijn mening over de **phishing-aanvallen** die zich de dag daarvoor hebben voorgedaan: Bedriegers stuurden hun bedrog-e-mails als e-mails van de DEHSt, waarin gebruikers werden gevraagd zich aan te melden op een valse website om zich, ironisch genoeg, te beschermen tegen zogenaamde hackeraanvallen. Met de gestolen toegangsgegevens konden de daders emissierechten overdragen, vooral naar Denemarken en Groot-Brittannië, en konden ze op die manier vermoedelijk drie miljoen euro buitmaken. Zoals u ziet: doelgerichte phishing-aanvallen kunnen bijzonder winstgevend zijn.

## Februari 2010

- 02.02. **Twitter-wachtwoorden** gereset: Verantwoordelijken bij de microbloggingservice Twitter hebben aanvallen op hun gebruikers geregistreerd, die waarschijnlijk met behulp van Torrent-pagina's zijn uitgevoerd - het gaat hoofdzakelijk om gebruikers die **dezelfde aanmeldingsgegevens** hebben gebruikt op meerdere platforms en hierdoor toegankelijk worden. Wachtwoorden moeten verschillen voor elke account. Het volstaat vaak om een eenvoudige variatie op een basiswachtwoord te maken.
- 03.02. De websites van populaire Duitse **online-nieuwsportalen** zijn het slachtoffer geworden van zogenaamde **malvertising**. Golem.de, Handelsblatt.com en ook Zeit.de bezorgden de bezoekers van hun website af en toe schadelijke codes via geïnfecteerde reclamebanners. Het risico op infecties is niet meer alleen beperkt tot de "duistere" pagina's van internet. Een betrouwbare virusbeveiliging moet de inhoud van websites op schadelijke codes controleren.
- 03.02. Edwin Andrew Pena werd voor het arrondissementsrechtbank veroordeeld omdat hij tussen 2004 en 2006 ongeveer 1.000.000 US\$ had verdiend met de **illegale verkoop van Voice over IP-minuten**. Pena sluisde de gegevenspakketten door via servers van de telecommunicatieproviders die hun server alleen "beveiligden" met de vooraf ingestelde **standaard wachtwoorden**.
- 09.02. Vijf dagen na een melding over twee geïnfecteerde **add-ons** moet **Mozilla** de gevolgen dragen van het feit dat een van beide add-ons ten onrechte aan hen werd gekoppeld. Een latere scan herkende het zogenaamde geïnfecteerde programma als een **False Positive**.

- 09.02. Een verwijderingshulpprogramma dat tegen Trojaanse paarden is gericht, brengt iets nieuws op de computer: „**Kill Zeus**” is de naam van het programma uit de "Spy Eye Toolkit", dat weliswaar de "Trojaan Zeus" van uw computer verwijdert, maar zelf boosaardige bedoelingen heeft en van zijn kant gebruikersgegevens en wachtwoorden uitleest. De **Zeus-toolkit** is al sinds eind 2009 in omloop in ondergrondse fora en wordt verkocht voor ongeveer 500 US\$.
- 09.02. Een **Nederlandse scareware** duikt op internet op. Zelfs al staat de gebruikersinterface vol taalfouten, wordt het bestaan van een niet-Engelse versie als overduidelijke uitbreiding gezien naar landen die niet Engelstalig zijn. In totaal ondersteunt deze scareware **19 talen**.
- 10.02. De **Australische regering** werd platgelegd door doelgerichte **DDoS-aanvallen** van de activistengroep "Anonymous". De aanvallen worden omschreven als politiek gemotiveerd "hacktivisme" en wordt zowel van de kant van de regering als van de kant van de censuur sterk veroordeeld. Reden voor de opwinding: Australië is voornemens **censuur** van bepaalde pornografische online-inhoud toe te passen. Tegenstanders van censuur vrezen hier een ongepast filtering.
- 17.02. **Opmerkelijk**: een groep jonge **Nederlanders** publiceert de site **PleaseRobMe.com** om gebruikers bewust te maken van het gevaar van ondoordachte afwezigheidsberichten op sociale netwerken. De gebruikers moeten eraan denken dat hun Tweets en posts over hun **verblijfplaats** voor iedereen beschikbaar is en dus meestal niet alleen voor vrienden. Zo weten dieven wanneer iemand zeker niet thuis is en kunnen ze van de gelegenheid gebruik maken om in te breken. Volgens de laatste geruchten zouden verzekeringsmaatschappijen hun verzekeringspremies verhogen wanneer kan worden bewezen dat de klant services gebruikt voor **geologische lokalisatie**.



Screenshot 1: Bron: pleaserobme.com

- 17.02. **Microsoft** verklaart dat de **rootkit Alureon** schuldig is aan de **Bluescreen**-crash van talrijke Windows XP- en enkele Windows 7-computers. De Bluescreens of Death (BSoD) stapelden zich op na de systeemupdate MS10-015 van de week daarvoor. De computers die voor de update met Alureon waren geïnfecteerd, zijn hiervan het slachtoffer geworden.
- 23.02. **Microsoft** maakt bekend dat een harde en tot nog toe unieke slag werd toegebracht aan "**Waledac**", een van de tien grootste botnets van de V.S. Na een gerechtelijke beslissing, konden 277 .com-internetdomeinen, waarvan wordt verondersteld dat er een samenhang is met het "Waledac"-botnet, van het net worden verwijderd. De geïnfecteerde **bot-computers** zouden hierdoor het contact met de te besturen Command&Control-servers verliezen. Het "Waledac"-botnet zou naar schatting meer dan **1,5 miljard spam-e-mails** per dag hebben verzonden.



Illustratie: G Data 2009

## Maart 2010

- 01.03. Over de voorvallen van de zogenaamde "**Operation Aurora**" tegen Google en meer dan honderd andere bedrijven, werd bekend dat de aanvallen mogelijk ook via **geïnfekteerde PDF-bestanden** zijn gebeurd. Op een aantal computers die door de forensische eenheid werd onderzocht, werden schadelijke PDF-documenten aangetroffen, die met de aanval te maken kunnen hebben. De bestanden vertoonden overeenkomsten met de tot nu toe ontdekte sporen op het gebied van tijd, herkomst en type. In dit verband maakt ook de chipfabrikant **Intel** in zijn financieel verslag bekend, dat er ook in januari een "**uitgekiend beveiligingsvoorval**" werd opgemerkt, maar het bedrijf geeft geen informatie over de omvang en de gevolgen.
- 03.03. De Spaanse overheid maakt bekend dat ze **drie vermoedelijke beheerders** van "**Mariposa**"-botnets (Spaans voor "vlinder") heeft gearresteerd. De Spaanse mannen waren tussen 25 en 31 jaar oud en zouden met behulp van het botnet vooral gegevens van internetbankieren en creditcards hebben gestolen. In schattingen werd berekend dat het net zich uitstreckte over **meer dan 13 miljoen computers** in 190 landen.
- 06.03. Een groot aantal **Twitter-accounts** werd **gehackt** en verspreidde spam via een zogenaamd dieet. "Check out this diet I tried, it works!" en "I lost 20 lbs in 2 weeks" waren de lokroepen. Nog niet bevestigd, maar denkbaar is de infectie van een account via **Brute Force-aanvallen** (woordenboekaanvallen) op Twitter-interfaces (API's).
- 07.03. Uit een rondvraag van GlobeScan in opdracht van BBC World Service blijkt dat bijna **80 % van de bevolking** de toegang tot het **internet als een fundamenteel recht** beschouwen. De meerderheid van de ongeveer 28.000 ondervraagde personen in 26 landen, waarvan 14.306 zelf internetgebruikers zijn, wil dat het internetgebruik door de wet wordt geregeld, zoals dat in Finland en Estland reeds het geval is.
- 09.03. **Twitter** start een nieuwe veiligheidsmaatregel met betrekking tot verzonden koppelingen. Alle koppelingen die naar Twitter worden gestuurd, worden voor het verzenden gecontroleerd op mogelijke schadelijke invloeden (phishing en andere aanvallen). Zo moet een verspreiding van schadelijke koppelingen via de Twitter-service worden opgevangen en verhinderd.
- 10.03. Gebruikers van de browser **Internet Explorer 6 en 7** zijn slachtoffers van een hacker. Microsoft publiceert een beveiligingswaarschuwing betreffende een **0-Day Exploit**. In bepaalde omstandigheden kunnen aanvallers schadelijke opdrachten uitvoeren op de aangevallen pc's. Vooral Internet Explorer 7 wordt nog steeds op grote schaal gebruikt. Daarom vermoeden experts dat er na de publicatie van de Exploit-code een massaal misbruik zal volgen van de beveiligingslekken.
- 11.03. Het aantal besturingsservers (Command&Control Server) van het **Zeus-botnet** heeft zich weer hersteld. Het Zwitserse initiatief Zeus Tracker nam in de dagen hiervoor een aanzienlijke vermindering van het aantal C&C-servers (van 249 naar 104) waar en schrijft dit toe aan de tijdelijke uitschakeling van de upstream-provider Troyak-as. Het **aantal servers** is nu weer verhoogd naar 191.

- 12.03. Het officiële jaarverslag van het **Internet Crime Complaint Centers** (afgekort IC3) registreert een stijging van **klachtmeldingen**. In 2009 waren er 336.655 gevallen, wat een verhoging betekent van 22,3 % ten opzichte van 2008. Het grootste deel van de berichten had te maken met internetbedrog in combinatie met financiële schade, waarbij het financiële verlies hier **559,7 miljoen US\$** bedraagt. Het IC3 is een samensmelting van de FBI met het National White Collar Crime Center en is de centrale klachtenlocatie voor internetcriminaliteit in de Verenigde Staten.
- 16.03. Twee **gymnasiasten** uit het Nederlandse Heeswijk-Dinther werden van school gestuurd omdat ze zich met behulp van **keyloggers** toegang hadden verschaft tot **19 e-mailaccounts** van leerkrachten. Ze stalen de examens en deelden die informatie met hun vrienden.
- 19.03. Een **kritisch veiligheidslek** in de browser **Firefox 3.6** zorgt ervoor dat het Bürger-CERT, een project van de Duitse federale instanties voor veiligheid in de informatietechniek (BSI), een gebruikswaarschuwing geeft. De gebruikers worden verzocht versie 3.6 voorlopig niet meer te gebruiken. Mozilla reageert snel en lanceert op 23.03 een veiligheidspatch die het beveiligingslek **CVE-2010-1028** sluit.
- 22.03. Vodafone, de mobiele telefoonprovider, geeft toe dat ze in totaal bijna 3.000 toestellen met **geïnfecteerde geheugenkaarten** hebben geleverd. Drie weken eerder had Vodafone gemeld dat het om een absoluut eenmalig feit ging, nadat een malware-analist de schadelijke code had ontdekt na aankoop van een **smartphone**. Het voorval zou beperkt zijn tot **Spanje**. De vermeende betrokken klanten werden aangeschreven en de hulpmiddelen voor het verwijderen van de schadelijke software kan worden gedownload. Het loont de moeite, nieuwe gadgets te controleren op virussen.
- 24.03. De organisatie **Messaging Anti-Abuse Working Group** (MAAWG) publiceert de resultaten van een onderzoek over het gebruikersgedrag rond het thema **e-mailbeveiliging**. Het in Amerika en West-Europa uitgevoerde onderzoek toont het volgende aan: 43 % van de 3.716 ondervraagde personen opende e-mails die ze zelf als **spam** hadden geclassificeerd en 11 % klikte zelfs op een koppeling in een van deze e-mails. 8 % van de ondervraagden denkt dat zij in geen geval het slachtoffer kunnen worden van een infectie door bots.
- 26.03. In de V.S. wordt **Albert Gonzalez** veroordeeld tot een gevangenisstraf van 20 jaar. De 28-jarige geldt als de figuur achter de schermen van dit "grootste en duurste voorbeeld van computerhacking in de geschiedenis van de Verenigde Staten", volgens het vonnis van de rechter. Samen met twee **Russische samenzweersers** zou Gonzales meer dan **130 miljoen gegevensrecords van creditcards en bankkaarten** hebben gestolen.
- 29.03. Veiligheidsexpert **Didier Stevens** gebruikt een **PDF-functie** om willekeurige programma's te starten bij het openen van een PDF-document. Het uitschakelen van de Java Script-functie zorgt in dit geval niet voor een bescherming. De Foxit Reader leidt tot de publicatie van een update van de code, zonder verdere vragen te stellen. De Adobe Reader toont het waarschuwingsbericht. De tekst van het gebruikte waarschuwingsvenster kan echter worden gewijzigd en opent mogelijkheden voor **social-engineering**.

30.03. Een **Facebook**-antivirustoepassing verspreidt zich binnen het sociale netwerk - in elk geval is dit een poging tot bedrog, omdat er geen specifieke beveiligingstoepassingen is voor dit sociale netwerk. Na de installatie van de **neptoepassing** voegt deze 20 kenmerken van vrienden toe aan om nog meer vrienden in de val te lokken.



Screenshot 2: "Fake Facebook Antivirus"

Bron: SecurityWatch Blog

31.03. **Facebook** haalt opnieuw de krantenkoppen: de netwerkgigant heeft **alle e-mailadressen** van de ongeveer 400 miljoen gebruikers, per ongeluk gedurende 30 minuten **openbaar** weergegeven op de profielen. De gebruikers hadden geen mogelijkheid het adres te verwijderen of te verbergen.

## April 2010

01.04. In **België** ontstaat een nieuw **expertcentrum rond het thema van de cybercriminaliteit**. De universiteit van Leuven zal daarvoor samenwerken met andere academische instituten, de Belgische regering, de Europese Commissie en enkele particuliere bedrijven. Het doel van het centrum is een geschikte opleiding te ontwikkelen en kennis door te geven.

15.04. Nadat twee dagen hiervoor details bekend raakten over een **beveiligingslek in de Java Development Toolkit**, was de Java 0-Day Exploit op deze datum "in the wild" zichtbaar. Tavis Ormandy en Rubén Santamarta maakten gedetailleerde informatie bekend over de beveiligingslekken. Sun ging echter meteen over tot een **extra-cyclische update** nadat de voorspellingen van een **infectiegolf** de ronde deden. Versie 6u20 kan worden gedownload en sluit het lek.

15.04. Door het downloaden van **vervalste Hentai-computerprogramma's** van P2P-netwerken, verspreidt zich een **schadelijk computerprogramma uit Japan**. Het haalt informatie van de geïnfecteerde computer en maakt dit openbaar toegankelijk op een startpagina. Het gaat hierbij om berichten gebaseerd op de naam van het slachtoffer, de favorieten uit IE, de browsergeschiedenis, enz. De slachtoffers ontvangen een e-mail en worden gevraagd een bedrag van **1.500 yen** te betalen zodat hun gegevens van de website worden verwijderd.

15.04. De **Nederlands Spoorwegen** rekest af met met **skimmers**. De onderneming verving sinds augustus 2009 alle kaartgleuven van hun ticketautomaten nadat in 2009 in totaal 467 skimming-apparaten in de automaten werden ontdekt. In 2010 werd tot nog toe geen vreemd apparaat geregistreerd.



Illustratie: G Data 2009

16.04. Een medewerker van de **politie van Gwent** (VK) **verzond** een explosieve Microsoft **Excel-tabel** met persoonlijke gegevens en informatie uit **het politiestrafregister** van 10.006 personen. Door de ingeschakelde functie "automatisch invullen" in het e-mailprogramma en nalatigheid, kwam de **ongecodeerde en onbeveiligde** lijst in handen van een journalist

- van "The Register". De lijst werd in samenwerking met de politie van het systeem van de journalist verwijderd en niet gepubliceerd.
- 19.04. De 22-jarige Nederlander Kevin de J., alias **de hacker "Woopie"**, wordt gearresteerd. Hij wordt aangeklaagd voor het hacken van de websites CrimeClub en ExtremeClub en voor het stelen en bekendmaken van **scripts** uit de beheerdersdatabase. Naar wordt beweerd, heeft hij deze pagina's platgelegd via **DDoS-aanvallen**. Zijn eigen website, woopie.nl, werd door de speciale politie-eenheid Team High Tech Crime in beslag genomen. Het is de eerste keer dat een website in Nederland in beslag werd genomen.
- 21.04. Sinds vandaag is er bij **Facebook** een vernieuwde, grote verandering van de **privacy-instellingen**. Deze functie noemt zich "**Instant Personalization**" en biedt aanbieders van webpagina's toegang tot het openbare profiel van de gebruiker, zodat de opgeroepen website persoonlijk kan worden aangepast. De functie "Instant Personalization" werd als zogenaamde **opt-out** opgemaakt. D.w.z. dat deze algemeen voor elke gebruiker geldt, tenzij hij dat weerlegt. Deze functie is een nieuwe stap op het pad naar de **doorzichtige gebruiker** en kan niet alleen voor marketingdoeleinden/doelgerichte reclame worden gebruikt, maar ook door **identiteitsdieven** voor research.
- 22.04. **Opmerkelijk**: Volgens de statistieken van zone-h.org, werden in april 2010 al bijna **900 .be-domeinen gehackt**. De weblog Belsec meldt dat het aantal hacks in die maand **ongewoon hoog** was. Als oorzaak werd het gebruik van shared hosting in aanmerking genomen, d.w.z. het beheer van meerdere websites op een webserver.
- 24.04. "**Blippy**" is een soort Twitter voor online shopping. Uitgevoerde **aankopen** werden aan het netwerk weergegeven als een **kort bericht**, inclusief prijsaanduidingen en beschrijvingen van de aangeschafte artikels. Vijf leden van de Web 2.0-services ontdekten echter dat hun **creditcardgegevens bij Google waren gepubliceerd**. Volgens "Blippy" gaat het om "geïsoleerde gevallen" die stammen uit de vroege bèta-testfase van de services.
- 27.04. Het project **Google Street View** krijgt in Duitsland al dagenlang scherpe kritiek. In zijn officiële Google Policy Europe Blog geeft de internetprovider Google details van gegevens die zijn verzameld via Street View Autos. Volgens de laatste verklaringen, werden de verzamelde WLAN-gegevens ook aangevuld met de SSID en het MAC-adres. Peter Schaar, de verantwoordelijke voor de beveiliging van de Duitse overheidsgegevens, eiste dat de gegevens onmiddellijk werden verwijderd en dat de verzameling van gegevens in de toekomst zou worden stopgezet. Google weerlegt dat er payloadgegevens, verzonden gegevenspakketten werden verzameld en opgeslagen. Deze informatie zal op 14 mei 2010 worden gecontroleerd.
- 29.04. Een **Bulgaarse skimmer** werd veroordeeld tot **vier jaar gevangenisstraf** na het skimmen in Brugge, Antwerpen en Brussel. Hij werd veroordeeld voor de onderbreking van het geldige bankverkeer en vanwege zijn lidmaatschap van een internationaal **criminele organisatie**.

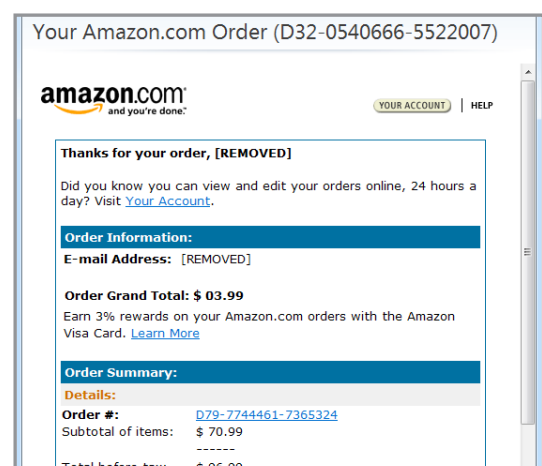
## Mei 2010

- 04.05. Twee van de vermoedelijke kopstukken achter het **Mariposa-botnet**, "Netkairo" en "Ostiator" hebben geprobeerd een baan te krijgen bij een Spaans bedrijf **voor beveiligingssoftware**. De bedrijfsleider verklaart hierover: "Ik weet niet wat ze dachten, maar Mariposa gebruiken als visitekaartje is niet echt een groot pluspunt, eerder het tegenovergestelde". Omdat de firma geen interesse toonde voor een aanwerving, dreigde een van de twee met het onthullen van veiligheidslekken in hun software.
- 04.05. Het internetportaal **netzpolitik.org** meldt opnieuw massale gegevensdiefstal bij het Duitse Web 2.0-platform voor leerlingen: **SchülerVZ**. Hoewel de beheerders van het VZ-portaal in de gegevensbeveiliging hadden geïnvesteerd en onder andere ook een **TÜV-keurmerk voor gegevensbescherming en functionaliteit** ontvingen, kon een student de gegevens van **meer dan twee miljoen** gebruikers, meestal minderjarigen, verzamelen. Zijn crawler zou evenzeer voor de platforms MeinVZ en StudiVZ werken, maar de programmeur vond het belangrijk de nadruk te leggen op de beveiliging van gegevens van minderjarigen. Volgens haar eigen gegevens telt SchülerVZ in mei 2010 meer dan 5,8 miljoen leden.
- 05.05. Een nieuw **beveiligingslek bij Facebook** baart opzien:  
De **weergaveoptie** van het eigen profiel dat te vinden is in de Privacy-instellingen, opent ongewenst inzage in de live-chats en contactaanvragen van de persoon die als voorbeeldtoeschouwer is geselecteerd. Facebook reageerde en nam de chatfunctie tijdelijk van het net.  
*Screenshot 3 Bron: Facebook.com*
- 
- 14.05. De informatie van eind april over de omvang van de verzamelde **WLAN-gegevens door Google Street View-Auto's** blijkt verkeerd te zijn. In een blogmelding geeft Google toe dat er "**bij vergissing monsters** van gebruiksgegevens werden verzameld uit geopende (bijv. uit niet door wachtwoorden beveiligde) **WiFi-netwerken**", schrijft Alan Eustace. "Daarnaast hebben wij besloten, met het oog op de ontstane twijfel, dat het de beste oplossing is om het verzamelen van WiFi-netwerkgegevens met onze Google Street View-Auto's volledig te staken."
- 17.05. Ongeveer 200 **soldaten van het Israëliëse leger** werden door de **Libanese Sjiitenmilitie** bekendgemaakt op het sociale netwerk Facebook. Verborgen achter de Israëliëse naam Reut Zukerman en met een foto van een vrouw, zouden de kopstukken de insiderinformatie achter het profiel van de militairen op een oneerlijke manier hebben verkregen. De soldaten waren al een jaar eerder gewaarschuwd dat internetvriendschappen een risico konden betekenen.
- 18.05. De Spaanse onderneming UPCnet maakt prognoses op basis van de eerste gegevens. Volgens deze gegevens vallen **Spaanse openbare instellingen** jaarlijks ten prooi aan ongeveer **5.400 cyberaanvallen**. De metingen werden uitgevoerd met behulp van het programma SIGVI van de technische universiteit van Catalonië, die alleen voor de universiteit al tussen **12 en 15 aanvallen per dag** registreerde.

- 19.05. Een van de grootste **criminele ondergrondse fora** wordt gehackt: „**Carders.cc**“, een platform dat voornamelijk met creditcardonderwerpen bezig is. De vermoedelijke aanvallers zouden dezelfde zijn die in november 2009 ook het forum van "**1337 Crew**" hebben gehackt. De buit van de huidige hackingaanval: een **database met e-mailadressen, IP-adressen en meer**.
- 24.05. Aza Raski, een medewerker van **Mozilla Labs** maakt een **Proof-of-Concept** bekend over het door hem gedoopte "**Tabnabbing**". Met behulp van Javascript worden het favicon en de pagina-inhoud van een geopend browsertabblad na een bepaalde tijd buiten de focus gewijzigd. De gewijzigde pagina kan dan een willekeurige **aanmeldingspagina nadoen** en de gebruiker doen geloven dat hij die zelf heeft opgeroepen. Als de gebruiker in dit geval zijn aanmeldingsgegevens invoert, is de **phishing-aanval** gelukt.

## Juni 2010

- 04.06. **Adobe** bericht op haar website over een bedrijfssysteemoverkoepelend, **kritisch beveiligingslek (CVE-2010-1297)** voor Adobe Flash Player 9.0.277.0 en 10.x, Adobe Reader 9 en Acrobat 9 en 8. De computers werden in gevaar gebracht met speciaal opgemaakte flash-bestanden.
- 07.06. De **Japane politie** heeft twee mannen veroordeeld wegens gegevensdiefstal en chantage, gekoppeld aan de verspreiding van een **schadelijk computerprogramma** via **Hentai-games**. Het schadelijke programma verzamelde persoonlijke informatie over het slachtoffer van zijn computer en publiceerde dit op een website. De twee boeven zouden al sinds eind 2009 samenwerken, **minstens 5.000** computers hebben geïnfecteerd en hierdoor op een oneerlijke manier meer dan **3,8 miljoen yen** (ca. 34.000 euro) hebben verkregen.
- 10.06. Microsoft bericht op haar website over een **beveiligingslek in het Help- en support-centrum van Microsoft** die op sommige versies van Windows XP en Windows Server 2003 kan worden gebruikt om **schadelijke codes te verspreiden**. Het oproepen van de Help-documenten kan de poort openen voor de aanval, die dan via het beveiligingslek programma's op de computer van het slachtoffer kan starten of daar later malware op kan laden.
- 25.06. Een golf van **vervalste orderbevestigingen van Amazon.com** en **Buy.com** belandt in de e-mailpostvakken. De gekoppelde website bevat schadelijke codes en downloadt op dat ogenblik een **Fake AV-software** op de computer van het slachtoffer. Het bijzondere aan deze **scareware**: dit type kan opgeslagen **wachtwoorden** uit Internet Explorer 6 uitlezen en weergeven.



Screenshot 4: "Fake Amazon Order"

28.06. Volgens een representatieve enquête van het Duitse **Bundesverbands Bitkom** verandert 41 procent van de Duitsers hun **wachtwoord** voor online-accounts, e-mailpostvakken, enz. niet uit eigen initiatief. Daarbij zijn vrouwen nog minder actief bij het wijzigen van hun aanmeldingsgegevens: 45 % verandert deze nooit, tegenover 38 % van de mannen. Als meest voorkomende reden voor deze **updateluiheid** wordt vermoedt dat het om de angst gaat het wachtwoord te vergeten. Hierdoor krijgen **gegevensdieven** vrij spel.