



MessageLabs Intelligence: augustus 2009

“Cutwail getroffen door de afsluiting van zijn provider, Donbot leurt met medicijnen”

Dit is de augustuseditie van het maandelijkse MessageLabs Intelligence Report. In dit rapport zijn de nieuwste trends in bedreigingen opgenomen, zoals waargenomen in augustus 2009, om u te informeren over de permanente strijd tegen virussen, spam en andere ongewenste inhoud.

In het kort

- *Spam – 88,5% in augustus (een afname van 0,9% ten opzichte van juli)*
- *Virussen – In augustus bevatte 1 op de 296,6 e-mails malware (vrijwel ongewijzigd ten opzichte van juli)*
- *Phishing – Een op de 341,2 e-mails bevatte een poging tot phishing (een afname van 0,01% ten opzichte van juli)*
- *Schadelijke websites – 3510 websites geblokkeerd per dag (een afname van 2,9% ten opzichte van juli)*
- *Afsluiting Letse internetprovider gevoelige klap voor Cutwail-botnet*
- *Aanhoudende spamaanvallen op websites voor verkorte URL's*
- *Sociale netwerksites getroffen door DDoS-aanvallen*

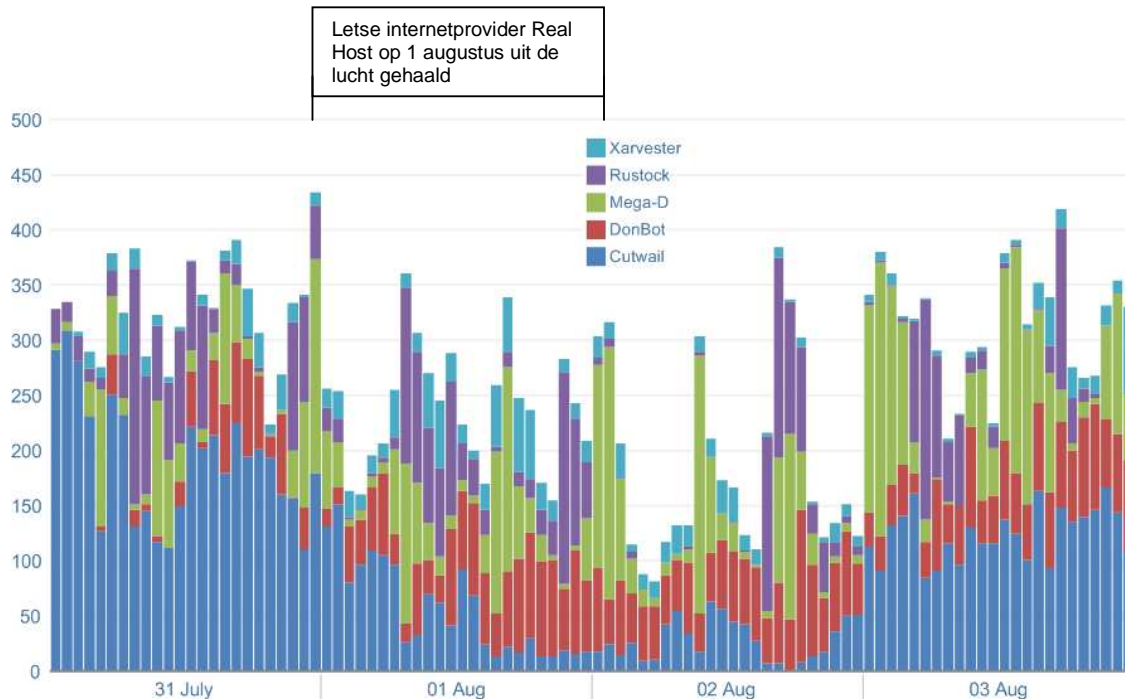
Analyse

Afsluiting Letse internetprovider gevoelige klap voor Cutwail-botnet

Op 1 augustus 2009 werd de Letse internetprovider Real Host door zijn upstreamproviders uit de lucht gehaald. De provider uit Riga zou niet alleen betrokken zijn bij command-and-control servers voor geïnfecteerde botnetcomputers, maar ook bij schadelijke websites, phishingwebsites en nep-antivirusproducten. Deze maatregel had meteen effect. De hoeveelheid spam nam in de eerstvolgende 48 uur af met 38% (zie afbeelding 1).

Veel van deze spam kwam uit de koker van Cutwail, dat verantwoordelijk is voor ongeveer 15 tot 20% van alle spam en hiermee momenteel een van de grootste botnets is. De activiteit van Cutwail kelderde met maar liefst 90% toen Real Host uit de lucht werd gehaald. Na enkele dagen had het botnet zich echter weer hersteld.

Afbeelding 1 toont het aandeel verzonden spam van de vijf grootste botnets ter wereld – Cutwail, Xarvester, Rustock, Mega-D en Donbot – in de betreffende periode. De gebruikte schaalverdeling is een relatieve index. Deze is gebaseerd op de relatieve hoeveelheden en het percentage spam afkomstig van elk botnet. De index biedt geen directe informatie over de omvang van het botnet of de absolute hoeveelheid spam. In de volgende editie van het MessageLabs Intelligence Report zullen we een aantal van deze grote botnets onder de loep nemen.



Afbeelding 1 – Relatief aandeel spam van de vijf actiefste botnets toen Real Host uit de lucht werd gehaald

Dit was niet de eerste keer dat een internetprovider werd afgesloten na beschuldigingen van malafide praktijken. Dit lot trof de afgelopen twaalf maanden in ieder geval drie Amerikaanse providers, namelijk Atrivo (alias InterCage), McColo en Pricewert (3FN). Pricewert werd uit de lucht gehaald door de Amerikaanse Federal Trade Commission.

Diensten die verkorte URL's aanbieden: een update

In de afgelopen twee maanden heeft MessageLabs Intelligence bijgehouden hoe diensten die verkorte URL's aanbieden, steeds vaker optraden in spamberichten. Veel van deze legitieme services worden op grote schaal misbruikt door spammers en hebben zich dan ook genoodzaakt gezien om hun diensten te beëindigen. Soms stuurden zij hun gebruikers een verontwaardigde bericht om deze beslissing toe te lichten (zie de voorbeelden in afbeeldingen 2 en 3 hieronder).

Etusivun linkinlyhentäjä.

Etusivun linkinlyhentäjä on toistaiseksi pois käytöstä.

Linkinlyhentäjä tulee jälleen saataville lähiaikoina, kunhan olen ensin lisännyt sisäänkirjautumisvelvoitteen linkkien lyhentämistä varten. Palvelua voivat jatkossa käyttää vain Etusivun viestitaululla keskusteluun osallistuvat käyttäjät, jotka olivat alunperinkin tämän palvelun kohdekäyttäjryhmä.

Huom! OLEN POISTANUT LINKKITIETOKANNAN. Minulla ei ole aikaa erotella satoja Viagran myynti-ilmoituksia sekä porno- ja online-kasino-mainoksia muutamista kunnollisista linkeistä. Valitan Etusivun käyttäjille mahdollisesti koitunutta vaivaa. Viagranmyyjät, olette syvältä!

Please note: the existing link database HAS BEEN PURGED! I don't have the time to sift through the links to separate few valid links from hundreds of Viagra, casino and porn peddlers' links. Viagra sellers, you suck!

Afbeelding 2 –
Website voor verkorte URL's die wordt misbruikt door spammers

Qurl.net is currently disabled due to links mostly being made by spamming assholes. Qurl.net is not a spamming service, and better it die than be abused like this.

If you're receiving spam email allegedly From: qurl.net, it isn't sent by me, so stop complaining to me about them; I can't do anything about it.

If you really want them to stop, bug your ISP to enable [SPF](#) (Sender Policy Framework) support, and to reject on SPF FAIL.

And stop replying to spam, you idiots; if you keep doing that, you'll end up getting more!

Afbeelding 3 –
Website voor verkorte URL's tijdelijk offline wegens misbruik door spammers

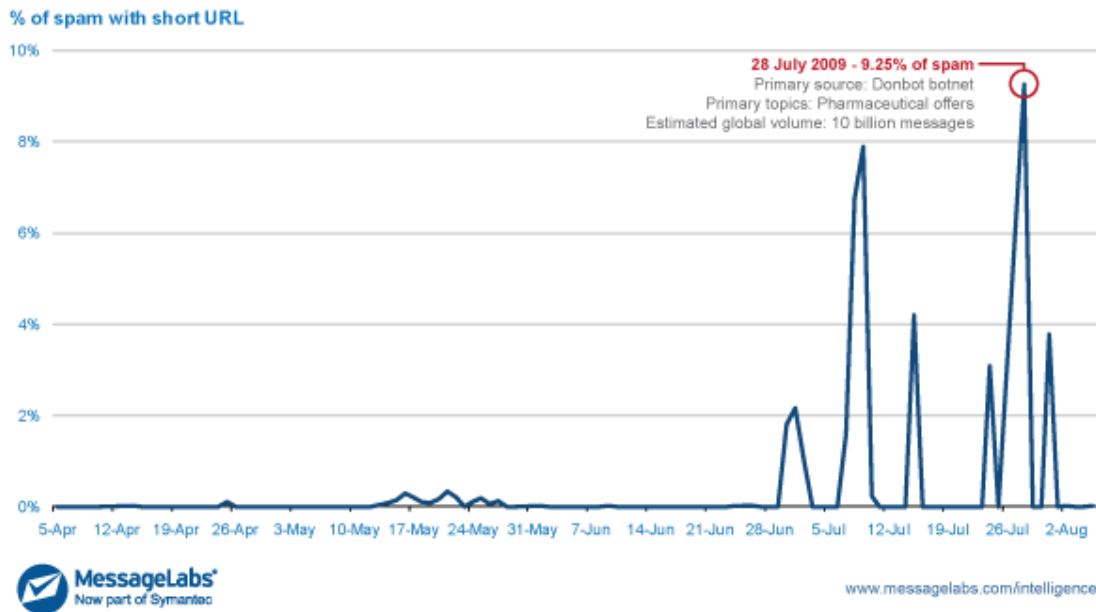
Spamacities met nieuwe verkorte URL's werden voortgezet in juli en augustus. Het hoogtepunt werd bereikt op 26 juli toen 9,25% van alle verzonden spamberichten van dit type was. Dit komt overeen met wereldwijd meer dan 10 miljard spamberichten per dag.¹ Zie afbeelding 4.

¹ Schatting hoeveelheden spam wereldwijd: http://www.symantec.com/business/security_response/landing/spam/index.jsp

Bij deze specifieke spamactie ging het om geneesmiddelen en (niet voor het eerst) leek Donbot, een ander botnet uit de top 5, daar achter te zitten.

Hier volgen enkele voorbeelden van onderwerpregels van dergelijke spamberichten:

Phentermine 37.5 Overnighted to your door
President Obama announced that he's providing affordable meds to people with no health care - Get meds now.
Purchase Meds Online
Obama has OK'd Online Sale of Meds
Zoloft For You
Online Dr. Notes
Obama wants to help YOU get the meds you NEED to be healthy and feel good, get them NOW.
Save 80% on Meds
Obama Opens Online Pharmacy



Afbeelding 4 – Percentage van alle spamberichten met koppelingen naar diensten voor verkorte URL's

DDoS-aanvallen tegen sociale netwerksites in combinatie met spam

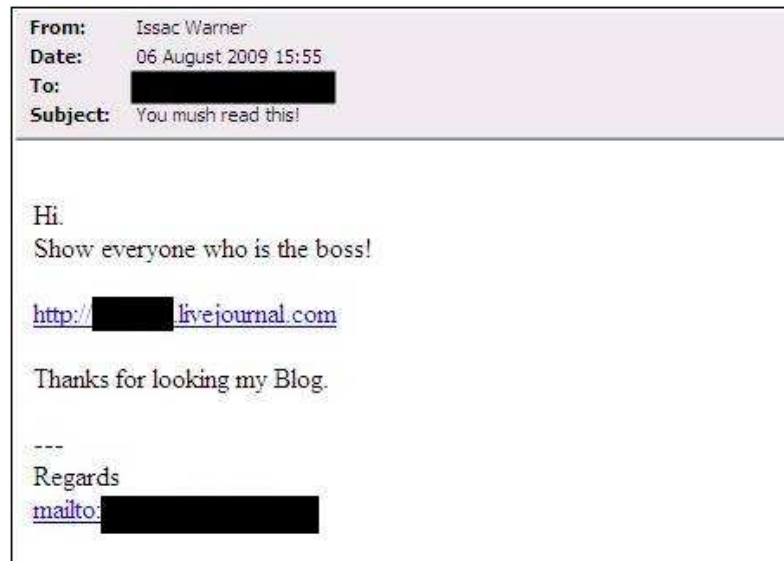
Begin augustus werden een aantal zeer bekende sociale netwerksites het slachtoffer van gedistribueerde denial-of-service-aanvallen (DDoS). Waarschijnlijk werden deze aanvallen in gang gezet door een zogenaamde 'Joe Job'-spamactie tegen een anti-Russische blogger. Dit is een spamtechniek waarbij in de regel *Van*: een bestaand e-mailadres van iemand wordt gebruikt, zodat het lijkt alsof de betreffende persoon die mail heeft verzonden, terwijl deze in werkelijkheid onschuldig is.

Bij deze spamaanval ging het volgens onze schattingen om minder dan één procent van alle spamberichten op dat moment. De berichten werden verstuurd door een nog onbekend botnet. De aanval was aanzienlijk kleiner dan andere recente spamacties, zoals de spamaanvallen van Donbot met verkorte URL's.

Hoewel wordt aangenomen dat deze spamactie een rol heeft gespeeld bij de DDoS-aanvallen op deze sociale netwerksites, is het niet waarschijnlijk dat alle gemelde verstoringen hieraan kunnen worden

toegeschreven. Waarschijnlijk was er nog een andere factor in het spel. Wij denken dat er ook een botnet is geweest dat gelijktijdig een DDos-aanval heeft uitgevoerd, waarbij besmette computers op commando van het botnet automatisch de startpagina van de betreffende sociale netwerksites openen.

Afbeelding 5 toont een voorbeeld van een 'Joe Job'-spambericht, dat feitelijk afkomstig was van een IP-adres in Brazilië, een land dat populair is bij botnets. Het e-mailadres in de regel *Van:* was gekaapt, zodat het leek alsof het bericht afkomstig was van een bedrijf in Ohio.

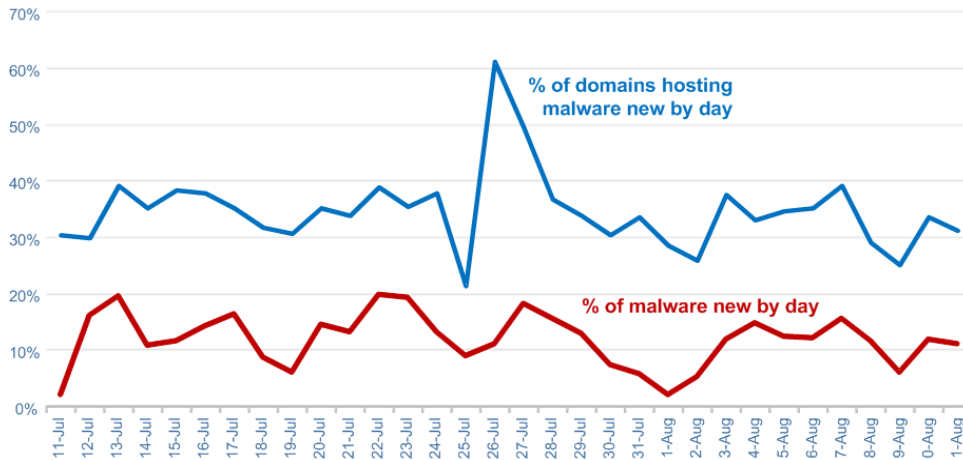


Afbeelding 5 – 'Joe Job'-e-mailbericht dat gebruikers uitnodigt om een weblog te bezoeken

De levenscyclus van malware op webbasis

Voor cybercriminelen die hun activiteiten willen kunnen blijven voortzetten zoals ze gewend zijn, is ontwikkeling van nieuwe malware vaak een kostbare aangelegenheid. Een veel goedkopere optie is het registreren van nieuwe domeinen. Verspreiding van de malware over zoveel mogelijk verschillende websites en domeinen zorgt ervoor dat de malware langer kan worden gebruikt. Bij server-side polymorfisme wordt malwarecode van dezelfde familie bij elk bezoek automatisch en op dynamische wijze verpakt in een nieuwe variant. Om deze adequaat te kunnen detecteren zijn dus telkens andere antivirussignaturen nodig. En doordat de criminelen daarnaast ook nog gebruikmaken van 'bullet-proof' hostingservices en 'fast-flux' hosting kunnen zij voorkomen dat malafide websites snel uit de lucht worden gehaald als er klachten over zijn.

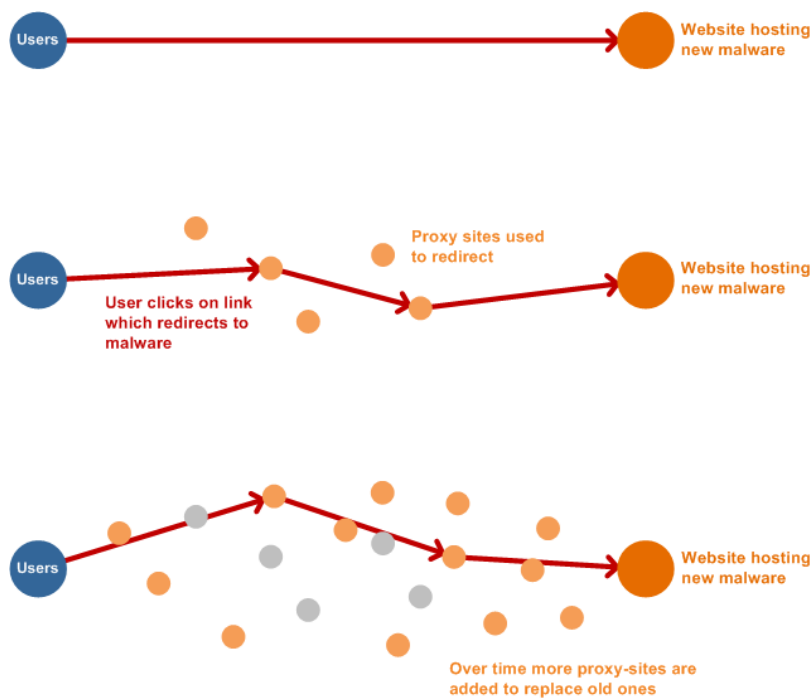
In veel gevallen maken de organiseerde criminelen gebruik van automatische technieken die nauwelijks of geen toezicht behoeven. Ze laten hun systemen dag en nacht draaien. Deze infecteren zoveel legitieme websites als ze kunnen en maken nieuwe aan. Wanneer dit proces goed functioneert, kunnen de hackers besmette websites op afstand opnieuw configureren, al naar gelang de methode die zij gebruiken.



Afbeelding 6 – Grafiek met de verspreiding van nieuwe malware en malafide websites die malware hosten

Uit een analyse van onze gegevens over augustus (zie afbeelding 6) blijkt dat er dagelijks 3510 websites werden geblokkeerd en dat dit voor gemiddeld 36,1% van deze domeinen de eerste keer was. Voorts blijkt uit analyse van de malware die dagelijks werd geblokkeerd, dat het bij 11,9% van de blokkeringen ging om nieuwe malwarevarianten die voor het eerst werden geblokkeerd.

Wanneer een slachtoffer malware rechtstreeks downloadt van een geïnfecteerde legitieme website, wordt hij automatisch via een ondoorzichtig systeem van doorverwijzingen naar de uiteindelijke malwarehost geleid. Daarnaast worden er vaak met tussenpozen nieuwe websites online gezet die dienen als verbinding tussen de geïnfecteerde website en de plek waar de malware zich bevindt (zie afbeelding 7).



Afbeelding 7 – Schematisch overzicht dat illustreert hoe in de loop der tijd steeds meer websites doorlinken naar nieuwe malwarecode

In de situatie van afbeelding 7 wordt er een nieuwe soort malware ontwikkeld die eerst alleen op een klein aantal websites wordt gehost of waarnaar direct wordt doorverwezen door kwaadaardige koppelingen op andere websites of in e-mailberichten. Na verloop van tijd worden er meer websites gebruikt en vaak wordt er gebruikgemaakt van een eenvoudige doorverwijzing om de bezoeker ongemerkt door te sturen naar een andere website of naar de malware zelf. Soms komt men pas na meerdere doorverwijzingen op de site met de malware. De gebruiker merkt hier niets van, behalve misschien dat het wat langer duurt om de pagina te laden. Dankzij deze 'wegwerpproxy's' blijven de websites die de malware zelf hosten, zo lang mogelijk buiten beeld.

Dit wijst erop dat er elke dag nieuwe legitieme websites worden besmet en nieuwe websites puur voor kwaadaardige doeleinden worden gecreëerd. Per 100 geblokkeerde domeinen in augustus (dagelijks) kom dit neer op het volgende:

- 36 hiervan zijn niet eerder geblokkeerd.
 - 30 gevallen (84,5%) betreffen blokkeringen van oudere, besmette legitieme domeinen.
 - 6 gevallen (15,5%) betreffen blokkeringen van onlangs geregistreerde domeinen.
- 64 hiervan zijn al dan niet legitieme domeinen, die eerder al bekend waren en vaker zijn geblokkeerd.

Het is niet ongebruikelijk dat topleveldomeinen worden gehost in een ander land dan de landcode van het topleveldomein doet vermoeden. Dit komt veel vaker voor bij nieuwe domeinen die zijn gecreëerd voor kwaadaardige doeleinden. Afbeelding 8 laat zien dat de locatie van malafide websites van recenter datum over het algemeen niet correspondeert met de landcodes van topleveldomeinen waarvoor ze zijn geregistreerd.

In het overzicht zijn ook algemene topleveldomeinen opgenomen om aan te geven waar de malafide website is gehost.

Hosting Locations For Most Frequent Top-Level Domains Blocked

| | Top-Level Domain | | | | | | |
|----------------|------------------|-------|-------|-------|-------|-------|-------|
| | .cn | .in | .ru | .us | .com | .info | .net |
| Canada | | | | | 18.8% | 61.6% | 11.0% |
| Cayman Islands | | | | | 10.1% | | |
| China | 46.0% | 33.3% | 18.2% | 3.2% | 7.2% | 1.2% | 8.7% |
| Estonia | | | 4.5% | | | | |
| France | | 4.8% | | | | | |
| Germany | | | | 3.2% | 6.4% | | |
| Hong Kong | | | | | | | 1.0% |
| Ireland | 17.0% | | | | | | |
| Latvia | | | 22.7% | | 2.4% | | 1.0% |
| Luxembourg | | | | | | 2.0% | 2.2% |
| Namibia | 2.4% | | | | | | |
| Netherlands | | | | | 2.9% | 5.0% | 2.0% |
| Panama | | 22.0% | | | | | |
| Poland | | 4.8% | | | 2.1% | | 3.0% |
| Romania | | | | | | | 9.0% |
| Russia | 7.1% | 7.0% | 40.9% | | 4.0% | | 18.0% |
| Serbia | | | | | 10.1% | | |
| Singapore | | | | | | | 3.0% |
| Taiwan | 4.0% | | | | | | |
| Ukraine | 23.0% | | | | 6.9% | | 15.0% |
| United Kingdom | | | 9.1% | | | | |
| United States | | 28.0% | 4.5% | 93.5% | 20.4% | 30.0% | 22.0% |

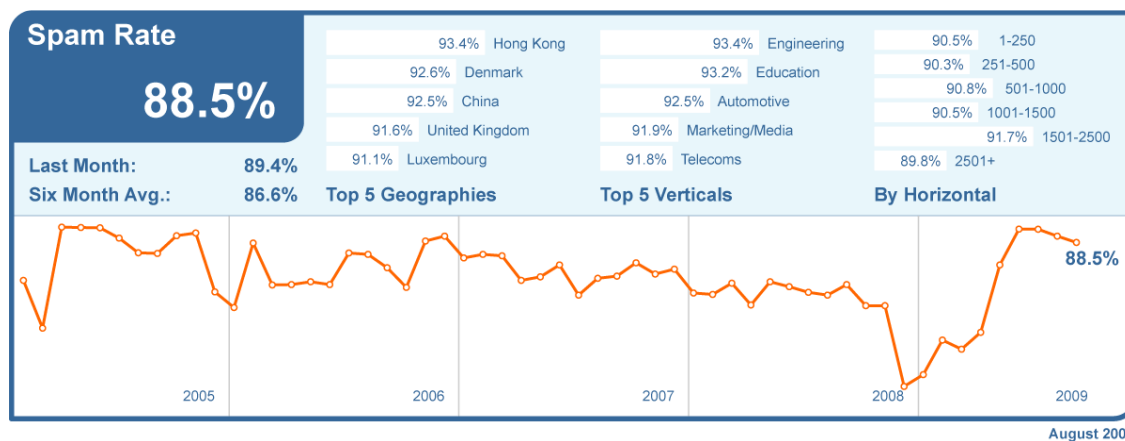
Afbeelding 8 – Topleveldomeinen die het vaakst worden gebruikt om websites met schadelijke content te hosten, uitgesplitst per land

Voor oudere geïnfecteerde legitieme websites ziet het plaatje er heel anders uit. Hiervoor geldt dat het topleveldomein veel vaker overeenkomt met het land dat men op basis van de landcode zou verwachten.

Wereldwijde trends en contentanalyse

De MessageLabs Anti-Spam en Anti-Virus Services zijn gericht op het herkennen en tegenhouden van ongewenste berichten die afkomstig zijn van onbekende malafide bronnen en gericht zijn aan bonafide e-mailadressen.

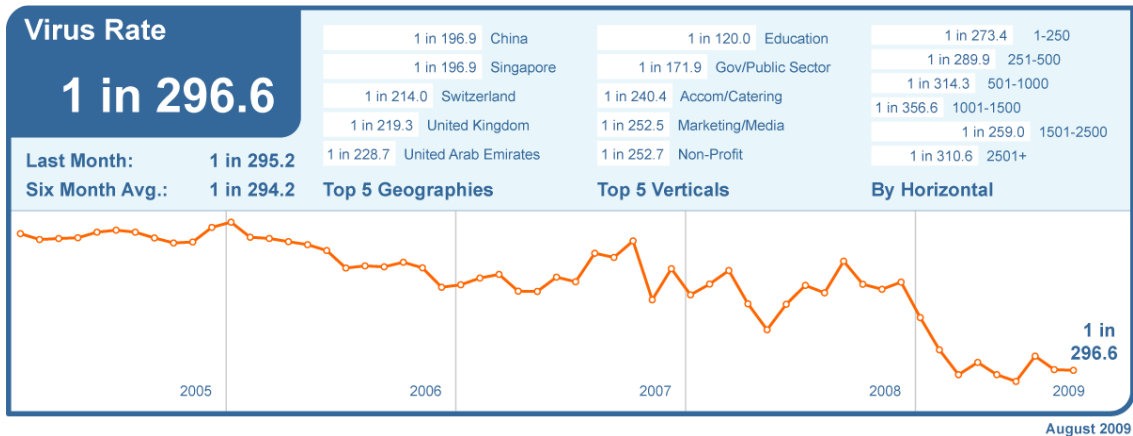
Skeptic™-bescherming tegen spam: In augustus 2009 daalde het aandeel spam in het e-mailverkeer ten opzichte van de voorgaande maand met 0,9% naar 88,5% (1 op de 1,13 e-mails).



Hongkong ontving in augustus de meeste spam, hoewel de hoeveelheid met 0,8% afnam tot 93,4%. In de Verenigde Staten en Canada steeg het spamniveau tot respectievelijk 89,5% en 88,7%. De meeste andere landen noteerden een daling: het Verenigd Koninkrijk tot 91,6%, Duitsland tot 90,4%, Frankrijk tot 90,7% en Nederland tot 86,3%. De hoeveelheid spam in Australië en Japan daalde tot respectievelijk 90,6% en 89,2%.

Skeptic™-bescherming tegen virussen en trojans: Het aandeel van berichten met virussen in het e-mailverkeer bedroeg in augustus 1 op de 296,6 (0,34%), vrijwel ongewijzigd ten opzichte van juli.

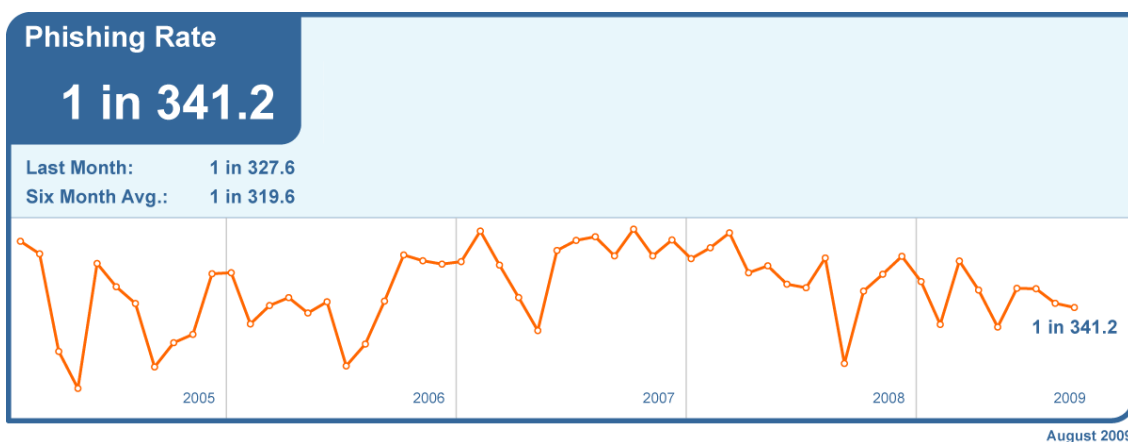
In april bevatte 14,8% van de via e-mail verstuurde malware koppelingen naar schadelijke websites, een afname van 0,4% ten opzichte van juli. In augustus was 21,3% van alle malafide koppelingen opgenomen in e-mailberichten die zogenaamd naar een Ansichtkaart op het internet verwezen.



Hoewel de virusactiviteit in China afnam tot 1 op de 196,9, stond het land wel bovenaan in de lijst van augustus. Singapore en Zwitserland handhaafden zich in de top 5 met een viruspercentage van respectievelijk 1 op de 196,9 en 1 op de 214,0. De top 5 werd gecompliceerd door het Verenigd Koninkrijk en de Verenigde Arabische Emiraten met respectievelijk 1 op de 219,3 en 1 op de 228,7.

In Duitsland en Nederland nam de virusactiviteit toe, met respectievelijk 1 op de 275,5 en 1 op de 612,18 e-mailberichten die een virus bevatten. De Verenigde Staten vertoonde met 1 op de 387,1 een lichte daling, terwijl Canada met 1 op de 309,9 een stijging noteerde. Australië, dat in juli het land was dat het meest getroffen werd door e-mailvirussen, belandde met 1 geïnfecteerd bericht per 308,3 e-mails op de twaalfde plaats. In Hongkong bedroeg de score 1 op de 297,7 en Japan liet een stijging zien (1 op de 400,76).

Phishing: In juli daalde de hoeveelheid phishing ten opzichte van juli met 0,01%: 1 op de 341,2 (0,29%) e-mailberichten bevatte een poging tot phishing. Als we kijken naar het aandeel van phishing in vergelijking met andere gevaren in e-mailberichten, zoals virussen en trojans, is dat met 6,0% gedaald naar 86,9% van alle via e-mail verstuurde malware- en phishing-aanvallen die in augustus zijn onderschept.



Skeptic™ Web Security versie 2.0: De meest gebruikelijke motivatie om over te stappen op filtering op basis van beleidsregels, zoals toegepast door de MessageLabs Web Security Service voor zakelijke klanten, wordt gevormd door de categorie 'Reclame en pop-ups' (58,03% in augustus, 2,07% minder dan in juli).

Een analyse van activiteiten op het gebied van webbeveiliging laat zien dat 45,4% van alle in augustus onderschepte malware op webbasis nieuw was. Dat komt neer op een toename van 44,7% ten opzichte van juli. Van de onderschepte spyware op webbasis was 19,5% nieuw, een afname van 0,01% ten opzichte van de voorgaande maand.

Bovendien werden dagelijks gemiddeld 3510 websites geïdentificeerd die malware en andere potentieel ongewenste programma's zoals spyware en adware bevatten, een afname van 2,9% ten opzichte van juli.

Web Security Services (Version 2.0) Activity:

| Policy-Based Filtering | | Web Viruses and Trojans | | Potentially Unwanted Programs | |
|-------------------------|--------|---------------------------------|-------|-----------------------------------|--------|
| Advertisements & Popups | 58.03% | Infostealer.Gampass | 7.90% | PUP:WebToolbar.Win32.MyWebSea... | 56.13% |
| Streaming Media | 11.76% | New Unclassified Trojan | 3.46% | PUP:WebToolbar.Win32.Zango.ca | 5.36% |
| Downloads | 5.04% | Suspicious.Graybird.1 | 3.20% | PUP:ZangoSearch | 3.36% |
| Games | 4.54% | New Unclassified VirusVirus | 3.06% | PUP:PSWTool.Win32.WinPassViewer.q | 1.54% |
| Peer-to-Peer | 2.39% | Trojan.Fakeavalert | 2.59% | PUP:RiskTool.VBS.DisReg.a | 1.45% |
| Chat | 2.12% | Infostealer.Bancos | 2.34% | PUP:NetTool.Win32.Portscan.c | 1.45% |
| Blogs & Forums | 2.04% | Trojan-Downloader.JS.Iframe.aqu | 2.27% | PUP:Client-IRC.Win32.mIRC.g | 1.36% |
| Adult/Sexually Explicit | 1.93% | Packed.Generic.233 | 1.63% | PUP:PUP:Win32.BHO.gtq | 0.91% |
| Computing & Internet | 1.49% | Suspicious.MH690 | 1.45% | PUP:BetterInternet | 0.91% |
| Personals & Dating | 1.49% | Bloodhound.DirActCOM | 2.14% | PUP:Win32.Shopper.v | 0.82% |

August 2009

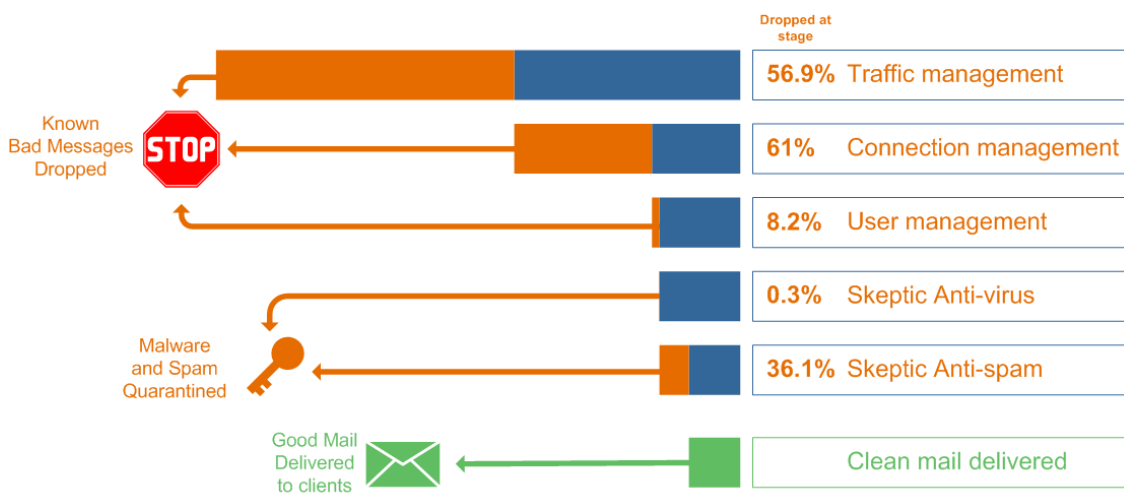
Het onderstaande diagram laat de toename zien van het aantal nieuwe spyware- en adwaresites dat in augustus gemiddeld per dag werd geblokkeerd, vergeleken met het aantal malwaresites op webbasis dat dagelijks werd geblokkeerd.



Traffic Management

Traffic Management blijft het totale berichtenvolume verminderen door middel van technieken die werken op protocolniveau. Daarmee worden ongewenste afzenders geïdentificeerd, terwijl verbindingen met de mailserver worden vertraagd met behulp van voorzieningen die zijn ingebed in het TCP-protocol. Inkomende herkende spam wordt aanmerkelijk vertraagd, terwijl de verwerking van legitieme e-mail wordt versneld.

In augustus heeft MessageLabs gemiddeld 3,95 miljard SMTP-verbindingen per dag verwerkt, waarvan 56,9% werd vertraagd vanwege Traffic Management-controles op verkeer dat beslist kwaadaardig of ongewenst was. Van het overige verkeer zijn de verbindingen vervolgens gecontroleerd met MessageLabs Connection Management en Skeptic™.



Connection Management

Connection Management is vooral effectief tegen directory-harvesting, brute force en denial-of-service-aanvallen via e-mail, waarbij malafide afzenders enorme aantallen berichten versturen om met spam een organisatie binnen te dringen of de bedrijfscommunicatie te ontwrichten. Connection Management werkt op SMTP-niveau, met *SMTP-validatietechnieken* die legitieme verbindingen met de mailserver verifiëren. Connection Management identificeert ongewenste e-mail afkomstig van bekende afzenders van spam en virussen als de bron ondubbelzinnig kan worden herkend als open proxy of botnet, en weigert de verbinding dienovereenkomstig. In augustus werd gemiddeld 61,0% van de inkomende berichten onderschept en geweigerd omdat ze afkomstig waren van botnets en andere bekende malafide bronnen.

User Management

In User Management vermindert *Registered User Address Validation* de totale hoeveelheid e-mail voor geregistreerde domeinen door verbindingen te negeren waarvan de ontvangstadressen zijn herkend als ongeldig of niet-bestaand. In augustus werd gemiddeld 8,2% van de inkomende berichten geïdentificeerd als ongeldig. Het ging daarbij om – vrijdelde – directory-aanvallen op domeinen.

Over MessageLabs Intelligence

MessageLabs Intelligence is een gezaghebbende bron van gegevens, analyses, trends en statistieken op het gebied van beveiliging van elektronische berichten. MessageLabs levert uitgebreide informatie over wereldwijde e-mailgevaren op basis van directe gegevens uit meer dan 14 datacenters op de hele wereld. Elke week scant MessageLabs miljarden berichten en webpagina's. In het MessageLabs-team van Skeptic™ zitten vele internationaal vermaarde deskundigen op het gebied van malware en spam, die een wereldwijd overzicht hebben van dreigingen op meerdere communicatieprotocollen, verkregen uit de miljarden webpagina's, e-mail en IM-berichten die ze elke dag voor 21.000 klanten in meer dan 99 landen in de gaten houden. Meer informatie is te vinden op de website www.messagelabs.com/intelligence.

Over Symantec

Symantec is wereldwijd toonaangevend als leverancier van beveiligings-, opslag- en systeembeheeroplossingen waarmee zowel particulieren als organisaties hun gegevens kunnen beveiligen en beheren. Onze software en services bieden completere en efficiëntere bescherming tegen meer risico's op meer verschillende punten, en zorgen voor de nodige betrouwbaarheid bij het gebruik en de opslag van gegevens. Meer informatie is te vinden op de website www.symantec.com.

Copyright © 2009 Symantec Corporation. Alle rechten voorbehouden.

Symantec, het Symantec Logo en MessageLabs zijn handelsmerken of geregistreerde handelsmerken van Symantec Corporation of zijn dochterbedrijven in de Verenigde Staten en overige landen. Overige namen kunnen handelsmerken zijn van hun respectieve eigenaren.

GEEN GARANTIE. De informatie in dit rapport wordt verstrekt in de staat waarin deze verkeert, en Symantec Corporation biedt geen garanties ten aanzien van de nauwkeurigheid of het gebruik van de informatie. Het gebruik van de onderhavige informatie geschiedt geheel op het risico van de gebruiker. Dit rapport kan technische fouten en overige onjuistheden of typefouten bevatten. Symantec behoudt zich het recht voor om zonder voorafgaande kennisgeving wijzigingen in deze informatie aan te brengen. Niets uit deze publicatie mag worden vermenigvuldigd zonder nadrukkelijke schriftelijke toestemming van Symantec Corporation, 20330 Stevens Creek Blvd., CA 95014 Cupertino, Verenigde Staten.