



G Data

Malware-rapport

Halfjaarlijks rapport juli-december 2009

Ralf Benzmüller & Sabrina Berkenkopf
G Data SecurityLabs

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

Inhoud

In één oogopslag	3
Malware: cijfers en informatie	4
Onbeperkte groei?	4
Malwarecategorieën.....	5
Familiebanden.....	6
Aanvalsdoel nr. 1: Windows	8
Vooruitzicht 2010	9
Prognoses.....	9
Web 2.0: sociale netwerken	10
Probleemgeval: gegevensbescherming	13
Gebeurtenissen en trends in de tweede helft van 2009	14
Juli 2009	14
Augustus 2009.....	14
September 2009.....	15
Oktober 2009.....	16
November 2009	17
December 2009	18

In één oogopslag

In de tweede helft van 2009 werden 924.053 nieuwe malwaretypes ontdekt. Dat is 39 % meer dan de eerste helft van het jaar en 60 % meer dan het jaar daarvoor en dus een nieuw record.

In 2009 werden in totaal 1.588.005 malwaretypes gevonden - 78 % meer dan in 2008.

Het aandeel Trojaanse paarden is gestegen met 9,0 %. Met 42,6 % hebben zij het grootste aandeel in de malwarestream.

Het aantal schadelijke items in de categorieën wormen, exploits en virussen is meer dan gemiddeld gestegen.

Het aantal malwaretypes dat gebruikmaakt van PDF's is bijna verdrievoudigd.

De hoeveelheid nieuwe adware is met 25 % gedaald.

Tijdens het volledige jaar zijn 2.908 families opgedoken, terwijl dat er in 2008 nog 3.069 waren. Dat betekent dat het nieuwe recordresultaat werd behaald door een kleiner aantal actieve malware-families.

De meest productieve malwarefamilies zijn "Genome" (3), "PcClient" (nieuw) en "Hupigon" (1)¹.

Het aanvalsdoel nummer 1 blijft Windows met 99,0 %. De daling met 0,3 % in vergelijking met de eerste helft van 2009 wordt gecompenseerd door .NET-malware (0,3 %). Scripttalen voor web-toepassingen behouden hun aandeel van 0,5 %.

Vooruitzicht

Downloaders, backdoors en rootkits behouden hun aandeel. Ze hebben een vaste plaats ingenomen in de ondergrondse economie.

Exploits zullen zich ook het komende jaar razendsnel blijven verspreiden.

Webtoepassingen worden steeds belangrijkere aanvalsdoelen.

Sociale netwerken, zoals MySpace, Facebook en Twitter, zullen steeds belangrijker worden als platform voor reclame (spam) en als informatiebron voor de voorbereiding en uitvoering van misdrijven.

De diefstal van gegevens is en blijft een winstgevende bezigheid. Bankingtrojanen, spyware en keyloggers zullen hun aandeel behouden.

Gebeurtenissen

"Koobface" bestaat één jaar en is actiever dan ooit.

"Gumblar" is de malware die de meeste websites infecteert.

Talrijke gevallen van gegevensverlies en gegevensdiefstal tasten ook het vertrouwen van consumenten in de betrouwbaarheid van creditcardbedrijven en banken aan.

¹ De cijfers tussen haakjes verwijzen naar de plaats op de ranglijst tijdens de eerste helft van 2009.

Malware: cijfers en informatie

Onbeperkte groei?

De hoeveelheid nieuwe malware neemt jaar na jaar toe, zoals blijkt uit diagram 1. In de tweede helft van 2009 werd met 924.053 nieuwe malwaretypes een nieuw recordaantal bereikt.

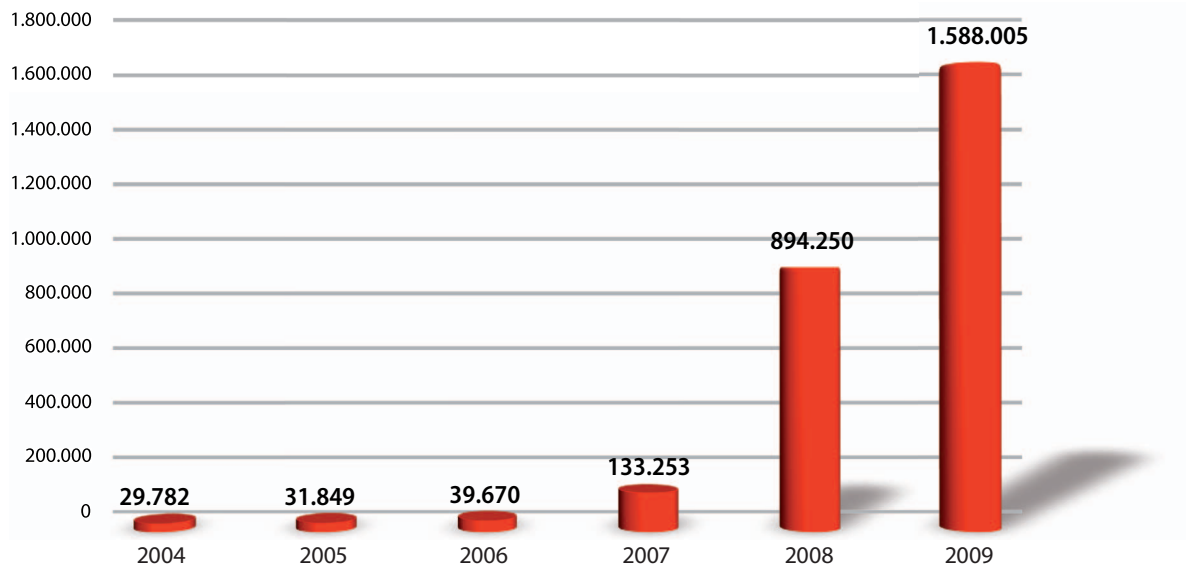


Diagram 1: aantal nieuwe malwaregevallen per jaar sinds 2004

Het groeicijfer ligt met 39 % ten opzichte van de eerste helft van 2009 en 60 % in vergelijking met dezelfde periode vorig jaar onder de cijfers van de afgelopen jaren. In heel 2009 werden 1.588.005 malwaretypes gevonden - 78 % meer dan in 2008. Het totaal aantal nieuwe malwaregevallen uit 2004 werd zelfs in één week overschreden.

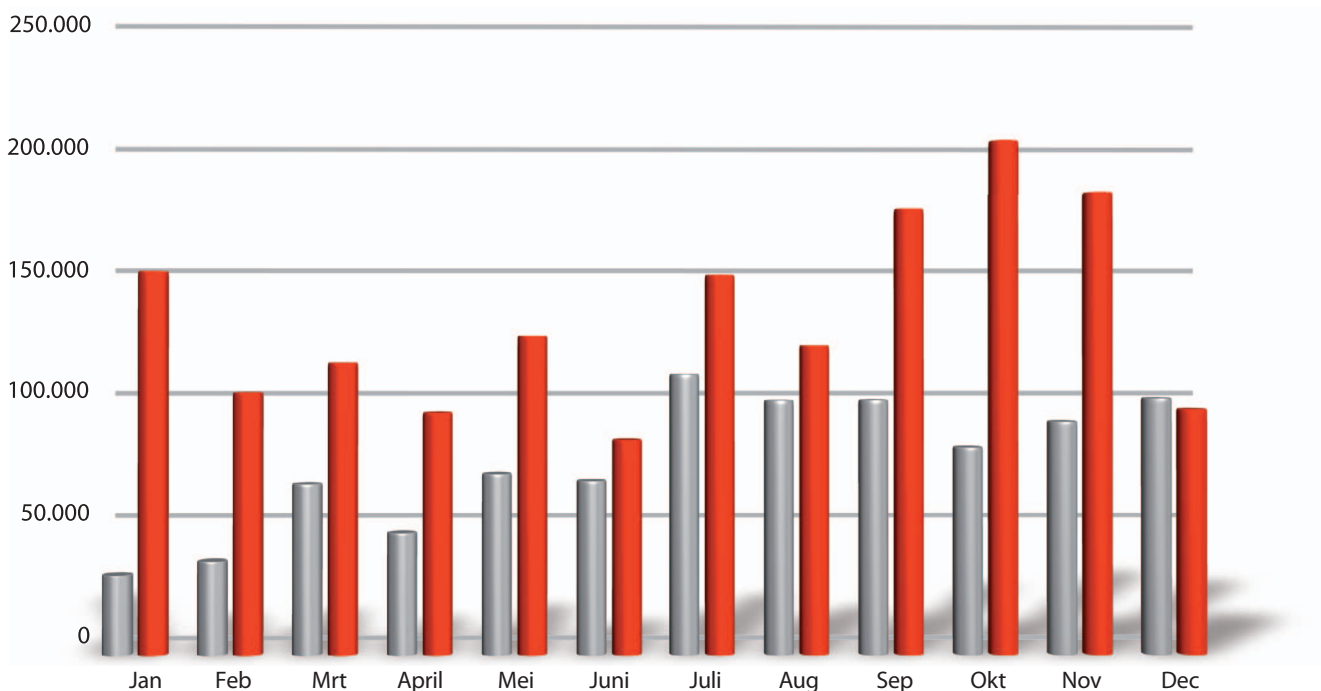


Diagram 2: aantal nieuwe malwaregevallen per maand voor 2008 en 2009

Malwarecategorieën

Het aantal Trojaanse paarden is in de tweede helft van het jaar duidelijk toegenomen. Hun aandeel ligt - met 42,6 % zoals blijkt uit tabel 1 - 9,0 % hoger dan in de eerste helft van 2009. Daardoor zijn ze met grote voorsprong de vaakst voorkomende malwarecategorie. Het aantal downloaders, backdoors en hulpprogramma's is ook bezig aan een opmars. De cijfers liggen iets onder de gemiddelde stijging van 39 % tijdens de eerste helft van het jaar en 60 % in vergelijking met vorig jaar. Deze categorieën zijn echter de belangrijkste componenten van de ondergrondse malware-economie. Downloaders zorgen voor de verspreiding, backdoors zorgen ervoor dat computers op afstand kunnen worden bediend (botnets) en hulpprogramma's geven beginners toegang tot de malwarescene en vergemakkelijken het dagelijkse werk van professionals.

Ook het aantal wormen is meer dan gemiddeld gestegen. Ten opzichte van de eerste helft van het jaar is hun aantal bijna verdubbeld en in vergelijking met dezelfde periode vorig jaar is het aantal ongeveer verdrievoudigd. De families "Basun", die als eerste worm sinds jaren weer in de top 10 staat, en "Autorun", de koploper bij de wormen in de eerste helft van het jaar, zijn daarvoor medeverantwoordelijk.

Het aandeel exploits is meer dan gemiddeld toegenomen, in tegenstelling tot het duidelijk afgenomen aantal bij CVE gemelde beveiligingslekken. Met 4.594 gemelde zwakke plekken in 2009 lag dat aantal duidelijk onder het recordaantal van 2008, toen 7.250 zwakke plekken werden opgetekend. Het aantal bekend geworden beveiligingslekken geeft ons maar een beperkt beeld van hoeveel zwakke plekken er door malware worden gebruikt. Dat aantal is namelijk duidelijk gestegen. Er wordt steeds vaker gebruik gemaakt van beveiligingslekken in veel gebruikte software om computers vooral via het internet aan te vallen. Computers met verouderde software zijn een gemakkelijke prooi voor cybercriminelen.

De sterkste groei kon worden geregistreerd voor een categorie die ondertussen verdwenen leek - de virussen. Tot deze categorie behoren de klassieke bestandsinfecties waarmee uitvoerbare bestanden worden besmet. Door het toegenomen gebruik van USB-sticks en andere verwisselbare opslagmedia loont het gebruik van dergelijke methodes opnieuw de moeite. Met een aandeel van 0,1 % blijft de verspreiding toch nog beperkt.

Categorie	# 2009 H2	Aandeel	# 2009 H1	Aandeel	Vgl. 2009H2 2009H1	# 2008 H2	Aandeel	Vgl. 2009H2 2008H2
Trojaanse paarden	393.421	42,6 %	221.610	33,6 %	+78	155.167	26,9 %	+154
Downloaders/droppers	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
Wormen	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
Hulpprogramma's	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
Virussen	637	0,1 %	143	0,0 %	+345	167	0,0 %	+281
Dialers	415	0,0 %	1.153	0,2 %	-64	1013	0,2 %	-59
Overige	5.543	0,5 %	4.593	0,7 %	+21	8.419	1,5 %	-34
Totaal	924.053	100 %	663.952	100 %	+39	576.002	100 %	+60

Tabel 1: aantal en aandeel nieuwe malwarecategorieën in de eerste en tweede helft van 2009 en hun wijziging

Het aantal nieuwe spywaregevallen is daarentegen gedaald. Hun aandeel is gedaald naar 9,4 %, dat is 5,2 % minder dan in de eerste helft van 2009 en 7,3 % minder dan het jaar daarvoor. Dat betekent echter niet dat er niet meer wordt bespioneerd. Integendeel zelfs. Spionagefuncties worden steeds vaker geïntegreerd in uitgebreide pakketten, die als Trojaanse paarden worden geclassificeerd.

Rootkits zijn een belangrijke manier om spyware en backdoors te verbergen. Tijdens de eerste helft van 2009 is hun aantal duidelijk toegenomen en hun gebruik in malware is inmiddels ingeburgerd. In de tweede helft van het jaar is het aantal nieuwe rootkit echter toch licht gedaald.

Wat adware betreft, is een daling merkbaar. Het aantal nieuwe adwaregevallen ligt 25 % lager dan vorig jaar. Dat heeft vooral te maken met de afname van "Monder". Tijdens de eerste helft van het jaar was "Monder" de meest productieve malwarefamilie. In de tweede helft van 2009 is hun productiviteit duidelijk gedaald.

Familiebanden

Aan de hand van de functies en eigenschappen kunnen schadelijke computerprogramma's in families worden onderverdeeld. De afgelopen jaren nam het aantal malwaregevallen weliswaar voortdurend toe, maar het aantal families daalde even constant. In de eerste helft van 2008 waren dat er nog 2.395, in de tweede jaarhelft 2.094. In de eerste helft van 2009 werden 1.948 verschillende vertegenwoordigers van virusfamilies geregistreerd. In de tweede helft van 2009 is het aantal malwarefamilies voor het eerst opnieuw toegenomen. In deze periode waren schadelijke programma's uit 2.200 verschillende families actief. Tijdens het volledige jaar 2009 waren er 2.908 families ten opzichte van 3.069 in 2008. De trend naar concentratie zet zich dus voort. Het stijgende aantal schadelijke computerprogramma's wordt nog altijd door steeds minder families veroorzaakt.

	# 2009 H2	Virusfamilie	# 2009 H1	Virusfamilie	# 2008 H2	Virusfamilie
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

Tabel 2: top 10 van de meest actieve virusfamilies in 2009 en de tweede helft van 2008

Tabel 2 bevat een overzicht van de families die de afgelopen 18 maanden de meeste varianten hebben voortgebracht. De huidige koploper "Genome" is goed voor gemiddeld 184 nieuwe varianten per dag. Ook de backdoors "PcClient" en "Hupigon" op plaats 2 en 3 brengen gemiddeld meer dan 100 varianten per dag voort.

Genome

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

PcClient

"PcClient" is een backdoor-programma waarmee computers op afstand kunnen worden bediend en gegevens kunnen worden gestolen. Zijn bestanden en registergegevens worden verborgen met rootkit-technieken.

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.

Scar

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

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.

Lipler

"Lipler" is een downloader die bijkomende malware van een website laadt. Bovendien wijzigt hij de startpagina van de browser.

Magania

Trojaanse paarden uit de familie "Magania", die actief is in Oost-Azië, 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.

Refroso

Dit Trojaanse paard is nieuw in de top 10. De eerste exemplaren werden eind juni 2009 ontdekt. Het is uitgerust met backdoor-functies en kan andere computers in het netwerk aanvallen.

Sasfis

Dit Trojaanse paard installeert een bestand op de computer en probeert bijkomende malware van het internet te downloaden. Deze varianten worden doorgaans als bijlage bij een e-mail verzonden.

Basun

Voor het eerst in twee jaar staat er opnieuw een worm in de top 10 van de meest productieve malwarefamilies."Basun" kopieert zich naar de computer onder de naam van de huidige gebruiker of de beheerder. Daarna valt hij andere computers in het lokale netwerk aan om zich te verspreiden.

Aanvalsdoel nr. 1: Windows

De laatste jaren concentreren malware-auteurs zich vooral op het Windows-platform. Hoewel absoluut gezien steeds meer malware wordt ontwikkeld, blijft ook het aandeel Windows-malware stijgen. Het afgelopen halfjaar ligt het aantal met 99,0 % iets onder de resultaten van de twee laatste jaarhelften (zie tabel 3). Deze lichte terugval wordt echter gerelativeerd door de malware voor het derde meest gebruikte platform. Schadelijke programma's die zijn opgesteld in de Microsoft Intermediate Language, zijn duidelijk toegenomen en hun aandeel is gestegen naar 0,3 %. MSIL is het tussenformaat waarin .NET-toepassingen in hun platform- en programmeertaalafhankelijke vorm worden vertegenwoordigd. Ook malware-auteurs maken steeds meer gebruik van de voordelen van de .NET-omgeving. De meeste .NET-toepassingen zijn op Windows gericht.

Scripts van webpagina's (zoals JavaScript, PHP, HTML en ASP) behouden hardnekkig hun aandeel van 0,5 %. Geïnfecteerde websites worden een steeds belangrijker infectiemethode. Van de 4.371 webscripts zijn er 3.295 JavaScript-malware. JavaScript wordt bovendien niet alleen op websites gebruikt. 1.624 schadelijke items maken gebruik van PDF's om zich te verspreiden. Terwijl er in 2008 nog maar 780 op PDF's gebaseerde schadelijke items voorkwamen, is hun aantal in 2009 gestegen naar 2.394 - bijna drie keer zoveel.

	Platform	# 2009 H2	Aandeel	# 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 %

Tabel 3: top 5-platformen in 2008 en 2009.

WebScripts zijn malware gebaseerd op JavaScript, HTML, Flash/Shockwave, PHP of ASP en gebruiken gewoonlijk de zwakke punten van de browser. "Scripts" zijn batch- of Shell-scripts of programma's die in de programmeertalen VBS, Perl, Python of Ruby zijn geschreven. MSIL is malware die opgeslagen is in de byte-code van .NET-programma's. NSIS is het installatieplatform dat ook door Winamp wordt gebruikt. Onder Mobile is malware voor J2ME, Symbian en Windows CE samengevoegd.

Het platform NSIS heeft met een duidelijke toename de 120 schadelijke items voor Mobile-platformen uit de top 5 verdrongen. Ondanks enkele op zichzelf staande gevallen neemt de hoeveelheid Mobile-malware niet toe. NSIS is het installatieplatform dat onder andere wordt gebruikt om de mediaspeler Winamp te installeren. NSIS wordt steeds populairder als installatieplatform, en niet alleen bij legale softwareontwikkelaars.

Voor op Unix gebaseerde systemen werden 37 nieuwe schadelijke programma's gevonden (in vergelijking met 66 in de eerste helft van 2009) en voor OS X van Apple werden 8 nieuwe schadelijke programma's gevonden. In vergelijking met de massa Windows-malware is de hoeveelheid malware voor andere platformen uiterst klein.

Vooruitzicht 2010

Het commerciële gebruik van malware houdt aan. Dankzij de enorme omzet in de ondergrondse economie kunnen snel nieuwe technologieën voor de verspreiding, het gebruik en de vermomming van malware worden ontwikkeld. Op die manier kan ook worden geïnvesteerd in opkomende toepassingen zoals sociale netwerken, mobiele terminals, spelconsoles en weinig gebruikte besturingssystemen. Om deze pogingen winstgevend te maken, zullen cybercriminelen het zwaartepunt van hun activiteiten zeker verschuiven. Momenteel zijn daarvoor echter geen aanwijzingen.

Daarom zal ook in het komende jaar de stroom van malware zeker niet afnemen - eerder het tegendeel. Downloaders, backdoors, hulpprogramma's en rootkits zijn een vast bestanddeel van deze ondergrondse economie en zullen met steeds sluwere methoden hun taken uitvoeren.

Wat exploits betreft, zullen nog steeds razendsnel beveiligingslekken in populaire desktoptoepassingen worden gebruikt. Door het lagere aantal gemelde beveiligingslekken en het gestegen veiligheidsbewustzijn van softwareontwikkelaars zou zich een verschuiving naar webtoepassingen kunnen voordoen. Naarmate het huren en gebruiken van software via het internet populairder worden, wordt het voor cybercriminelen des te lucratiever om de gehuurde webtoepassing te hacken. Hetzelfde geldt voor het gebruik van gehuurde computers (trefwoord: cloud computing). Het blijft afwachten of de ontwikkelaars van webtoepassingen dezelfde zorgvuldigheid zullen toepassen bij de omzetting van veiligheidsrichtlijnen, zoals ondertussen gebruikelijk is voor desktopsoftware.

Voor het komende jaar zijn nieuwe besturingssystemen en computerplatformen aangekondigd. Het blijft echter afwachten hoe deze markten zullen evolueren. Het aantal schadelijke programma's voor Apple-computers, Unix-computers en notebooks zou kunnen stijgen. Ook de langzame overschakeling naar 64-bit-versies van Windows 7 zal een aanpassing van de malware-auteurs vragen.

Prognoses

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

Web 2.0: sociale netwerken

Het internet heeft zich in de loop van de tijd ontwikkeld van een medium met een wetenschappelijke basis tot een alledaags medium voor de grote massa. Een op vier personen maakt gebruik van het internet.² Dat cijfer alleen is al behoorlijk indrukwekkend. Als men dan nog rekening houdt met de gebruikersstatistieken van 's werelds grootste sociale netwerk, Facebook, dan wordt pas echt duidelijk welk aandeel in het internetgebruik de online community intussen heeft. Volgens de stichter van Facebook, Mark Zuckerberg, waren in december 2009 meer dan 350 miljoen mensen actief³ op Facebook - dat betekent ook dat statistisch gezien 1 op 5 internetgebruikers een profiel heeft bij de Amerikaanse Web 2.0-aanbieder!

Er bestaan echter niet alleen sociale netwerken in het veelvoud aan Web 2.0-toepassingen: Google Docs, Google Maps, Picasa, Flickr, Identi.ca, Jaiku enz. zijn slechts enkele voorbeelden voor het "meedoen"-internet. Hoe handig en aantrekkelijk het uitgebreide gamma Web 2.0-toepassingen ook is, elke dienst houdt zijn eigen gevaren in. Deze ontstaan enerzijds doordat gebruikers veel, en vaak te veel, persoonlijke informatie over zichzelf op community-sites plaatsen en anderzijds door de technische structuur van de platformen. Hoewel de basisstructuur op zich al door cybercriminelen kan worden aangevallen, zoals uit verschillende gevallen is gebleken, implementeren de netwerken bovendien steeds meer toepassingen, die op hun beurt eigen aanvalsmogelijkheden bieden.



De populairste netwerksite Facebook als voorbeeld

Aan de hand van het voorbeeld van de Facebook-community kunnen heel wat aanvallen en onaangename gebeurtenissen voor gebruikers worden geschetst. Behalve de steeds opnieuw bekritiseerde privacyinstellingen van het netwerk en de te beperkte bescherming van jonge mensen lopen gebruikers op verschillende manieren gevaar.

Half november werden meer dan 200 Facebook-groepen door een initiatief met de naam "Control Your Info" overgenomen hoefde. De groep wilde met deze onschuldig lijkende actie wijzen op een beveiligingslek, waardoor de inhoud van groepen kon worden veranderd zonder dat Facebook zelf hoefde te worden gehackt. De groep "Control Your Info" hoefde zich enkel te registreren als

- 2 Wereldwijd zijn er volgens www.internetworldstats.com 1.733.933.741 internetgebruikers, wat overeenkomt met ongeveer 25 procent van de wereldbevolking.
- 3 Bron: <http://blog.facebook.com/blog.php?post=190423927130>

beheerder van groepen die door de oorspronkelijke beheerder waren verlaten. De wijziging van de naam en inhoud van de groep moest aanzetten tot waakzaamheid, maar kan ook de reputatie van onwetende gebruikers beschadigen, wanneer de aanvallers bijvoorbeeld onwettige inhoud op de website plaatsen. Beheerders van groepen kunnen onder andere berichten naar alle leden van de groep verzenden en op die manier doelgericht spam verspreiden.

Spam uit de eigen vriendenkring

Berichten verzonden door contactpersonen uit het Facebook-adresboek of uit een Facebook-groep worden door de meeste gebruikers als ernstig beschouwd. Als spam echter wordt verzonden via een gehackte groep of via de onrechtmatig overgenomen Facebook-account van een vriend, dan is controle beter dan vertrouwen alleen: men ontvangt een bericht, dat een grappige video, schokkerende foto's of gewoon gloednieuwe en interessante inhoud aanprijst.

Een ingesloten link, die bij het aanklikken de computer op verschillende manieren kan infecteren, een onopgemerkte drive-by-download of een valse en geïnfecteerde codec om de grappige video te kunnen bekijken, zijn de populairste trucs. Wat jarenlang als een e-mail-truc werd gebruikt, verspreidt zich nu ook via sociale netwerken. Facebook-gebruikers worden nu al vaak het slachtoffer van deze ernstige truc.

Koobface in overvloed

Al meer dan een jaar is de worm "Koobface" actief in Web 2.0-portals en hij hield in 2009 ook de fabrikanten van antivirusprogramma's druk bezig. Het jongste voorbeeld dat verband houdt met het Amerikaanse Facebook, is de verspreiding van een video met de naam "SantA". Door op de video te klikken, opent een website met de zogenaamd benodigde codec. Door de installatie van de valse codec installeert "Koobface" zich op de computer van het slachtoffer en verspreidt zich vervolgens in alle mogelijke sociale netwerken van het slachtoffer.

In de tweede helft van het jaar had "Koobface" al talloze andere nieuwe toegangspoorten naar de sociale netwerken gevonden: het annuleren van de captcha-functie bij aanmeldingen, de registratie van een nieuwe gebruiker met volledig profiel, de verspreiding van valse videocodes voor steeds nieuwe video's en veel meer. Altijd op zoek naar nieuwe gegevens die door de worm kunnen worden gelezen, opgeslagen en verspreid. Zodra de worm zich in de vriendenkring van een lid van de community heeft geïntegreerd, begint hij druk aan zijn taak als verzamelaar en verspreidt zich.

Een variant van deze worm werd bij Skype ontdekt. Het Trojaanse paard verspreidt zich via geïnfecteerde websites, steelt de aanmeldingsgegevens van de Skype-gebruiker en leest de gegevens uit het Skype-adresboek uit. Ook gebruikers van andere grotere sociale netwerken (zoals MySpace, Hi5) worden getroffen.

Ook Twitter biedt aanvalsmogelijkheden

De microbloggingdienst Twitter is een van de populairste webtoepassingen om medemensen op de hoogte te houden. Door het verlangen om altijd en overal te kunnen "tjilpen", ontstaan er ook steeds nieuwe beveiligingslekken. Zo werd in augustus een Twitter-account gebruikt om met behulp van Base64-gecodeerde korte berichten een botnet aan te sturen. Twitter blokkeerde de account onmiddellijk.

Vooral bij "short message"-blogdiensten vormen verkorte URL's een bijkomend risico op infecties. Gebruikers kunnen de echte link achter de afkortingen niet zien en worden op die manier snel het slachtoffer van geïnfecteerde webpagina's. Bekende URL-verkortingsdiensten zijn TinyURL, bit.ly, is.gd, tr.im en twi.bz.

Gebruikers kunnen beter niet vertrouwen op de verkorte link en ook het vertrouwen in de persoon die hem gepubliceerd heeft, kan de gebruiker in de val lokken, bv. wanneer Twitter-accounts worden gehackt. Voordat gebruikers op een verkorte URL klikken, kunnen ze gebruik maken van de door de verkortingsdiensten ter beschikking gestelde veiligheidsmaatregelen om een mogelijk gevaar te herkennen. Daarvoor kunnen de infopagina's van de dienst over de respectieve verkorte URL worden opgeroepen.

Enkele voorbeelden van bekende diensten en hun infoadressen:

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

	Korte URL	Actie	Voorbeeldweergave URL
TinyURL	http://tinyurl.com/yzuwcwd	preview. voor de URL	http://preview.tinyurl.com/yzuwcwd
bit.ly	http://bit.ly/7jH8xP	/info achter bit.ly	http://bit.ly/info/7jH8xP
is.gd	http://is.gd/5yGtz	- achter de URL	http://is.gd/5yGtz-
twi.bz	http://gdata.de.twi.bz/b	/e achter de URL	http://gdata.de.twi.bz/b/e
tr.im	http://tr.im/lqpj	-	-

Tabel 4: een voorbeeld van korte URL's en hun voorbeeldweergave

Besluit

Het aantal aanvallen op Web 2.0-toepassingen zal blijven toenemen. Gebruikersgegevens vormen heel interessante en winstgevende informatie voor handelaars op de zwarte markt en identiteitsdieven. De nieuwe malwarevarianten die in 2009 zijn ontstaan, zullen zich verder verspreiden en malware-auteurs zullen deze verfijnen om steeds nieuwe zwakke plekken in portals en API's te benutten.

Probleemgeval: gegevensbescherming

In de tweede helft van 2009 hebben zich bovengemiddeld veel problemen op het vlak van gegevensbescherming voorgedaan. De reikwijdte van de gemelde problemen is heel uitgebreid: van gegevensdiefstal over de verkoop en het misbruik van gegevens tot illegale controle.

Bij gegevensdiefstal moet een onderscheid worden gemaakt tussen het geval dat de gegevens verloren gaan, omdat externe aanvallers gebruik maken van een beveiligingslek in een computersysteem of een ander elektronisch systeem, of dat de diefstal van gegevens met de hulp van insiders gebeurt.

Het grootste probleem met gegevenslekken is dat de gegevens, wanneer die in omloop zijn, ongecontroleerd verder kunnen worden verspreid en niet meer kunnen worden teruggehaald. Slachtoffers kunnen de vermenigvuldiging ervan nauwelijks tegen gaan.

Een belangrijk onderwerp in november 2009 was het gegevenslek bij een Spaans creditcardbedrijf. Het lek bevond zich blijkbaar bij een Spaanse dienst voor kaartafrekeningen. Als gevolg daarvan werden meer dan 100.000 creditcards van hoofdzakelijk Duitse en Britse klanten vervangen. Dankzij dit voorval werd duidelijk welke risico's gebruikers lopen, zeker omdat het aantal vervangen kaarten in vergelijking met het totale aantal maar een klein percentage bedroeg. Creditcardgegevens kunnen op veel plaatsen verloren gaan:



- Bij de betaling worden met aangepaste leesapparaten de gegevens van de kaart gekopieerd.
- De gegevens worden door keyloggers en andere spionageprogramma's op de computer bespioneerd, bv. bij het online winkelen.
- Op valse websites (phishing) of in frauduleuze webshops met aantrekkelijke aanbiedingen worden de gegevens in een formulier gevraagd en door het slachtoffer ingevoerd.
- Onvoldoende beveiligde databases van online winkels, betaaldiensten en banken bevatten transactiegegevens. Deze vormen telkens opnieuw het doelwit van aanvalspogingen.

De eigenaars van creditcards hebben geen controle over alle aspecten van de gegevensverwerking. Het gebeurt steeds vaker dat iemand het slachtoffer wordt van creditcardfraude. Heel wat consumenten worden hierdoor onzeker en denken erover geen creditcards meer te gebruiken, maar dat is alleszins geen alternatief.

Gebruikers van creditcards kunnen zich actief beschermen tegen de gevaren van aanvallers:

- Steeds de nieuwste versie van het besturingssysteem en de browser gebruiken
- Een betrouwbare en uitgebreide virusbescherming gebruiken en deze up-to-date houden
- Zich bij het invoeren van gegevens in formulieren altijd afvragen of de beheerder van de website de gevraagde informatie echt nodig heeft. Pincodes, TAN-codes of beveiligingscodes van creditcards (CCV) wanneer men daadwerkelijk iets betaalt
- Gevoelige gegevens alleen via https, d.w.z. gecodeerd, verzenden

Gebeurtenissen en trends in de tweede helft van 2009

Ook de tweede helft van 2009 werd sterk gekenmerkt door aanvallen op sociale netwerken. Of het nu gaat over Twitter, MySpace, Facebook of andere websites, de aantrekkingskracht voor phishers en verspreiders van malware blijft ongewijzigd.

Juli 2009

01-07 De "**Month of Twitter Bugs**" begint. Aviv Raff, die al sinds 2006 aan "Month of Bugs"-projecten deelneemt, wil gebruikers en programmeurs attent maken op de zwakke plekken van het Web 2.0-medium. Hij concentreert zich daarbij momenteel op dubieuze Twitter Browser API's, Tiny-URL-diensten en aangepaste foto's met schadelijke wormcode.

04-07 Amerikaanse en Zuid-Koreaanse computers worden aangevallen op **Independence Day. Gerichtte DDoS-aanvallen** houden de beveiligingsexperts van beide regeringen bezig. Een botnet bestaande uit meerdere tienduizenden zombiecomputers voert een aanval uit op overheidswebsites en andere websites die economisch belang hebben, zoals de beurs in New York en Zuid-Koreaanse banken. De geheime diensten vermoeden dat Noord-Korea hiervoor verantwoordelijk is.

08-07 De **exploit-portal Milw0rm** kondigt zijn sluiting aan. Na intensieve onderhandelingen kan de sluiting worden afgewend. Hoewel de redenen niet expliciet worden vermeld, gaan experts ervan uit dat het aantal in te voeren exploits de capaciteiten van de exploitant overstijgt. De portal is een meldpunt voor IT-beveiligingsexperts uit beide kampen.

09-07 **Opmerkelijk: een Zuid-Afrikaanse bank neemt maatregelen tegen skimming** aan geldautomaten. Bij een routinecontrole door een technicus gaat het alarm van het afweersysteem af en zet het systeem een **aanval met pepperspray** in. Drie technici moeten in het ziekenhuis worden behandeld.



23-07 Een tot heden **onbekend beveiligingslek** in de component authplay.dll in **Adobe Acrobat** of **Adobe Flashplayer** wordt in geïnfecteerde PDF-bestanden en op gemanipuleerde websites per drive-by-download gebruikt.

Augustus 2009

"**Koobface**" bestaat één jaar en is nog altijd even agressief.

04-08 De **BSI** distantieert zich van een zogenaamd door hen verstuurd e-mail, die gebruikers naar een **scareware**-pagina stuurt. Hier worden onoplettende gebruikers in een val gelokt, waardoor ze onbedoeld een contract van twee jaar met een kostprijs van 192 euro aangaan.

06-08 De microbloggingdienst **Twitter** is een aantal uren **buiten dienst**. Zowel de hoofdtoepassing als de API-clients zijn getroffen. De oorzaak was vermoedelijk een combinatie van

verdeelde overbelastingaanvallen (DDoS) en een schijnbaar gerichte aanval tegen de bloggers met de naam "Cyxymu" door extra kliks, die in spammails naar bepaalde Twitter-pagina's verwijzen.

13-08 Er wordt bekendgemaakt dat **Microsoft** al twee jaar op de hoogte was van een kritisch **zero-day-lek** en pas in juli 2007 op de Patch Day daarop reageerde.

14-08 **Twitter** wordt mogelijk als **botnetcommunicator** misbruikt: een Arbor Security Researcher ontdekt gecodeerde Twitter-berichten in een account, die mogelijk opdrachten voor botnets bevatten.



24-08 Het kantongerecht van Stockholm veroordeelt de internetprovider "**Black Internet**" ertoe alle verkeer van de website "**The Pirate Bay**" te stoppen of 500.000 Zweedse kronen (ongeveer 48.000 euro) te betalen. Korte tijd later vindt "The Pirate Bay" een andere provider.

27-08 Een gewezen werknemer van een beveiligingsfirma publiceert programmacode voor het binnensmokkelen van een **softwarebug in Skype**. De bug kan onopgemerkt gesprekken opnemen en als mp3 naar vooraf ingestelde adressen verzenden.

29-08 In **China** worden **vier softwarepiraten** veroordeeld tot gevangenisstraffen en een boete van ongeveer 1,6 miljoen USD. Ze worden ervan beschuldigd illegale kopieën van Windows XP en andere software te hebben verdeeld.

September 2009

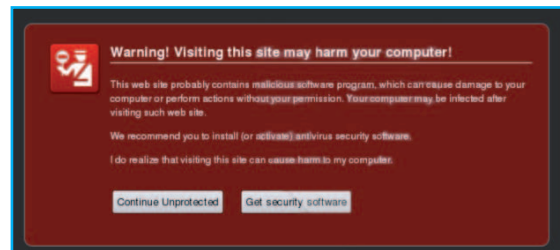
04-09 **Klanten van T-Online** in Duitsland moeten af en toe dagenlang op hun e-mails wachten. Enkele computers van klanten zijn geïnfecteerd en werken samen in een **botnet** om spam te verspreiden. De vertraging van de e-maildienst wordt opgelost door de verbinding van de zombiecomputers met het internet te verbreken.

08-09 **Opmerkelijk:** een vindingrijke **Oostenrijker** heeft het **ongecodeerde gegevensverkeer** tussen een centrale en mobiele eenheden van de brandweer, hulpdiensten en het ziekenvervoer afgeluisterd. Zo achterhaalde hij informatie over de interventieplaatsen, patiëntgegevens en details over de interventies.

14-09 Bezoekers van de **website van de New York Times** worden het slachtoffer van een **social engineering-aanval**. Hackers hebben scareware-reclamebanners op de startpagina gezet en nietsvermoedende bezoekers aangespoord tot het downloaden van betalende en valse antivirussoftware.

15-09 Najat M'jid Maalla, rapporteur van de VN, wijst op een drastische **toename van websites met kinderpornografie**. Ze licht toe dat het aantal webpagina's met massaal misbruik is verviervoudigd tussen 2003 en 2007. Volgens schattingen van UNICEF zijn er meer dan vier miljoen van dergelijke websites in omloop.

- 16-09 **Opmerkelijk:** in de VS heeft een man zijn **twee gestolen laptops** kunnen opsporen met behulp van een **remote access**-programma. De man kon de daders via remote access in het oog houden wanneer ze surfen, chatten, e-mails schreven, videochatten en pornosites bezochten en filmde alles met een videocamera. De **politie** moest de daders enkel nog arresteren.
- 18-09 **Microsoft** dient een klacht in tegen bedrijven die zich bezighouden met zogenaamde **malvertising**. In het eerste proces van deze soort wil Microsoft de verspreiding van onbetrouwbare reclamebanners met schadelijke code tegengaan.
- 21-09 Met het **Trojaanse paard** "Trojan.FakeAlert.BFW" geïnfecteerde systemen sturen het volledige URL-verkeer naar een valse beveiligingswaarschuwing. Deze waarschuwing imiteert die van de browser Firefox en spoort gebruikers aan tot de installatie van de **scareware** "Personal Antivirus".



Screenshot 1: de valse beveiligingswaarschuwing van de scareware "Personal Antivirus"

Oktober 2009

- 01-10 **Crackers** hebben de **captcha**-veiligheidsvraag van **Facebook** gekraakt en zijn in staat om automatisch profielen aan te maken. De aangemaakte profielen lokken gebruikers dan via een link naar een zogenaamde video en proberen de gebruiker te overhalen tot de installatie van valse antivirussoftware (rogueware).
- 02-10 **Google** verwijdert de startpagina van de illegale file-sharing-service "**The Pirate Bay**" en zeven andere websites die behoren tot de BitTorrent Tracker-website uit zijn zoekresultaten.
- 06-10 Een lijst met tienduizenden gebruikersnamen en bijbehorende wachtwoorden van Microsoft Live Hotmail-account duikt op het net op. De gegevens werden waarschijnlijk bemachtigd door **phishing-aanvallen** en in de lijst samengevoegd. Niet veel later wordt bekend dat ook accounts van Yahoo, Gmail, Comcast en Earthlink getroffen zijn.
- 07-10 **Opmerkelijk:** de **directeur van de FBI**, Robert Mueller, wordt bijna het slachtoffer van een **phishing-e-mail** van een bank. Naar eigen zeggen zag de mail er verbluffend echt uit en was hij bijna ingegaan op de vraag om zijn gegevens te verifiëren, tot hij begreep wat er aan de hand was. Zijn vrouw legt hem vervolgens een verbod op online banking op.
- 08-10 De **FBI-operatie "Phish Fry"** leidt tot de aanklacht van 100 personen in verband met phishing-aanvallen. Het systeem van phishers: Egyptische hackers sporen **persoonlijke gegevens en bankgegevens** van slachtoffers op, sturen deze door naar Amerikaanse "collega's", die de gegevens misbruiken voor illegale financiële transacties.
- 08-10 Het zes maanden durende **pilootproject De-Mail** gaat van start in Berlijn. De-Mail moet in Duitsland als gecodeerde elektronische verzenddienst de uitwisseling van rechtsgeldige documenten mogelijk maken.

- 09-10 **Zombiecomputers** die deel uitmaken van het **Bahama-botnet** leiden surfers om naar bedrieglijk echt uitzierende kopieën van websites, in plaats van de echte website te laden. De zoeksites van Google, Bing en Yahoo worden het zwaarst getroffen. Het doel van de actie: geld verdienen door klikfraude.
- 17-10 De website **netzpolitik.org** krijgt een gegevensrecord met persoonlijke **gegevens** van meer dan honderdduizend gebruikers van de Duitse portal **schülerVZ** doorgespeeld. De gegevens werden met behulp van een programma voor gegevensverzameling (crawler) verzameld.
- 19-10 Een Zweedse rechtbank verdaagt het **proces** tussen leden van de illegale P2P-site "**The Pirate Bay**" en de entertainmentindustrie tot de zomer van 2010. Twee rechters van het proces worden beschuldigd van partijdigheid. Het proces had moeten beginnen op 13 november 2009.
- 23-10 De firma Click Forensics publiceert een rapport waaruit blijkt dat in het derde kwartaal van 2009 42,6 % van de **frauduleuze kliks (click fraud)** afkomstig zijn van computers uit botnets - een stijging van 5,7 %.
- 31-10 De twee weken eerder gearresteerde 20-jarige die de gebruikersgegevens van de Duitse online community **schülerVZ** heeft uitgelezen, pleegt **zelfmoord** in zijn cel.

November 2009

- 01-11 De **worm Conficker** heeft deze week ongeveer zijn **zeven miljoenste slachtoffer** geïnfecteerd. Door zijn combinatie van verspreidings-, vermommings- en beveiligingsmechanismen is dit de meest succesvolle malware van het jaar.
- 03-11 In Manchester wordt een 20-jarig koppel gearresteerd. De twee zijn de vermoedelijke **verspreiders** van de **spyware Zbot**. Deze spyware steelt gegevens van online banking, creditcardgegevens en wachtwoorden. Dit is de eerste arrestatie van deze aard in Europa.
- 05-11 **Opmerkelijk:** Macintosh-computers kunnen worden aangevallen door een "schadelijk programma". Het schadelijke programma is nagemaakt op het spel Space Invaders en verwijdert een bestand uit de map "Documenten" van zodra men in het spel "**Lose/Lose**" een alien neerschiet. De ontwikkelaar wijst de spelers daar vóór het spel zelfs uitdrukkelijk op.

Screenshot 2: spelscène uit "Lose/Lose"



- 10-11 De auteurs van "**Koobface**" slagen er voor het eerst in een variant te programmeren die zich in het sociale netwerk Facebook als een mens gedraagt. De malware registreert accounts, maakt een normaal uitzierend profiel aan, verstuurt uitnodigingen voor vriendschap en plaatst zelfs berichten op de prikborden van andere gebruikers.
- 17-11 Het Britse **T-Mobile** is verwickeld in een gegevensschandaal. Medewerkers hebben gegevens van duizenden klanten verkocht aan een verdeler.

- 20-11 **Microsoft** is verplicht om te reageren. Crackers posten een **zero-day-exploit** voor de webbrowsers Internet Explorer 5, 6 en 7. De code is weliswaar niet in alle gevallen en op alle computers schadelijk, toch werken crackers ijverig om de code te optimaliseren.
- 24-11 Slag tegen de **online criminaliteit**. Meer dan 200 politieagenten uit Duitsland en Oostenrijk voeren **razzia's** uit in 50 woningen en nemen vier personen in voorlopige hechtenis. De verdachten worden ervan beschuldigd gestolen creditcardgegevens, toegangsgegevens, rekeninggegevens en schadelijke software te hebben geruild en verhandeld. De "Elite Crew" zou bovendien een botnet met meer dan 100.000 computers onder zijn controle hebben.
- 24-11 In de VS wordt de zelfverklaarde "**godfather of spam**", de 64-jarige Alan Ralsky, **veroordeeld** tot 51 maanden cel, vijf jaar voorwaardelijk en een geldboete van 250.000 USD. Hij verspreidde samen met zijn handlangers, die ook aanzienlijke straffen kregen, op grote schaal e-mails met spam.
- 25-11 **Opmerkelijk**: Zuid-Korea legt het sms-verkeer aan banden. De strijd van **Zuid-Korea** tegen **spam** heeft gevolgen voor de sector van de mobiele telefonie. Per mobiele telefoon mogen dagelijks nog maximaal 500 **sms'en** worden verzonden. Hoewel er in de republiek aanzienlijke straffen staan op de verspreiding van ongewenste berichten, is de stroom aan spam extreem hoog. Statistisch gezien bezat in oktober 98 % van de Zuid-Koreaanse bevolking een mobiele telefoon, wat overeenkomt met 47,7 miljoen toestellen.
- 27-11 Een nieuwe **spamgolf** treft vooral **spelers van World of Warcraft**. Een e-mail met foto's van jonge, Aziatische vrouwen zet ontvangers aan om op de video in de bijlage te klikken, die zich ontpopt als een Trojaans paard en gericht WoW-accountgegevens bespioneert.
- 29-11 Opmerkelijk: het Engelstalige "top word 2009" is "Twitter", volgens de beheerder van de website Global Language Monitor. "Twitter" verbant de woorden "Obama", "H1N1", "stimulus" en "vampier" naar de plaatsen twee tot vijf. De woorden van het decennium waren "klimaatopwarming", "9/11" en "Obama".

December 2009

- 04-12 De gebruikers van het **virtuele hotel "Habbo"** worden geconfronteerd met een internationale golf van **phishing-aanvallen**. Online criminelen proberen met phishing-websites de toegangsgegevens en creditcardgegevens van spelers te bekomen. Ook frauduleuze blogberichten worden steeds talrijker. Het opvallendste is: de online game richt zich vooral op kinderen en jongeren.



Screenshot 3: gebruikers van het virtuele Habbo-hotel worden in de val gelokt door bedriegers

- 06-12 De Duitse **kinderportal** haefft.de is volgens **Chaos Computer Club** helemaal niet beveiligd tegen gegevensdieven. De CCC maakt bekend dat ze zonder een wachtwoord en volledig zonder technische manipulatie vrij binnen de community konden bewegen en zo gegevens bemachtigen. De website wordt van het net gehaald.
- 08-12 Service "WLAN-codering kraken": een onderneming uit de VS biedt aan om met 400 cloud-CPU's en **woordenboekaanvallen** de **WPA-codering** van een mobiel net in 20 minuten te kraken. Kostprijs: 34 USD.
- 15-12 In de programma's Adobe Reader en Adobe Acrobat 9.2 en ouder wordt een **tot dan toe- onbekende zwakke plek** in de functie "Doc.media.newPlayer" bekendgemaakt. Via deze weg kunnen aanvallers in het ergste geval het getroffen systeem overnemen. Adobe kondigt de patch aan voor 12 januari 2010.
- 16-12 De **illegale kopieerder** van de film "X-Men Origins: Wolverine" wordt na negen maanden speurwerk gearresteerd in New York. De 47-jarige heeft de onafgewerkte film verspreid via file-sharing-netwerken voordat hij in de bioscoop te zien was, maar blijkt toch niet de eigenlijke bron te zijn. Het is nog niet bekend wie de film oorspronkelijk stal.
- 17-12 Een aanval op **Twitter** legt de startpagina lam door **gemanipuleerde DNS-berichten** en toont een website van het "Iranian Cyber Army". De beheerders van Twitter vermoeden dat de achterliggende reden een aanval tegen Twitter als aanbieder en niet tegen de gebruikers is. Er is geen verdere schade bekend.