Rapport

# McAfee-dreigingsrapport: eerste kwartaal 2009

Door McAfee® Avert® Labs

# Inhoudsopgave

Het *McAfee-dreigingsrapport* bevat de laatste statistieken en analyses over e-mail- en internetdreigingen. Dit kwartaalrapport is opgesteld door de onderzoekers van McAfee Avert Labs. Het wereldwijde onderzoeksteam van Avert Labs biedt een uniek perspectief op het dreigingslandschap, variërend van consumenten tot ondernemingen en van de Verenigde Staten tot allerlei landen over de hele wereld. Dit rapport bevat de resultaten van het onderzoek naar de belangrijkste beveiligingsproblemen van de afgelopen drie maanden. Als u na het lezen van dit rapport behoefte hebt aan meer informatie, kunt u terecht bij het McAfee Threat Center op: http://www.mcafee.com/us/threat_center/default.asp, of www.trustedsource.org.

In het eerste kwartaal van 2009 heeft het dreigingslandschap veel belangrijke wijzigingen ondergaan, vergeleken met een jaar of zelfs enkele maanden geleden. Een jaar geleden had niemand gedacht dat de hoeveelheid spam zou afnemen, maar dankzij de sluiting van McColo in november 2008 gebeurde dat wel. Momenteel is het spamniveau nog steeds 30 procent lager dan het hoogst gemeten niveau. Ook de gebruikelijke toename in maart heeft zich dit jaar niet voorgedaan. De vraag is echter niet *of* maar *wanneer* het oude niveau weer zal worden bereikt. Informatie over de ontwikkeling van nieuwe zombies en botnets wijst erop dat dit niet zo lang meer zal duren.

Elke dag worden er duizenden nieuwe sites online geplaatst, dus ook meer kwaadaardige websites en meer sites die als host voor malware optreden. Ook worden er elke dag nieuwe vormen van malware ontwikkeld. Dit rapport bevat gedetailleerde uitleg over de malwaredreigingen die momenteel het meeste voorkomen.

Van alle recente beveiligingsrisico's heeft de Conficker-worm (officieel W32/Conficker.worm genaamd) de meeste media-aandacht gekregen. In dit rapport gaan we in op de vraag of deze aandacht als hype of als realiteit moet worden beschouwd. Daarnaast nemen we dreigingen onder de loep die minder aandacht in de media krijgen, maar die soms gevaarlijker zijn dan hun populaire tegenhangers.

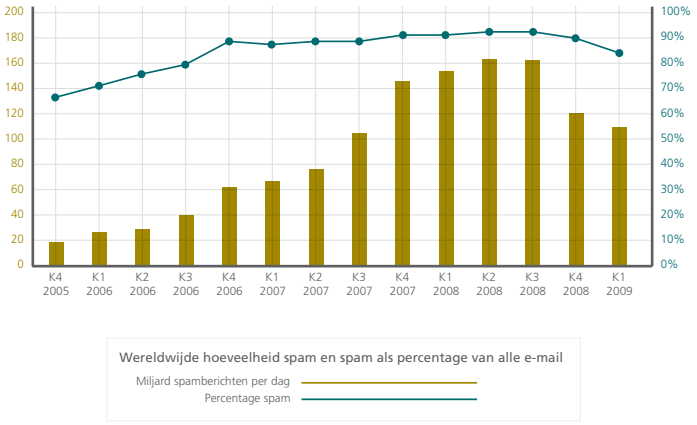
De geografie van het dreigingslandschap is doorlopend in ontwikkeling. U vindt in dit rapport analyses van de mate waarin de geografie van invloed is op dreigingen. Zo wordt er aandacht besteed aan de herkomst van spam, de implementatie van zombiecomputers, de locaties van malwaresites en de identificatie van nieuwe spelers op de 'dreigingsmarkt'. Daarnaast bevat dit rapport interessante details die erop wijzen dat landen die dreigingen ontwikkelen deze ook tegen entiteiten binnen hun eigen grenzen gebruiken.

Tot slot besteden we aandacht aan enkele prognoses uit ons in januari uitgebrachte rapport *Verwachte dreigingen in 2009* en kijken we of en hoe deze voorspellingen zijn uitgekomen. Opvallend is het gebruik van actuele gebeurtenissen en sociale netwerksites voor het verspreiden van dreigingen onder nietsvermoedende gebruikers.

## Spam: nog steeds een wereldwijd probleem

### Welke recessie?

In het eerste kwartaal van 2009 bevond de totale hoeveelheid e-mail en spam zich op het niveau van bijna twee jaar geleden. Hebben spammers net als de rest van de economie te maken met zware economische tijden? Helaas is dat niet het geval. Het spamniveau heeft zich nog niet volledig hersteld na de sluiting van McColo in november 2008. De hoeveelheid spam in 2009 is 20 procent lager dan in hetzelfde kwartaal van vorig jaar en 30 procent lager dan in het derde kwartaal van 2008, waarin de tot nu toe hoogste hoeveelheid spam per kwartaal werd geregistreerd. Nadat spamhost McColo offline werd gehaald, heeft het spamniveau zich voor ongeveer 70 procent hersteld. De hoeveelheid spam is dus nog niet terug op het oude niveau.



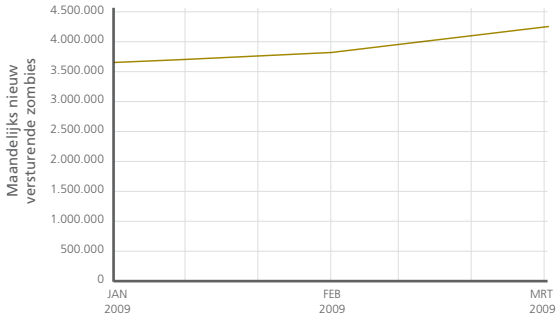

In de afgelopen jaren werden in de maand maart altijd de meeste e-mails verzonden, maar dit jaar is dat niet het geval. Terwijl er vorig jaar in maart gemiddeld 153 miljard berichten per dag werden verzonden, kwam de teller dit jaar niet hoger dan 100 miljard.

Spam is, als percentage van de totale hoeveelheid e-mail, onder de 90 procent gezakt, een niveau dat sinds 2006 niet meer is voorgekomen. In 2008 bestond de totale hoeveelheid e-mail nog voor 90 procent uit spam, maar in het afgelopen kwartaal was dat 'slechts' 86 procent. E-mailaccounts en e-mailactiviteiten kunnen aanzienlijk variëren, maar uit onze schattingen blijkt dat individuele personen zes tot twaalf e-mails minder per dag ontvangen (ten opzichte van vorig jaar).

Wij zijn ervan overtuigd dat de hoeveelheid spam het niveau van 2008 binnen afzienbare tijd weer zal bereiken. De reorganisatie van commandocentra en botnets na de sluiting van McColo heeft echter langer geduurd dan velen in eerste instantie dachten. Het lijdt overigens geen twijfel dat er hard aan het herstel wordt gewerkt, want voor spammers is deze reorganisatie uiteindelijk ook een kwestie van rendement, net als voor elk ander bedrijf.

### Nieuwe zombies brengen de productielijn op gang

In dit kwartaal hebben we bijna twaalf miljoen nieuwe IP-adressen gedetecteerd die dienst doen als zombies (computers die op afstand door spammers of andere criminelen worden bestuurd). Dit is een stijging van bijna 50 procent ten opzichte van het laatste kwartaal van 2008. In het derde kwartaal van 2008 werd ook al een recordaantal nieuwe zombies gedetecteerd, maar in dit kwartaal werd het record met een miljoen 'verbeterd'. De hoeveelheid spam is nog niet terug op het oude niveau van voor de sluiting van McColo, maar uit de hoge activiteit van nieuwe zombies kan worden afgeleid dat de spammers hard werken aan het herstel van de verloren infrastructuur en dat de hoeveelheid spam binnenkort weer het oude niveau zal hebben bereikt.




De geïnfecteerde systemen kunnen per land worden gerangschikt. In het afgelopen kwartaal waren de tien landen die de meeste spam produceren verantwoordelijk voor 63 procent van de nieuwe zombies. Dit is een kleine daling ten opzichte van de vorige twee kwartalen. Spammers proberen blijkbaar in meer landen computers in handen te krijgen ter ondersteuning van hun activiteiten.

| Kwartaal 1 2009 | | Kwartaal 4 2008 | | Kwartaal 3 2008 | |
|---|---|---|---|---|---|
| **Land** | **Percentage IP's** | **Land** | **Percentage IP's** | **Land** | **Percentage IP's** |
| Verenigde Staten | 18,0 | China | 15,8 | China | 20,4 |
| China | 13,4 | Verenigde Staten | 15,4 | Verenigde Staten | 16,5 |
| Australië | 6,3 | Duitsland | 6,5 | Duitsland | 6,8 |
| Duitsland | 5,3 | Verenigd Koninkrijk | 6,0 | Verenigd Koninkrijk | 6,0 |
| Verenigd Koninkrijk | 4,7 | Brazilië | 4,9 | Brazilië | 4,8 |
| Brazilië | 4,0 | Spanje | 4,3 | Spanje | 3,7 |
| India | 3,1 | Australië | 4,1 | India | 2,5 |
| Spanje | 3,0 | Italië | 3,5 | Rusland | 2,4 |
| Zuid-Korea | 2,8 | Rusland | 3,1 | Zuid-Korea | 2,4 |
| Rusland | 2,5 | Zuid-Korea | 2,4 | Italië | 2,2 |
| | | | | | |
| **Totaal** | **63,3** | **Totaal** | **66,0** | **Totaal** | **67,5** |

Spammers in China en de Verenigde Staten hebben de meeste zombiecomputers in handen. In de afgelopen drie kwartalen namen beide landen beurtelings de eerste plaats in beslag. Australië zorgt voor een opmerkelijke verschuiving. Het land, dat in het derde kwartaal van 2008 nog niet in de top tien stond, is in twee kwartalen gestegen naar de derde plaats en daarmee verantwoordelijk voor zes procent van alle nieuwe zombies. Het land van onze tegenvoeters is blijkbaar zeer geschikt voor het rekruteren van zombies.

| Kwartaal 1 2009 | | Kwartaal 4 2008 | |
|---|---|---|---|
| **Land** | **% van totaal** | **Land** | **% van totaal** |
| Verenigde Staten | 35,0 | Verenigde Staten | 34,3 |
| Brazilië | 7,3 | Brazilië | 6,5 |
| India | 6,9 | China | 4,8 |
| Zuid-Korea | 4,7 | India | 4,2 |
| China | 3,6 | Rusland | 4,2 |
| Rusland | 3,4 | Turkije | 3,8 |
| Turkije | 3,2 | Zuid-Korea | 3,7 |
| Thailand | 2,1 | Spanje | 2,4 |
| Roemenië | 2,0 | Verenigd Koninkrijk | 2,3 |
| Polen | 1,8 | Colombia | 2,0 |
| | | | |
| | **70,0** | | **68,3** |

Spam per land: Verenigde Staten weer wereldleider

De autofabrikanten in de VS hebben weliswaar productie- en verkoopproblemen, maar de Amerikaanse spamindustrie, die 35 procent van de totale wereldproductie van spam voor zijn rekening neemt, blijft wereldwijd leider. Hoewel het beheer van spam via een internationale infrastructuur wordt uitgevoerd, geven spammers voor het produceren van spam nog steeds de voorkeur aan het gebruik van computers uit de Verenigde Staten. De tien landen die de meeste spam produceren, zijn verantwoordelijk voor bijna 70 procent van de totale spamproductie, waarmee ze de meer dan tweehonderd andere landen ver voorbijstreven.

Uit de laatste twee kwartalen blijkt dat India het hoogste groeipercentage heeft en nu verantwoordelijk is voor bijna zeven procent van de wereldwijde spam. De spamproductie van India is verdubbeld ten opzichte van het vorige kwartaal. Wellicht is spam de laatste bedrijfstak die probeert activiteiten aan India uit te besteden.

Ook Thailand, Roemenië en Polen zijn nieuwkomers in de top tien. Uit deze gegevens kan worden afgeleid dat spammers overal zoeken naar nieuwe voedingsbronnen voor hun spammachines.

| Kwartaal 1 2009 | | Kwartaal 4 2008 | | Kwartaal 3 2008 | |
|---|---|---|---|---|---|
| Geneesmiddelen | 25,0 | Geneesmiddelen | 37,0 | Penisvergroters | 31,2 |
| Advertenties | 21,9 | Advertenties | 19,3 | Advertenties | 19,3 |
| Productreplica's | 18,8 | Penisvergroters | 16,8 | Geneesmiddelen | 10,7 |
| Penisvergroters | 17,5 | DSN | 9,5 | Storm | 8,0 |
| DSN | 7,1 | Dating | 3,9 | DSN | 7,7 |
| Storm | 1,6 | Productreplica's | 2,6 | Belangrijk nieuws | 6,7 |
| Diploma's | 1,1 | Banen | 1,7 | Productreplica's | 6,0 |
| Software | 1,1 | Software | 1,5 | Leningen | 1,6 |
| Leningen | 1,0 | Leningen | 1,2 | Bankieren | 1,1 |
| Anders | 4,9 | Anders | 6,5 | Anders | 7,7 |
| | **100,0** | | **100,0** | | **100,0** |

Spam per type: seks, drugs en nog veel meer

Spam over penisvergroters, geneesmiddelen en algemene advertenties scoren het hoogst van alle typen spam. Deze drie typen alleen zijn verantwoordelijk voor ongeveer 60 procent van de spam die de afgelopen drie kwartaal verzonden is. Het lijkt wel of de slogan "seks, drugs en rock-'n-roll" door spam nieuw leven is ingeblazen. Maar dat is niet helemaal waar. Tegenwoordig zou de slogan beter "seks, drugs en economie" kunnen luiden.

Spam over productreplica's (meestal voor nagemaakte merkhorloges) is dit kwartaal enorm toegenomen en is nu verantwoordelijk voor bijna 19 procent van de totale hoeveelheid spam. Dit type spam was ook het afgelopen jaar al erg populair. Het lijkt erop dat spammers ons in moeilijke economische tijden willen helpen onze koopkracht te verhogen door goedkope namaakproducten aan te bieden.

Berichten over de leveringsstatus van producten zijn nog steeds verantwoordelijk voor acht procent van de totale spamproductie. Een dergelijk bericht is bijna altijd aan een phishingaanval gekoppeld en bestaat meestal uit een bounce-melding waarbij via e-mail-spoofing misbruik van het e-mailadres van het slachtoffer wordt gemaakt. Phishingaanvallen zijn dus nog lang niet verleden tijd. Veel van deze berichten hebben betrekking op financiële zaken en zijn in feite een poging de persoonlijke gegevens van een gebruiker in handen te krijgen.

### Spammers hebben geen respect voor de soevereiniteit van landen, inclusief hun eigen land

In de beveiligingsgemeenschap gaat men er vaak vanuit dat online criminelen, waarvan velen mogelijk in Oost-Europa gevestigd zijn, zich bij voorkeur richten op doelen in Westerse landen en liever geen mensen of bedrijven in hun eigen rechtsgebied aanvallen. Onze gegevens zijn in tegenspraak met deze mythe. Internet kent geen geografische grenzen. Het wordt steeds duidelijker dat cybercriminelen elk doel aanvallen dat ze de moeite waard achten. We hebben bewijzen onder ogen gehad waaruit blijkt dat cybercriminelen belangrijke Russische en Oost-Europese overheidsinstellingen en -bedrijven hebben aangevallen, alsmede topbestuurders bij die organisaties.

McAfee TrustedSource™ heeft onlangs met malware geïnfecteerde e-mail en spam ontdekt die afkomstig was van verschillende overheidsinstellingen en banken in Rusland. Op grond van onze analyse komen wij tot de conclusie dat de volgende Russische banken zijn gehackt:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Uit onze gegevens blijkt dat ook de computersystemen van de volgende Russische overheidsinstanties in handen van cyberbendes zijn gevallen:

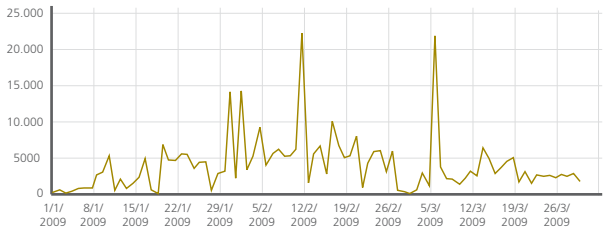
- Ministerie van Belastingzaken, regio Nazran
- Internetnetwerk van de Russische overheid
- Regionaal financieel en economisch instituut
- Gezamenlijk instituut voor nucleair onderzoek
- Medisch centrum van de presidentiële afdeling van de Russische Federatie
- Pensioenfonds van de Russische Federatie
- Persoonlijk netwerk van het justitieapparaat van de Russische Federatie
- JSC Chechen cellulaire communicatie

Uit deze gegevens over Rusland kan worden afgeleid dat internetcriminelen vrijwel geen onderscheid maken ten aanzien van hun doelen. Elke organisatie, financiële instelling of andere instantie die in hun ogen de moeite waard is, wordt aangevallen. Hoewel Rusland duidelijk op kop loopt bij dit type activiteit (en de hoeveelheid spam die daarbij wordt geproduceerd), blijkt uit onze analyse dat dezelfde activiteiten ook voorkomen in andere voormalige landen van de Sovjet Unie, onder andere Armenië, Azerbeidzjan, Georgië, Kazachstan, Kirgizië, Moldova, Oekraïne, Oezbekistan, Tadzjikistan, Turkmenistan en Wit-Rusland.

## Internet: elke dag nieuwe sites met kwaadaardige reputaties

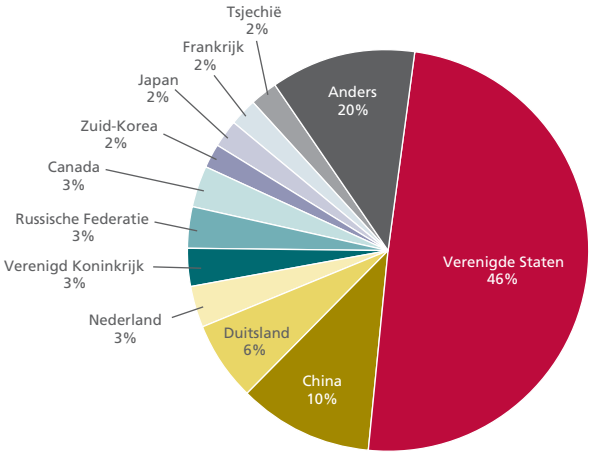
Veel dreigingen die voor het eerst opdoken in het laatste kwartaal van 2008 waren ook dit kwartaal nog actief en de intensiteit van de dreigingen was bovendien hoger. Hoewel de mediahype en -aandacht grotendeels op Conficker was gericht, was deze worm absoluut niet de enige dreiging in dit kwartaal. Zelfs als de Conficker-activiteit buiten beschouwing wordt gelaten, laten onze gegevens nog steeds een lichte toename van activiteiten zien ten opzichte van vorig jaar en een duidelijke toename ten opzichte van vorige kwartalen. Valse antivirusproducten veroorzaakten nogal wat problemen op internet. Datzelfde geldt voor de toegenomen oplichtings- en phishingactiviteiten.

De kwaadaardige domeinen waarmee Conficker contact moest maken zijn niet opgenomen in de daggrafieken of gegevens in deze paragraaf, behalve in de grafiek "Distributie van websites met een kwaadaardige reputatie". De Conficker-gegevens vormen een belangrijk onderdeel van het dreigingslandschap, maar vervormen het totaalbeeld van de kwaadaardige activiteiten. Er zijn heel veel andere dreigingen die steeds actiever worden. Malwareschrijvers en oplichters maken misbruik van economische problemen en bezorgdheden om gebruikers naar allerlei oplichtingssites te lokken. Het vermijden van gedwongen huizenverkopen is bijvoorbeeld een populair onderwerp en er worden phishingsites over allerlei onderwerpen ontwikkeld; zelfs bonuskaarten van winkels worden via internet aangeboden. Ook valse antivirussites blijven hun pijlen op nietsvermoedende gebruikers richten. Bovendien worden de methoden waarmee mensen naar websites worden gelokt steeds geavanceerder. Zelfs wanneer alle Conficker-activiteit buiten beschouwing wordt gelaten, blijkt dat het aantal URL's met een kwaadaardig (of rood) reputatieniveau aanzienlijk is gestegen ten opzichte van de laatste twee kwartalen van 2008.




Elke dag nieuwe sites met kwaadaardige reputaties

Welke landen zijn verantwoordelijk voor deze URL's met slechte webreputaties? Niet de landen die meestal als schuldige worden aangewezen.



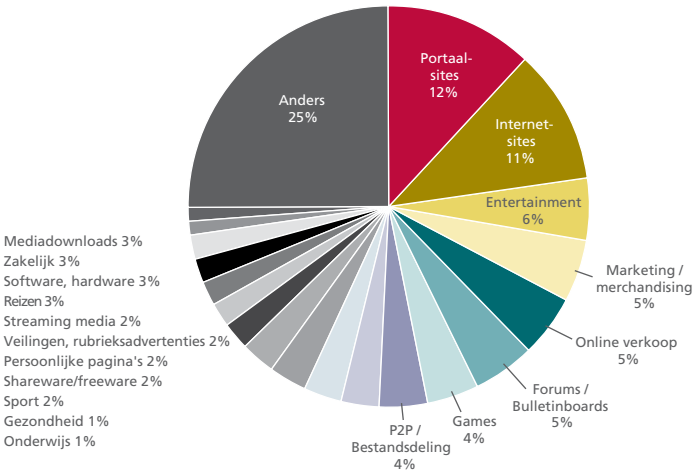

Distributie van websites met een kwaadaardige reputatie

Op het gebied van kwaadaardige webactiviteiten is er een plotselinge verschuiving opgetreden in de landen die door velen als de 'norm' worden beschouwd (een top drie bestaande uit de Verenigde Staten, China en Rusland).[1] Dit betekent niet dat sommige van deze landen minder URL's met een kwaadaardige reputatie hebben. Het duidt in plaats daarvan op de toegenomen groei in andere landen. Een groot deel van deze groei heeft te maken met de locaties waar Conficker bepaalde domeinen heeft gehost waarmee de worm contact gaat maken (of reeds heeft gemaakt). Nederland heeft zijn gedeelde vierde plaats in feite aan de Conficker-worm te danken. Hoewel Nederland lange tijd zeer in trek was voor het hosten van phishing-URL's, veroorzaakte Conficker een belangrijke toename van de met malware geïnfecteerde websites en andere kwaadaardige inhoud. Deze verschuiving kan echter niet alleen aan Conficker worden toegeschreven. Ook Canada is momenteel een van de tien landen met de meeste kwaadaardige webservers, vanwege de vele verschillende soorten malware en spyware waarmee de sites besmet zijn.

Een belangrijke les is dat dezelfde landen ook hoog scoren bij meerdere aanvalsvectoren: kwaadaardige sites, sites met spyware/adware, phishingtrucs en spam. De zeven landen die de meeste websites met kwaadaardige reputaties hebben, behoren tevens tot de tien landen die de meeste sites met phishingtrucs, spam en malware/spyware hosten.

1. In het derde kwartaal van 2008 was dit de rangorde: VS 41 procent, China 12 procent, Rusland 7 procent, Duitsland en Nederland 5 procent, Zuid-Korea 4 procent, Hongkong 3 procent, Taiwan, Canada en Tsjechië 2 procent en de overige landen 17 procent.

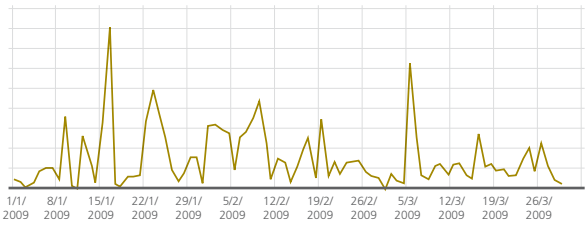
Sites met kwaadaardige reputaties kunnen zeer uiteenlopende doelen hebben, hetzij legitieme, twijfelachtige of bedrieglijke doelen. Mensen die een porno- of goksite bezoeken, lopen nog steeds een hoger risico als de site niet aan een erkend en legitiem bedrijf is gerelateerd. Elke site is echter kwetsbaar en elk type inhoud dat interessant is voor een gebruiker biedt malwareverspreiders een kans om misbruik te maken.




Top 20 legitieme categorieën die het predicaat 'Kwaadaardige website' van TrustedSource verdienen

Dit kwartaal is de populariteit van inhoudsservers onder cybercriminelen toegenomen. Criminelen gebruiken deze servers als middel voor het verspreiden van kwaadaardige en illegale inhoud. Deze trend wordt niet alleen waargenomen bij sites die door bekende en gerespecteerde providers worden onderhouden, maar ook bij sites die door onbekende en dubieuze providers worden aangeboden. Als gevolg van deze dreiging, in combinatie met het wijdverbreide gebruik van blogs en zoekmachineoptimalisaties, is het nu van essentieel belang dat elke computer over volledige internetbeveiliging beschikt.

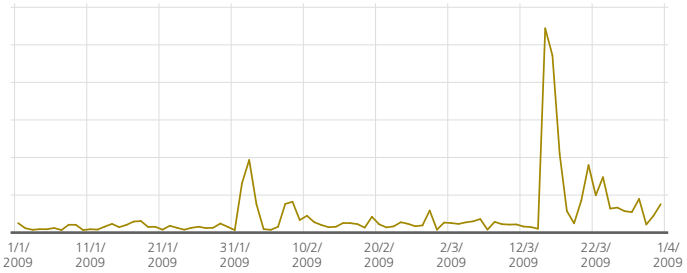
Tot zover de *locatie* van dreigingen, we gaan nu verder met de *typen* dreigingen die momenteel in omloop zijn. In dit kwartaal zijn er naast Conficker veel nieuwe malwaredreigingen en exploits op internet uitgebracht.




Nieuwe websites met malware en potentieel ongewenste programma's

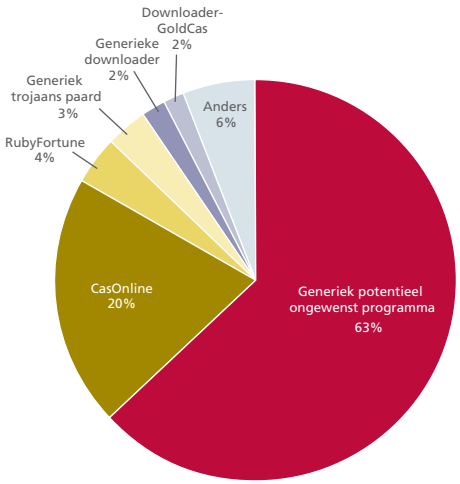
De bovenstaande grafiek geeft een beeld van het aantal websites met malware en potentieel ongewenste programma's dat in dit kwartaal door het McAfee TrustedSource-netwerk is gedetecteerd. (In de bovenstaande grafiek ziet u sites die daadwerkelijk malware hosten, alsmede het gebruikersverkeer naar die sites. De grafiek omvat geen legitieme sites die worden misbruikt om gebruikers om te leiden naar malwaresites. Bovendien zijn onze proactieve onderzoeksresultaten uit deze grafiek verwijderd, om een getrouw beeld te geven van de unieke nieuwe dreigingen die zich aandienen tijdens het normale surfen op school, thuis of op het werk.)

In de onderstaande grafiek ziet u welke unieke, nieuwe malwaredownloads (die door verschillende websites worden aangeboden) met behulp van onze proactieve methode zijn opgespoord. De grafiek toont enkele interessante pieken waar nieuwe exploits of "goudmijnen" van kwaadaardige downloads en potentieel ongewenste programma's zijn aangetroffen.




Gedownloade malware en potentieel ongewenste programma's, proactief geïdentificeerd per dag

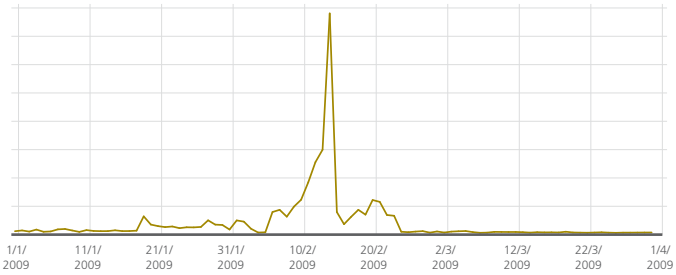
Onze proactieve observaties (d.w.z. websites regelmatig verkennen en verifiëren, plus unieke methoden voor het verzamelen van overige kwaadaardige informatie) tonen aan het eind van januari en het begin van februari een grote piek in nieuwe casinogerelateerde malwaredownloads, alsmede aan het eind van het kwartaal een piek in generieke potentieel ongewenste programma's. Deze activiteiten zijn verantwoordelijk voor de vier meest gedownloade typen malware in het afgelopen kwartaal. (Zie de volgende grafiek). Ander interessant malwarenieuws is de blijvende aanwezigheid van het trojaanse paard Vundo, dat in de afgelopen drie maanden actiever is geworden.




Prevalentie van gedownloade malware en potentieel ongewenste programma's, per type

Een van de amorfe internetdreigingen is de *exploit*, een term die veel (verschillende) dingen kan betekenen voor onderzoekers en gebruikers. Avert Labs spoort tijdens het verkennen en bewaken van internet nieuwe pagina's op die browserexploits bevatten. Daarnaast worden regelmatig nieuwe kwetsbaarheden in de browserbeveiliging vastgesteld. Als browsers (en hun plug-ins) niet voortdurend worden bijgewerkt, kunnen deze 'zandbakken' gemakkelijk als speelplaats door malwareschrijvers worden gebruikt. Wanneer een malwareschrijver op deze manier eenmaal de touwtjes in handen heeft gekregen, kan er programmacode naar de computer van een gebruiker worden gestuurd, zodat infecties met adware, het registreren van toetsaanslagen en andere kwaadaardige activiteiten worden toegestaan.

*Als browsers (en hun plug-ins) niet voortdurend worden bijgewerkt, kunnen deze 'zandbakken' gemakkelijk als speelplaats door malwareschrijvers worden gebruikt.*

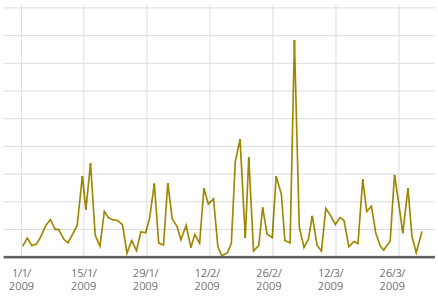



Gedetecteerde websites die browserexploits hosten

## Het gebruik van anonymizers

Malwareschrijvers maken veel gebruik van aanvallen via omgeleide URL's, hetzij met behulp van een anonymizer of via een Web 2.0-interface en een inhoudsserver. Op deze wijze kan de normale detectie worden vermeden (door zich als ingesloten URL in plaats van bron-URL voor te doen) en kan worden geprofiteerd van de reputatie van de site die de malware lijkt te verspreiden.

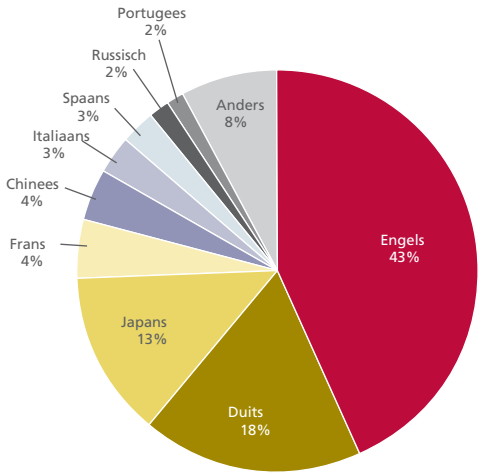
Een anonymizer is een programma dat de identiteit van de gebruiker op internet verbergt. De meeste anonymizers zijn niet kwaadaardig en zijn daarom niet opgenomen in onze eerdere besprekingen van beveiligingsrisico's. Het gebruik van een anonymizer kan echter de deur openen voor een 'man-in-the-middle'-aanval, waarbij een kwaadaardige of gekaapte anonymizer code injecteert in berichten die tussen gebruiker en server heen en weer worden verzonden. Hiermee loopt niet alleen de gebruiker een risico, maar ook de hosts en netwerken die anders beschermd zouden zijn. Het gebruik van anonymizers is dit kwartaal toegenomen ten opzichte van het vierde kwartaal van 2008. Ook ten opzichte van vorig jaar is er een lichte toename in het gebruik van anonymizers.




Nieuwe anonymizers per dag

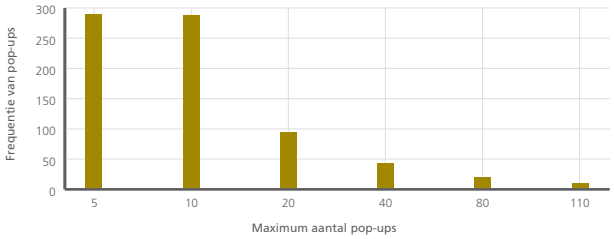
## Algemene internettrends

Internet is een wereldwijde gemeenschap. Eén blik op de verbindingen tussen gebruikers van professionele of sociale netwerksites zegt genoeg. Webpagina's geven steeds meer ondersteuning voor meerdere talen. De blogaanvallen die opduiken op belangrijke sites in de Verenigde Staten worden ook verspreid via Chinese blogs, Braziliaanse blogs, enzovoort. De hedendaagse aanvallen kunnen gebruik maken van een wijdvertakt net. Daarnaast maken malwareverspreiders misbruik van belangrijke sportevenementen en wereldwijde merken om doelgroepen in alle talen te bereiken (bijvoorbeeld door malware in toernooiklassementen en jpg-afbeeldingen van spelers te verbergen).




Distributie van talen in webinhoud

Pop-ups zijn nog steeds een grote bron van ergernis. Toch maken de meeste websites, ondanks pop-upblokkeringen en vergelijkbare programma's, gretig gebruik van pop-ups. Op één website hebben we zelfs 116 pop-ups geteld.




Distributie van pop-ups op sites met ten minste vijf pop-ups

Legitieme Web 2.0-toepassingen en bedrijfsgerelateerde URL's worden nog steeds veel gebruikt voor de verspreiding van malware. Zo'n tien jaar geleden waren gebruikers min of meer veilig als ze bepaalde inhoud links lieten liggen, maar tegenwoordig lijken de dreigingen ons altijd te vinden, ongeacht waar we naartoe surfen. Elke website die kan worden misbruikt (via een van de talloze kwetsbaarheden) zal ook worden misbruikt. Beheerders merken regelmatig dat er scans worden uitgevoerd om te controleren of hun servers misbruikt kunnen worden. Veel scans zijn afkomstig van sites en servers die aan allerlei verschillende zaken gerelateerd zijn, van illegale software en kwaadaardige sites tot anonymizers. Als een drukbezochte website kwetsbaar is, dan is het niet de vraag óf er misbruik van die website zal worden gemaakt, maar wannéér dat misbruik zal plaatsvinden.

*Internetbedrijven zijn min of meer vergelijkbaar met colporteurs en moeten met dezelfde voorzichtigheid worden behandeld.*

Er heeft zich op internet een opvallende stijging van oplichtingspraktijken voorgedaan. Deze stijging zal zich naar verwachting voortzetten nu oplichters via spam-e-mail en internet misbruik proberen te maken van de problemen en zorgen van de wereldbevolking. Bovendien is het vaak moeilijk te bepalen of een organisatie legitiem is. Internetbedrijven zijn min of meer vergelijkbaar met colporteurs en moeten met dezelfde voorzichtigheid worden behandeld. Gebruikers moeten beseffen dat wanneer zij hun creditcardgegevens voor een online donatie of een valse service aan een oplichter verstrekken, de kans groot is dat deze er met hun gegevens vandoor gaat.

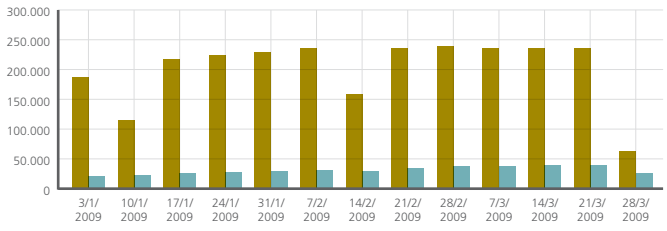
Uit ons onderzoek blijkt echter ook dat er weer wat hoop voor de economie is. Huizenverkoopsites maken dit kwartaal een opvallende groei door en doen het zelfs beter dan de sites met de tien beste categorieën inhoud (zelfs sport werd uit de top 10 verdreven).

## Malware: Conficker-hype versus autorun-malware

In de afgelopen paar maanden hebben de media veel aandacht aan de Conficker-worm besteed. Soms lijkt het wel of deze worm momenteel de enige serieuze dreiging is. Maar de werkelijke cijfers schetsen een heel ander beeld. Conficker is beslist niet de dag des oordeels.

Natuurlijk is Conficker om veel redenen een ernstige malwaredreiging. Een zeer groot aantal hosts is met deze worm geïnfecteerd. Conficker wordt actief ontwikkeld, beheerd en besproken. Maar het daadwerkelijke aantal detecties is niet zo groot als men zou verwachten van malware die zoveel aandacht heeft gekregen.

Er is dit kwartaal echter malware gedetecteerd die grote reden tot bezorgdheid geeft. Autorun-malware maakt bijvoorbeeld voornamelijk gebruik van USB-sticks en flashgeheugens om zichzelf te vermenigvuldigen. Dit type malware is in dit kwartaal veel vaker aangetroffen dan de Conficker-worm. Laten we beide typen malware eens met elkaar vergelijken:




Computers die detecties van autorun-malware en Conficker-wormen rapporteren

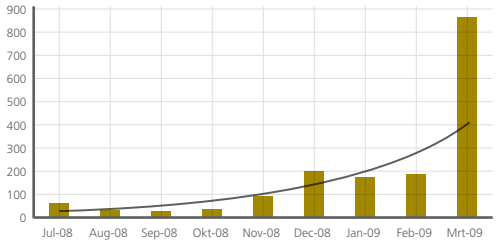
In de afgelopen 30 dagen bestond minder dan 10 procent van alle gerapporteerde detecties uit autorun-wormen. Conficker begon met ongeveer 1 procent en heeft zich sindsdien 12 maal vermenigvuldigd. Toch is dat nog steeds minder dan de 15 procent van het aantal autorun-wormen dat in de hoogtijdagen van laatstgenoemde werd gedetecteerd.

## Update van de voorspellingen

McAfee Avert Labs heeft begin dit jaar het rapport *Verwachte dreigingen in 2009*[2] uitgebracht. Verschillende van onze onderbouwde voorspellingen zijn dit kwartaal uitgekomen.

### Slachtoffers van eigen vuur

In de afgelopen tien jaar is een van de populairste dreigingsvectoren, het ontvangen van virussen van uw vrienden, grotendeels naar de achtergrond verdrongen. Met de komst van Web 2.0 is deze klassieke aanvalsmethode echter weer nieuw leven ingeblazen. In dit kwartaal werden duizenden gebruikers verrast door Koobface-varianten. Ze ontvingen het virus van hun vrienden op Facebook. De slachtoffers wisten niet dat de koppelingen in de (door het virus) verstuurde berichten naar websites leidden die de worm verspreiden. Kort daarna werden hun computers besmet met het virus en werden geïnfecteerde berichten naar hun vriendenkring gestuurd. Aanvallers blijven sociale netwerken gebruiken als populaire vector voor social engineering-aanvallen.

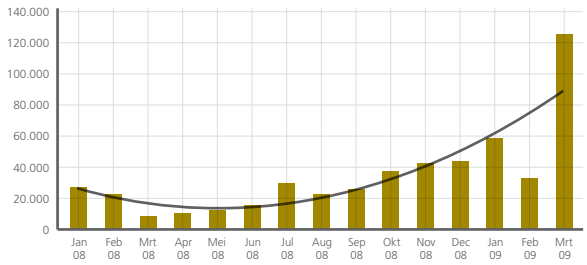



Gedetecteerde unieke binaire Koobface-bestanden

2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_nl.pdf

### Wereldwijd corrupt web

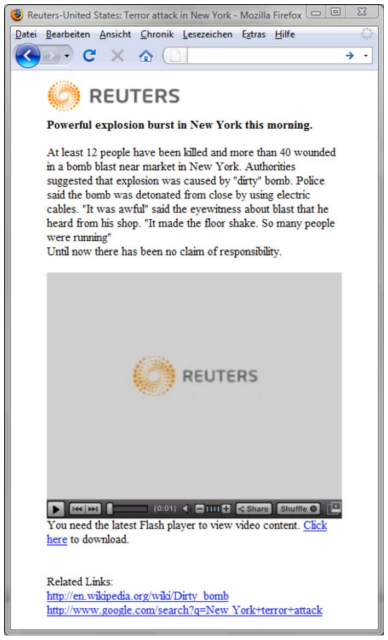
In februari werd Facebook misbruikt door aanvallers die valse toepassingen maakten met behulp van het Facebook-platform. Veel gebruikers trapten erin en installeerden deze toepassingen. In de media werd aandacht besteed aan deze gebeurtenissen, waardoor McAfee Avert Labs een grote zoekmachineoptimalisatie op het spoor kwam die zich richtte op de belangrijkste zoektermen van Google. De aanvallers hadden niet alleen copyrightmateriaal van bekende sites gestolen, maar ook misbruik gemaakt van andere populaire sites (zoals Democrats.org) om hun Google-zoekmachineresultaten te verbeteren. De aanvallers wilden de geoptimaliseerde zoekresultaten gebruiken om valse antivirussoftware te installeren. In dit geval ging het om een valse Facebook-toepassing, die leidde tot valse zoekresultaten, die op hun beurt weer leidden tot valse beveiligingssoftware. Uit deze incidenten blijkt duidelijk hoe belangrijk veilig surfen is.




Gedetecteerde unieke valse binaire antivirusbestanden

### Dreigingen in uw eigen taal

Aanvallers weten dat een persoon eerder actie onderneemt naarmate een aanval relevanter is. Bij een relevante aanval zijn slachtoffers eerder geneigd op een koppeling te klikken, een gebruikersnaam en wachtwoord in te voeren of een toepassing te installeren. Gebeurtenissen die zich in onze achtertuin voordoen trekken eerder onze aandacht dan gebeurtenissen die aan de andere kant van de wereld plaatsvinden. In februari en maart werd dit concept toegepast door de cybercriminelen die verantwoordelijk waren voor het Waledac-virus. Nietsvermoedende slachtoffers werden naar websites gelokt die waren aangepast aan hun locatie om hen een gevoel van authenticiteit te geven. Terwijl de gebruikers het "plaatselijke nieuws" lazen, probeerde de website heimelijk het virus te installeren via een drive-by exploitcode.




## McAfee Avert Labs Blog

### Misbruik van Google en andere zoekmachines

Google. Deze naam betekent veel verschillende dingen voor veel verschillende mensen. Voor mensen die op zoek zijn naar een baan is het een manier om de nieuwste vacatures te bekijken. Voor werkgevers is het een manier om gekwalificeerde mensen te vinden. Voor consumenten is het een effectief middel om lage prijzen te zoeken voor de goederen die ze willen kopen. En voor malwareschrijvers en cybercriminelen is het een steeds effectiever middel om malware te verspreiden en cybermisdaden te plegen. Veel internetactiviteit wordt tegenwoordig door zoekmachines gegenereerd. Het is daarom geen wonder dat malwareschrijvers proberen de kracht van zoekmachines te gebruiken voor het verspreiden van hun waren. Op onze blogs is veel aandacht aan dit onderwerp besteed, bijvoorbeeld in de volgende McAfee Avert-blogartikelen:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

De gecombineerde kracht van indexen en populaire zoekwoorden, plus de verleiding van gemakkelijk verdiend geld, vormen een duidelijke aanwijzing dat criminelen dit type misbruik voorlopig niet zullen laten rusten.

### De economie en angst

De wereldwijde economische problemen blijven veel mensen zorgen baren. Anderen zijn in de greep van de angst en de veiligheidsproblematiek. Malwareschrijvers en cybercriminelen kunnen deze angsten eenvoudig in winst omzetten. In dit kwartaal is op veel zorgwekkende manieren van deze economische trend (een van onze verwachte dreigingen voor 2009) gebruik gemaakt. Angst is een krachtige drijfveer wanneer cybercriminelen hier via social engineering-trucs misbruik van maken:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Oplichtingstrucs, spam en phishing werken goed in goede tijden, laat staan in slechte tijden. Houd er altijd rekening mee dat criminelen hetzelfde nieuws lezen als wij en proberen in te spelen op krantenkoppen en actuele gebeurtenissen. Waakzaamheid blijft dus geboden.

## McAfee Avert Labs

McAfee Avert Labs is het wereldwijde onderzoeksteam van McAfee, Inc. Avert Labs heeft een brede kijk op beveiliging, dankzij de onderzoeksteams die speciaal zijn gericht op malware, mogelijk ongewenste programma's, hostinbraken, netwerkinbraken, mobiele malware en openbaarmaking van ethische kwetsbaarheden. Dankzij deze brede visie kunnen onderzoekers van McAfee de beveiligingstechnologieën continu verbeteren en het publiek beter beveiligen.

## McAfee, Inc.

McAfee, Inc. is het grootste bedrijf ter wereld dat gespecialiseerd is in beveiligingstechnologie. Het hoofdkantoor is gevestigd in Santa Clara, in de Amerikaanse staat Californië. McAfee streeft voortdurend naar het oplossen van 's werelds grootste beveiligingsproblemen. Het bedrijf biedt proactieve en bewezen oplossingen en services die systemen en netwerken over de hele wereld helpen beveiligen, zodat gebruikers veiliger op internet kunnen surfen en winkelen. McAfee kan dankzij haar bekroond onderzoeksteam vernieuwende producten ontwikkelen die thuisgebruikers, bedrijven, de overheid en serviceproviders de mogelijkheid bieden om regelnaleving te bewijzen, gegevens te beveiligen, onderbrekingen te voorkomen, kwetsbaarheden te identificeren en hun beveiliging voortdurend te controleren en te verbeteren. http://www.mcafee.com/nl.

McAfee®

McAfee Inc.
Gatwickstraat 25,
Postbus 58326, 1043 GL
Amsterdam,
The Netherlands,
+ 31 (0)20 5863800
www.mcafee.com/nl


5395rpt_avert_quarterly-threat_0409