

German
Data
Security



G Data

Malware-rapport

Halfjaarlijks rapport januari-juni 2009

Ralf Benzmüller & Werner Klier
G Data SecurityLabs



Go safe. Go safer. G Data.

G Data Malware-rapport Januari-juni 2009

Ralf Benzmüller & Werner Klier

G Data SecurityLabs



In één oogopslag

Cijfers en informatie

- In de eerste helft van 2009 identificeerde G Data 663.952 nieuwe schadelijke programma's. Dat zijn er ruim dubbel zoveel als in dezelfde periode vorig jaar. In vergelijking met de tweede helft van 2008, is slechts sprake van een lichte stijging van 15%. Het aantal actieve malwarefamilies daalde met 7%.
- De meest voorkomende categorieën schadelijke bestanden zijn Trojaanse paarden, downloaders en de backdoors. Terwijl de Trojaanse paarden en downloaders hun positie wisten uit te bouwen, daalde het aandeel backdoors. Daarnaast nemen Rootkits verder toe: Hun aantal is ten opzichte van dezelfde periode vorig jaar meer dan verachtvoudigd.
- Malware met eigen verspreidingsroutines vormt slechts 4,0% van de schadelijke computerprogramma's.
- Tot de meest actieve malwaretypen behoren Trojaanse paarden, backdoors en online-game-accountstellers. Eveneens toegenomen is de wormfamilie "Autorun". Het aantal van deze schadelijke bestanden is in vergelijking met de eerste helft van 2008 bijna vervijfvoudigd tot 1,6%.
- Van alle malware van de tweede helft van het jaar draait 99,3% onder Windows. De focus op de marktleider in besturingssystemen zet zich dus voort.
- Schadelijke code voor mobiele platformen heeft dit keer een positie in de top 5 van de platformen behaald. Met 106 schadelijke bestanden blijft dit aandeel echter nog steeds op een laag niveau.
- Ook gebruikers van MacOS X worden door malware aangevallen. Het aantal nieuwe schadelijke programma's voor MacOS X bedraagt 15. Het eerste botnet van Apple-computers werd in april ontdekt.

Gebeurtenissen en trends

- Sociale netwerken worden steeds vaker voor de verspreiding van spam en malware gebruikt.
- Conficker ontwikkelde zich tot een succesnummer. Hij infecteerde miljoenen pc's en haalde op 1 april met een nieuwe update-routine het nieuws. Daarna werd het stil.

Prognoses

- Steeds meer schadelijke code verplaatst zich naar internet. De infectiemethoden worden steeds geavanceerder.
- De malware-stroom zal in de komende maanden weliswaar toenemen, maar op basis van nog minder malwarefamilies. Ook zal de groei verder stagneren.
- Gebruikers van MacOS X en smartphones zullen steeds vaker het doelwit worden van auteurs van malware.

Inhoud

In één oogopslag	2
Cijfers en informatie.....	2
Gebeurtenissen en trends	2
Prognoses.....	2
Inhoud	3
De Malware-stroom stijgt verder - maar in minder mate	4
Malware-categorieën	4
Familiebanden	6
Platformen	8
Vooruitzicht 2009	9
Prognoses.....	9
Gebeurtenissen en trends in de eerste helft van 2009	10
Januari 2009	10
Februari 2009	11
Maart 2009.....	13
April 2009	14
Mei 2009	15
Juni 2009.....	16

Malware: Cijfers en informatie

De Malware-stroom stijgt verder - maar in minder mate

In de afgelopen jaren is het aantal nieuwe schadelijke programma's continu gestegen. Met steeds hogere groeicijfers werden steeds weer nieuwe records behaald. Ook in de eerste helft van 2009 is het aantal schadelijke computerprogramma's opnieuw gestegen. In vergelijking met dezelfde periode van vorig jaar is het aantal meer dan verdubbeld tot 663.952. Maar zoals we in het laatste G Data malware-rapport hebben aangekondigd, is de groeisnelheid afgenomen. In vergelijking met de tweede helft van 2008 is het aantal schadelijke programma's met slechts 15% gestegen.

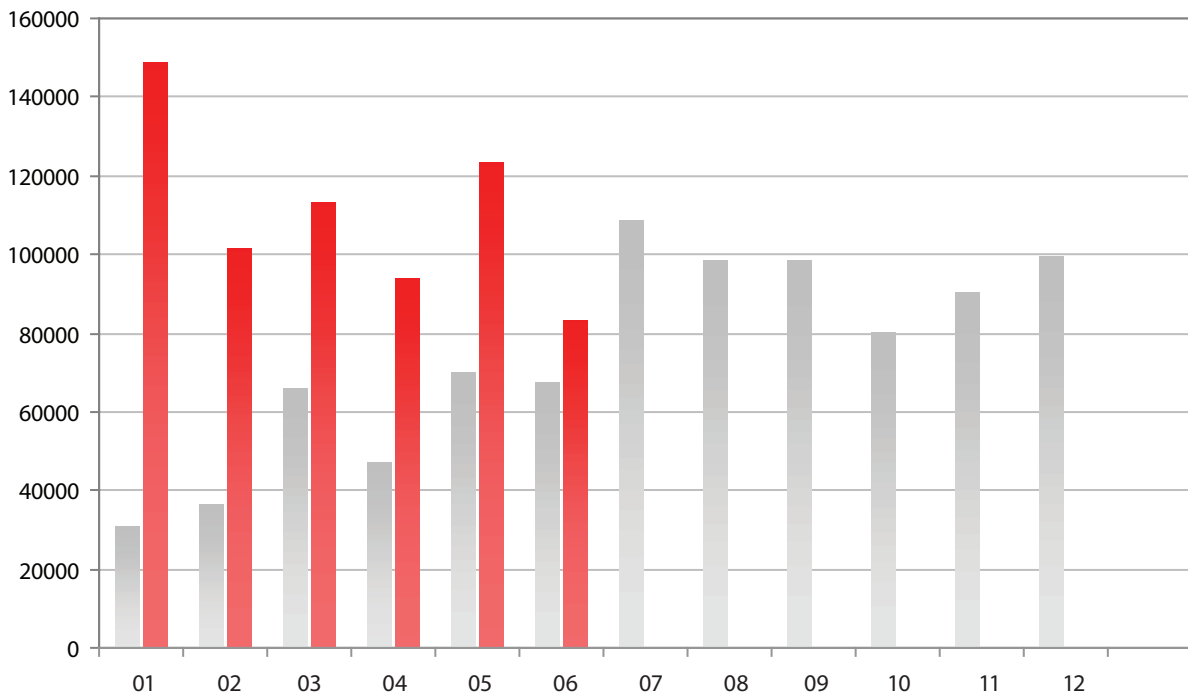


Diagram 1: Aantal nieuwe malware per maand voor 2008 (grijs) en 2009 (rood).

Malware-categorieën

Een kijk op de veranderingen bij de afzonderlijke categorieën van malware geeft een verklaring voor deze daling. Terwijl backdoors, adware en spyware onder het gemiddelde blijven, overtreft het aantal rootkits en Trojaanse paarden de gemiddelde toename duidelijk. Ook het aantal downloaders en droppers ligt boven het gemiddelde.

Backdoors worden gebruikt om zombie-computers in een botnet te integreren en op afstand bestuurbaar te maken. Een daling op dit gebied is een teken dat de uitbreiding van botnets aan belang heeft ingeboet. De sterke toename van rootkits wijst erop dat steeds meer schadelijke bestanden (ook backdoors) voor de virusbeveiliging en nieuwsgierige ogen worden verborgen. Blijkbaar zijn de beschikbare capaciteiten voldoende om de vraag naar botnet-activiteiten, zoals spamverzending en DDoS-aanvallen, uit te voeren. Ook de adware-markt schijnt op hoog niveau te stagneren. Mogelijk werken hier awareness-campagnes. Maar ook de in de huidige economische crisis met daarbij behorende beperkte reclamebudgetten dragen ertoe bij dat ook in de eCrime-economie moet inbinden.

Het totaal aan spyware is licht gedaald. Wanneer wij nauwkeuriger kijken, blijkt dat het aantal keyloggers is verdubbeld, terwijl bankingtrojanen en gegevensdieven voor wachtwoorden of online-spellen met ca. 30% zijn teruggelopen. De verbeterde beveiliging bij banken en exploitanten van online-spellen kunnen niet meer met eenvoudige middelen worden omzeild. Op het gebied van gegevensdiefstal gaat de trend naar steeds universele en krachtigere schadelijke programma's.

Categorie	# 2009 H1	Aan-deel	# 2008 H2	Aan-deel	Diff 2008H1 2008H2	# 2008 H1	Aan-deel	Diff 2008H1 2009H1
Trojaanse paarden	221.610	33,6%	155.167	26,9%	143%	52.087	16,4%	425%
Backdoors	104.224	15,7%	125.086	21,7%	83%	75.027	23,6%	139%
Downloaders/droppers	147.942	22,1%	115.358	20,0%	128%	64.482	20,3%	229%
Spyware	97.011	14,6%	96.081	16,7%	101%	58.872	18,5%	165%
Adware	34.813	5,3%	40.680	7,1%	86%	32.068	10,1%	109%
Wormen	26.542	4,0%	17.504	3,0%	152%	10.227	3,2%	260%
Hulpprogramma's	11.413	1,6%	7.727	1,3%	148%	12.203	3,8%	94%
Rootkits	12.229	1,9%	6.959	1,2%	176%	1.425	0,4%	858%
Exploits	2.279	0,3%	1.841	0,3%	124%	1.613	0,5%	141%
Dialers	1.153	0,2%	1013	0,2%	114%	4.760	1,5%	24%
Virussen	143	0,0%	167	0,0%	86%	327	0,1%	44%
Overige	4.593	0,7%	8.419	1,5%	55%	5.170	1,6%	89%
Totaal	663.952	100,0%	576.002	100,0%	115%	318248	100,0%	209%

Tabel 1: Het aantal en het aandeel van nieuwe malwarecategorieën in de eerste helft van 2008 en 2009 inclusief verandering

Tabel 1 geeft ook weer dat het aantal dialers tot een kwart van het volume van vorig jaar is gedaald. Het bedrijfsmodel dialer is blijkbaar niet meer in trek. Ook het aantal klassieke virussen (d.w.z. bestandsinfectoren) is in vergelijking met dezelfde periode vorig jaar duidelijk gedaald. Deze verspreidingsmethode vormt eerder de uitzondering. De wormen - waaronder ook de grote groep autorun-infectoren - wist te stijgen naar 4,0%. Hun aantal is ten opzichte van de eerste helft van 2008 met het 2,6-voudige gestegen en in vergelijking met de tweede helft van 2008 met het 1,5-voudige.

Familiebanden

Aan de hand van de functies en de eigenschappen van de gebruikte codes worden schadelijke computerprogramma's in families onderverdeeld. Sinds jaren is het aantal virusfamilies dalende. In de eerste helft van 2008 waren er nog 2395 en in de tweede helft 2094. In de eerste helft van 2009 werden 1948 verschillende vertegenwoordigers van virusfamilies geteld. Dat wil zeggen: het opnieuw gestegen aantal schadelijke programma's is gebaseerd op een gedaald aantal families. Hieruit blijkt de concentratie van de markt.

	# 2009 H1	Virusfamilie	# 2008 H2	Virusfamilie	# 2008 H1	Virusfamilie
1	34.829	Monder	45.407	Hupigon	32.383	Hupigon
2	26.879	Hupigon	35.361	OnlineGames	19.415	OnLineGames
3	18.576	Genome	20.708	Monder	13.922	Virtumonde
4	16.719	OnlineGames	18.718	MonderB	11.933	Magania
5	16.675	Buzus	15.937	Cinmus	7.370	FenomenGame
6	13.889	Fraudload	13.133	Buzus	7.151	Buzus
7	13.104	Bifrose	13.104	Magania	6.779	Zlob
8	11.106	Inject	12.805	PcClient	6.247	Cinmus
9	10.322	Poison	11.530	Zlob	6.194	Banload
10	10.312	Magania	10.412	Virtumonde	5.433	Bifrose

Tabel 2: Top 10 van de meest actieve virusfamilies in de eerste helft van 2009 en 2008

Terwijl sommige families slechts uit een handje vol varianten bestaan, zijn andere zeer productief. Enkele daarvan staan al jaren in de top 10. Hiertoe behoren de backdoors van de Hupigon- en Bifrose-familie, die hun topositie hebben verloren, de gegevensdieven voor online-spellen uit de families OnlineGames en Magania en de Trojaanse paarden van de familie Buzus. De nieuwe koplopers zijn de Adware/Scareware-trojanen van Monder, die in de voetsporen van Virtumonde treden. Samen met de nieuweling Fraudload laten zij zien hoe populair Scareware met vervalste virusbeschermingsoplossingen bij cybercriminelen geworden is. Nieuw in de top 10 zijn tevens de families Genome, Poison en Inject.

Plaats 1: Monder

De talloze Monder-varianten zijn Trojaanse paarden die op het geïnfecteerde systeem veiligheidsinstellingen manipuleren en het systeem op deze manier kwetsbaar maken voor verdere aanvallen. Aanvullend kan een infectie met Adware volgen die ongewenste reclamespotjes op het geïnfecteerde systeem weer geeft, in het bijzonder voor vervalste beveiligingssoftware. Het slachtoffer denkt dat het systeem op infecties wordt onderzocht. Om deze zogenoemde infecties te verwijderen, wordt het slachtoffer ertoe overgehaald de "volledige versie" te kopen en per creditcard (!!) te betalen. Enkele varianten downloaden aanvullende schadelijke software en geven de aanvaller gegevens door over het surfgedrag van het slachtoffer, zonder dat de gebruiker hierover wordt geïnformeerd.

Plaats 2: Hupigon

De backdoor Hupigon maakt het voor de aanvaller onder andere mogelijk de pc op afstand te bedienen, toetsenbordaanslagen te bekijken, toegang tot het bestandssysteem te krijgen en de webcam in te schakelen.

Plaats 3: Genome

De trojanen van de familie Genome combineren functionaliteiten zoals downloaders, keyloggers of bestandscodering.

Plaats 4: Buzus

Trojaanse paarden van de Buzus-familie doorzoeken geïnfecteerde systemen van de slachtoffers naar persoonlijke gegevens (creditcards, online-banking, e-mail en FTP-toegangen) die aan de aanvaller worden doorgegeven. Bovendien wordt geprobeerd veiligheidsinstellingen van de computer te verlagen en het systeem van het slachtoffer daardoor extra kwetsbaar te maken.

Plaats 5: OnlineGames

De leden van de OnlineGames-familie stelen vooral de toegangsgegevens van online-spellen. Hiervoor worden bepaalde bestanden en registry-gegevens doorzocht en/of een keylogger geïnstalleerd. In het laatstgenoemde geval worden dan niet alleen de gegevens van spellen gestolen. De aanvallen zijn voornamelijk gericht op games die in Azië populair zijn.

Plaats 6: Fraudload

De Fraudload-familie omvat talloze varianten van zogenoemde Scareware-programma's die zich bij de gebruiker presenteren als zijnde beveiligingssoftware of systeemtool. Het slachtoffer denkt dat het systeem op infecties wordt onderzocht. Om deze zogenoemde infecties te verwijderen, wordt het slachtoffer ertoe overgehaald de "volledige versie" te kopen en zijn creditcardgegevens op een speciale website in te voeren. De infectie geschiedt doorgaans via ongepatchte veiligheidshiaten in het besturingssysteem of via kwetsbare toepassingssoftware van het slachtoffer. Er bestaan echter ook aanvalsmethoden waarbij het slachtoffer naar pagina's wordt gelokt waarop zogenoemde video's met erotische inhoud of nieuwsberichten te zien zijn. Om de zogenaamde video's te kunnen bekijken, moet het slachtoffer een speciale video-codec installeren waarin de schadelijke software is verstopt.

Plaats 7: Bifrose

Via de backdoor Bifrose krijgen de aanvallers toegang tot geïnfecteerde computers en koppelen deze aan een IRC-computer. Vanaf hier ontvangt het schadelijke programma commando's van de aanvaller.

Plaats 8: Poison

Via de Poison-backdoor krijgt de aanvaller ongeautoriseerde toegang op afstand tot het systeem van het slachtoffer dat vervolgens bijv. voor verdeelde DDoS-aanvallen kan worden misbruikt.

Plaats 9: Magania

Trojaanse paarden van de uit China afkomstige Magania-familie hebben zich op de diefstal van gaming-accountgegevens van de Taiwanese softwarefabrikant Gamania gespecialiseerd. Doorgaans worden Magania-exemplaren via mail verspreid, 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 aanvullende bestanden in het systeem worden opgeslagen. Bovendien nestelt Magania zich per DLL in Internet Explorer en kan op deze manier alle webverkeer meelesen.

Plaats 10: Inject

De Inject-familie omvat een groot aantal Trojaanse paarden die zich in lopende processen nestelen en op deze manier de controle over het betreffende proces kunnen overnemen. Hierdoor kan de aanvaller de betreffende processen naar wens in zijn voordeel manipuleren.

De meest actieve **wormfamilie** is "Autorun" met 9.689 varianten en een aandeel van 1,6%. Vertegenwoordigers van deze familie maken gebruik van het mechanisme dat bij het plaatsen van cd's/dvd's of bij het aansluiten van USB-gegevensdragers automatisch bestanden uitvoert. Hiervoor kopieert het zich op de gegevensdrager en maakt een passend bestand namens autorun.inf. Vanwege de weide verspreiding van dit schadelijke programma raden wij u aan het autorun-mechanisme van Windows te deactiveren. Om ervoor te zorgen dat dit ook daadwerkelijk lukt, heeft Microsoft een eigen patch gemaakt.

De meest voorkomende **exploits** waren gericht op het WMF-veiligheidskwaad en de zwakke plekken in PDF's. Het aantal schadelijke PDF-bestanden is in de afgelopen maanden duidelijk toegenomen. Hierbij wordt niet alleen gebruik gemaakt van veiligheidshiaten. Ook de mogelijkheid om in PDF's JavaScript-code uit te voeren, wordt bij malware-auteurs steeds populairder.

Platformen

Ook in de eerste helft van 2009 concentreerden malware-auteurs zich op Windows-computers als doelwit. Met 99,3% is het aandeel Windows-malware opnieuw gestegen. Schadelijke software voor andere besturingssystemen komt erg zelden voor. Voor Unix-gebaseerde systemen verschenen 66 schadelijke programma's (ter vergelijking: dit waren er 16 in de tweede helft van 2008) en voor OS X van Apple werden 15 nieuwe schadelijke programma's gevonden. In de tweede helft van 2008 waren dit er 6. Ook al blijkt hier een stijgende tendens van malware voor andere besturingssystemen uit, de groei hiervan blijft sterk achter bij die van Windows-malware.

	Platform	#2009 H1	% 2009 H1	#2008 H2	% 2008 H2	#2008 H1	Aandeel
1	Win32	659.009	99,3%	571.568	99,2%	312.656	98,2%
2	WebScripts	3.301	0,5%	2.961	0,5%	3.849	1,4%
3	Scripts	924	0,1%	1.062	0,2%	1.155	0,3%
4	MSIL	365	0,1%	318	0,1%	252	0,1%
5	Mobile	106	0,0%	70	0,0%	41	0,0%

Tabel 3: Top 5 platforms 2008 en in de eerste helft van 2009. WebScripts is malware die is gebaseerd op JavaScript, HTML, Flash/Shockwave, PHP of ASP en gewoonlijk de zwakke punten van de browser gebruikt. "Scripts" zijn batch- of Shell-scripts of programma's die in de scripttalen VBS, Perl, Python of Ruby zijn geschreven. MSIL is malware die opgeslagen is in de byte-code van .NET-programma's. Onder Mobile wordt malware voor J2ME, Symbian en Windows CE samengevat.

Het totaal aan nieuwe malware voor smartphones en mobiele computers is met ongeveer de helft toegenomen en schadelijke programma's voor mobiele eindapparatuur hebben weer een positie in de top 5 behaald. In totaal hebben 106 nieuwe schadelijke programma's de kop opgestoken. Circa 90 van deze schadelijke bestanden hebben geen eigen verspreidingsroutine en worden voor de verzending van SMS aan voornamelijk Russische en Chinese telefoongebruikers gebruikt. Alleen de familie Yxe verspreidt zich zelfstandig per SMS met een link op een website. Het bestand dat hier als download wordt aangeboden, is door Symbian gesigneerd. Hierdoor wordt de vereiste gebruikeractie tot één klik gereduceerd.

Vooruitzicht 2009

Met malware zal ook in de komende maanden erg veel geld worden verdiend. De eCrime-economie heeft zich een vaste plaats veroverd in de economie en de beproefde bedrijfsmodellen rond spam, spyware en adware zullen ook in de toekomst voor gevulde kassa's bij de auteurs, verspreiders en gebruikers van malware zorgen. Hieraan zullen ook de incidentele successen van de opsporingsinstanties niets veranderen. Gebruikers van Windows zullen ook in de toekomst het doelwit van cybercriminelen zijn.

De malware-stroom zal verder toenemen. Het is echter te verwachten dat het toenemende aantal op steeds minder families zal zijn gebaseerd. De groeipercentages zullen niet meer zo enorm uitvallen als in de afgelopen jaren.

Vanwege de professionaliteit van de schaduwconomie is het niet verwonderlijk dat veiligheidshiaten in het besturingssysteem en in populaire toepassingen al na enkele dagen na de publicatie ook door malware worden gebruikt. Binnen de kortste keren staan zij ook voor leken via eenvoudig te bedienen tools voor de productie van malware ter beschikking. De zwakste schakel van de keten is momenteel de browser en zijn componenten. Hier worden de meeste veiligheidshiaten gevonden en gebruikt. Wie zijn computer niet up-to-date houdt, is een makkelijk doelwit voor malware-aanvallen.

Maar ook op andere platformen wordt verder geëxperimenteerd. Het aantal schadelijke bestanden voor Apple-, Unix- en mobiele computers zal verder toenemen. Een massaal gebruik is echter (nog) niet te verwachten.

Omdat intussen veel invalspoorten voor malware door veiligheidstechnologieën beschermd zijn, wijken de aanvallers uit naar minder goed beveiligde gebieden. Hier bieden websites met hun talloze toepassingen momenteel de grootste kansen op succes. Daarom is het te verwachten dat dit gebied ook in de komende maanden met steeds nieuwe en gehaaidere aanvalsscenario's wordt gebruikt. Hierbij zouden tot nu toe onderschatte media zoals Flash of PDF in toenemende mate kunnen worden gebruikt. Ook de trukendoos van de bedriegers, waarmee internetgebruikers worden verleid tot een bezoek van een website of het uitvoeren van bestanden, zal zeker worden uitgebreid. Vooral in sociale netwerken houden wij rekening met nieuwe schijnmanoeuvres. Twitter biedt hier momenteel de meeste mogelijkheden.

Prognoses

Categorie	Trend
Trojaanse paarden	↗
Backdoors	→
Downloaders/droppers	→
Spyware	→
Adware	→
Virussen/wormen	↘
Hulpprogramma's	↗

Categorie	Trend
Rootkits	↗
Exploits	↗
Win32	↗
WebScripts	↑
Scripts	→
MSIL	→
Mobile	↑

Gebeurtenissen en trends in de eerste helft van 2009

De belangrijkste gebeurtenissen rond malware geven wij onderstaand met een tijdlijn weer. Het opvallendst zijn de gebeurtenissen rond Conficker die in de eerste maanden van het jaar veel opzien baarden. Opvallend zijn echter ook de vele gebeurtenissen in populaire sociale netwerken, zoals Twitter, LinkedIn, MySpace en Facebook. Intussen pikken malware-designers dergelijke trends razendsnel op en profiteren van de nieuwe kansen. Afgezien van de afzonderlijke gebeurtenissen blijkt er echter ook uit andere trends dat sociale netwerken aantrekkelijker worden. Voor het eind van het jaar beperkte phishing zich alleen tot banken en eBay, maar in de tweede helft van het jaar hebben Google en de sociale netwerken Facebook, Sulake en MySpace een vaste plaats gekregen in de Phishtank top 10. Sociale netwerken fungeren voor cybercriminelen al sinds enige tijd als informatiebron voor de voorbereiding van gerichte aanvallen en gepersonaliseerde spam. Sociale netwerken worden steeds populairder - ook bij auteurs van malware.

Dat blijkt vooral uit de ontwikkeling van de worm **Koobface**. In het begin - zoals uit de naam blijkt - concentreerde hij zich vooral op Facebook en daarna op MySpace als verspreidingsplatform, maar in de afgelopen maanden is de lijst uitgebreid met sociale netwerken als hi5.com, friendster.com, myyearbook.com, bebo.com, tagged.com, netlog.com, fubar.com en livejournal.com. De links die hier worden geplaatst, verwijzen naar websites waar de beproefde fraudepatronen "nep-antivirus" of "codec/Flash-download" worden toegepast. Maar Koobface neemt ook in aantal toe, zoals uit onderstaande tabel blijkt. In juni is het aantal van de varianten bijna vertienvoudigd.

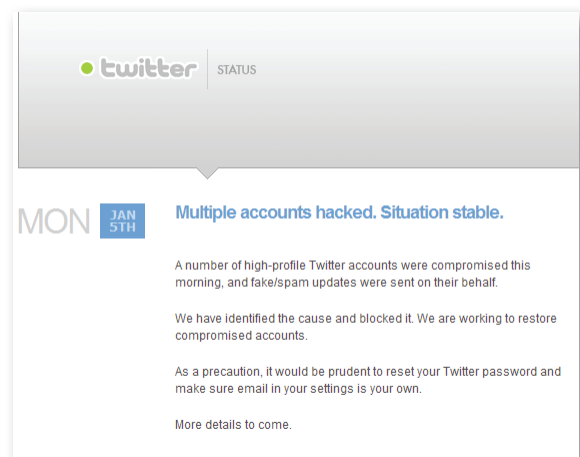
Maand	Jan 09	Feb 09	Mrt 09	Apr 09	Mei 09	Jun 09
# Varianten Koobface	18	14	23	50	56	541

Tabel 4: Aantal Koobface-varianten in de eerste helft van 2009

In de komende maanden houden wij rekening met meer malware in sociale netwerken. Met de groeiende gebruikersaantallen stijgt ook de aantrekkelijkheid voor malware-distributeurs.

Januari 2009

- 05.01. Gebruikers van de microblog Twitter worden door gerichte korte berichten naar een vervalste loginpagina van de dienst gelokt om toeganggegevens voor toekomstige spamaanvallen te stelen.
- 06-01 **Twitter** waarschuwt: "Multiple accounts hacked. Situation stable". Hierbij betrokken zijn onder andere accounts van Britney Spears en Barack Obama. Namens de slachtoffers worden deels hatelijke berichten verstuurd.



- 07-01 Op de social-networking-pagina **LinkedIn** worden valse profielen van celebrities aangemaakt. Zij bevatten links die verwijzen naar een valse virusscanner of een met Trojaanse paarden geïnfecteerde versie van Windows Media Player. Bekende slachtoffers: Victoria Beckham, Beyoncé Knowles, Salma Hayek en nog veel meer.
- 08-01 Bij de landsregering van de Oostenrijkse deelstaat Karinthië vallen 3000 computers uit door een infectie met de **Conficker**-worm. Reden: De door Microsoft al in oktober 2008 uitgebrachte veiligheidsupdate, dat een door Conficker gebruikt veiligheidsgat moet dichten, werd niet geïnstalleerd.
- 12-01 **Conficker** slaat opnieuw toe in Karinthië, dit keer in ziekenhuizen van de vereniging van verpleeginrichtingen KABEG. Hierbij zijn opnieuw ca.3000 computers betrokken.
- 14-01 Schattingen gaan uit van reeds 2.5 ml. **Conficker**-infecties. Voor het eerst wordt bekend dat Conficker via een speciaal algoritme permanent domeinnamen genereert waarmee volgens het toevalsprincipe contact wordt opgenomen. Doel: De aanvallers hebben veel toevalsdomeinen vooraf geregistreerd en kunnen deze gebruiken om nog meer schadelijke code te uploaden of geïnfecteerde computers van aanvullende instructies te voorzien.
- 21-01 De **Conficker**-epidemie breidt zich gestaag uit: Grote delen van de Britse strijdkrachten zijn getroffen.
- 23-01 Een Trojaanse kopie van de lay-out- en presentatiesoftware **iWork 09** van Apple circuleert binnen het BitTorrent-netwerk. Ongeveer 20.000 gebruikers schijnen de sinds het begin van de maand verspreide kopie al te hebben gedownload.
- 25-01 De vacaturebeurs **Monster.com** maakt bekend slachtoffer van een gegevensdiefstal te zijn geworden. Door een "onbeoorloofde toegang" op de database van het bedrijf zouden toegangsgegevens, namen, telefoonnummers, e-mailadressen en enkele demografische gegevens buit gemaakt zijn.

Februari 2009

- 01-02 Door een veiligheidsgat kan in de betaversie van **Windows 7** met behulp van een eenvoudige script de gebruikersaccountbesturing (UAC) buiten werking worden gesteld, waardoor aanvallers ongemerkt aanvullende schadelijke code op het besturingssysteem kunnen achterlaten.
- 02-02 Aanvallers manipuleren de website van de krant **Hamburger Abendblatts** om bezoekers van de webpagina's met schadelijke software te infecteren.
- 04-02 Via een vervalste loginpagina van het bij RTL behorende sociale netwerk **wer-kennt-wen.de** worden toegangsgegevens van de gebruikers gestolen.
- 08-02 Via een gericht verdeelde **Denial-of-Service**-aanval worden diverse security-websites zoals Metasploit, Milw0rm of Packetstorm tijdelijk uit de lucht gehaald.
- 10-02 Slechts twee dagen na de eerste aanval is de website van het project **Metasploit** opnieuw het doelwit van een DDoS-aanval. De aanvallers kiezen meerdere keren voor een andere aanvalstechniek.

- 11-02 Via een daags tevoren bekend geworden veiligheidsgat in het content-managementsysteem **Typo 3** worden diverse Duitstalige websites, die de betreffende veiligheidsupdate nog niet hebben geïnstalleerd, gemanipuleerd. Getroffen wordt bijv. de website van **FC Schalke 04**, waar over het ontslag van Kevin Kuranyi verslag wordt gedaan, of de website van Wolfgang Schäuble, waar een link over het thema dataretentie wordt geplaatst.



- 12-02 **Microsoft** looft een **beloning** van 250.000 dollar uit voor de arrestatie en berechting van de grondlegger van de **Conficker**-worm. Tegelijkertijd kondigt de softwarefabrikant aan voor de beperking van de toenemende infectie nauw samen te werken met de ICANN en de exploitanten van centrale DNS-servers.
- 14-02 Honderden computers van de Duitse Bundeswehr worden door **Conficker** getroffen.
- 17-02 Op grond van een verkeerde routerconfiguratie bij een Tsjechische internetprovider wordt de stabiliteit van de gegevensoverdracht in enkele delen van het wereldwijde internet sterk verstoord.
- 23-02 Malware-onderzoekers analyseren de varianten B en B++ van de Conficker-worm en stellen vast dat deze door hun modulaire structuur nog veel flexibeler kunnen functioneren dan de oorspronkelijke A-variant.
- 25-02 Met behulp van geprepareerde Flash-banners verdelen aanvallers via de website van het online-tijdschrift eWeek en andere websites van het Ziff-Davis-netwerk gemanipuleerde PDF-documenten die een vervalste antivirussoftware op de computers van de slachtoffers installeren.

Maart 2009

- 01-03 Malware-onderzoekers ontcijferen het algoritme dat wordt gebruikt door **Conficker** om domeinnamen van een controlserver te genereren. Hij maakt ook namen aan die al worden gebruikt. In de loop van de maand maart worden de legitieme domeinen jogli.com (muziek-zoekmachine), wnsux.com (luchtvaartmaatschappij Southwest-Airlines), qhflh.com (Chinees vrouwen netwerk) en praat.org (audio-Analyse) door verbindingsoogingen van Conficker-computers gestoord.
- 04-03 Een team van specialisten van de recherche Baden-Württemberg legt het illegale handelsplatform **codesoft.cc** stil waar Trojaanse paarden en illegale informatie over het stelen van gegevens en het vervalsen van creditcards te koop worden aangeboden.



- 09-03 **Conficker** gebruikt een nieuw algoritme dat in plaats van 250 nu 50.000 domeinen per dag berekent. Bovendien worden op geïnfecteerde computers processen beëindigd die bepaalde tekenreeksen bevatten die met speciaal tegen de worm gerichte analysetools in verbinding staan. De schadelijke code verdedigt zich dus actief tegen maatregelen voor de beperking van de epidemie.
- 12-03 De Britse tv-zender **BBC** neemt naar aanleiding van een onderzoek de controle over een **botnet** met rond 22.000 computers over. Omdat na de overname verwijten jegens de BBC volgen, laat de zender weten dat het onderzoek in het publieke belang is en dus voldoet aan de richtlijnen van de Britse media-inspectiedienst OFCOM. De vraag of voor de overname van het botnet geld is betaald, wordt door de BBC niet beantwoord.



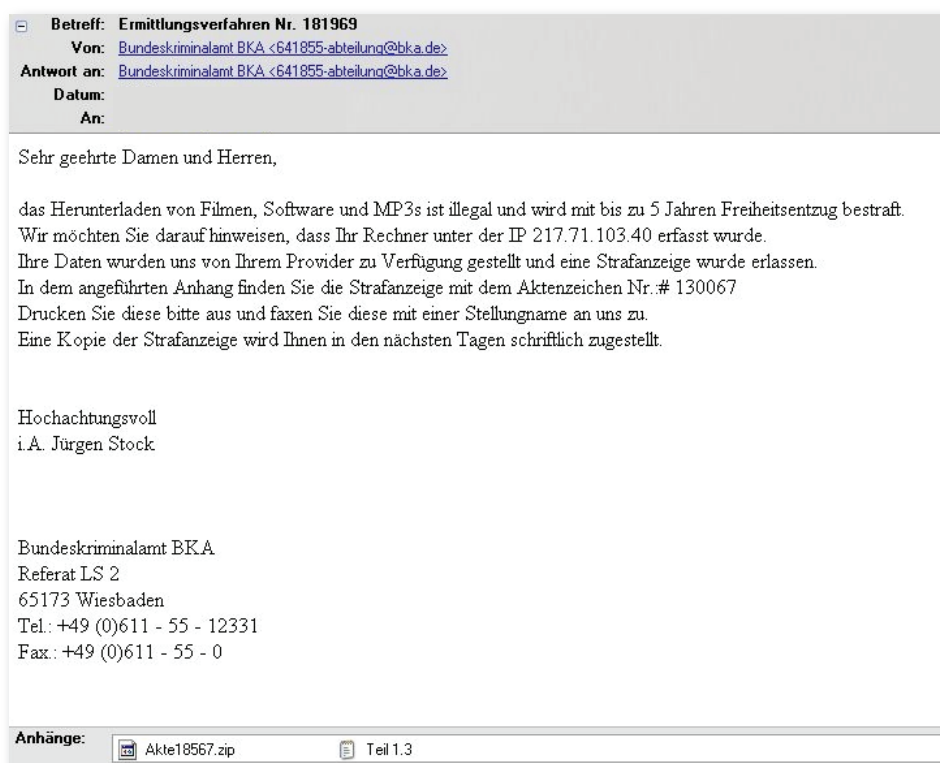
- 17-03 Door gebruik te maken van het authentiek lijkende domein `dhl-packstation.info` lokken internetcriminelen binnen het kader van een phishing-campagne **Packstation**-gebruikers naar een vervalste loginpagina om hun toegangsgegevens te stelen.
- 23-03 **DSL-routers** van het type Netcomm NB5 zijn op grond van een verouderde firmware per webinterface en SSH-toegang via internet zonder wachtwoord manipuleerbaar en vormen een botnet genaamd **Psybot**, diens grootte op 80.000 tot 100.000 geïnfecteerde routers wordt geschat.
- 30-03 Volgens informatie van experts zal **Conficker** op 1 april beginnen de talloze, door zijn algoritme gegenereerde domeinen naar updates te doorzoeken. Wat door de contactopname precies zal gebeuren, weet op dit moment niemand.
- 31-03 De brede media-interesse voor **Conficker** zorgt ervoor dat meelopers het plan opvatten gemanipuleerde websites met zogenaamde desinfectietools in de trefferlijsten van de zoekmachine Google te plaatsen. In werkelijkheid gaat het bij de zogenaamd nuttige tools om **Scareware**, dus vervalste antivirussoftware, die het slachtoffer wijsmaakt dat de computer is geïnfecteerd en dat hij/zij creditcardgegevens moet doorgeven.

April 2009

- 01-04 De verwachte update-pogingen van **Conficker** lopen in het begin op niets uit. Geïnfecteerde systemen nemen weliswaar zoals verwacht contact met bepaalde domeinen op. Vermoedelijk staat hier op dat moment echter nog geen update klaar.
- 09-04 Tegen de oorspronkelijke verwachtingen in, laadt **Conficker** updates niet via de door een algoritme gegenereerde domeinnamen. In plaats daarvan maakt hij gebruik van een alternatief P2P-mechanisme en communiceert zo direct met andere geïnfecteerde systemen. De nieuwe variant blokkeert gericht de toegang tot websites van antivirusfabrikanten om de toegang tot speciale removal-tools te bemoeilijken.
- 12-04 **Conficker** laadt van een Oekraïense server de scareware "SpywareProtect2009" die op de systemen van de slachtoffers vervalste viruswaarschuwingen uitgeeft. Voor de verwijdering van de gemelde (en in feite niet bestaande) schadelijke programma's moet het slachtoffer 49,95 dollar betalen.
- 18-04 Veiligheidsexperts ontdekken aanwijzingen voor een eerste **botnet van Apple-computers**. Blijkbaar bestaat er een relatie met de aan het begin van het jaar ontdekte Trojaanse versies van iWork 09 van Apple uit de ruilbeurs BitTorrent. Er zou ook een Trojaanse versie van Adobe Photoshop CS4 in omloop zijn.
- 22-04 Het **grootste ooit ontdekte botnet** ter wereld wordt opgespoord. Het omvat bijna twee miljoen geïnfecteerde zombie-pc's. Exploitant is vermoedelijk lid van een bende van slechts zes personen die in de Oekraïne de bijbehorende Command & Control-server exploiteert.
- 23-04 In het Russische deel van het World Wide Web duikt een **Trojaans paard** dat de toegang tot een Windows-pc blokkeert en voor de vrijgave **loggeld** eist. Getroffen gebruikers moeten een SMS aan een erg duur premium-nummer sturen en zouden vervolgens een vrijgavecode ontvangen.

Mei 2009

- 07-05 Uit een studie van het telecommunicatieconcern BT blijkt dat gegevens van gebruikte **vaste schijven** voor de doorverkoop vaak ontoereikend worden verwijderd en mogelijk zeer gevoelige gegevens kunnen bevatten. Bij een testkoop van 300 gebruikte vaste schijven vonden de experts onder andere vertrouwelijke details over testreeksen van een Amerikaans raketafweersysteem en blauwdrukken van het Amerikaanse wapenconcern Lockheed Martin.
- 08-05 Volgens een verslag van de Amerikaanse luchtvaartinspectiedienst FAA zouden in de afgelopen jaren meerde keren **hackers in systemen van de vluchtbewaking zijn binnengedrongen**. De hackers zouden toegang verkregen hebben tot bijna 50.000 persoonlijke gegevensrecords van FAA-medewerkers. Bovendien hadden zij de mogelijkheid belangrijke servers uit te schakelen.
- 09-05 Vervalste installatiepakketten van een vermeende Release Candidate van **Windows 7** bevatten een **Trojaans paard** dat tijdens de uitvoering van de set-up wordt geactiveerd.
- 24-05 De **Duitse recherche** waarschuwt voor valse mails die namens de recherche worden verstuurd en de ontvangers verzoeken een boete te betalen vanwege een zogenoemde door de recherche opgestelde aangifte voor het illegaal downloaden van films, software en MP3-bestanden.



- 30-05 Door een artikel van het tijdschrift InformationWeek wordt bekend dat Turkse activisten meerdere keren **webservers van de US-Army gekaapt** zouden hebben. Toegangen tot de getroffen websites werden naar andere websites omgeleid waarop politieke leuzen stonden.

Juni 2009

- 03-06 Tienduizenden legitieme websites worden het slachtoffer van een **massahack**. Bezoekers van de gemanipuleerde websites worden naar een Oekraïense server omgeleid die exploits voor Internet Explorer, Firefox en Quicktime verspreid.
- 05-06 De Californische Internet-Service-Provider **Pricewert LLC**, die ook onder de aliasnamen **3FN** en **APS Telecom** actief is, wordt onder druk van de Amerikaanse handelsinspectiedienst FTC van het net gehaald. Naast de hosting van Command & Control-servers voor de besturing van ruim 4500 Spyware-programma's zou het bedrijf actief criminelen hebben gerekruteerd en de vervolging van illegale inhoud gericht hebben bemoeilijkt. In tegenstelling tot de ingrijpende shutdown van McColo in november 2008 heeft deze actie slechts weinig effect op de verzending van spam en malware.
- 09-06 Onbekenden dringen in de systemen van de Britse webhost **VAserv** in en manipuleren of verwijderen gegevens van meer dan 100.000 daar gehoste websites.
- 17-06 Rond 2,2 miljoen URL's van de URL-verkortingsdienst **cli.gs** worden gemanipuleerd en naar een ander doel omgeleid.
- 24-06 Het Pentagon stelt in opdracht van de Amerikaanse minister van Defensie een **Cyber-war-commando** in dat in staat moet zijn aanvallen op de globale veiligheidsomgeving te verhinderen.
- 25-06 Het Openbaar Ministerie van Hannover doet onderzoek vanwege massale oplichting van computergebruikers door exploitanten van de website **mega-downloads.net** en bevriest binnen het kader van het onderzoek o.a. bedrijfsrekeningen van bijna een miljoen euro. Volgens schattingen van consumentencentrales zijn per maand bijna 20.000 computergebruikers door abonnementsfraude opgelicht.

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