

MESSAGELABS INTELLIGENCE JANUARY 2010



Spam Sustains High Volumes Into the New Year and Targeted Zero-Day Attacks Uncovered

Welcome to the January edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for January 2010 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

REPORT HIGHLIGHTS

- Spam – 83.9% in January (a decrease of 0.3% since December)
- Viruses – One in 326.9 emails in January contained malware (a decrease of 0.03% since December)
- Phishing – One in 562.3 emails comprised a phishing attack (a decrease of 0.11% since December)
- Malicious websites – 3,086 websites blocked per day (an increase of 32.1% since December)
- 41.4% of all malicious domains blocked were new in January (an increase of 0.6% since December)
- 12.1% of all web-based malware blocked was new in January (a decrease of 2.0% since December)
- New Year Spam Winds Down
- Free Webmail Spam Trends
- Tracking the Spammers' Price of the "Little Blue Pills"
- New Zero-Day Threats
- New, Short Lived Botnet: Lethic

REPORT ANALYSIS

Happy New Year!

The holiday season is almost over and St. Valentine's Day is drawing closer. As is normal for this time of year, spammers have launched into an enormous campaign of spam related to 2010 festivities, including special New Year offers and deals related to pharmaceuticals and products such as fashion accessories, watches and jewelry. Other offers include weight loss products, online dating offers loan and job offers.

MessageLabs Intelligence identified a relatively small amount of spam activity at the end of October 2009, which started to increase significantly beginning in December 2009 onwards. As the New Year arrived, spam volumes increased markedly and have sustained high levels ever since. As we move into

February, MessageLabs Intelligence expects to see New Year related spam trail off as spammers realize they have likely capitalized as much as possible on the New Year themes, moving on to the next thing, such as St. Valentine's Day related spam.

Breaking down the New Year's themed spam by botnet shows that 40% was sent from the Grum botnet and 12% from Cutwail meaning more than 50% of the seasonal spam has been sent from just two botnets: Grum and Cutwail.

The Festi botnet was surprisingly active too, responsible for around 6% of New Year related spam. Rustock sent about 5% of New Year spam and Donbot about 3%. Other bots were involved in less than 1% of all spam.

At its peak, New Year related spam accounted for 7.7% of all spam in a single day, and on average during January 2010, it has accounted for around 4.6% of spam. Based on Symantec's global average spam per day estimate for 2009, of 107 billion spam emails, New Year's themed spam could have averaged around 5 billion spam emails per day so far.

Some of the most frequent subjects where the spam message related to the New Year in the subject or the body include the following:

- New Year Sales*
- Resolve to Bed More Chicks in 2010? Get Free trial*
- Julia 22y.o, new message for you*
- Look BIGGER this coming new year with these free trial pills*
- Decade in words*
- Replica Watches*
- Watches*
- Exquisite Replica*
- Start the New Year with a new Rolex or Gucci Product*
- Begin the new year with a new Rolex or Cartier Product*
- ROLEX, GUCCI, LOUIS VUITTON at Cheap Prices until New Years ONLY!*
- RE: January 70% OFF on PFIZER*
- Blowout Prices to start the New Year!*

Free Webmail Spam Trends

It seems that despite the large number of freely available webmail service providers that may be found on the Internet, most of the spam from these services originates from just three main providers.

As we know, botnets make up the vast majority of spam, at around 83.4% at the end of 2009, and of the remainder, just under one tenth originated from free webmail accounts. These email accounts are available for anyone to register for free, and may be accessed from anywhere in the world through an Internet connection.

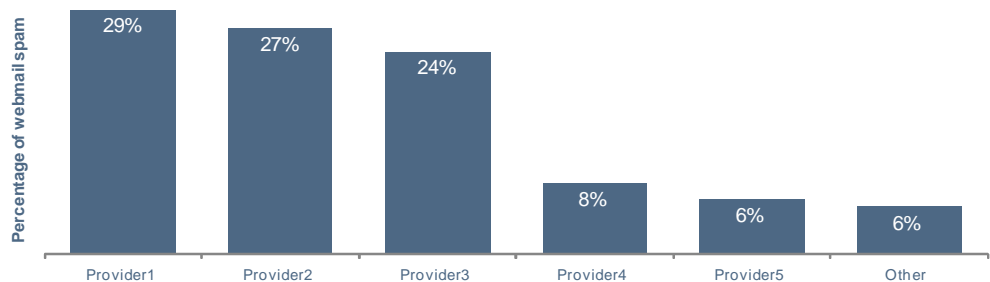


Figure 1

The chart in Figure 1, shows the trend over the December 2009 and January 2010 period, and shows that webmail averages around 0.9% of all spam, which may sound like a relatively small number, but this translates to approximately 900 million spam emails originating from webmail accounts each day.

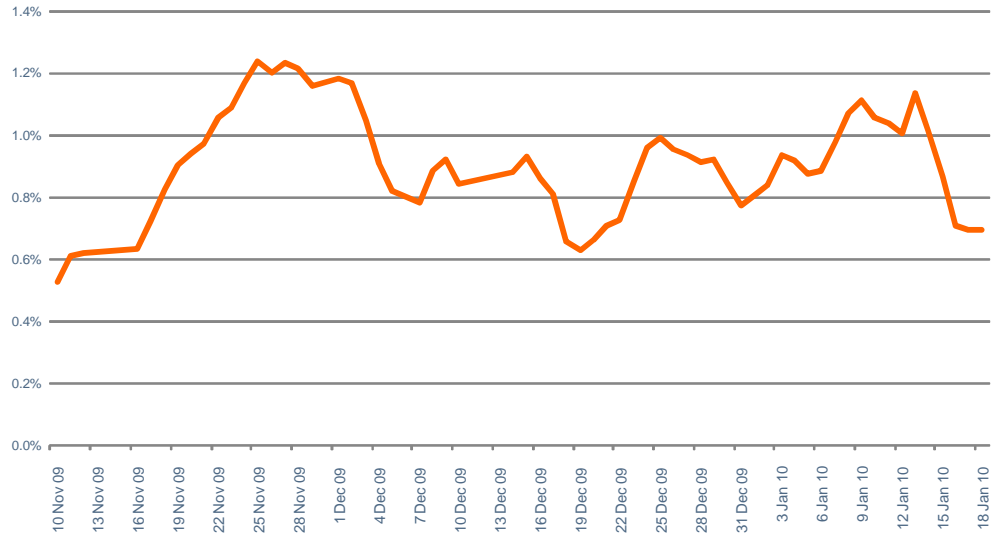


Figure 2

It is also interesting to note that over 79% of webmail spam came from just three well-known free webmail services, as seen in Figure 2. Despite the best efforts of the providers to prevent this abuse of their services, there is still a viable market in the underground economy for buying and selling legitimate, useable accounts.

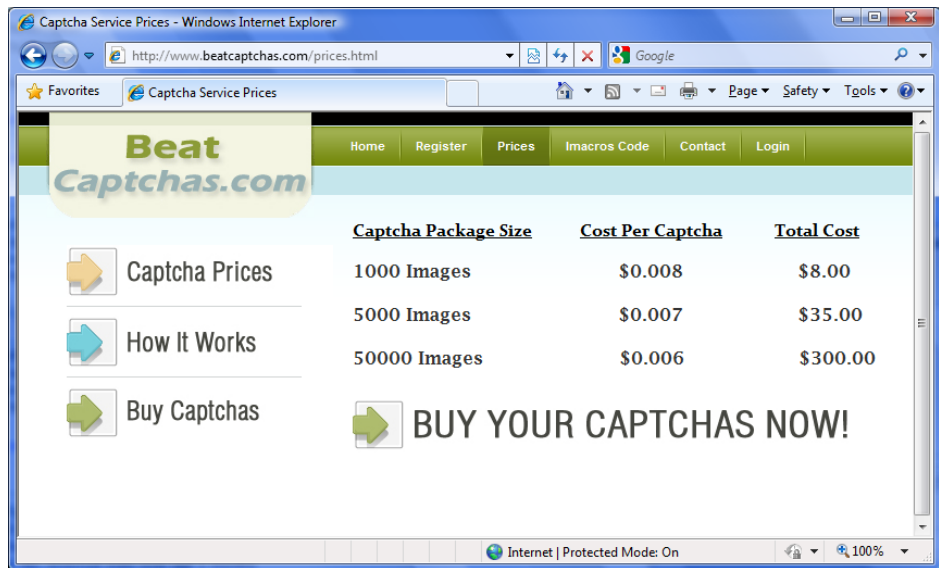


Figure 3

Cyber criminals often pay a specific amount for a certain number of valid accounts, or solved CAPTCHAs (where the process can be automated), as seen in Figure 3, USD \$8 will pay for one thousand CAPTCHAs to be broken.

Tracking the Spammers' Price of "Little Blue Pills"

Spam has often been associated with pharmaceuticals and medicines of one type or another, but the most popular connection is with male impotence drugs, particularly if they are blue. Much of this type of spam includes the price of the medications and the weight, and using this information, MessageLabs was interested to see how the advertised price per 100mg has

changed over the last year, and whether this trend reflects in any way how the spammers may have been affected by the global financial crisis.

The analysis presented in Figure 4, found that the spammers' price peaked at around USD \$6 per 100mg, in early 2009, but then fell rapidly during June and July to between USD \$2 and USD \$3. This trend continued through the remainder of the year and the price stabilized at around USD \$1.60, where it remained through the beginning of 2010.

It isn't really possible to speculate whether this is a true reflection of the state of the spam economy, but it will be interesting to see if the spammers' prices are stimulated into returning to their former higher levels, perhaps as the global economy continues with its recovery.

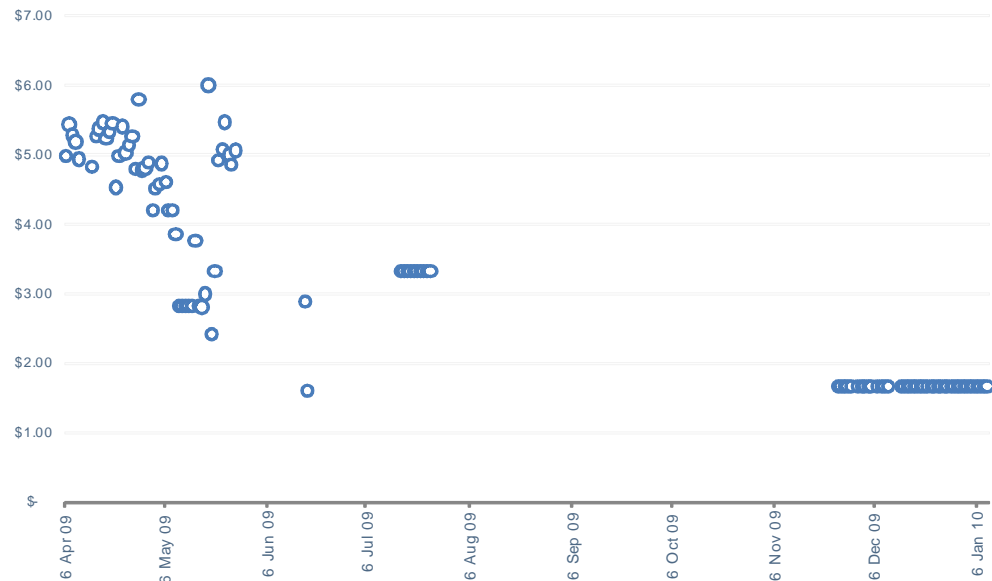


Figure 4

Zero-Day Targeted Attacks

On 15 December 2009, the existence of a new zero-day vulnerability in a popular version of a .PDF viewer was disclosed. The vulnerability was designated CVE-2009-4324 and MessageLabs Intelligence tracked the first examples of exploits in the wild on 20 November 2009 as JS/Decoder, a name given to malicious attacks detected using certain malicious JavaScript exploits. These are often found in targeted attacks where JavaScript exploits exist within office documents, including .PDF files.

The attack had been observed targeting high-level individuals in the public sector, education sector, and a number of large international businesses and financial organizations. The attack arrived as a .PDF file containing embedded JavaScript. The JavaScript was heavily obfuscated using a custom encryption technique to conceal the payload. There was a social engineering aspect to the attack too, which varied according to the individual and organization being targeted.

Email subjects varied in topics from corporate bait such as "Interview Request" or "Hotel booking confirm" to international stories such as "proposal-university of Science and Technology of [...]" and "Reports on recent situation in the DPRK."

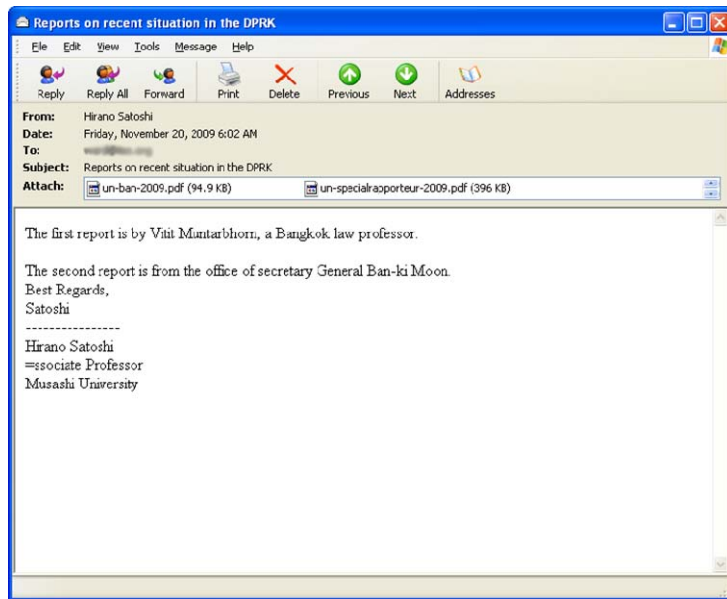


Figure 5

Figure 5 shows an example of one of the first targeted attacks of this nature. The email attachment *un-ban-2009.pdf* is clean, but the attachment *un-specialrapporteuru.pdf* exploits the zero-day vulnerability. The contents of the clean .PDF attachment shows a convincing-looking United Nations document, which may in fact be legitimately sourced from the UN and is likely to have been included for social engineering purposes, in order to make the email seem more legitimate to the intended victim.

However, the malicious .PDF contained no text and was simply a blank page when viewed. Figure 6 shows some of the malicious JavaScript embedded in the .PDF. Note that the attacker(s) even took the time to add comments to the code in English; however, this may indicate that the JavaScript was simply copied and pasted from a template file.

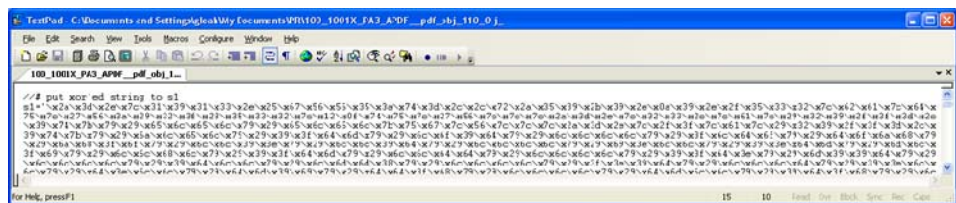


Figure 6

Some of the subjects used in these attacks, included:

- Agenda 2010*
- Currency Reform in the DPRK*
- deliver shipt today top urgent top urgent # 3948404262*
- Denavit-Hartenberg convention*
- FW: reference*
- Fwd: reference*
- Hotel booking confirm*
- IAEA Meeting Materials*
- Interview Request*
- Inviting you to the 2010 Korea Festival*
- letter of hotel confirmation*
- North Korea food shortage worsens : WFP Report*
- proposal-university of Science and Technology of [...]*
- Prospect of [...]’s NK visting*
- RE:Reply*
- Report*

Reports on recent situation in the DPRK
Special interview
World Economy Outlook 2010 ([...])

The unique .PDF file names observed in the wild also include the following:

Denavit-Hartenberg convention.pdf
economy outlook.pdf
agenda 2010.pdf
outline of interview.pdf
HotelConfirm.pdf
Invitation Proposal to 2010 Korea Festival.pdf
Urgent_3948404262.pdf
(Urgent) letter of Ambassador.pdf
Letter of hotelconfirmation.pdf
price(discount).pdf
Interview.pdf
Report.pdf
Visit Report.pdf
Vist Report.pdf
note_20091203.pdf
note_20091210.pdf
note200911.pdf
article.pdf
Currency.pdf
proposal.pdf
un-specialrapporteur-2009.pdf

Symantec Hosted Services clients were protected from these attacks before they even began. The first attacks were being conducted 25 days before the existence of the vulnerability was disclosed; it was a further 28 days before the application vendor made the patches available to the general public. This example perhaps served as a harsh warning of what may be expected over the coming months during 2010, as we expect more sophisticated targeted malware attacks of this nature.

New Lethic Botnet

On 31 December 2009, MessageLabs Intelligence began tracking a new botnet called Lethic, which accounted for 2.5% of all spam at the end of the year. On 1 January 2010, spam from this new botnet increased to just under 4% and continued roughly at around that level for the following week. On 8 January, it peaked at 5.25% of all spam, but over the following two days its spam traffic dropped off to nothing, and seems to have disappeared almost as quickly as it arrived.

The spam it had been sending was roughly an even mix of pharmaceutical (all linked to the ubiquitous Canadian Pharmacy spam websites) and some spam for replica watches. The pharmaceutical websites linked in the spam emails were all hosted in Beijing, whilst the replica watch sites were all hosted in Seoul.

Furthermore, the Bagle botnet had also been sending exactly the same spam as the Lethic botnet over the same time period. The templates for the pharmaceutical and watch spam were identical from both botnets, and included hyperlinks to the same spam websites. Perhaps the people who created the Bagle botnet have also created this newer Lethic botnet and were using both to send out spam for their clients, or it may have been that the people behind the spam hired the resources of more than one botnet gang to increase output.

[For further information, please read the MessageLabs Intelligence blog posting: <https://www-secure.symantec.com/connect/blogs/message-labs-intelligence-tracks-new-botnet>]

Haiti Scams

In the wake of the recent tragic events in Haiti, it was unsurprising to discover that scammers were quick to take advantage of the situation to generate a number of 419-style scams on the topic. While people all over the world were feeling a great deal of sympathy for the victims in Haiti and offering humanitarian aid and relief, some scammers were using any means possible to exploit donation efforts as is common with any global tragedy.

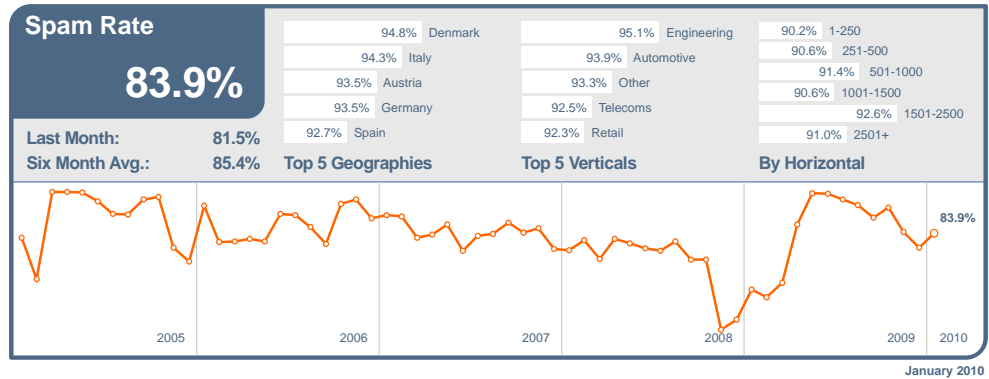
'419' advance fee fraud scams are common and the perpetrators are always looking for new attention-grabbing topics which will trick people into handing over their money. Something like the crisis of the Haiti earthquake is, sadly, a prime target for these scammers. They count on the public's good nature, concern, and desire to help, and hope that they won't see through the scam email which they are reading. The desire to help can often cloud a person's good judgment.

[For further information, please read the MessageLabs Intelligence blog posting: <https://www-secure.symantec.com/connect/blogs/419-style-scammers-seeking-exploit-appeal-donations-support-victims-haitian-earthquake>]

GLOBAL TRENDS & CONTENT ANALYSIS

MessageLabs Hosted Email AntiSpam and Hosted Email AntiVirus 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 2010, the global ratio of spam in email traffic decreased by 0.3% from the previous month to 83.9% (1 in 1.2 emails).

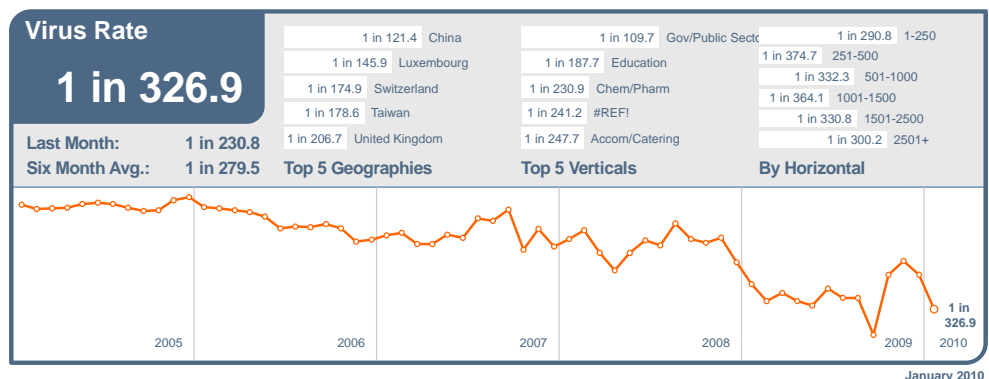


Spam levels in Denmark fell by 0.6% in January, but remained the most spammed country with levels of 94.8% of all email. In the US, spam activity also decreased to 91.6% and to 89.7% in Canada. Spam levels also fell to 90.0% in the UK. In The Netherlands, spam activity reached 92.4%, whilst spam levels in Australia reached 90.6%; 92.1% in Hong Kong and 88.2% in Japan.

In January, the most spammed industry sector with a spam rate of 95.1% was the Engineering sector. Spam levels reached 92.1% for the Education sector, and 91.0% for the Chemical & Pharmaceutical sector; 91.5% for IT Services, 92.3% for Retail, 89.3% for Public Sector and 90.1% for Finance.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic was 1 in 326.9 emails (0.31%) in January, a decrease of 0.03% since December.

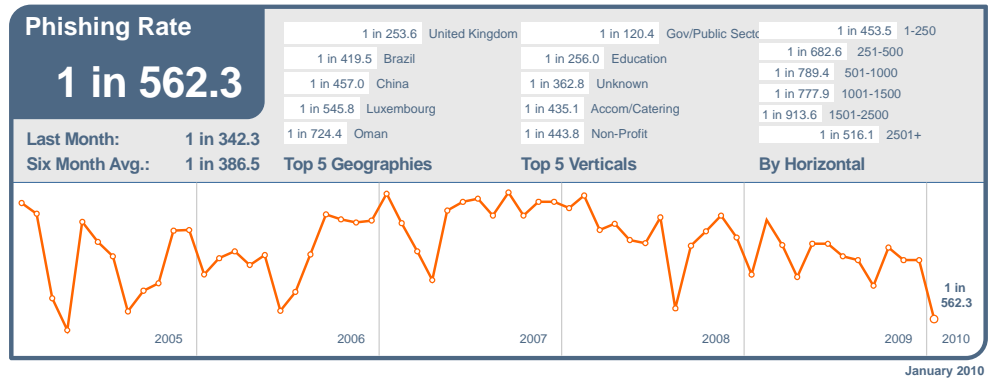
In January, 13.2% of email-borne malware contained links to malicious websites, a decrease of 5.9% since December. Spoofed postcard mails were responsible for 62.0% of malicious links in January.



Virus activity in China rose by 0.13% to 1 in 121.4 emails, placing it at the top of the table in January. Virus levels for the US were 1 in 440.3 and 1 in 383.1 for Canada. In Germany virus levels were 1 in 271.6 and in The Netherlands reached 1 in 496.4. In Australia, virus activity was at 1 in 644.1 and in Hong Kong virus activity reached 1 in 331.9; for Japan it was 1 in 396.5.

Virus activity in the Public Sector fell by 0.33%, but moved to the top of the table with 1 in 109.7 emails being infected. Virus levels for the Chemical & Pharmaceutical sector were 1 in 230.9 and 1 in 353.4 for the IT Services sector; 1 in 607.2 for Retail, 1 in 187.7 for Education and 1 in 391.5 for Finance.

Phishing: In January, phishing activity decreased by 0.11%; 1 in 562.3 emails (0.18%) comprised some form of phishing attack. When judged as a proportion of all email-borne threats intercepted in January, including viruses and Trojans, the proportion of phishing emails fell by 14.3% to 65.3% of all email-borne malware and phishing threats combined.



Phishing activity in the UK fell by 0.18% to 1 in 253.6 emails, taking the country to the top of the table in January. Phishing levels for the US were 1 in 1,558 and 1 in 811.5 for Canada. In Germany phishing levels were 1 in 1,351 and for The Netherlands reached 1 in 2,573. In Australia, phishing activity was at 1 in 1,156 and in Hong Kong phishing activity reached 1 in 1,663; for Japan it was 1 in 1,888.

Phishing activity in the Public Sector decreased by 0.93%, but was positioned at the top of the table with 1 in 120.4 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 832.4 and 1 in 987.2 for the IT Services sector; 1 in 1,307 for Retail, 1 in 256.0 for Education and 1 in 505.0 for Finance.

Skeptic™ Web Security Version 2.0: The most common trigger for policy-based filtering applied by the MessageLabs Hosted Web Security Service for its business clients was the “Advertisements & Popups” category, down by 0.41% since December, to 56.3% in January. Blocking of online Computing & Internet sites increased by 0.49%, the largest rise in any category.

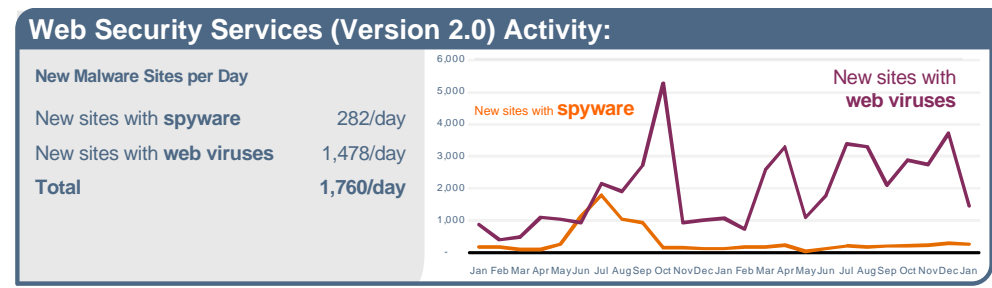
MessageLabs Intelligence identified an average of 1,760 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 56.2% since December. Further analysis also revealed that 41.4% of all malicious domains blocked were new in January; an increase of 0.6% since December. Furthermore, 12.1% of all web-based malware blocked was new in January; a decrease of 2.0% since the previous month.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	55.9%	New Unclassified Virus	23.3%	PUP:NetTool.Win32.Proxy.g	39.3%
Streaming Media	10.0%	Hoax.HTML.FakeAntivirus.a	8.1%	PUP:WebToolbar.Win32.MyWebSear...	34.4%
Downloads	4.2%	Trojan-Clicker.JS.Iframe.db	5.5%	PUP:WebToolbar.Win32.Zango.dk	6.2%
Games	3.7%	Trojan-Downloader.JS.Gumblar.x	4.5%	PUP:AdWare.Win32.HotBar.da	3.1%
Chat	3.6%	Trojan.Malscript.B	3.3%	PUP:AdWare.Win32.Zwangi.fs	2.6%
Blogs & Forums	2.6%	Trojan.Malscript!html	2.9%	PUP:WebToolbar.Win32.Sahat.b	1.7%
Computing & Internet	2.5%	New Unclassified Trojan	2.8%	PUP:AdWare.Win32.GameZTar.b	1.3%
Personals & Dating	2.0%	Bloodhound.DirActCOM	2.8%	PUP:AdWare.Win32.Shopper.l	0.9%
Adult/Sexually Explicit	2.0%	Downloader	1.5%	PUP:AdWare.Win32.Shopper.ax	0.8%
Web-based E-mail	1.9%	Trojan-Downloader.JS.Agent.ewh	1.5%	PUP:Server-FTP.Win32.SFH.cr	0.7%

January 2010

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

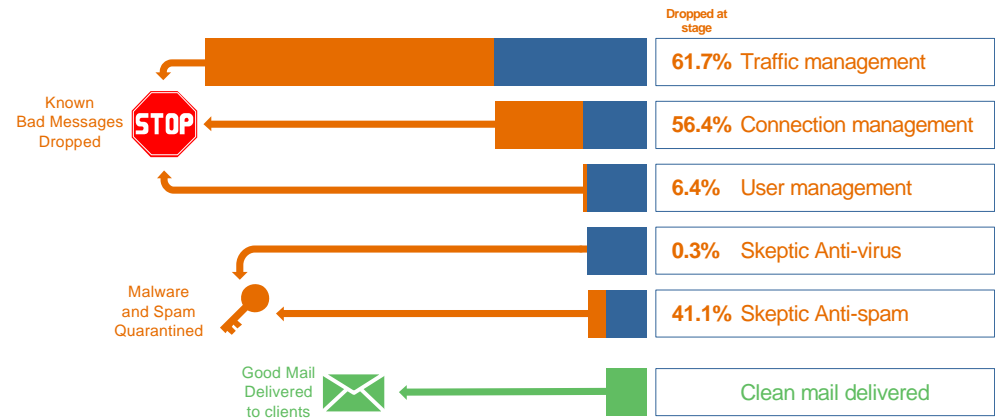


January 2010

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 10.6 billion SMTP connections per day, of which 61.7% 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 56.4% 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 6.4% 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™ 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 21,000 clients in more than 99 countries. More information is available at 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.

Copyright © 2010 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, 350 Ellis Street, Mountain View, CA 94043.