Rapport

McAfee-dreigingsrapport: eerste kwartaal 2010

Door McAfee Labs™

Voornaamste bevindingen

Bedrijfsnetwerken zijn steeds moeilijker te beschermen als gevolg van de wildgroei aan externe apparaten. Maar de gadgets zijn er nu eenmaal en gaan ook niet meer weg. Het IT-team zal de beveiliging moeten uitbreiden, zodat de gebruikers altijd en overal beschermd zijn.

Scammers blijven misbruik maken van actuele tragedies. Aardbevingen en andere rampen vormen lucratieve kansen voor cybercriminelen.

Na een daling en een piek in 2009 heeft het spamvolume zich weer hersteld naar het niveau van medio 2008. Verderop in dit rapport vindt u een overzicht van de spamonderwerpen die het populairst zijn in 34 landen. De gegevens zijn afkomstig van onze wereldwijde spamverzamelaars.

De groei van malware lijkt zich te stabiliseren en in sommige gebieden zelfs af te nemen, maar de cumulatieve cijfers zijn nog steeds onvoorstelbaar hoog. Wij verwachten dat we dit jaar minstens evenveel malware zullen catalogiseren als in 2009.

Operatie Aurora is een van de belangrijkste gerichte aanvallen in de geschiedenis van internet. Aurora kan de komende jaren een grote invloed hebben op de ontwikkeling van bedrijfsgerichte cybercriminaliteit.

Het voorjaar is in veel landen belastingtijd en de oplichtingstrucs met belastingdiensten steken ook nu weer de kop op. Sommige vervalste berichten zijn bijna niet te onderscheiden van die van legitieme banken en belastingkantoren.

Cybercriminelen genereren inkomsten uit het manipuleren van zoekresultaten (meestal ten behoeve van valse beveiligingssoftware) en profiteren tevens van advertentiegeld dat via klikfraude wordt verkregen.

Het trojaanse paard Zeus is slechts een van de instrumenten die veel door cybercriminelen worden gebruikt, onder andere voor het koppelen van wachtwoordstelers aan andere typen illegaal online materiaal, zoals porno of valse beveiligingssoftware. Het primaire doelwit van deze aanvallers? Gebruikers van Facebook.

Bijna alle URL's die door McAfee's TrustedSource-technologie als kwaadaardig zijn geclassificeerd, bevinden zich in de Verenigde Staten. De reden is waarschijnlijk dat verspreiders van malware veel en graag gebruik maken van Web 2.0-functies, die in dit land in overvloed aanwezig zijn.

De populairste aanvallen op clients (inclusief operatie Aurora) zijn gericht op Microsoft Internet Explorer, Adobe Reader en Adobe Acrobat.

Justitie heeft verschillende cybercriminelen aangehouden voor zaken die variëren van diefstal van creditcard-nummers tot het onrechtmatig kopen en verkopen van tickets voor concerten en sportevenementen.

Een van de populairste typen cybercriminaliteit is scareware (of valse beveiligingssoftware). De software, die onzichtbaar wordt geïnstalleerd, laat gebruikers geloven dat hun systeem is geïnfecteerd en dat ze onmiddellijk een programma moeten kopen om de infectie te verwijderen. Ontwikkelaars van scareware verdienen een enorme hoeveelheid geld aan hun slachtoffers.

Het politiek hacktivisme houdt aan: hackers hebben diensten verstoord en websites verminkt van een Russisch tijdschrift, de belastingdienst in Letland en de Australische regering.

Inhoudsopgave

Vormen technologische ontwikkelingen een bedreiging voor het netwerk?

Hebt u gemerkt dat aankondigingen van hightechproducten vaak veel opwinding teweegbrengen? Nieuwe gadgets die ons arbeidsleven productiever en ons privéleven leuker moeten maken, wedijveren om onze aandacht en ons geld. Wilt u op meer plaatsen meer doen in minder tijd én ook nog meer plezier aan internet beleven? Schrijf u in!

De netwerkgrens is verschoven tot ver voorbij de muren van het kantoor en het datacenter, en wordt nu alleen nog beperkt door de geografische verspreiding van de werknemers. Met andere woorden, uw netwerk is overal waar uw mensen ook zijn. Als gevolg van de ontwikkelingen op het gebied van technologie en connectiviteit kan deze uitbreiding zich zo snel voltrekken dat IT-afdelingen het niet meer kunnen bijbenen. IT-teams proberen uit alle macht de veranderingen bij te houden en tegelijkertijd enige controle uit te oefenen over wie of welk apparaat verbinding met het netwerk maakt. Deze razendsnelle ontwikkelingen worden nog verder bemoeilijkt als leidinggevenden voortdurend de allernieuwste gadgets aanschaffen en de IT-afdeling de schuld geven als hun nieuwe speelgoed niet met het netwerk wil communiceren.

Elk nieuw apparaat dat werknemers meenemen, vormt een nieuw risico om van binnenuit toegang tot het netwerk te krijgen. Bedrijven die verstandig te werk gaan, hebben grote investeringen gedaan in het tegenhouden van externe dreigingen. Als gevolg daarvan kunnen de meeste wijd verspreide aanvallen eenvoudig worden opgespoord en gestopt voordat ze het netwerk in gevaar brengen. Deze beveiligingsbolwerken hebben ertoe geleid dat cybercriminelen op zoek gaan naar manieren om van binnenuit toegang tot een netwerk te krijgen, omdat de bescherming daar meestal iets minder geweldig is. In veel gevallen richten hackers zich op de zwakste schakel in de beveiligingsketen: de gebruiker. Operatie Aurora werd in januari breed uitgemeten in de pers en trekt nog steeds veel aandacht nu steeds meer bedrijven erachter komen dat ze mogelijk ook door Aurora-achtige aanvallen zijn gehackt. Dit is een eersteklas voorbeeld van misbruik van gebruikers dat kan leiden tot het verlies van waardevolle intellectuele eigendommen.

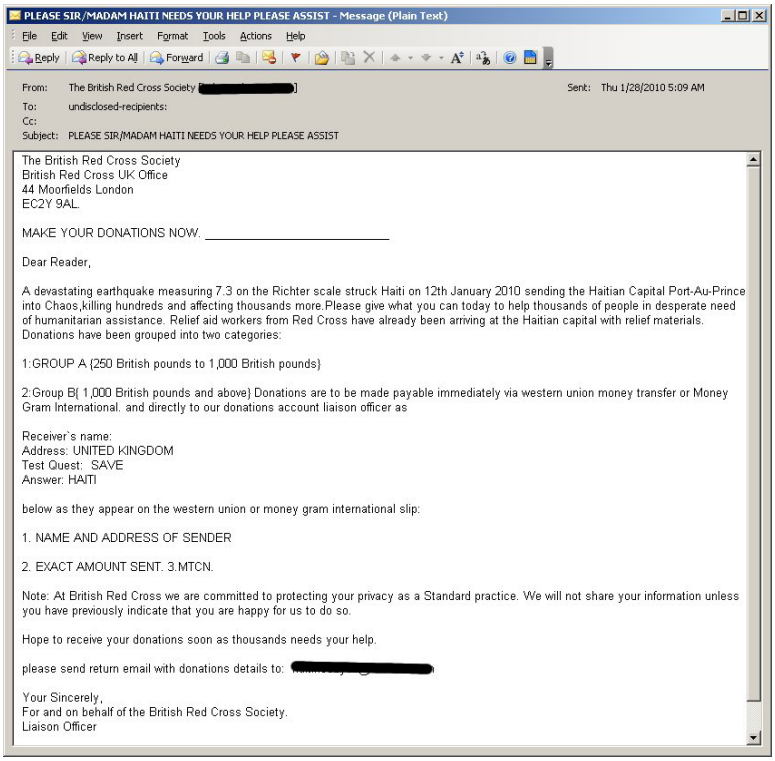
Computerapparatuur in alle soorten en maten wordt regelmatig op zowel het bedrijfsnetwerk als het thuisnetwerk van de gebruiker aangesloten, maar helaas is een thuisnetwerk meestal veel minder streng beveiligd. Infecties in het thuisnetwerk kunnen hierdoor het kantoor binnendringen en de veiligheid van het bedrijfsnetwerk en de bedrijfsgegevens in gevaar brengen. Het toelaten van technologie kan leiden tot een hogere arbeidsproductiviteit en meer voldoening op de werkplek. Zorg er echter altijd voor dat u op de hoogte bent van de potentiële risico's voor uw organisatie, met name als er geen toezicht wordt uitgeoefend op de bedrijfsgegevens en de wijze waarop deze het netwerk in- en uitstromen.

Tragedies kunnen het slechtste in mensen naar boven brengen

Een grote ramp vormt een ideale gelegenheid om mensen samen te brengen voor een gemeenschappelijk doel. In tijden van crisis verenigen mensen uit de hele wereld zich om vreemden te helpen die alles hebben verloren door een aardbeving, orkaan, overstroming of andere calamiteit. De grote stroom hulpgoederen en hulpverleners die bij dergelijke rampen op gang komt, is een eerbetoon aan de goedheid van de mens.

Dergelijke gebeurtenissen wekken echter niet alleen naastenliefde op, maar kunnen ook het slechtste in de mens naar boven brengen. In de wereld van de internetbeveiliging is het een bekend gegeven dat cybercriminelen nergens voor terugdeinzen om gulle gevers zoveel mogelijk geld uit de zak te kloppen. Ze maken misbruik van de goedheid van anderen, door met behulp van phishingtrucs geld en identiteitsgegevens te stelen van bezorgde mensen over de hele wereld. De trucs die ze gebruiken zijn bijna niet te onderscheiden van de legitieme hulpacties die voor de slachtoffers van de ramp op touw worden gezet.

De recente aardbevingen in Haïti zijn een goed voorbeeld van dit criminele gedrag. Kort nadat het straatarme eiland door de eerste vreselijke beving was getroffen, stroomde niet alleen de hulp toe, maar staken ook de oplichtingstrucs massaal de kop op. Zo werden er bijvoorbeeld valse e-mails naar nietsvermoedende slachtoffers verzonden waarin om een donatie werd gevraagd.


PLEASE SIR/MADAM HAITI NEEDS YOUR HELP PLEASE ASSIST - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: The British Red Cross Society [redacted] Sent: Thu 1/28/2010 5:09 AM

To: undisclosed-recipients:

Cc:

Subject: PLEASE SIR/MADAM HAITI NEEDS YOUR HELP PLEASE ASSIST

The British Red Cross Society
British Red Cross UK Office
44 Moorfields London
EC2Y 9AL.

MAKE YOUR DONATIONS NOW. _____

Dear Reader,

A devastating earthquake measuring 7.3 on the Richter scale struck Haiti on 12th January 2010 sending the Haitian Capital Port-Au-Prince into Chaos,killing hundreds and affecting thousands more.Please give what you can today to help thousands of people in desperate need of humanitarian assistance. Relief aid workers from Red Cross have already been arriving at the Haitian capital with relief materials. Donations have been grouped into two categories:

1:GROUP A {250 British pounds to 1,000 British pounds}

2:Group B{ 1,000 British pounds and above} Donations are to be made payable immediately via western union money transfer or Money Gram International. and directly to our donations account liaison officer as

Receiver`s name:
Address: UNITED KINGDOM
Test Quest: SAVE
Answer: HAITI

below as they appear on the western union or money gram international slip:

1. NAME AND ADDRESS OF SENDER

2. EXACT AMOUNT SENT. 3.MTCN.

Note: At British Red Cross we are committed to protecting your privacy as a Standard practice. We will not share your information unless you have previously indicate that you are happy for us to do so.

Hope to receive your donations soon as thousands needs your help.

please send return email with donations details to: [redacted]

Your Sincerely,
For and on behalf of the British Red Cross Society.
Liaison Officer

Afbeelding 1: dit donatieverzoek werd veel gebruikt in valse e-mails die werden verzonden na de aardbevingen in Haïti.

Op het eerste gezicht lijken deze verzoeken de belangen van de Haïtianen op het oog te hebben, maar als u een bedrag via deze "diensten" overmaakt, zal uw geld waarschijnlijk nooit op de bedoelde plek terechtkomen. In afbeelding 1 ziet u dat er met name om donaties van meer dan 1000 Britse ponden (ongeveer 1160 euro) wordt gevraagd en dat de lezer wordt aangemoedigd het bedrag direct over te maken via een overboekingsservice.

Natuurlijk zijn niet alle hulporganisaties onbetrouwbaar. Er zijn veel legitieme organisaties die er streng op toezien dat uw geld goed wordt besteed en rechtstreeks naar de slachtoffers gaat. Het is echter belangrijk dat u zelf onderzoek uitvoert en alleen in zee gaat met goed bekend staande organisaties die erop toezien dat de hulpgelden goed terechtkomen. Wees voorzichtig met verzoeken om geld die u via e-mail bereiken en neem goede voorzorgsmaatregelen om uw identiteit op internet te beschermen.

Spamvolume weer op het niveau van medio 2008

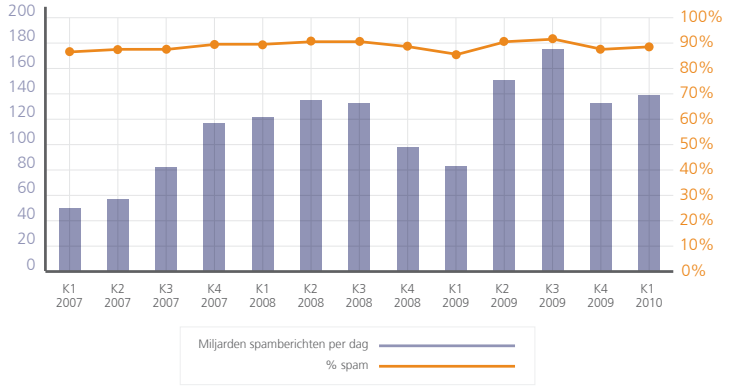
Het spamvolume in het huidige kwartaal is niet veel veranderd ten opzichte van het vierde kwartaal van 2009. Er deed zich een kleine stijging voor van circa vijf procent. Tussen januari en maart werden er per dag gemiddeld 139 miljard spamberichten verstuurd, goed voor 89 procent van het wereldwijde e-mailverkeer. In het vorige kwartaal werden er 133 miljard spamberichten per dag verzonden.

In het *McAfee-dreigingsrapport: vierde kwartaal 2009* werd al voorspeld dat de daling van het spamvolume (met 24 procent) aan het eind van vorig jaar van korte duur zou zijn.[1] Na de recordpiek in de zomer van 2009 (toen er gemiddeld 175 miljard berichten per dag werden verstuurd), is het volume nu weer terug op het niveau van medio 2008, net voordat spamhost McColo in november van dat jaar uit de lucht werd gehaald.

De meeste spam in dit kwartaal had betrekking op pillen en penisvergroters: meer dan 71 procent van het spamverkeer. E-mails met generieke aanbiedingen volgen op grote afstand als tweede en nemen slechts tien procent van het spamverkeer voor hun rekening. Spam met contactadvertenties of aanbiedingen voor opleidingen en (universitaire) graden zijn elk goed voor minder dan twee procent.

1. Het McAfee-dreigingsrapport is in negen talen verkrijgbaar op: http://www.mcafee.com/us/threat_center/white_paper.html

Wereldwijde spamvolumes



Afbeelding 2: wereldwijde spamvolumes en spam als percentage van alle e-mail.

Spamtrends over de hele wereld

McAfee heeft op verschillende plekken over de hele wereld een aantal nodes geplaatst die gegevens over e-mailstromen verzamelen. De verzamelde gegevens worden gebruikt om trends in spam op te sporen. Door nauwkeurig onderzoek van deze gegevens is het mogelijk het land van oorsprong van bepaalde typen spam te achterhalen. Het is niet eenvoudig om onbewerkte gegevens uit verschillende regio's nauwkeurig met elkaar te vergelijken, maar de gegevens bieden wel een goed inzicht in het type spam dat het vaakst uit een bepaald land komt. Het onderwerp van de spamberichten heeft vaak betrekking op de problemen waarmee mensen uit die landen te maken hebben.

Deze paragraaf bevat een reeks cirkeldiagrammen waarmee de populairste typen spam uit 34 landen worden weergegeven. We hebben de typen spam in deze diagrammen tevens in categorieën ingedeeld en van een toelichting voorzien. Houd er rekening mee dat deze verzamelingen alleen de populairste typen spam bevatten, dus niet álle spam die uit een bepaald land afkomstig is.

De berichten in deze categorieën nemen qua volume circa veertig tot zeventig procent van alle verzamelde gegevens in de regio voor hun rekening. Persoonlijke berichten, algemeen communicatieverkeer en spam-campagnes met een laag volume zijn niet meegeteld. De gepresenteerde resultaten zijn zeer interessant, maar geven dus geen volledig beeld van de typen e-mail die uit de afzonderlijke landen afkomstig zijn.

We hebben twintig algemene categorieën gekozen voor het classificeren van deze spamberichten. Hieronder volgt een opsomming van de categorieën met een korte beschrijving:

Aandelen: deze categorie berichten maakt deel uit van een "pump and dump"-aandelentruc (waarbij valse beleggersinformatie in omloop wordt gebracht). Iemand koopt laaggeprijsde aandelen en stuurt vervolgens een reeks spamberichten de wereld in om een valse vraag te creëren, zodat de spammer de aandelen met winst kan verkopen.

Bezorgingsstatusbericht: dit zijn meldingen over de status van een e-mailbericht dat mogelijk met vertraging of helemaal niet kan worden bezorgd. Dergelijke meldingen worden ook wel DSN's (Delivery Status Notification) of NDR's (Non-Delivery Receipts) genoemd. Deze berichten kunnen legitiem zijn, maar in veel gevallen gaat het om spamberichten die naar een vals afzenderadres worden teruggestuurd. Als het aandeel bezorgingsstatusberichten toeneemt, kan dit wijzen op grotere hoeveelheden afzonderlijk beheerde e-mailservers.

Casino's: spamberichten waarin reclame wordt gemaakt voor online casino's. In deze berichten, die vaak afkomstig zijn van botnets, worden slachtoffers opgeroepen de software voor het spelen van de spellen te downloaden en installeren.

Derden: deze categorie ligt tussen de categorie Marketing en de categorie Producten in. Het bedrijf aan de afzenderzijde van de spamberichten handelt legitiem, maar de ontvangers hebben waarschijnlijk per ongeluk partneradverteerders toestemming gegeven hen e-mail te sturen. De lijsten met e-mailadressen kunnen ook zijn gekocht van bedrijven die failliet gaan, of soms mogen bedrijven op grond van hun privacyverklaring e-mailadressen van klanten verkopen. Gratis T-shirts, verzekeringen en medische apparatuur zijn bekende voorbeelden van deze categorie spamberichten. De berichten worden vaak verzonden vanuit hostingfaciliteiten in andere landen, zodat het indienen van klachten ernstig wordt bemoeilijkt. Dit soort spammers leeft de wet CAN-SPAM tot in de details na, maar slaagt er toch in de bedoeling van de wet volledig te omzeilen door gebruik te maken van anonieme domeinen, verkeerd gevormde woorden, onjuist gespelde woorden en ingesloten verborgen tekstblokken.

Diploma's: deze berichten verwijzen naar sites waar valse diploma's kunnen worden gekocht. Klanten kunnen vervalste documenten aanvragen die "bewijzen" dat ze een bepaalde opleiding met succes hebben afgerond. Het gaat hier uiteraard niet om legitieme academische instellingen en daadwerkelijke opleidingen. Deze berichten worden meestal door botnets verstuurd.

Eenzame vrouwen: ook bij deze categorie staat het winnen van vertrouwen centraal. De criminelen (meestal mannen die zich voordoen als vrouwen) proberen bij hun slachtoffer geld los te krijgen voor vliegtickets, douanekosten, eten, reiskosten of andere uitgaven die ze zogenaamd moeten maken om het slachtoffer met de bankrekening te "ontmoeten". Spamberichten over Russische bruiden komen het meest voor.

Erotische producten: spamberichten waarin reclame wordt gemaakt voor porno, meestal gaat het om dvd's of downloadsites. Porno vormt qua volume niet zo'n groot deel van het totale spamverkeer als de meeste mensen denken, maar het effect dat één pornografische e-mail op de ontvanger heeft, is exponentieel groter dan bij andere typen spam. Bovendien is de kans dat een klacht over dit type spam wordt ingediend ook veel groter dan bij andere spamberichten.

Geneesmiddelen: deze categorie omvat onder andere spamberichten over valse Canadese apotheken (meestal gehost in China), açaibessen en voedselsupplementen. Deze berichten worden in veel gevallen door botnets verstuurd, maar kunnen ook afkomstig zijn van gehoste webfarms die e-mail naar een ander land sturen.

Horloges: deze eenvoudig te herkennen berichten zijn een zeer veel voorkomende vorm van spam in de categorie Producten.

Lijsten: via deze spamberichten worden lijsten met contactpersonen aangeboden, bijvoorbeeld een lijst met artsen of tandartsen in uw omgeving.

Loterijen: uw e-mailadres is willekeurig geselecteerd uit onze database en u ontvangt zakken vol geld. U hoeft ons alleen maar 3000 dollar te sturen voor het afhandelen van de transactie. Dit is ook een vorm van oplichting die draait om het winnen van vertrouwen.

Malware: alle berichten met een virus of trojaans paard in de bijlage, of berichten waarin u met klem wordt verzocht een geïnfecteerde website te bezoeken. "UPS tracking number" en "Conficker.B Infection Alert" zijn voorbeelden van veelgebruikte berichtonderwerpen.

Marketing: via deze berichten wordt een product aangeprezen of geprobeerd een product te verkopen aan een ontvanger die heeft aangegeven berichten te willen ontvangen. Bijvoorbeeld luchtvaartmaatschappijen of reisbureaus die een lijst met aanbiedingen naar de ontvanger versturen. Deze e-mailadvertenties zijn rechtstreeks van de andere partij afkomstig; de ontvanger weet dus waarom hij of zij de e-mail ontvangt. Dit type bericht wijkt af van advertenties die wel van derden afkomstig zijn (deze komen verderop aan bod).

Nieuwsbrieven: een informatieve e-mail waarvoor ontvangers zich inschrijven. Via een nieuwsbrief worden meestal niet rechtstreeks producten verkocht, maar door middel van leuke en opvallende teksten worden deze wel bij de klant aangeprezen. Voorbeelden zijn een aankondiging van een nieuwsmedium of updates van discussielijsten.

Nigeriaanse scam: een truc die draait om het winnen van vertrouwen. Iemand probeert met een tragisch verhaal of de belofte van een beloning geld los te krijgen van zijn slachtoffer. Het verhaal wordt meestal met een paar officieel uitziende documenten aannemelijk gemaakt. Deze typen berichten zijn meestal afkomstig van hosts die gratis e-mailaccounts bieden, maar deze berichten worden ook steeds vaker vanaf geïnfecteerde hosts verstuurd.

Phishing: elke e-mail waarmee wordt geprobeerd een slachtoffer persoonsgegevens te ontfutselen. De bekendste voorbeelden zijn waarschuwingen van banken waarvoor u uw gebruikersnaam en wachtwoord moet opgeven.

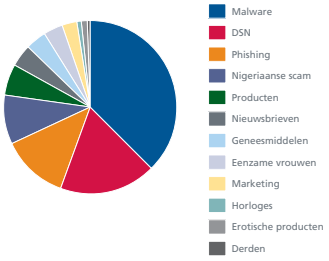
Producten: elk ongevraagd toegezonden bericht waarmee wordt geprobeerd goederen te verkopen (meestal namaaktassen of -sieraden). Deze e-mails zijn niet afkomstig van legitieme bedrijven en worden vaak door botnets verstuurd.

Sociale netwerksites: deze spam wordt door sociale netwerksites gegenereerd en naar de abonnees van de site gezonden. Dergelijke sites sturen vaak ongevraagde e-mails naar het hele adresboek van een gebruiker, meestal zonder de abonnee hiervan op de hoogte te stellen. Dit "spamachtige" gedrag is onwenselijk en daarom wordt er in onze gegevensverzamelingen geen onderscheid tussen gewenste en ongewenste e-mails van sociale netwerksites gemaakt.

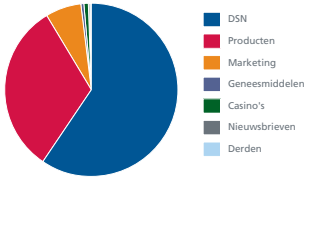
Software: pogingen om OEM-licenties (een OEM is meestal een hardwarefabrikant) als losse licenties te verkopen, of pogingen om gehackte of gekraakte softwarekopieën met hoge kortingen te verkopen.

Vacatures: het grootste deel van deze categorie bestaat uit een vorm van Nigeriaanse scam of een truc die draait om het winnen van vertrouwen. De mensen achter deze berichten azen op werklozen (of mensen die geen volledige baan hebben) en proberen hen geld te ontfutselen door middel van chequefraude of door ze over te halen geld wit te wassen of activiteiten uit te voeren die niet volledig legitiem zijn.

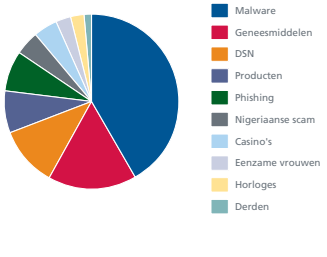
Argentinië



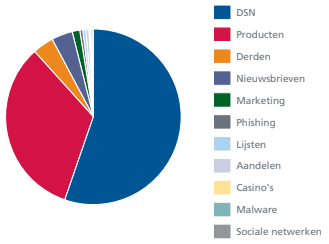
Australië



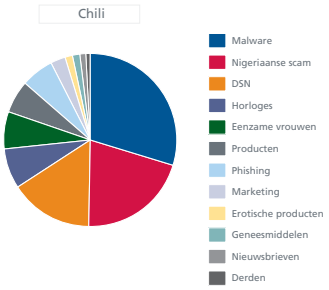
Brazilië



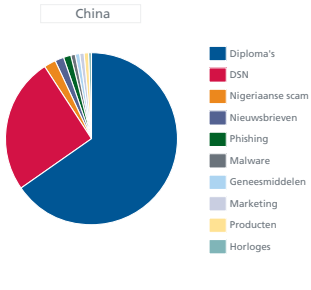
Canada



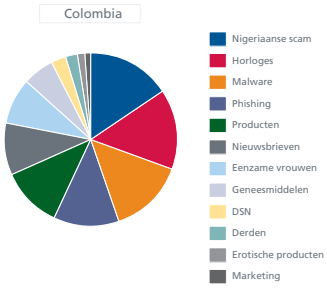
Chili



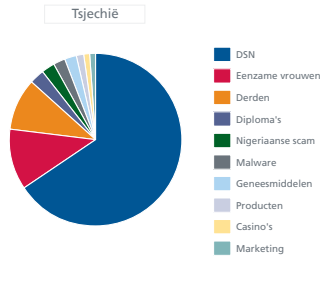
China



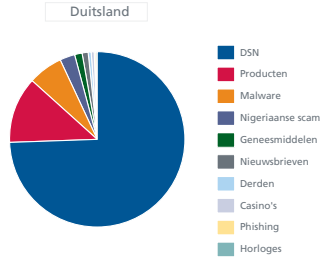
Colombia



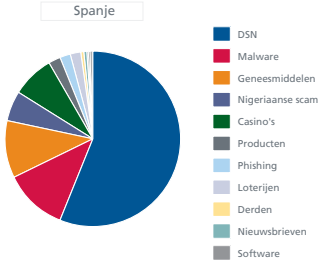
Tsjechië



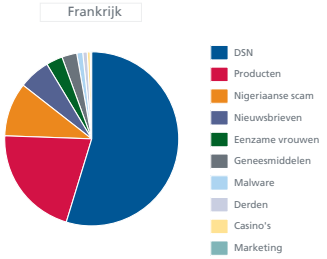
Duitsland



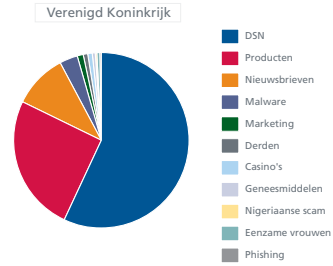
Spanje



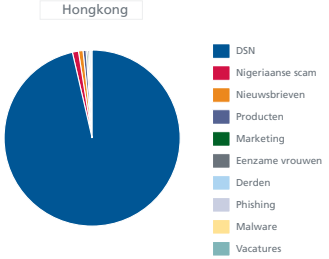
Frankrijk



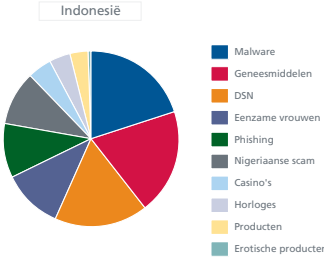
Verenigd Koninkrijk



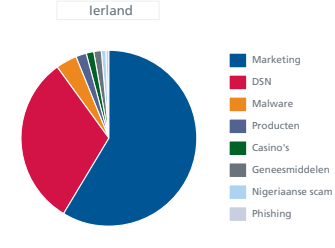
Hongkong



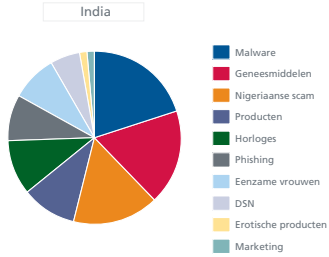
Indonesië



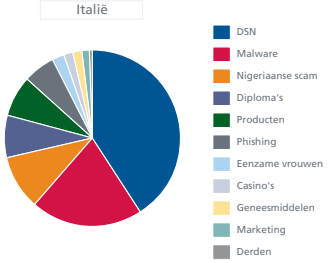
Ierland



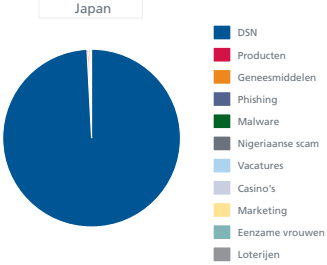
India



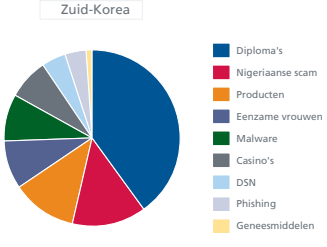
Italië



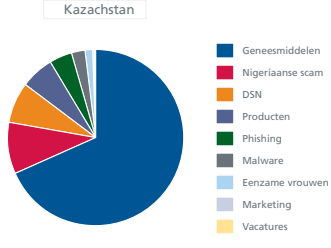
Japan



Zuid-Korea



Kazachstan



Afbeelding 3: spamonderwerpen kunnen per land grote verschillen vertonen. Deze cirkeldiagrammen geven aan hoe groot het aandeel van de populairste onderwerpen is (in elk land). De diagrammen vertegenwoordigen niet al het spamverkeer, alleen de populairste onderwerpen.

Een paar verrassingen

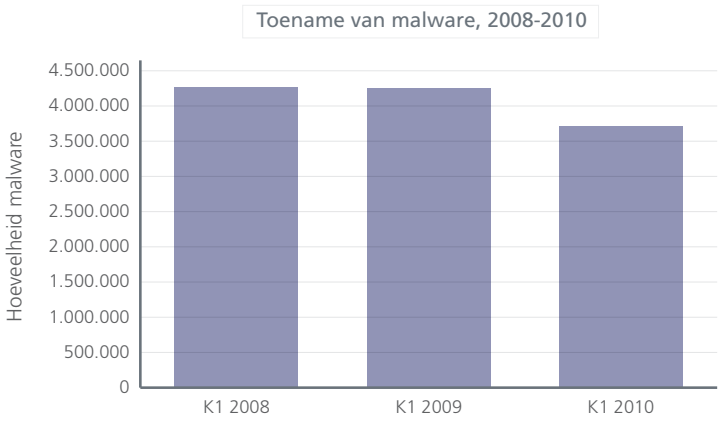
Het meest verrassende resultaat van deze analyse is de grote hoeveelheid diplomaspam uit China, Zuid-Korea en Vietnam. Met diplomaspam wordt reclame gemaakt voor valse documenten waarmee kwalificaties voor banen en andere activiteiten kunnen worden "aangetoond".

Singapore, Hongkong en Japan hebben allemaal een uitzonderlijk hoog percentage bezorgingsstatusberichten (DSN). Deze aantallen kunnen wijzen op problemen met e-mailfilters, waardoor spam niet vroeg genoeg wordt onderschept en tegengehouden om het aanmaken van deze berichten naar het valse afzenderadres te voorkomen.

Thailand, Roemenië, de Filippijnen, India, Indonesië, Colombia, Chili en Brazilië hebben de afgelopen vijf jaar allemaal grote vorderingen gemaakt op het gebied van internetontwikkeling. Deze snelle groei en de focus op toegang (in plaats van beveiliging) heeft mogelijk geleid tot een groter aandeel malware-infecties en spam.

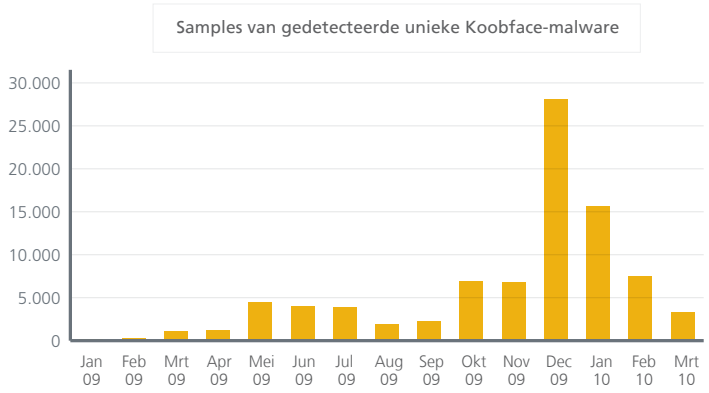
De groei van malware blijft "gezond"

In 2009 heeft McAfee Labs meer dan 16 miljoen malware-items gecatalogiseerd en bescherming tegen deze items ontwikkeld. Ter vergelijking: in 2008 was dit aantal iets meer dan 10 miljoen. Eind maart 2010 hebben we al meer dan drie miljoen malware-items gevonden en bescherming tegen deze items geboden. De resultaten van het eerste kwartaal wijzen erop dat de totale groei is gestabiliseerd. Wij verwachten echter dat we in 2010 *minstens* evenveel malware als in het voorgaande jaar zullen catalogiseren.

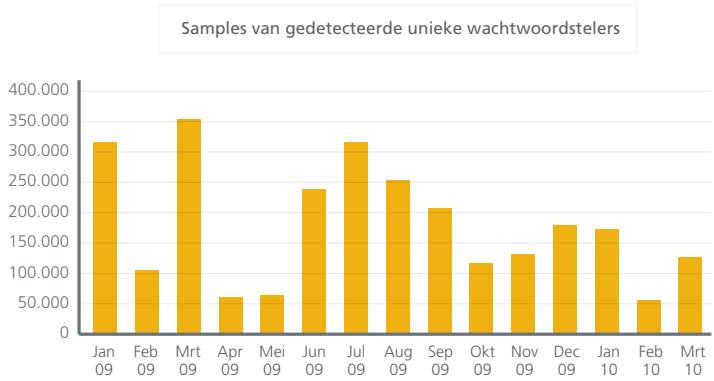


Afbeelding 4: een vergelijking van de toename van malware in het eerste kwartaal van de afgelopen drie jaar toont een lichte daling in 2010.

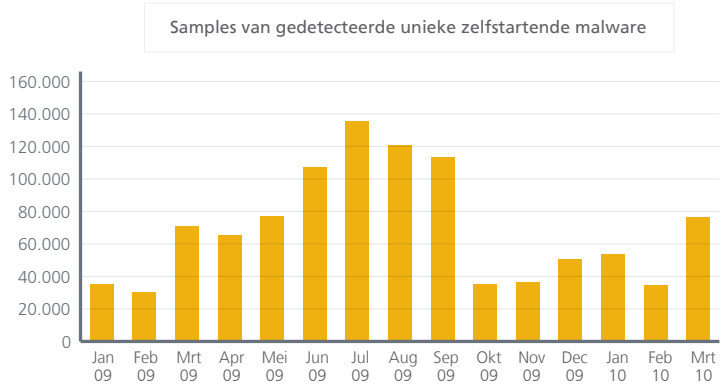
In andere grote malwaregebieden hebben we deze stabilisering ook geconstateerd. Houd er echter wel rekening mee dat deze cijfers incrementeel zijn, met andere woorden, ze geven de nieuwe malware weer die elk kwartaal door ons geregistreerd wordt. Het is nog steeds noodzakelijk om beschermd en alert te blijven. Hoe u het ook bekijkt, drie miljoen malware-items - bijna 40.000 items per dag - is nog steeds heel veel.



Afbeelding 5: het aantal nieuwe Koobface-varianten is snel gedaald sinds de piek in december, maar Facebook-gebruikers blijven veel hinder ondervinden.



Afbeelding 6: wachtwoordstelende trojaanse paarden richten zich vooral op de bankrekeninggegevens van hun slachtoffers.



Afbeelding 7: een van de meest actieve malwarecategorieën van dit kwartaal is de categorie zelfstartende wormen (malware op verwisselbare opslagapparatuur, voornamelijk USB-sticks). Aangezien zowel particuliere als zakelijke gebruikers over de hele wereld veel en graag gebruik maken van USB-sticks, blijft deze infectiedrager een belangrijk knelpunt.

Laten we even de "populairste" malware van dit moment doornemen. De volgende lijst bevat de meest gemelde malwaredetecties van consumenten over de hele wereld. (Deze lijst is meestal niet in alle delen van de wereld gelijk, maar dit kwartaal hebben alle gevolgde regio's dezelfde belangrijkste dreigingen gerapporteerd).

Top 5 van de wereldwijde malware

1. Generic! Atr: generieke malware voor verwisselbare apparaten.
2. Generic.dx: generieke downloaders en trojaanse paarden.
3. W32/Conficker.worm!inf: detecties van Conficker-wormen op verwisselbare apparaten.
4. Generieke potentieel ongewenste programma's: potentieel ongewenste programma's voor algemene doeleinden.
5. GameVance: online gamesoftware die anoniem statistische gegevens verzamelt.

Deze top 5 verschilt maar weinig van de resultaten uit vorige kwartalen. Twee malware-items uit de top 5 zijn zelfstartende malwareproducten (zelfs één met Conficker). Andere items zijn bedoeld voor verschillende wachtwoordstelende trojaanse paarden. Vaak kunnen we op generieke wijze valse beveiligingsproducten detecteren, zoals potentieel ongewenste programma's. Daarnaast is Internet Explorer altijd een favoriet doelwit voor cybercriminelen geweest. En dat brengt ons op operatie Aurora.

Operatie Aurora

Operatie Aurora was een van de meest besproken aanvallen dit kwartaal. Deze aanval vond eigenlijk eind 2009 plaats, maar operatie Aurora wordt nu als een van de belangrijkste gerichte aanvallen in de geschiedenis van internet beschouwd. De aanval maakt misbruik van een zero-day kwetsbaarheid en exploit in Internet Explorer. Met behulp van op maat gemaakte malware en vele versluieringslagen slaagden criminelen erin een zeer nauwkeurige aanval uit te voeren op meer dan dertig bedrijven en hun gegevens. Aurora kan de komende jaren een grote invloed hebben op de ontwikkeling van bedrijfsgerichte cybercriminaliteit.

Raadpleeg de volgende McAfee-blogs voor een gedetailleerde analyse van de aanval:

http://siblog.mcafee.com/cto/source-code-repositories-targeted-in-operation-aurora/

http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/

http://www.avertlabs.com/research/blog/index.php/2010/01/14/more-details-on-operation-aurora/

http://www.avertlabs.com/research/blog/index.php/2010/01/15/operation-aurora-leading-to-other-threats/

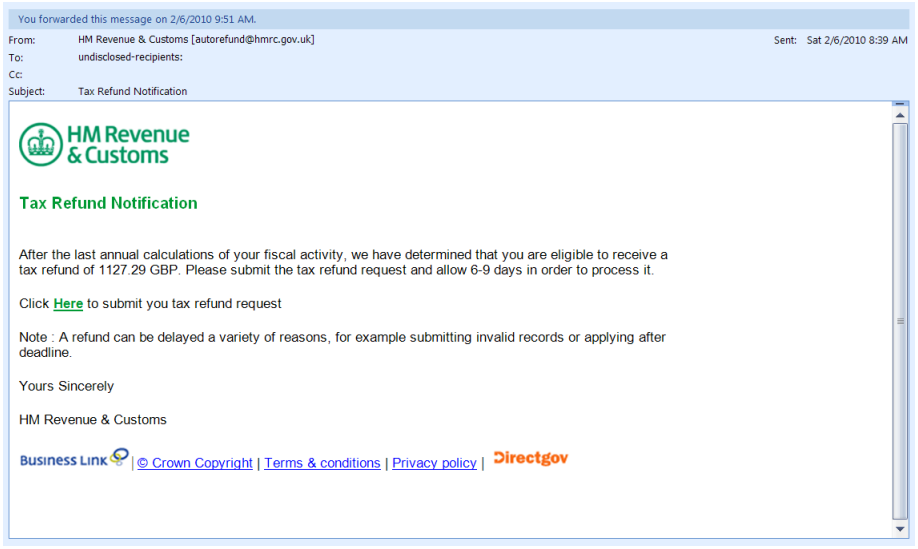
http://www.avertlabs.com/research/blog/index.php/2010/01/18/an-insight-into-the-aurora-communication-protocol/

Een uitstekende white paper biedt gedetailleerde informatie over Aurora en hoe vergelijkbare aanvallen kunnen worden voorkomen:

http://resources.mcafee.com/forms/Aurora_VDTRG_WP

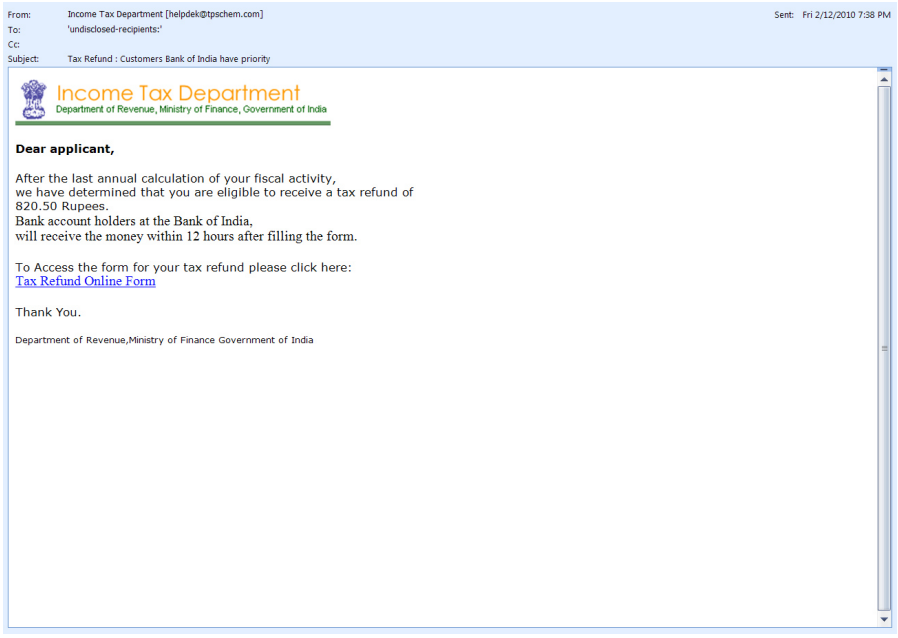
Belastingen: oplichtingstrucs, phishingpraktijken en valse websites

Belastinggerelateerde berichten zijn nog altijd een populair lokmiddel van cybercriminelen. In Amerika moeten de belastingaangiften omstreeks 15 april zijn ingediend en naarmate deze datum dichterbij komt, neemt het aantal berichten sterk toe. Dit jaar staken de oplichtingstrucs al vroeg de kop op: eind januari zijn we al begonnen met het opsporen en volgen van belastinggerelateerde oplichtingstrucs, phishingpraktijken en valse websites. Dit jaar heeft bovendien een internationaal tintje, omdat veel oplichtingstrucs en phishingpraktijken betrekking hebben op valse financiële instellingen in het buitenland.



Afbeelding 8: dit valse bericht van de "HM Revenue & Customs" (Britse belastingdienst) is de laatste tijd zeer populair.

Nietsvermoedende gebruikers worden bestookt met de gebruikelijke trucs, maar het lokaas heeft meestal wel betrekking op de tijd van het jaar: de lezer komt in aanmerking voor een belastingteruggave als hij of zij zo vriendelijk wil zijn de juiste papieren via internet in te dienen. Er is natuurlijk geen sprake van een echte teruggave, wel dreigt er gevaar voor identiteitsdiefstal en financiële verliezen.



Afbeelding 9: veel oplichtingspraktijken en spamberichten lijken afkomstig te zijn van de Bank of India.

En ook valse websites van de Internal Revenue Service (Amerikaanse belastingdienst) zijn populair:

Afbeelding 10: deze site werd gehost op een Braziliaanse server, maar dit soort sites wordt overal ter wereld aangetroffen.

Vanaf het midden van februari begon dit type websites een piek te vormen. Deze sites verspreiden "belasting-formulieren" en "belastingprogramma's", die het indienen van de belastingaangifte vergemakkelijken. Alle sites zijn echter vals en kwaadaardig.

Manipulatie van zoekmachines wordt steeds ingewikkelder

McAfee Labs constateerde in 2009 een aanzienlijke stijging in het aantal manipulaties van zoekmachines. Aanvallers maakten misbruik van de techniek achter de zoekmachineresultaten om de positie van koppelingen naar kwaadaardige websites omhoog te brengen. De cybercriminelen maakten uiteraard gebruik van de meest actuele termen en onderwerpen om zoveel mogelijk slachtoffers te maken. In het eerste kwartaal van 2010 werden de volgende zoekonderwerpen het vaakst gemanipuleerd:

- Aardbeving in Haïti
- Aardbeving in Chili/tsunami-alarm voor Hawaï
- Terugroepactie van Toyota
- Apple iPad
- 2010 NCAA-divisie/March Madness (laatste basketbaltoernooien in maart)
- Excuses van Tiger Woods (publiek schandaal)
- Aanval op orkatrainer in Shamu Stadium/haaiaanval in Florida

- Dodelijk bobslee-ongeluk
- Groundhog Day
- Wetsvoorstel tot hervorming gezondheidszorg (VS)

Aanvallers koppelen webpagina's vaak aan populaire zoektermen, die ze uit RSS-feeds, zoals Google Trends, hebben verkregen. De manipulatie wordt meestal snel duidelijk bij het volgen van een kwaadaardige koppeling: in plaats van de verwachte inhoud, wordt er een pagina geopend met alleen een stukje tekst en een aantal koppelingen. De laatste tijd plaatsen aanvallers hun inhoud in pdf-documenten om nog makkelijker slachtoffers te kunnen maken.

De gemanipuleerde pdf-documenten worden door Google verkend, geïndexeerd en naar QuickView geconverteerd, zodat er nog meer onwetende slachtoffers in de val kunnen trappen. Het doel van deze aanvallen is in de meeste gevallen het omleiden van gebruikers naar een valse antivirussite, waar valse beveiligingsproducten worden aangeboden.

Afbeelding 11: na het voltooien van de "scan" meldt het valse product dat er malware is gevonden en kan het slachtoffer waardeloze beveiligingssoftware kopen om de "infecties" te verwijderen.

McAfee Labs is onlangs een vorm van zoekmachinemanipulatie op het spoor gekomen die leidde tot verschillende soorten klikfraude en netwerkmisbruik. Een voorbeeld uit dit kwartaal is een truc waarbij de reputatie van Digg (een Amerikaanse website die nieuws publiceert) werd gebruikt om de aanval uit te voeren. Wanneer nietsvermoedende gebruikers de hyperlink op Digg volgden, werd de video in afbeelding 12 afgespeeld.

Afbeelding 12: bij deze Google-klikfraude werden de slachtoffers via de nieuwssite Digg in de val gelokt.

Deze "Hot Video" hield een paar JavaScript- en Google-advertenties verborgen. Als de slachtoffers ergens op de pagina klikten, leverde dit de scammer advertentie-inkomsten op. Andere voorbeelden zijn minder omslachtig: browsers worden omgeleid naar een andere pagina met zoekresultaten, die - hoewel ze gelijk zijn aan de oorspronkelijke resultaten - de aanvaller mogelijk advertentie-inkomsten opleveren.

De hoeveelheid spam die wordt verstuurd op basis van gemanipuleerde zoekresultaten is nog lang niet zo hoog als de hoeveelheid "gewone" spam-e-mail (circa 90 procent van het totale e-mailverkeer). De toegenomen manipulatie van zoekresultaten is echter wel zorgelijk.

Wachtwoordstelers en valse beveiligingssoftware dringen door tot sociale netwerken

In ons rapport *Verwachte dreigingen in 2010*, gepubliceerd in december 2009, spraken we de verwachting uit dat het aantal aanvallen op sociale netwerken door wachtwoordstelende trojaanse paarden en andere malware in 2010 zou stijgen.[2] In het huidige kwartaal hebben we verschillende voorbeelden gezien die deze verwachting bevestigden.

De Zeus-familie, die we meestal als PWS-Zbot en Spy-Agent.bw tegenkomen, is het wachtwoordstelende trojaanse paard bij uitstek. Deze malware is gespecialiseerd in het onderscheppen van aanmeldingsgegevens van banksites. Zeus is slechts een van de instrumenten die veel door cybercriminelen worden gebruikt, onder andere voor het koppelen van wachtwoordstelers aan andere typen illegaal online materiaal. Zo wordt Zeus bijvoorbeeld gehost op computers waarop ook kinderporno is opgeslagen, of samen met andere soorten trojaanse paarden geïnstalleerd, bijvoorbeeld valse beveiligingssoftware (ook wel valse waarschuwingssoftware of valse antivirussoftware genoemd).

In dit kwartaal hebben we allerlei soorten verrassingen onder ogen gehad die samen met Zeus werden geïnstalleerd. En wie waren het primaire doelwit van deze aanvallen? Gebruikers van Facebook.

De meeste aanvallen volgen dit patroon:

- De aanvallers lanceren een grote oplichtingscampagne. In de meeste gevallen wordt met een vals bericht over het opnieuw instellen van een wachtwoord de aandacht van de slachtoffers getrokken, bijvoorbeeld:
  - » "Wij hebben enkele maatregelen genomen om de veiligheid van onze klanten beter te kunnen garanderen. Als gevolg daarvan is uw wachtwoord gewijzigd. U vindt uw nieuwe wachtwoord in het bijgesloten document".
- Het bijgesloten document bevat meestal een variant van het trojaanse paard Bredolab of Pushdo.
- Het Bredolab/Pushdo-netwerk doet dienst als installatieprogramma voor de Zeus-familie en vereist geen tussenkomst van de gebruiker. Maar dat is niet alles. Zodra de gebruiker de bijlage opent, wordt Bredolab/Pushdo geïnstalleerd en vervolgens kan ook Zeus worden geïnstalleerd en beheerd, alsmede elk ander trojaans paard dat de aanvallers nodig denken te hebben.
- In dit kwartaal zijn we het vaakst installaties van trojaanse paarden voor valse beveiligingssoftware tegengekomen.

Waarom valse antivirussoftware? Omdat zowel malwareontwikkelaars als malwareverspreiders er geld mee verdienen. De meeste trojaanse paarden voor valse waarschuwingssoftware werken via een partnerprogramma, waarbij een tussenpersoon een klein deel van de winst krijgt voor elke nieuwe installatie van de software.

Gebruikers van Facebook hadden niet alleen te maken met Zeus en aanvallen van valse beveiligingssoftware, maar ook met nieuwe varianten van de W32/Koobface-worm. In maart werden er meer dan 150 websites ontdekt met kwaadaardige bestanden in de map .sys (die verborgen is op UNIX-systemen).

Enkele voorbeelden van deze websites:

brand[verwijderd]b.dk/.sys/?getexe=p.exe

brand[verwijderd]b.dk/.sys/?getexe=v2captcha21.exe

brand[verwijderd]b.dk/.sys/?getexe=go.exe

alv[verwijderd]n.dk/.sys/?getexe=pp.14.exe

alv[verwijderd]n.dk/.sys/?getexe=v2prx.exe

car[verwijderd]ort.com.au/.sys/?getexe=pp.14.exe

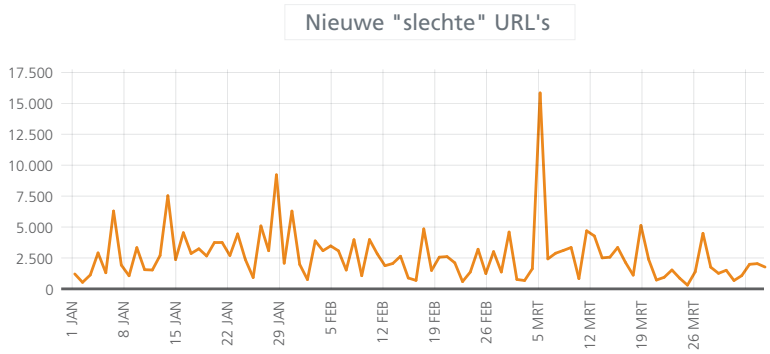
car[verwijderd]ort.com.au/.sys/?getexe=fb.101.exe

2. Het rapport is verkrijgbaar in negen talen. http://www.mcafee.com/us/threat_center/white_paper.html

De bestanden die door deze gehackte hosts werden aangeboden, bestonden voornamelijk uit Koobface-malware, maar omvatten tevens generieke downloaders, wijzigingsprogramma's voor hostbestanden, wachtwoordstelers, enzovoort.

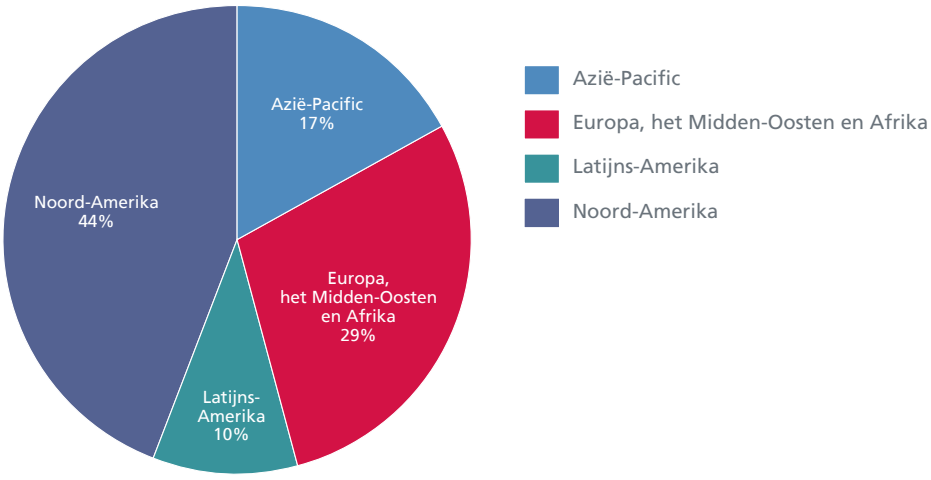
Toename van kwaadaardige domeinen

In dit kwartaal waren de internetdreigingen zeer actief. McAfee Labs heeft verschillende trends geïdentificeerd: van servers die zeer gerichte aanvallen ondersteunen tot de gebruikelijke Koobface-malware, Zeus-malware, phishingpogingen met betaalpassen, romantische formules, belastingformulieren en generieke accountgegevens. We hebben ook een aanzienlijke stijging geconstateerd in het aantal bedrijven dat als spyware- of adwarebedrijf werd aangemerkt en hiertegen protest aantekende.



Afbeelding 13: nieuwe websites met een kwaadaardige reputatie, dagelijks gerapporteerd door McAfee's TrustedSource-technologie. In dit kwartaal werden er weer meer kwaadaardige domeinen geregistreerd, er ontstond zelfs een piek van meer dan 15.000 nieuwe kwaadaardige sites op één dag.

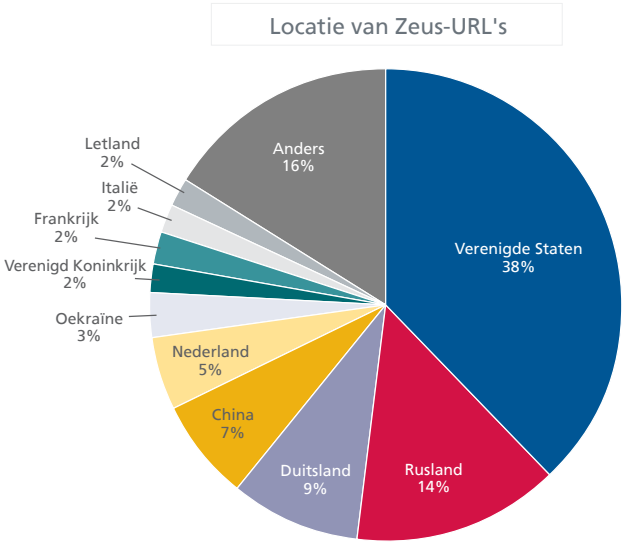
In afbeelding 13 ziet u het patroon van de kwaadaardige activiteiten die door ons in kaart zijn gebracht. Nieuwe populaire exploits of botnets veroorzaakten een duidelijke piek in het aantal websites met een kwaadaardige reputatie. Binnen een dag of twee was het aantal nieuwe slechte sites echter weer tot het gebruikelijke niveau gedaald. McAfee Labs heeft tevens een duidelijke stijging geconstateerd in de hoeveelheid communicatie naar en van kwaadaardige servers die botnets beheren. Het grootste deel van deze servers vertoont in dat geval bepaalde kenmerken die door onze unieke kruiscorrelatie van dreigingsvectoren kan worden geïdentificeerd. De plotselinge toename van slechte URL's op 2 maart werd bijvoorbeeld voorafgegaan door een duidelijke piek in e-maildreigingen op 14 februari.



Afbeelding 14: zoals gebruikelijk bevinden de meeste servers die kwaadaardige internetinhoud hosten zich in de Verenigde Staten.

Deze samenklontering in de VS wordt nog duidelijker wanneer we niet alleen naar de locatie van de servers maar ook naar de locatie van de kwaadaardige URL's kijken. Het blijkt dat 98 procent van de kwaadaardige URL's op een server in de Verenigde Staten wordt gehost. Dit komt hoofdzakelijk omdat de meeste algemene internetdiensten die essentieel zijn voor Web 2.0 in overvloed in dit land aanwezig zijn en omdat deze diensten op grote schaal door malwareverspreiders worden misbruikt. Van de resterende twee procent wordt 61 procent in China en 34 procent in Canada gehost.

Een van de grootste stijgers op het gebied van kwaadaardige URL's en websites is de snelgroeiende Zeus-familie. Zeus is gebruiksvriendelijk en zeer populair onder cybercriminelen. Het is daarom niet verrassend dat er dit kwartaal een grote verschuiving heeft plaatsgevonden naar zeer kwaadaardige servers die gebruik maken van geautomatiseerde domeinregistraties en fast flux-technieken (waarbij in één domein een groot aantal IP-adressen wordt gebruikt om detectie te vermijden). Als we eenmaal één Zeus-computer hebben gevonden, is het niet moeilijk nog tientallen andere op te sporen. Een van de door ons opgespoorde Zeus-beheerservers had de regie over 160 andere kwaadaardige domeinen, die voor van alles werden gebruikt, van sociale netwerksites en infecties die via het delen van media worden overgebracht, tot phishingtrucs voor belastingsites en andere aanmeldingsgegevens.



Afbeelding 15: de Zeus-URL's worden voornamelijk aangetroffen in de Verenigde Staten, terwijl Europa circa 40 procent voor zijn rekening neemt.

Aanvallen op clients

De problemen met clientbeveiliging blijven de lijst met belangrijke kwetsbaarheden dit kwartaal domineren. Onze sensoren hebben meerdere aanvallen via het SSL-communicatieprotocol (Secure Sockets Layer) geregistreerd die afkomstig waren uit het Pushdo-botnet. Daarnaast waren er pogingen tot het lanceren van gerichte DoS-aanvallen met behulp van SSL-aanvragen.

McAfee Labs heeft dit kwartaal meerdere zero-day aanvallen geregistreerd. Enkele van de belangrijkste aanvallen waren gericht op Microsoft Internet Explorer, Adobe Acrobat en Adobe Reader.

- *"Operatie Aurora" MS10-002 HTML Object Memory Corruption Vulnerability* (Beveiligingslek met betrekking tot een beschadigd geheugen door HTML-objecten): CVE-2010-0249. Op 13 januari identificeerde McAfee Labs een gerichte zero-day aanval op een voorheen onbekende kwetsbaarheid in Internet Explorer. Microsoft werd hiervan op de hoogte gebracht en bevestigde het probleem. De volgende dag publiceerde Microsoft een advies.[3] Een dag later bracht Metasploit een werkende exploit uit. Aangezien deze kwetsbaarheid op brede schaal werd misbruikt, bracht Microsoft op 21 januari een noodpatch uit. Onze live sensoren registreren nog steeds vele pogingen om dit lek te misbruiken.
- *Internet Explorer Dynamic OBJECT tag and URLMON sniffing vulnerabilities* (Beveiligingslekken [sniffing] met betrekking tot Internet Explorer Dynamic OBJECT-tags en URLMON): CVE-2010-0255. Op 3 februari 2010 werd de Black Hat conferentie gehouden in Washington, DC. Een groep onderzoekers presenteerde tijdens deze conferentie twee kwetsbaarheden in Internet Explorer. De problemen werden verder besproken op de Core Security-website.

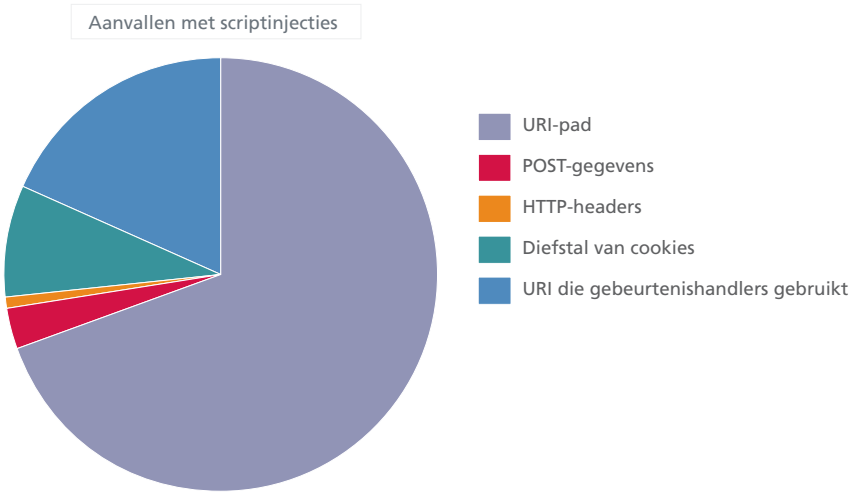
3. http://www.microsoft.com/technet/security/advisory/979352.mspx

De kwetsbaarheden leiden tot een domeinoverschrijdende blootstelling van gegevens, waarmee een aanvaller toegang kan krijgen tot gevoelige bestanden die later voor gerichte aanvallen kunnen worden gebruikt. Op het moment dat dit rapport werd samengesteld, waren er nog steeds geen patches voor deze problemen uitgebracht.

- *Adobe Acrobat and Reader Remote Code Execution Vulnerability* (Beveiligingslek met betrekking tot het extern uitvoeren van code in Adobe Acrobat en Reader): CVE-2010-0188. Op 16 februari heeft Adobe een essentiële kwetsbaarheid in Reader gepatcht die kon leiden tot het extern uitvoeren van code. McAfee Labs heeft malwaresamples gevonden die dit probleem actief in het wild misbruiken. Gebruikers van Acrobat en Reader wordt aangeraden een update uit te voeren met behulp van deze patches.[4]
- *Uninitialized Memory Corruption Vulnerability* (Beveiligingslek met betrekking tot beschadiging van niet-geïnitialiseerd geheugen): CVE-2010-0806. Op 9 maart maakte Microsoft bekend dat er misbruik werd gemaakt van een voorheen onbekende kwetsbaarheid in Internet Explorer, versie 5, 6 en 7 (Internet Explorer 8 bleef buiten schot). Gebruikers van Internet Explorer wordt geadviseerd een update uit te voeren met behulp van deze noodpatch die op 30 maart werd uitgebracht.[5]

XSS-aanvallen (cross-site scripting) openen de deur

Onze live sensoren hebben dit kwartaal meerdere pogingen tot scriptinjecties geregistreerd. We hebben de gegevens over de aanvallen (waarbij gebruik werd gemaakt van HTTP) in enkele brede categorieën ondergebracht.



Afbeelding 16: XSS-aanvallen (met behulp van HTTP) per categorie.

Justitie en cybercriminaliteit

DarkMarket: Devilman en JiLsi bekennen schuld

Tussen 2006 en 2008 was DarkMarket een van de drukst bezochte ondergrondse forums op het gebied van "carding" (een plaats voor het verhandelen van onder andere gestolen creditcard- en betaalpasnummers). Hoewel belangstellenden alleen op uitnodiging tot DarkMarket werden toegelaten, waren er meer dan 2000 geregistreerde gebruikers.

Het forum werd in oktober 2008 geïnfiltreerd en platgelegd door de FBI. Met de hulp van andere politie-organisaties kon de FBI meer dan 50 arrestaties verrichten in de Verenigde Staten, het Verenigd Koninkrijk, Turkije en Duitsland. Tot de arrestanten behoorden Cagatay Evyapan (alias Chao, in Turkije), Mert Ortac (alias Kier, in Turkije) en Markus Kellerer (alias Matrix001, in Duitsland).

Twee vooraanstaande DarkMarket-leden hebben dit kwartaal schuld bekend voor het Blackfriars Crown Court (rechtbank voor strafzaken) in Londen. De rechtbank kan hen een maximale gevangenisstraf van tien jaar opleggen.

Het eerste DarkMarket-lid was Renukanth Subramaniam, ook wel "JiLsi" genoemd. Deze 33-jarige Sri Lankaan was websitebeheerder en een van de eerste forumleden.[6] Het tweede lid was John McHugh. De 69-jarige John McHugh, alias "Devilman", voerde allerlei controles uit. Tot zijn taken behoorde bijvoorbeeld het controleren van gehackte creditcards die nieuwe abonnees bij het bestuur moesten inleveren om als lid te worden geaccepteerd.[7]

4. http://www.adobe.com/support/security/bulletins/apsb10-07.html
5. http://www.microsoft.com/technet/security/Bulletin/MS10-018.mspx
6. "Pizza delivery man cops to life in DarkMarket" (Pizzabezorger komt tot leven in DarkMarket), The Register. http://www.theregister.co.uk/2010/01/14/darkmarket_fraudster_guilty_plea/
7. "OAP internet fraud expert" (Gepensioneerde internetfraude-expert), The Star. http://www.thestar.co.uk/doncaster/OAP-internet-fraud-expert.5985536.jp

Wiseguys-botnet

We lezen regelmatig dat spammers erin slagen de CAPTCHA-verificatie (Completely Automated Public Turing test to tell Computers and Humans Apart) te omzeilen. Zo kunnen spammers met behulp van bot-geïnfecteerde computers een groot aantal willekeurige e-mailaccounts aanmaken die vervolgens voor spamdoeleinden kunnen worden gebruikt.

In februari onthulde een federale rechter in Newark (in de Amerikaanse staat New Jersey) het nieuwste gebruik van een door botnets ondersteunde CAPTCHA-kraker. De verdachten gebruikten de "bots" om op websites van legitieme ticketverkopers kaartjes voor belangrijke concerten en sportevenementen te kopen. De botnetbeheerders verkochten deze tickets vervolgens weer op internet tegen een flink hogere prijs.

Volgens de aanklacht was de gedistribueerde software ontwikkeld door programmeurs in Bulgarije. De toepassing slaagde erin de beveiligingsmaatregelen (die ontwikkeld waren om het aantal individuele ticketaankopen te beperken) te omzeilen en er met de beste plaatsen vandoor te gaan. Deze truc werd, in tegenstelling tot veel andere trucs, niet via gewone botnets uitgevoerd, maar met computers die speciaal voor dit doel waren bestemd. Het netwerk slaagde erin tussen eind 2002 en januari 2009 meer dan 1,5 miljoen eersteklas tickets voor evenementen te kopen. De winst bedroeg naar schatting 28,9 miljoen dollar.

De werknemers, contractanten en beklaagden achter deze oplichterij staan bekend onder de naam Wiseguys. Deze naam is gebaseerd op de naam van het bedrijf in Nevada dat door hen werd opgericht (Wiseguy Tickets, Inc.). Het Wiseguys-botnet bestond uit een landelijk netwerk van computers dat duizenden tickets per minuut kocht. Het netwerk moest een imposante lijst met taken afwerken:

- De websites van online ticketverkopers in de gaten houden om het exacte moment te bepalen waarop tickets voor populaire evenementen te koop worden aangeboden.
- Duizenden verbindingen openen zodra de tickets in de verkoop gaan.
- De CAPTCHA-verificatie in een fractie van een seconde omzeilen. Aangezien een mens vijf tot tien seconden nodig heeft, werden de legitieme kopers meteen op achterstand gezet.
- Vrijwel meteen een lijst met honderden van de beste tickets opstellen (onder toezicht van de werknemers van Wiseguys).
- Alle velden invullen die nodig zijn om de koop te voltooien, inclusief creditcardgegevens en valse e-mailadressen.

Afbeelding 17: een online aanbieding van Wiseguy Tickets. (Bron: McAfee)

De aanklacht beschrijft hoe de Wiseguys profiteerden van populaire evenementen, zoals de BCS Football Championship Game (BCS-kampioenschap American football), een concert van Barbra Streisand in Chicago, concerten van Hannah Montana in New Jersey en de 2008 Bruce Springsteen Tour.[8] Voor dit laatste evenement kocht het botnet circa 11.800 tickets.

8. "United States of America v. Kenneth Lowson et al." (Verenigde Staten van Amerika versus Kenneth Lowson e.a.), Amerikaanse District Court, District of New Jersey. http://media.nj.com/ledgerupdates_impact/other/Wiseguys%20Indictment%20-%20Filed.pdf

Een van hun laatste misdaden vond plaats in januari 2009, toen het botnet zich uitgaf voor 1000 individuele kopers van tickets voor de NFL-voorronde tussen de New York Giants en de Philadelphia Eagles, in het Giants Stadium in East Rutherford, New Jersey.

Operatie laatste stuiver

De FTC (de Amerikaanse mededingingsautoriteit) heeft dit kwartaal zeven zaken in behandeling tegen criminelen die zich schuldig hebben gemaakt aan oplichtingspraktijken op het gebied van thuiswerk en vacatures.[9] Uit de in februari aangekondigde juridische stappen blijkt dat de autoriteit zeven instellingen heeft aangeklaagd. Dit brengt het totaal aantal zaken van het afgelopen jaar op elf.

Een van de aangeklaagde bedrijven, Real Wealth Inc., maakte meer dan 100.000 slachtoffers door mensen boekjes te verkopen waarin zogenaamd werd uitgelegd hoe ze geld konden verdienen door overheidssubsidies aan te vragen en door vanuit huis kaarten en enveloppen te versturen, aldus de aanklacht van de Amerikaanse mededingingsautoriteit. Met behulp van directmailcampagnes die soms op ouderen en gehandicapten waren gericht, wist Real Wealth consumenten met bedrieglijke teksten te verleiden, bijvoorbeeld "Ontvang maximaal 9250 dollar met mijn eenvoudige drieminutenformulier" of "Ik hoef alleen maar elke dag 30 kaarten te versturen en ik verdien 350 dollar per week!". Real Wealth beweerde ook dat consumenten "1500 dollar per week of meer in contant geld konden verdienen" door gebruik te maken van "geheimen" over de "financiële injectie van 700 miljard dollar in de bankensector".

Een andere aanklacht had betrekking op Darling Angel Pin Creations. Dit bedrijf hield consumenten in internetadvertenties voor dat ze via de aankoop van een startpakket tot wel 500 dollar per week konden verdienen met het verzamelen van angel pins (speldjes met een engeltje).

Mariposa-botnet

In februari arresteerde de Spaanse Guardia Civil verschillende leden van een criminele bende die het Mariposa-botnet beheerden. Dit botnet, dat voor het eerst actief werd in mei 2009, was erin geslaagd via verschillende soorten malware meer dan 13 miljoen pc's in 190 landen te kapen[10], voordat het in december 2009 werd uitgeschakeld. Het Mariposa-botnet was ontworpen voor het stelen van creditcardgegevens, online wachtwoorden voor banksites, accountgegevens voor sociale netwerksites en andere gevoelige gegevens.
De malware verspreidde zich via peer-to-peer-netwerken, geïnfecteerde USB-sticks en MSN-koppelingen via welke surfers naar geïnfecteerde websites werden geleid. Als er weer een slachtoffer was gevonden, installeerde de Mariposa-botclient verschillende soorten malware om meer controle over de gehackte systemen te krijgen, bijvoorbeeld geavanceerde keyloggers, trojaanse paarden voor banksites (zoals Zeus), trojaanse paarden voor externe toegang, enzovoort.

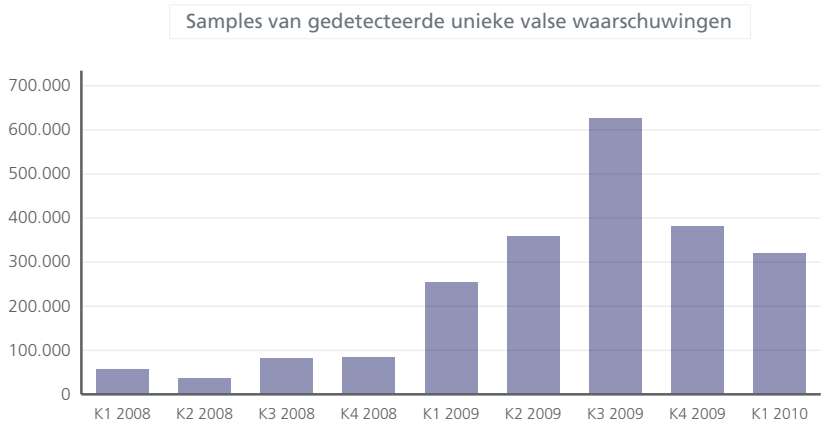
De criminele bende noemde zichzelf het DDP Team (een afkorting van *días de pesadilla*, of nachtmerriedagen). We vonden deze verwijzing door middel van enkele WHOIS-query's, via welke we terechtkwamen bij websites die deze criminelen hadden gemaakt voor het verspreiden van hun malware.

Cyberaanvallen

In maart maakte McAfee consumenten erop attent dat "scareware" (valse beveiligings- of valse antivirussoftware) mogelijk de duurste online oplichtingstruc van 2010 is. Deze scareware kan veel geld kosten en schade aan computers van gebruikers veroorzaken.[11] In deze paragraaf geven we u details en achtergrondinformatie over de cijfers die in deze aankondiging stonden vermeld.

Bij McAfee gebruiken we het label Fake Alert voor deze trojaanse familie, die scareware, valse antivirus-programma's en andere software omvat. Zoals u ziet in afbeelding 18 heeft deze categorie malware in 2009 een zeer snelle stijging doorgemaakt. In het huidige kwartaal konden we alleen al tussen 1 en 10 maart 45.000 nieuwe samples aan onze malwareverzameling toevoegen. (Met samples bedoelen we alle typen malware die gerelateerd zijn aan scareware: downloaders, droppers, scripts, installatieprogramma's en de vele bestanden waaruit elk product bestaat.)

9. "FTC Cracks Down on Con Artists Who Target Jobless Americans" (FTC treedt op tegen oplichters die zich richten op werkloze Amerikanen), Federal Trade Commission. http://www.ftc.gov/opa/2010/02/bottomdollar.shtm
10. "How FBI, Police Busted Massive Botnet" (Hoe FBI en politie een enorm botnet platlegden), Hacking Expose. http://hackingexpose.blogspot.com/2010/03/how-fbi-police-busted-massive-botnet.html
11. "McAfee, Inc. Unveils New Consumer Threat Alert Program: A Warning for Consumers about the Most Dangerous Online Threats" (McAfee Inc. biedt consumenten nieuw waarschuwingsprogramma: een waarschuwing aan consumenten over de gevaarlijkste internetdreigingen), McAfee. http://newsroom.mcafee.com/article_display.cfm?article_id=3631



Afbeelding 18: het aantal samples van valse beveiligingssoftware bereikte een piek in het derde kwartaal van 2009; het totale aantal samples blijft echter hoog voor deze lucratieve vorm van cybercriminaliteit.

Tussen januari 2004 en december 2009 werden er meer dan 3000 scarewareproducten door McAfee Labs gedetecteerd. Een groot deel van deze producten heeft een korte levensduur (enkele weken of maanden), maar andere producten, die misschien al in 2004 zijn gemaakt, circuleren nog steeds op internet. Van de helft van deze scarewareproducten weten we het jaar waarin ze voor het eerst verschenen. In dit kwartaal zijn er meer dan 170 uitgebracht.

Voor veel producten wordt alleen de naam gewijzigd. Hierdoor wordt de kans om slachtoffers te maken veel groter en tegelijkertijd de hoeveelheid werk voor de ontwikkelaars verminderd. Scarewarebedrijven creëren bijvoorbeeld een groot aantal websites met één valse aanbieding die onder verschillende namen wordt herhaald.

Afbeelding 19: de vormgeving van valse waarschuwingssoftware blijft vaak gelijk, terwijl de productnaam wordt veranderd.

We hebben duizenden valse waarschuwingsproducten onder ogen gehad, maar toch hebben we slechts een klein aantal scarewarebedrijven gevonden, misschien 30 tot 50. De ontwikkelaars werken met veel dochterondernemingen en partners om hun sporen te verbergen en de verkoop te verhogen. Tijdens onze analyse van 2000 producten zijn we erin geslaagd voor elk product de naam van het bedrijf te achterhalen.

Scarewarebedrijven werken vaak openlijk; sommige deinzen er bijvoorbeeld niet voor terug om LinkedIn-profielen aan te maken. Als de druk te hoog wordt, beginnen ze eenvoudig een "nieuw" bedrijf. Scarewarebedrijven die de verkoop willen opdrijven, huren dochterondernemingen in en beloven hoge provisies voor hun diensten, soms tot wel 75 procent van de verkoopprijs.

Een collega uit de beveiligingswereld heeft zes maanden lang de productieservers van een van de grootste scarewarebedrijven geobserveerd. In slechts tien dagen telde hij vier miljoen downloads (dat wil zeggen vier miljoen scareware-infecties). Het ging hierbij nog maar om één bedrijf, en sommige slachtoffers haalden meerdere downloads per dag op. Op basis van deze cijfers kunnen we ervan uitgaan dat er wereldwijd per dag één miljoen mensen het slachtoffer van scareware worden.[12]

Niet alle downloads worden bewust opgehaald. Toch ontving dit scarewarebedrijf in elf maanden tijd meer dan 4,5 miljoen bestellingen, daadwerkelijke verzoeken van gebruikers dus. We kunnen er daarom rustig vanuit gaan dat dit bedrijf een jaaromzet van meer dan 180 miljoen dollar behaalde.

Maar dat is niet alles: deze bedrijven verkopen niet alleen scareware. Ze bieden vaak ook andere valse producten aan (multimediasoftware, fitnesssoftware, gezinssoftware, enz.). En natuurlijk pornografie. Het is dus aannemelijk dat hun omzet nog veel groter is.

Hacktivisme

Naast aanvallen van cybercriminelen worden er ook veel politiek gemotiveerde aanvallen uitgevoerd. In januari lag de Wit-Russische mensenrechtenorganisatie Charter97 weer eens onder vuur. Deze nieuws- en oppositiewebsite werd de afgelopen maanden regelmatig met DDoS-campagnes bestookt.[13] In januari werd de website van de Russische *Novaya Gazeta* een week lang verlamd door een aanhoudende aanval van hackers.[14] "Dit was niet het werk van amateurs of hooligans", zegt Andrei Lipsky van de *Novaya Gazeta*. "Het was een weloverwogen actie. We kunnen alleen maar raden wie hier achter zit."

In februari kraakte een hacker de database van het elektronisch declaratiesysteem van de belastingdienst in Letland.[15] Een groep die zichzelf het "vierde leger van het ontwaakte volk" (4ATA) noemt, had zich toegang verschaft tot meer dan zeven miljoen documenten van de belastingdienst. "Het doel van de groep is het ontmaskeren van de mensen die het land hebben geplunderd", vertelt een van de vermoedelijke hackers (die de alias Neo gebruikt) aan de producers van de Letse talkshow Kas Notiek Latvija. Het interview staat op de website van de show. Een andere wereldwijde hackergroep, met de niet zo originele naam Anonymous, heeft op duidelijke wijze het Project Chanology aangekondigd. Dit in 2008 gestarte project is een doorlopende campagne die het uiteenvallen van de Scientologykerk tot doel heeft.[16] In februari van dit jaar begon de groep websites van de Australische regering met DoS-aanvallen te bestoken. De protestactie, die Operation Titstorm werd genoemd, is gericht tegen een voorstel van de regering om internetinhoud te filteren en toegang tot sites met extreme seksuele inhoud te blokkeren. Hun doelwitten zijn onder andere het Australische ministerie van communicatie (dat een pilot van de controversiële plannen uitvoert) en de homepage van premier Kevin Rudd. (De homepage van de premier werd met porno bezoedeld).[17] Hackers hebben ook aanvallen gericht op een website van de Australian Communications and Media Authority.

12. Panorama de la cybercriminalité–Année 2009 (Overzicht van de cybercriminaliteit, 2009), Club de la Sécurité de l'Information Français. http://www.clusif.asso.fr/fr/infos/event/#conf100113
13. "DDoS attack on charter97.org" (DDoS-aanval op charter97.org), Charter97. http://ww.charter97.org/en/news/2010/1/29/25857/?1
14. "Russia's Novaya Gazeta Web Site Hacked, Paralyzed" (Website van Russische Novaya Gazeta gehackt, verlamd), NBC4i. http://www2.nbc4i.com/cmh/news/local/article/russias_novaya_gazeta_web_site_hacked_paralyzed/31084/
15. "Massive security breach suspected at Latvian tax office" (Enorm beveiligingslek vermoed bij belastingkantoor in Letland), Monsters and Critics News. http://www.monstersandcritics.com/news/europe/news/article_1533738.php/Massive-security-breach-suspected-at-Latvian-tax-office
16. "The Assclown Offensive: How to Enrage the Church of Scientology" (Het Assclown-offensief: hoe kunt u de Scientologykerk tot razernij brengen), Wired. http://www.wired.com/culture/culturereviews/magazine/17-10/mf_chanology
17. Kathy Marks, "Operation Titstorm—Hackers Declare War on Aussie" (Operation Titstorm: hackers verklaren Australië de oorlog), The New Zealand Herald. http://www.nzherald.co.nz/compute/news/article.cfm?c_id=1501832&objectid=10625493

Afbeelding 20: hackers verspreidden deze flyer om deelnemers te werven voor een actie tegen het censureren van pornosites.

Over de auteurs

Dit rapport is geschreven door Pedro Bueno, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar en Adam Wosotowsky van McAfee Labs.

McAfee Labs™

McAfee Labs, het wereldwijde onderzoeksteam van McAfee Inc., is de enige onderzoeksorganisatie die zich volledig richt op alle dreigingsvectoren (malware, internet, e-mail, netwerk en kwetsbaarheden). McAfee Labs verzamelt informatie die afkomstig is van zijn miljoenen sensoren en zijn technologieën voor internetreputaties, zoals Artemis en TrustedSource. McAfee Labs beschikt over 350 multidisciplinaire onderzoekers in 30 landen. Deze onderzoekers volgen het volledige scala aan dreigingen in real time, identificeren kwetsbaarheden in toepassingen, analyseren en correleren risico's en maken onmiddellijk herstel mogelijk om bedrijven en consumenten te beschermen.

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. www.mcafee.com/nl.

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

9395rpt_quarterly-threat-q1_0410_ETMG