



## MessageLabs Intelligence: January 2009

### “New Botnets Boost Spam Growth To Near Pre-McColo Levels”

Welcome to the January edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for January 2009 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

#### Report Highlights

- *Spam – 74.6% in January (an increase of 4.9% since December 2008), which is approximately 80-90% of spam levels before the McColo ISP shutdown in November 2008.*
- *Viruses – One in 257.3 emails in January contained malware (a decrease of 0.12% since December 2008)*
- *Phishing – One in 396.2 emails comprised a phishing attack (a decrease of 0.14% since December 2008)*
- *Malicious websites – 1,208 new sites blocked per day (an increase of 6.2% since December 2008)*
- *Botnet activity continues to rise*
- *A Return to Stock Spam?*
- *Terrorist Spam*
- *Obama Presidential Inauguration Spam*

#### Report Analysis

##### A Post-McColo Botnet Review

MessageLabs Intelligence analysis of recent botnet activity has revealed that the top ten most active botnets responsible for distributing spam are as follows:

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	Xarvester	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	WarezoV/Stration	10,000	131,401,720	91,251	0.1%	320	410,150	284.8	0.2

Below the top ten are a number of new, smaller botnets that have also appeared in recent weeks. With the apparent disappearance of the Srizbi botnet in the wake of the McColo shutdown in 2008, Mega-D (Ozdok) has increased in capacity to fill the gap left by Srizbi, which had been responsible for about 50% of global spam before its apparent demise.

Mega-D has the highest throughput, working the hardest by sending around 26 million spams per minute on average (based on the daily volume sent and taking into account where machines may be

switched on and off and bots may not be sending spam constantly). Spam from Mega-D appears steady, but can often increase in short, high-volume bursts.

If we look at the average number of spam per IP per day, we can see for example with Mega-D, each infected PC is sending more than 589,000 mails per day.

Although Cutwail (Pandex) remains the largest botnet, it doesn't seem to send spam at as high of a rate as some other botnets (average five million spams per minute). If the throughput of Cutwail increases considerably, the potential use of such a large botnet for spamming in large volumes remains a major concern. This may be one of the key botnets to watch in 2009.

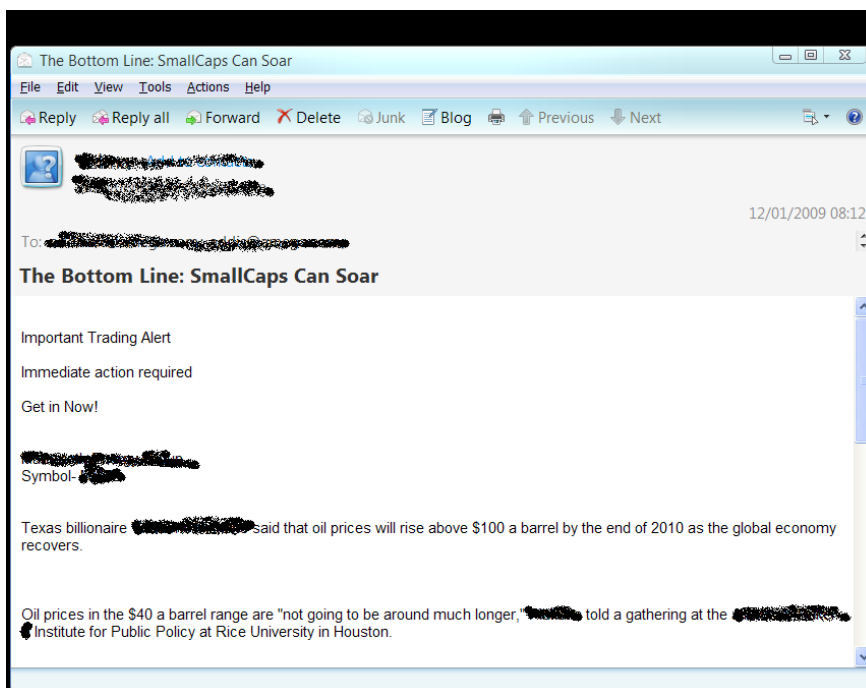
The Xarvester botnet, which is new on the scene, is responsible for less than 5% of all spam, but has a high spam throughput rate that makes it an interesting one to watch in 2009.

Another new botnet, called Donbot also has a large potential capacity, in terms of its size, but like Cutwail it does not seem to be used to its full potential.

One botnet not listed in the top-ten is called Waledac, believed to be a next generation of the Storm (Peacomm) botnet. Waledac malware is being spread at an alarming rate in January, but as yet there is not a great volume of spam coming from those infected machines. The botnet controllers are clearly focusing on growing and developing this new botnet resource, rather than sending spam through it at this stage. Skeptic has intercepted around 25,000 emails per day containing Waledac malware, totaling 216,000 in the first two weeks of January 2009.

### A Return to Stock Spam?

Stock spam levels in 2008 were practically non-existent since the indictment of Alan Ralsky 12 months ago. However in January 2009, MessageLabs Intelligence research identified a number of examples of spam messages that were touting penny stocks in significant volumes. Many of these new spams seemed to have been sent from email addresses created through CAPTCHA-breaking tools, aimed at some of the major email providers. In the current financial climate this apparent opportunity to raise capital from very little investment may seem a very attractive proposition for anyone who may be finding it hard to obtain credit by other means.



## Terrorist Spam

Also, in January the MessageLabs Intelligence team identified a number of examples of spam messages that were apparently being used to further the aims of terrorist organizations.

**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.*

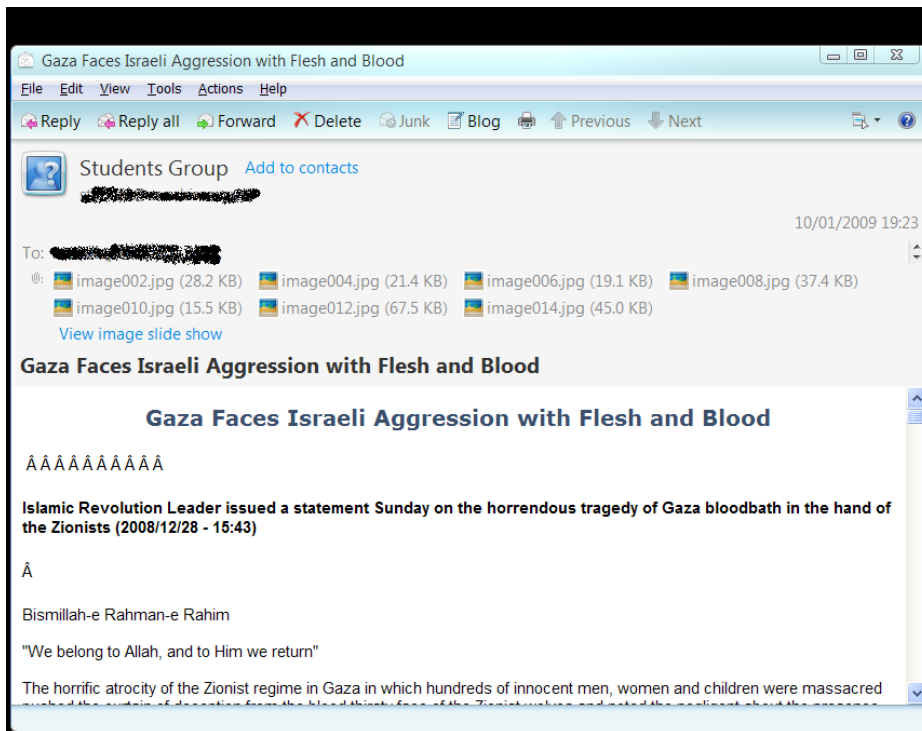
*NOTE: MY EMPLOYER HAS A SECRET AGENT WORKING WITH YOU IN YOUR HOTEL,THEREFORE THIS INFORMATION MUST NOT BE KNOWN OR EXPOSED TO ANYBODY,ELSE MY EMPLOYER WILL SENCE BETRAYAL AND YOU KNOW WHAT THAT MEANS.(I WILL NOT ACCEPT ANY APOLOGY IF YOU PEOPLE MAKE ANY MISTAKE)*

*DO WILL HAVE A DEAL OR NOT*

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

Another example originated from an Iranian University, and using the recent conflict in Gaza as a backdrop, included comments from the Supreme Leader of Iran and links to websites believed to be used by Hezbollah, a paramilitary organization based in Lebanon.

The example email below also included a number of images of victims of the conflict, which some people may find offensive or shocking.



### Obama Presidential Inauguration Spam

Finally, in January on the day of the Presidential Inauguration, MessageLabs Intelligence researchers identified low volumes of spam marking this unique event in US history.

RE: President Barack -Obama- Inaugural Dollar

File Edit View Tools Actions Help

Reply Reply all Forward Delete Junk Blog Previous Next

 **[REDACTED]** Add to contacts  
**[REDACTED]**

20/01/2009 08:04

To: **[REDACTED]**

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 **[REDACTED]**. 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.



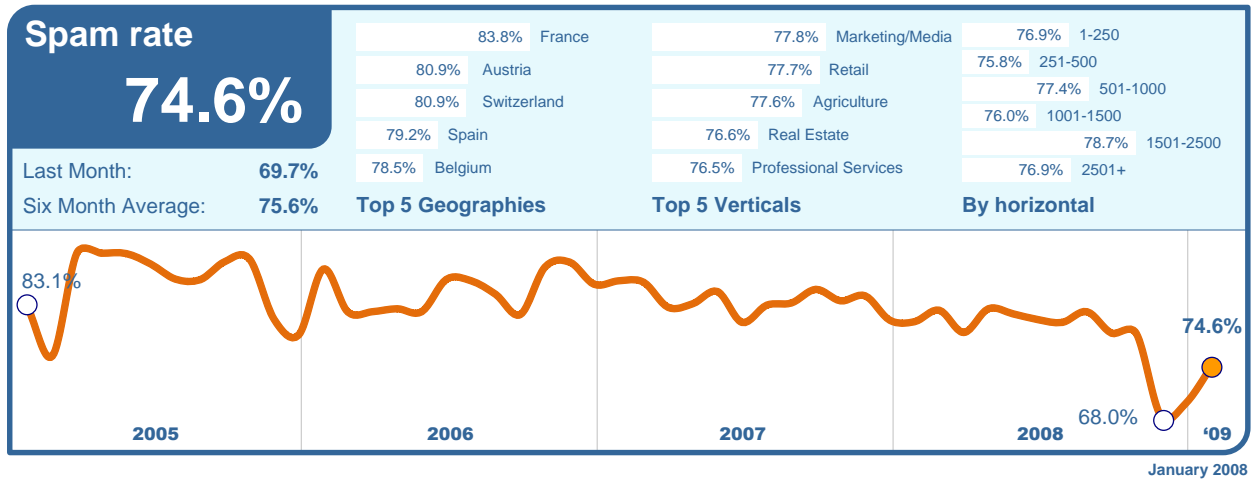
Each coin comes with a serial numbered Certificate of Authenticity, with earliest orders receiving the lowest numbers. Now you can own a piece of American History.

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

## Global Trends & Content Analysis

MessageLabs Anti-Spam and Anti-Virus Services focus on identifying and averting unwanted communications originating from unknown bad sources and which are addressed to valid email recipients.

**Skeptic™ Anti-Spam Protection:** In January 2009, the global ratio of spam in email traffic from new and previously unknown bad sources, was 74.6% (1 in 1.92 emails), an increase of 4.9% since December 2008.

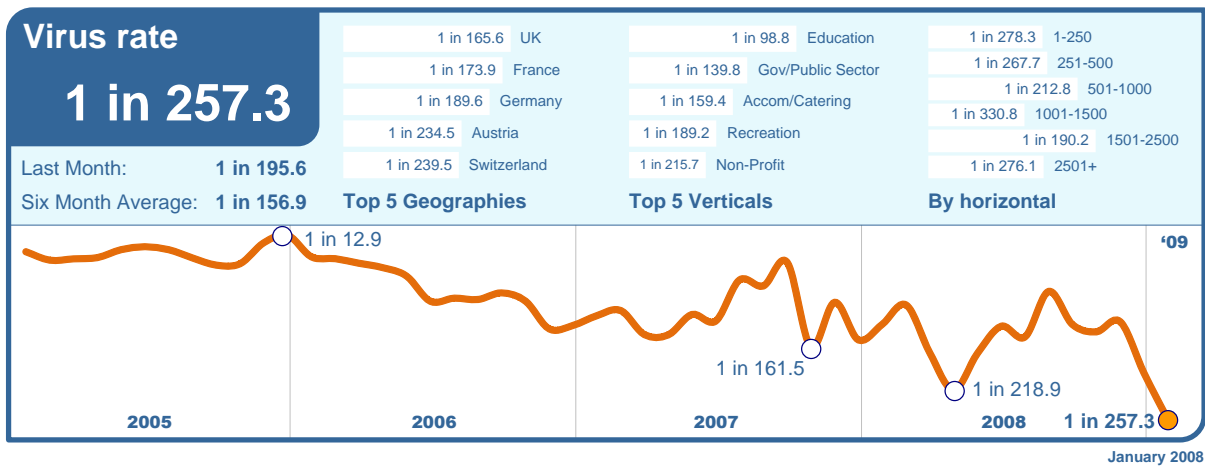


Although, the spam level in France fell by 0.3% in January, France topped the list as the most spammed country with levels reaching 83.8% of all email. Spam levels in the US reached 76.9% in January, 75.1% in Canada and 77.2% in the UK. Germany's spam rate reached 77.9% and 78.2% in the Netherlands. Spam levels in Australia were 73.5%, 73.0% in China and 70.7% in Japan.

With an increase of 0.5%, the Marketing & Media sector was positioned as the most spammed industry sector in January, with a spam rate of 77.8%. Chemical & Pharmaceutical sector spam levels reached 75.8%, 77.7% for Retail, 75.1% for Public Sector and 74.2% for Finance.

**Skeptic™ Anti-Virus and Trojan Protection:** The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources, was 1 in 257.3 emails (0.39%) in January, a decrease of 0.12% since December 2008.

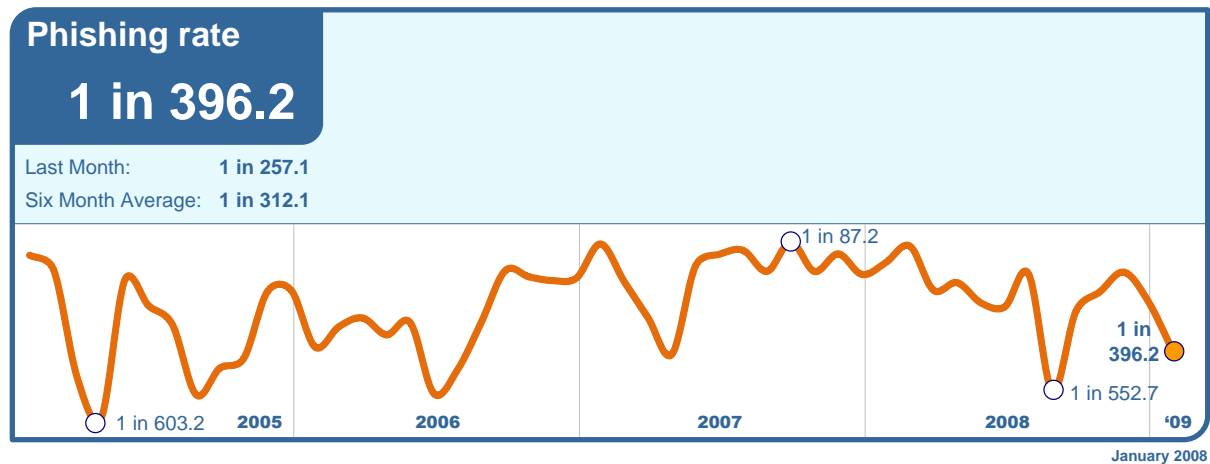
In January, 11.8% of email-borne malware contained links to malicious sites, an increase of 9.1% since December 2008. Spoofed postcard mails were responsible for 17.7% of malicious links in January, with a resurgence in the Storm botnet contributing to 56.2% of emails containing malicious links.



Virus activity in UK fell by 0.26% to 1 in 165.6 emails, where it takes the unenviable position at the top of the league table. Virus levels for the US were 1 in 455.7, 1 in 324.4 for Canada and 1 in 337.9 for Australia. Virus levels in Germany were 1 in 189.6 and in Japan they reached 1 in 500.6.

Although virus activity fell by 0.57% in the Education sector, it remained at the top of the table with 1 in 98.8 emails being infected. Virus levels for the IT Services sector were 1 in 276.3, 1 in 306.7 for Retail and 1 in 245.5 for Finance.

**Phishing:** January saw a decrease of 0.14% in the proportion of phishing attacks compared with December 2008. One in 396.2 (0.25%) emails comprised some form of phishing attack. When judged as a proportion of all email-borne threats such as viruses and Trojans, the number of phishing emails had fallen by 11.2% to 64.9% of all email-borne malware threats intercepted in January.



**Skeptic™ Web Security Version 2.0:** The most common trigger for policy-based filtering applied by the MessageLabs Web Security service for its business clients was the “Advertisements & Popups” category, down by 0.6% since December 2008, to 45.0% in January.

Analysis of web security activity shows that 11.5% of all web based malware intercepted was new in January. MessageLabs Intelligence also identified an average of 1,208 new sites per day harboring malware and other potentially unwanted programs such as spyware and adware; an increase of 6.2% since December 2008.

## Web Security Services (Version 2.0) Activity:

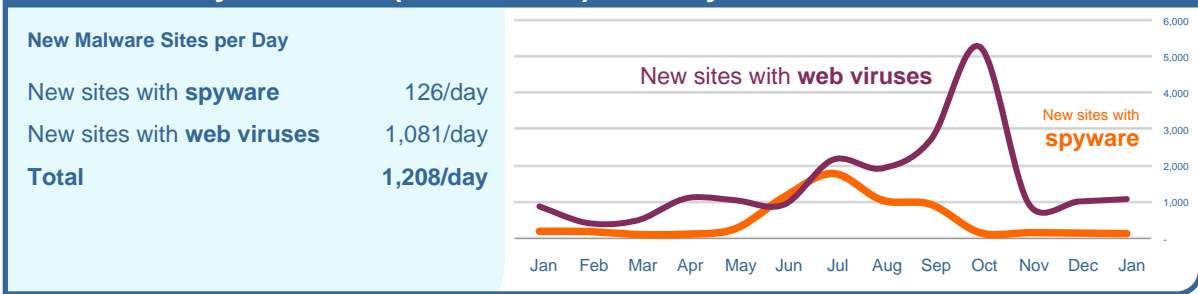
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	44.4%	Trojan-Clicker.HTML.IFrame.kr	21.9%	PUP:Server-FTP.Win32.Tftpd.274	72.1%
Chat	24.1%	New Virus	11.8%	PUP:WebToolbar.Win32.MyWebSea...	10.1%
Unclassified	6.2%	Exploit-MS06-006.gen	10.7%	PUP:180SA	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

The “Unclassified” category identifies new and previously uncategorized sites. While these sites can be used for disreputable purposes, such as hosting phishing and spam sites, they may also be new sites and domains set up by legitimate organizations in the process of being categorized. By using the MessageLabs service, customers can take a flexible approach to these sites as all content downloaded from such sites are virus scanned by our unique combination of commercial virus engines and Skeptic technology ensuring that customers do not need to have a default block on these sites to maintain security.

The chart below shows the increase in the number of new spyware and adware sites blocked each day on average during January compared with the equivalent number of web-based malware sites blocked each day.

## Web Security Services (Version 2.0) Activity:



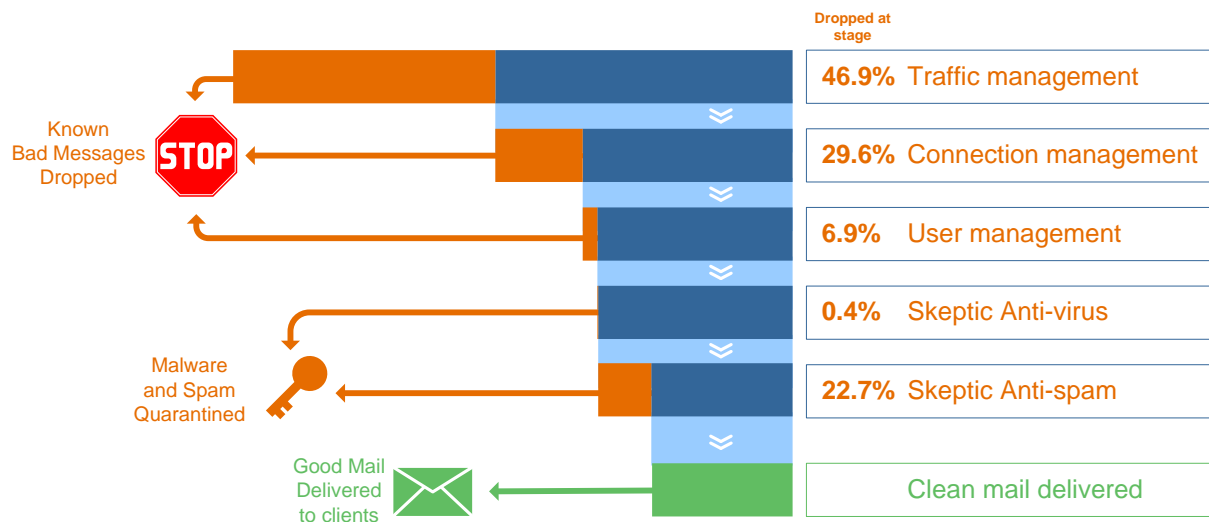
January 2008

The number of legitimate websites that were infected by SQL injection attacks and Cross-Site Scripting attacks continues in January, with other attacks seeming to originate from links shared via social networking sites.

## Traffic Management

Traffic Management continues to reduce the overall message volume through techniques operating at the protocol level. Unwanted senders are identified and connections to the mail server are slowed down using features embedded in the TCP protocol. Incoming volumes of known spam are significantly slowed, while ensuring legitimate email is expedited.

In January, MessageLabs services processed an average of 2.5 billion SMTP connections per day, of which 46.9% were throttled back as a result of traffic management controls for traffic that was unequivocally malicious or unwanted. The remainder of these connections was subsequently processed by MessageLabs Connection Management controls and Skeptic™.



## Connection Management

Connection Management is particularly effective in stopping directory harvest, brute force and email denial of service attacks, where unwanted senders send high volumes of messages to force spam into an organization or disrupt business communications. Connection Management works at the SMTP level using techniques that verify legitimate connections to the mail server, using *SMTP Validation* techniques. It is able to identify unwanted email originating from known spam and virus sending sources, where the source can unequivocally be identified as an open proxy or a botnet, and rejects the connection accordingly. In January, an average of 29.6% of inbound messages was intercepted from botnets and other known malicious sources and rejected as a consequence.

## User Management

User Management uses *Registered User Address Validation* techniques to reduce the overall volume of emails for registered domains, by discarding connections for which the recipient addresses are identified as invalid or non-existent. In January, an average of 6.9% of inbound messages was identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

**About MessageLabs Intelligence**

MessageLabs Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. MessageLabs Intelligence publishes a range of information on global security threats based on live data feeds from more than 14 data centers around the world scanning billions of messages and web pages each week. MessageLabs Team Skeptic,<sup>™</sup> comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of web pages, email and IM messages they monitor each day on behalf of 19,000 clients in more than 86 countries. More information is available at [www.messagelabs.com/intelligence](http://www.messagelabs.com/intelligence).

**About Symantec**

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at [www.symantec.com](http://www.symantec.com).

Copyright © 2009 Symantec Corporation. All Rights Reserved.

Symantec, the Symantec Logo and MessageLabs are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.