

MessageLabs Intelligence: Januari 2009

“Met nieuwe botnets is spam weer bijna terug op het oude niveau”

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

In het kort

- *Spam – 74,6% in januari (een toename van 4,9% sinds december 2008), wat neerkomt op circa 80-90% van het spamvolume vóór het uit de lucht halen van malafide provider McColo in november 2008.*
- *Virussen – Een op de 257,3 e-mails in januari bevatte malware (een afname van 0,12% ten opzichte van december 2008)*
- *Phishing – Een op de 396,2 e-mails bevatte een poging tot phishing (een afname van 0,14% ten opzichte van december 2008)*
- *Schadelijke websites – 1238 nieuwe sites geblokkeerd per dag (een toename van 6,2% sinds december 2008)*
- *Botnetactiviteiten blijven toenemen*
- *Weer terug naar aandelensпам?*
- *Terroristensпам*
- *Spam over de inauguratie van president Obama*

Analyse

Overzicht van botnetactiviteiten na McColo

Volgens een analyse van MessageLabs Intelligence van recente botnetactiviteiten ziet de top tien van actiefste spambotnets er als volgt uit:

Rank (average spam per day)	Botnet	Estimated botnet size: at least X active Ips in last 30d	average spam per day	average spam per minute	% spam (based on average spam per min)	Average active Ips per day	spam per IP per day	spam per IP per min	Each IP sends 1 spam every X seconds
1	Mega-D (Ozdok)	660,000	38,225,669,306	26,545,604	38.2%	64,855	589,402	409.3	0.1
2	Cutwail (Pandex)	1,080,000	7,741,703,816	5,376,183	7.7%	93,873	82,470	57.3	1.0
3	Rustock (Rustock)	410,000	6,219,110,041	4,318,826	6.2%	51,293	121,248	84.2	0.7
4	Xanvester	260,000	4,438,707,255	3,082,436	4.4%	15,915	278,896	193.7	0.3
5	DonBot	800,000	4,015,511,013	2,788,549	4.0%	63,904	62,836	43.6	1.4
6	Gheg	140,000	2,736,881,174	1,900,612	2.7%	15,708	174,238	121.0	0.5
7	Grum (Grum)	100,000	888,549,737	617,048	0.9%	12,880	68,987	47.9	1.3
8	Bagle (Beagle)	150,000	505,413,807	350,982	0.5%	14,654	34,490	24.0	2.5
9	Unknown New (TBC)	20,000	163,011,924	113,203	0.2%	2,076	78,532	54.5	1.1
10	Warezow/Stration	10,000	131,401,720	91,251	0.1%	320	410,150	284.8	0.2

Na de top tien volgen een aantal nieuwe, kleinere botnets die de afgelopen weken zijn opgedoken. Na de schijnbare verdwijning van het Srizbi-botnet na het buiten gebruik stellen van McColo in 2008, is de capaciteit van Mega-D (Ozdok) toegenomen. Zo werd het gat opgevuld dat werd achtergelaten door het Srizbi-botnet, dat vóór zijn schijnbare buitengebruikstelling verantwoordelijk was voor circa 50% van alle spam wereldwijd.

Mega-D heeft de hoogste throughput en verzendt gemiddeld circa 26 miljoen spamberichten per minuut (op basis van het dagelijks verzonden volume en rekening houdend met de mogelijkheid dat bepaalde computers ook wel eens zijn uitgeschakeld en dat spambots niet continu spam verzenden). Het spamvolume van Mega-D lijkt stabiel, maar kan soms kortstondig sterk toenemen.

Gelet op het gemiddelde aantal spamberichten per IP-adres per dag geldt bijvoorbeeld voor Mega-D dat vanaf elke geïnfekteerde pc meer dan 589.000 e-mails per dag worden verzonden.

Hoewel Cutwail (Pandex) nog altijd het grootste botnet is, lijkt dit niet zoveel spam te verzenden als sommige andere botnets (gemiddeld vijf miljoen spamberichten per minuut). Mocht de throughput van Cutwail sterk toenemen, dan zou dit grote botnet kunnen worden gebruikt voor het verzenden van grote volumes spam. Dit wordt mogelijk een van de belangrijkste botnets om in de gaten te houden in 2009.

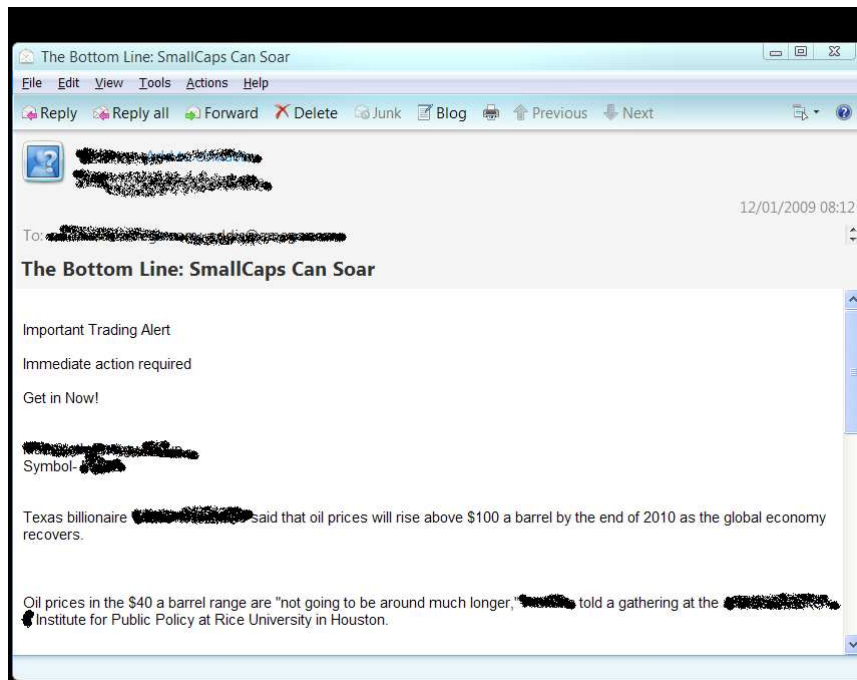
Het compleet nieuwe Xarvester-botnet is verantwoordelijk voor minder dan 5% van alle spam, maar heeft een hoge throughput, zodat ook deze spambot mogelijk veel van zich zal doen spreken in 2009.

Ook het nieuwe botnet Donbot heeft een grote potentiële capaciteit wat de omvang betreft, maar net als bij Cutwail lijkt zijn potentieel niet volledig te worden benut.

Een botnet die niet in de top tien voorkomt is Waledac, die wordt beschouwd als een nieuwe generatie van het Storm-botnet (Peacomm). In januari is schrikbarend veel Waledac-malware verspreid, maar tot nog toe wordt er vanaf de geïnfekteerde computers niet veel spam verstuurd. Blijkbaar richten de mensen achter het botnet zich in dit stadium voornamelijk op het uitbreiden en ontwikkelen van dit nieuwe botnet. Sceptic heeft dagelijks circa 25.000 e-mails met Waledac-malware onderschept, wat voor de eerste twee weken van januari 2009 neerkomt op een totaal van 216.000 stuks.

Weer terug naar aandelensпам?

De hoeveelheid aandelensпам was in 2008 praktisch nihil sinds Alan Ralsky 12 maanden geleden werd aangeklaagd. In januari 2009 werden bij onderzoek door MessageLabs Intelligence echter toch weer grote hoeveelheden spamberichten over aandelen, de zogenaamde 'penny stocks', aangetroffen. Veel van deze spamberichten lijken te zijn verzonden vanaf e-mailadressen die met CAPTCHA-brekers zijn aangemaakt, waarvoor enkele grote e-mailproviders zijn misbruikt. In het huidige financiële klimaat lijkt deze kans om met slechts een kleine inleg veel geld te verdienen misschien aantrekkelijk voor mensen die op een andere manier niet aan krediet kunnen komen.



Terroristenspam

In januari 2009 trof het MessageLabs Intelligence-team ook een aantal voorbeelden van spamberichten aan waarin terroristische doelen leken te worden nagestreefd.

From: [redacted]
Sent: 14 January 2009 16:13
Subject: TO THE MANAGER.....

ATTENTION PLEASE

MAKE SURE THIS GETS TO THE MANAGER AS SOON AS POSSIBLE,BECAUSE THIS IS THE ONLY WAY TO PASS THIS INFORMATION TO YOU AND GET THIS CASE SETTLED, WE HAVE BEEN PAID TO SET AN ELECTRONIC EXPLOSIVE DEVICE(BOMB)IN YOUR HOTEL WHICH WE HAVE DONE,BUT I FEEL LIKE HELPING YOU PEOPLE, I HAVE A CONCRETE EVIDENCE OF THIS INFORMATION ON A TAPE RECORD AND THE SECOND TAPE CONTAINS THE INFORMATION AND CONTACT OF OUR EMPLOYER,I DEMAND \$130,000(USD) WHICH MUST BE PAID BEFORE I COULD DISCLOSE ANY INFORMATION TO YOU,I NEED TO SETTLE MY TEAM WITH THIS MONEY SO THEY CAN GO BACK TO THERE DESTINATIONS, I TRAVELED TO AFRICA ON A BUSINESS TRIP BUT I HAVE EVERY THING UNDER MY CONTROL,I WILL MAIL YOU THE TAPES BUT THAT WILL BE AFTER MY BOYS HAVE GONE AND AM ASSURED OF YOUR MAXIMUM CO-OPERATION.

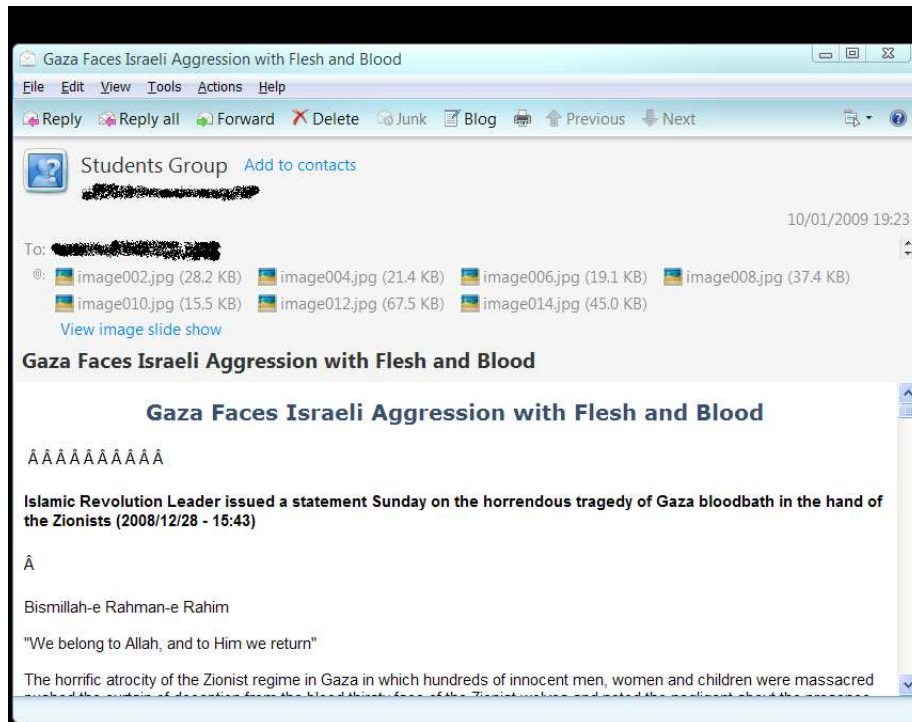
NOTE: MY EMPLOYER HAS A SECRET AGENT WORKING WITH YOU IN YOUR HOTEL,THEREFORE THIS INFORMATION MUST NOT BE KNOWN OR EXPOSED TO ANYBODY,ELSE MY EMPLOYER WILL SENCE BETRAYAL AND YOU KNOW WHAT THAT MEANS.(I WILL NOT ACCEPT ANY APOLOGY IF YOU PEOPLE MAKE ANY MISTAKE)

DO WILL HAVE A DEAL OR NOT

**REPLY THIS EMAIL AS SOON AS POSSIBLE.
MIND YOU,TIME IS OF ESSENCE.**

Een ander voorbeeld was afkomstig van een Iraanse universiteit. Tegen de achtergrond van het recente conflict in Gaza bevatte dit spambericht enkele uitspraken van een Iraanse geestelijk leider en koppelingen naar websites die vermoedelijk worden gebruikt door Hezbollah, een paramilitaire organisatie in Libanon.

Het onderstaande voorbeeld bevatte ook een aantal afbeeldingen van slachtoffers van het conflict, die sommige mensen mogelijk aanstootgevend of choquerend vinden.



Spam over de inauguratie van president Obama

Op de dag van de inauguratie van president Obama vonden onderzoekers van MessageLabs Intelligence bovendien kleine hoeveelheden spam die verband hield met deze politieke gebeurtenis.

RE: President Barack -Obama- Inaugural Dollar

File Edit View Tools Actions Help

Reply Reply all Forward Delete Junk Blog Previous Next

 Add to contacts

20/01/2009 08:04

To: 

RE: President Barack -Obama- Inaugural Dollar

Own A Piece Of American History

President Barack Obama is being honored on brilliant, uncirculated U.S. Mint Presidential Dollars by The . These limited edition coins are now available to the American public for the first time ever through this special offer. President Barack Obama is depicted in glorious full color on a genuine United States Inaugural Presidential Dollar and layered in genuine 24 karat gold.



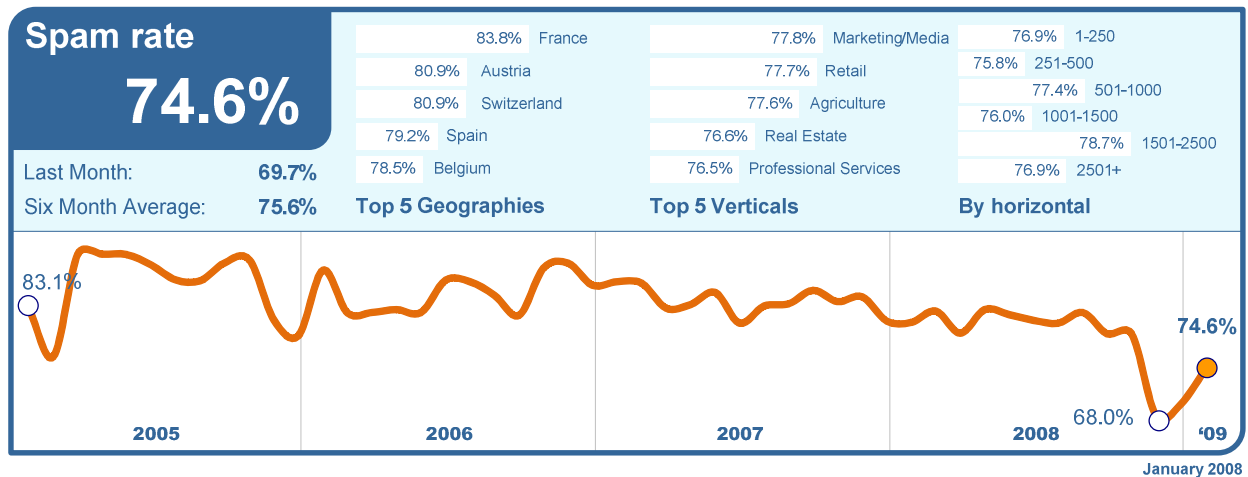
Each coin comes with a serial numbered Certificate of Authenticity, with earliest orders receiving the lowest numbers. Now you can own a piece of American History.

[Click Here for Additional Ordering Details and Special Bonus Offer:](#)

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 januari 2009 bedroeg het aandeel spam in het e-mailverkeer vanuit nieuwe en tot dusver onbekende malafide bronnen wereldwijd 74,6% (1 op 1,92 e-mails), een toename van 4,9% ten opzichte van december 2008.

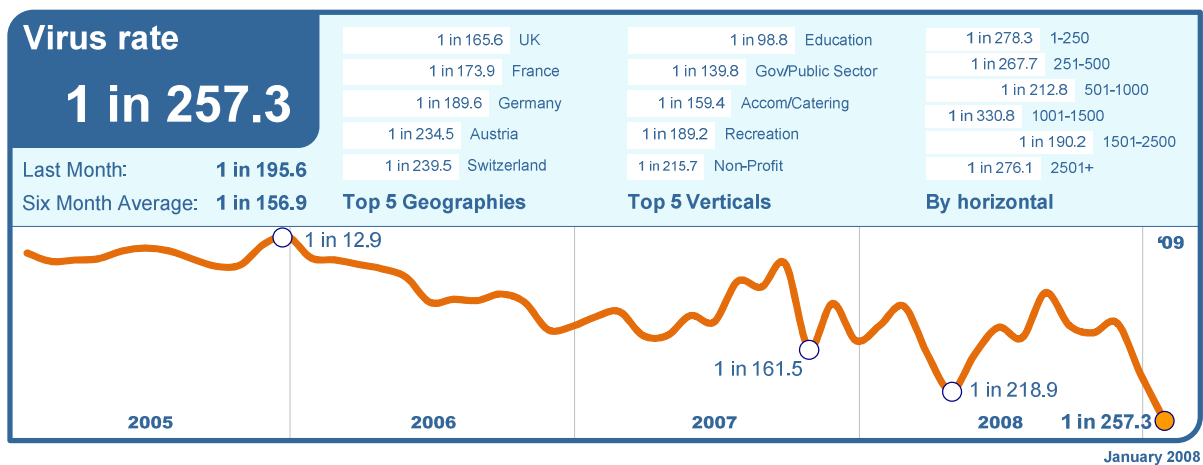


Hoewel de hoeveelheid spam in Frankrijk in januari met 0,3% afnam, voerde Frankrijk de lijst aan als belangrijkste doelwit van spam, met een aandeel van maar liefst 83,8% van alle e-mail. In januari bedroeg de hoeveelheid spam 76,9% in de Verenigde Staten, 75,1% in Canada en 77,2% in het Verenigd Koninkrijk. In Duitsland bedroeg het spampercentage 77,9% en in Nederland 78,2%. In Australië maakte spam 73,5% uit van alle e-mail, in China 73,0% en in Japan 70,7%.

In de sector marketing en media werd een toename van 0,5% genoteerd, waarmee dit de bedrijfstak met de meeste spam werd, met een spampercentage van 77,8%. In de chemische en farmaceutische sector bedroeg het spampercentage 75,8%, in de detailhandel 77,7%, in de publieke sector 75,1% en 74,2% in de financiële sector.

Skeptic™-bescherming tegen virussen en trojans: Het aandeel van berichten met virussen in het e-mailverkeer van nieuwe en voorheen onbekende malafide bronnen bedroeg in januari wereldwijd 1 op de 257,3 (0,39%), een afname van 0,12% ten opzichte van december 2008.

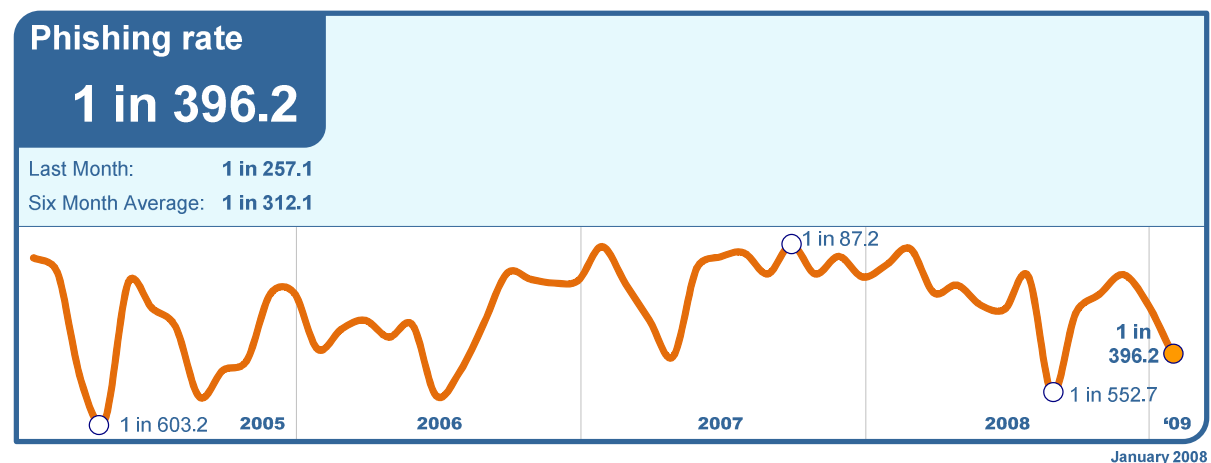
In januari bevatte 11,8% van de via e-mail verstuurd malware koppelingen naar schadelijke sites, een toename van 9,1% ten opzichte van december 2008. E-mailberichten die zogenaamd naar een ansichtkaart op internet verwezen, waren verantwoordelijk voor 17,7% van de schadelijke koppelingen in januari. Het opgeleefde Storm-botnet droeg bij aan 56,2% van de e-mailberichten die schadelijke koppelingen bevatten.



De virusactiviteit in het Verenigd Koninkrijk daalde met 0,26% naar 1 op de 165,6 e-mailberichten, waarmee het land de lijst aanvoert. De virusactiviteit bedroeg in de Verenigde Staten 1 op 455,7, in Canada 1 op 324,4 en in Australië 1 op 337,9. In Duitsland was de score 1 op 189,6 en in Japan 1 op 500,6.

In de onderwijssector daalde de virusactiviteit met 0,57%, maar deze sector bleef boven aan de lijst staan met 1 geïnfecteerd bericht op 98,8. Voor de IT-servicesector bedroeg de virushoeveelheid 1 op 276,3, voor de detailhandel 1 op 306,7 en voor de financiële sector 1 op 245,5.

Phishing: In januari nam het aandeel phishingaanvallen af met 0,14% ten opzichte van december 2008. Een van de 396,2 (0,25%) e-mails bevatte enigerlei phishing-aanval. Als we kijken naar het aandeel van phishing in vergelijking met andere gevaren in e-mailberichten, zoals virussen en trojans, is dat met 11,2% gedaald tot 64,9% van de via e-mail verstuurde malware die in januari is 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' (45,0% in januari, 0,6% minder dan in december).

Uit een analyse van activiteiten op het gebied van webbeveiliging blijkt dat 11,5% van alle in januari onderschepte malware op webbasis nieuw was. MessageLabs Intelligence spoorde bovendien dagelijks gemiddeld 1208 nieuwe sites op die malware en andere potentieel ongewenste programma's zoals spyware en adware bevatten, een toename van 6,2% ten opzichte van december 2008.

Web Security Services (Version 2.0) Activity:

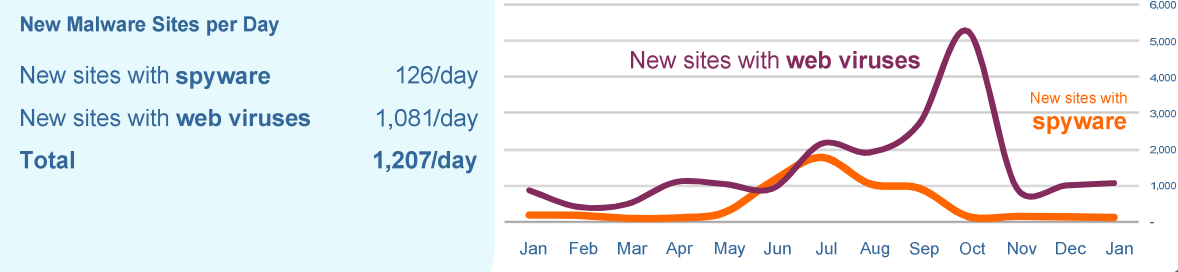
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	44.4%	Trojan-Clicker.HTML.IFrame.kr	21.9%	PUP:Server-FTP.Win32.Tftpd.274	72.1%
Chat	24.1%	New Virus	11.8%	PUP:WebToolbar.Win32.MyWebSea...	10.1%
Unclassified	6.2%	Exploit-MS06-006.gen	10.7%	PUP:180SA	2.3%
Streaming Media	6.2%	Generic Packed Virus	2.4%	PUP:BDSearch	2.0%
Downloads	3.4%	JS/Exploit-DDay	2.2%	PUP:RemoteAdmin.Win32.WinVNC.ab	1.2%
Personals & Dating	2.5%	FakeAlert-AB.dldr.gen.c	2.0%	PUP:WebToolbar.Win32.Zango.bm	1.0%
Games	2.2%	Generic Dropper.bw	2.0%	PUP:RemoteAdmin.Win32.WinVNC.ac	0.8%
Blogs & Forums	1.6%	JS/Tenia.d	2.0%	PUP:ISTBar	0.8%
Computing & Internet	1.6%	JS/Obfuscated	1.8%	PUP:RemoteAdmin.Win32.WinVNC...	0.7%
Adult/Sexually Explicit	1.4%	Trojan-Downloader.Win32.Agent.azjn	1.5%	PUP:RemoteAdmin.Win32.WinVNC.1370	0.6%

January 2008

In de categorie 'Ongeclassificeerd' zijn nieuwe en voorheen ongeclassificeerde sites opgenomen. Hoewel deze websites mogelijk worden gebruikt voor malafide doeleinden, zoals het hosten van phishing- en spamsites, kunnen dit ook nieuwe sites en domeinen zijn die door bonafide organisaties zijn opgezet en nog moeten worden gecategoriseerd. Door gebruik te maken van de MessageLabs-service, kunnen klanten deze websites flexibel benaderen. Alle inhoud die van dergelijke websites wordt gedownload, wordt gescand op virussen door onze unieke combinatie van commerciële virusengines en Sceptic-technologie. Klanten hoeven deze websites dus niet om veiligheidsredenen permanent te blokkeren.

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

Web Security Services (Version 2.0) Activity:

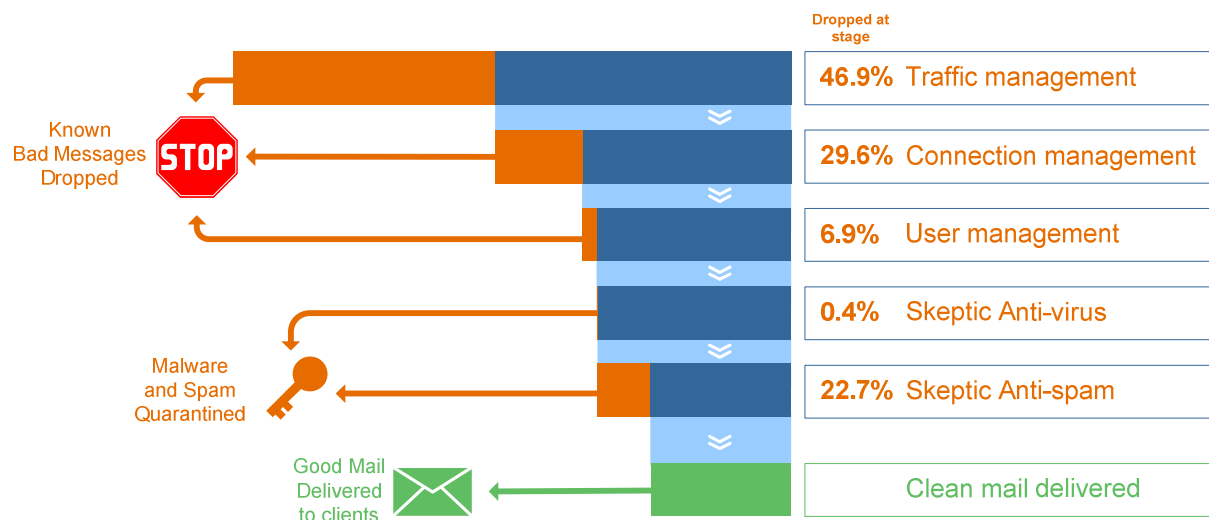


Ook in januari werden bonafide websites geïnfecteerd door SQL-injectieaanvallen en cross-site scripting-aanvallen. Ook zijn aanvallen waargenomen via koppelingen die via sociale netwerksites werden gedeeld.

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 januari zijn met de MessageLabs-services gemiddeld 2,5 miljard SMTP-verbindingen per dag verwerkt, waarvan 46,9% 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, bruto geweld 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 januari werd gemiddeld 29,6% van de inkomende berichten onderschept en geweigerd omdat die afkomstig was 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 januari werd gemiddeld 6,9% van de inkomende berichten geïdentificeerd als ongeldig. Het ging daarbij om verijdelde 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 19.000 klanten in meer dan 86 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 VS 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.