MESSAGELABS INTELLIGENCE FEBRUARY 2010

Spam Surges in February while Message Size Shrinks

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

REPORT HIGHLIGHTS

- Spam – 89.4% in February (an increase of 5.5% since January)
- Viruses – One in 302.8 emails in February contained malware (an increase of 0.02% since January)
- Phishing – One in 456.3 emails comprised a phishing attack (an increase of 0.04% since January)
- Malicious websites – 4,998 websites blocked per day (an increase of 184% since January)
- 41.6% of all malicious domains blocked were new in February (a decrease of 0.1% since January)
- 13.3 of all web-based malware blocked was new in February (an increase of 1.2% since January)
- Grum and Rustock to Blame for February Spam Surge
- While Volume Grows, Spam File Size Shrinks
- Waledac Botnet Makes a Comeback before its Demise
- Olympics-Themed Targeted Malware
- Gumblar Update

REPORT ANALYSIS

Grum and Rustock to Blame for Surge in February Spam

As expected this time of year, spammers launched a number of spam campaigns related to St. Valentine's Day, celebrated on February 14. Around this time, spammers often change their spam runs to include references to the special date. However, the 5.5% increase in spam this month cannot be completely blamed on St. Valentine's Day alone.

Figure 1 highlights the most recent spam surges in February, and further analysis reveals the underlying cause of these increases.

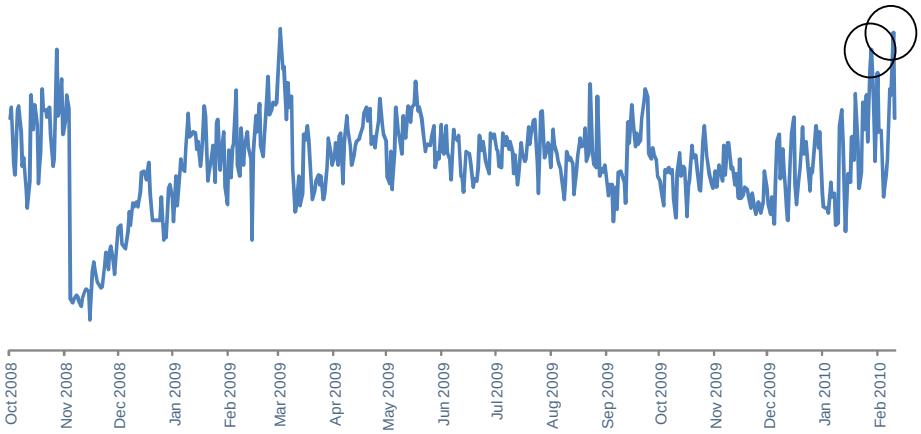


Figure 1 - Global surges in February spam volumes

Figure 2, shows the output from ten of the most active spam-sending botnets around the world during the last quarter. It can be seen that an increase in activity from the Grum and Rustock botnets are to blame.

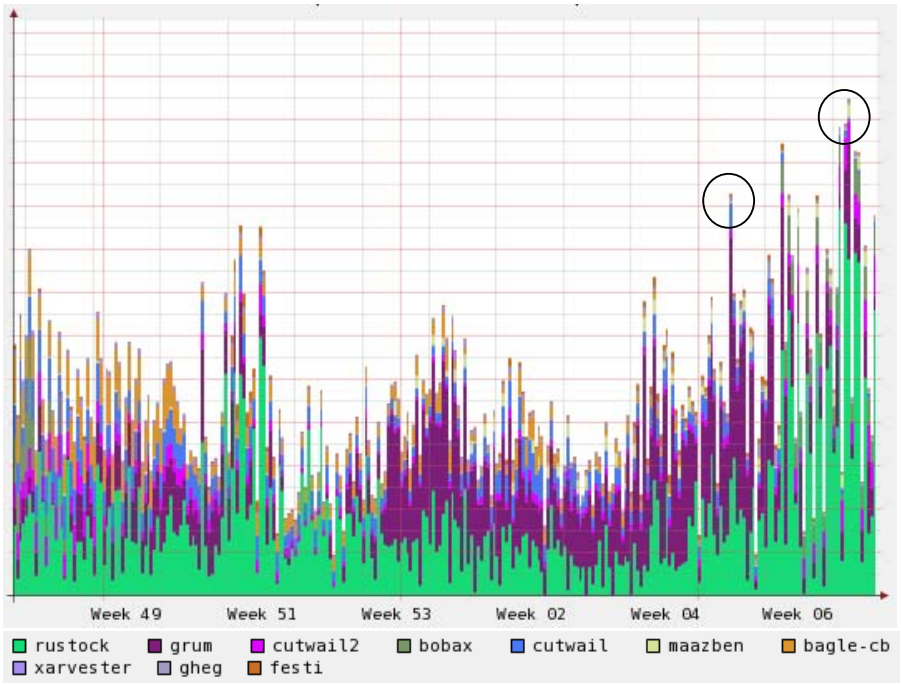


Figure 2 – Spam from top-10 global botnets for the last quarter

Figure 3 highlights relatively little change in spam volume emanating from the Grum botnet over the last 12 months and shows that from February 5 2010, its output increased by 51%.

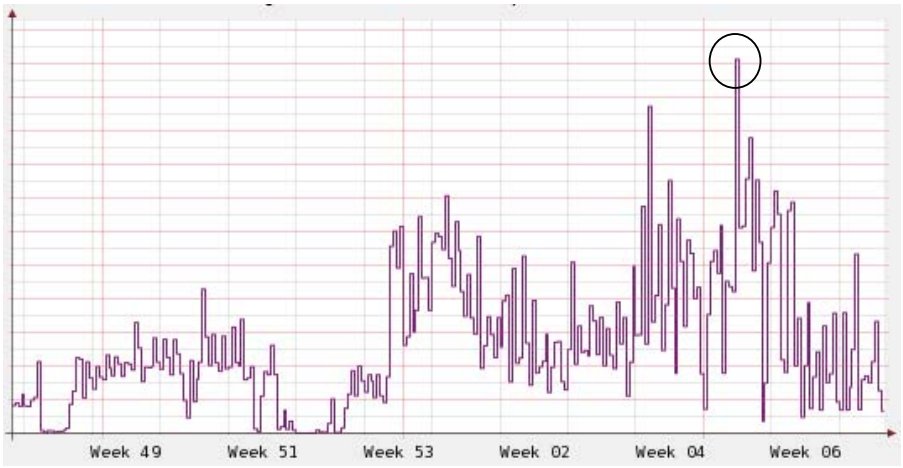


Figure 3 – Spam from the Grum botnet for the last quarter

Spam output from Grum relaxed again a few days later. Typically, spam from Grum accounts for approximately 17% of all spam, but during the recent spam surges, spam from Grum was responsible for 26% of all spam. With the other major botnets continuing as normal, the total spam volume in global circulation rose significantly, by as much as 25%.

From February 5, Grum continued to distribute the same spam campaigns that it had been in the days previously, but increased the volume on one run in particular, with Subject: "Hi."

A closer look at the 'Hi' spam run, as shown in figure 4, indicates that it is a "Canadian Pharmacy"-style spam run typical of the kind MessageLabs Intelligence has already seen in significant volumes throughout 2009 and in 2010 to date.

Pharmaceutical spam now accounts for about 65% of all spam, followed by watches (14%), Casino (5%) and weight loss (5%).

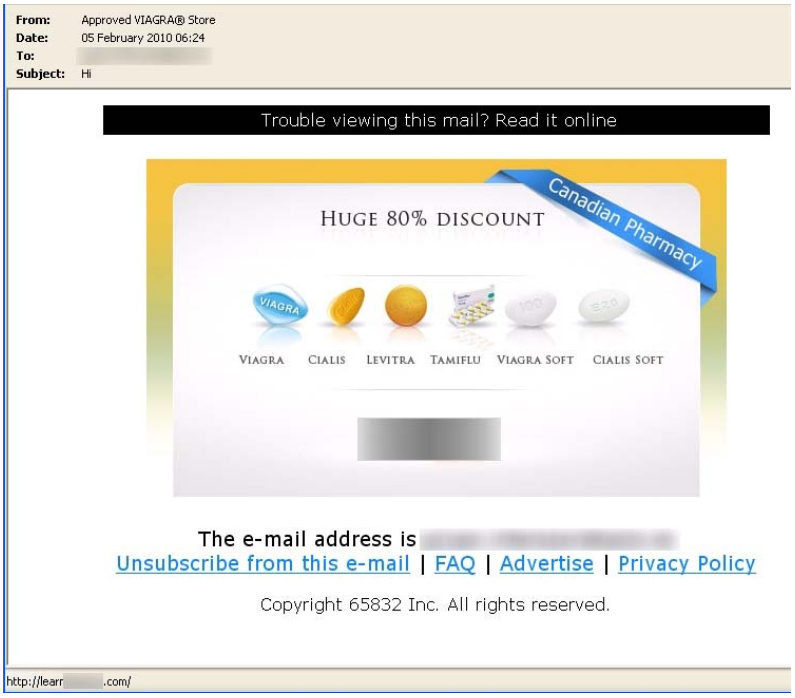


Figure 4 – Example of "Hi" Canadian Pharmacy spam

Although we don't know for sure, the spammers may have been trying to clear this particular spam run more quickly, or had perhaps discovered that this spam run was working very well, and so issued instructions to send more. It's also possible that resources elsewhere in the Grum botnet had been freed from other activities and so Grum was able to allocate more of its resources to spamming.

MessageLabs Intelligence also identified another significant spike that occurred on February 17, when global spam volumes increased by 25% on that day, pushing spam volumes even higher than they were on February 5. This was caused by a substantial increase in spam output from the Rustock botnet, as seen in figure 5.

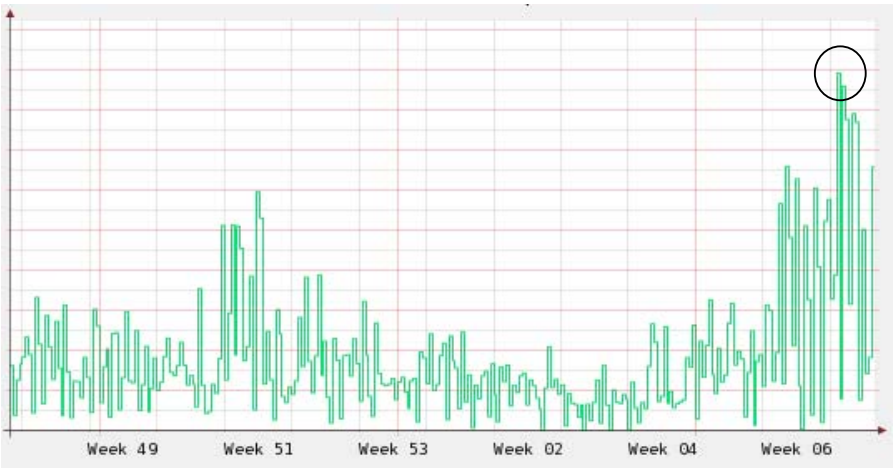


Figure 5 – Rustock spam for the last quarter

The majority of the increased spam activity was messages such as the example in figure 6.

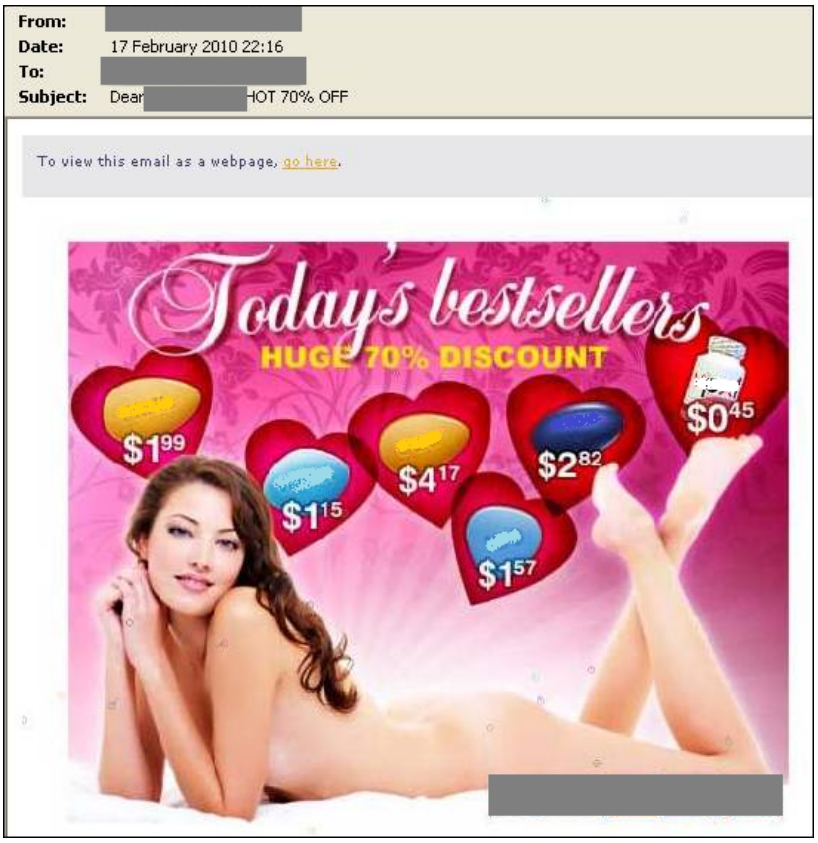


Figure 6 – Example of Canadian Pharmacy spam sent from Rustock botnet

Following the hyperlinks in these spam emails again leads to domains belonging to the same "Canadian Pharmacy" spam operation as highlighted earlier. It certainly appears that the spammers promoting these "Canadian Pharmacy" websites have been using multiple botnets to distribute several high-volume spam campaigns during February, all leading to the same "Canadian Pharmacy" websites, such as in figure 7.

Figure 7 – Banner taken from a typical Canadian Pharmacy spam website

The activities of this single spam operation have been driving the recent surges in global spam rates and strongly impacting global spam levels. Based on this latest pattern of spikes we can predict likely surges in spam over the coming weeks.

While Volume Grows, Spam File Size Shrinks

In figure 8, it can be seen that the number of spam emails that contain attachments has been diminishing over the past 12 months, from 10% in April 2009, to less than 1% in February 2010.

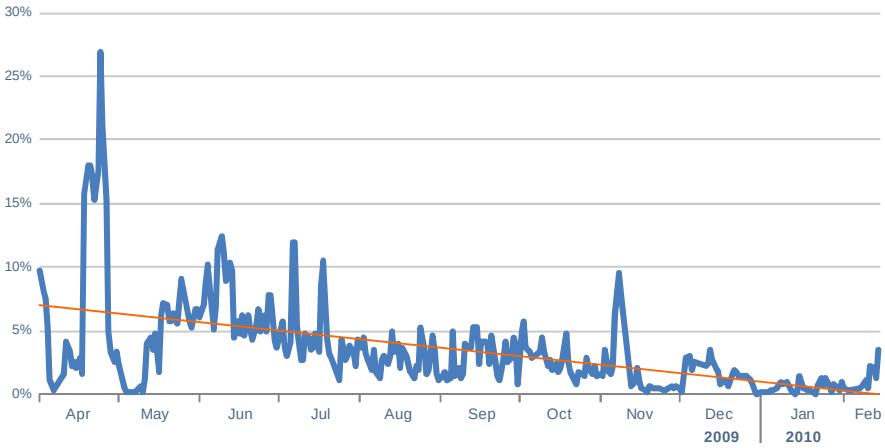


Figure 8 – Percentage of spam with a file attachment over time

In Figure 9, the average file-size (shown in bytes) of spam emails has also decreased over the past year. There are a number of reasons for this, for example, there are now more spam emails that include images which are hosted online, typically using free image-hosting services, rather than attaching the images to the emails directly.

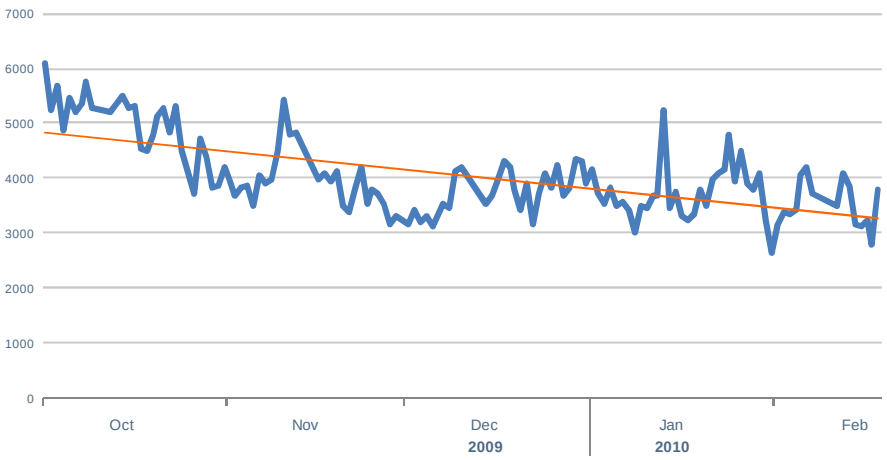


Figure 9 - Average file size of spam messages over time (bytes)

Moreover, with a reduction in the average file-size of a spam email, botnets are able to send a greater volume of spam per minute.

The average file-size of a spam email with no attachment (which accounts for approximately 99% of all spam) is 3.3Kb. Of the remaining 1% with an attachment, figure 10 highlights largest attachment types:

File Type	Average message size (Kb)
wmv	9,759.8
png	195.0
pdf	163.4
bmp	97.4
doc	94.0
jpg	78.2
post	65.6
jpeg	55.1
mail	52.6
gif	50.9
html	45.7
xls	37.0
zip	32.1

Figure 10 – Spam attachment types and sizes

To date in 2010, only 0.56% of botnet spam contains an attachment, although some botnets use attachments more so than others. For example, 6.2% of spam from the Cutwail botnet contains an attachment. Most recently, a large proportion of this relates to malware, including the latest wave of Bredolab[1] attacks, where the attachment is typically a .zip archive, such as in these typical subjects and respective attachments:

Subject: updated account agreement (agreement.zip)
Subject: Do you like to find a girlfriend like me ? (myphoto.zip)
Subject: You've received a postcard (ecard.zip)
Subject: Conflicker.B Infection Alert (open.zip)
Subject: Notification of Limited Account Access RXI034 (resolution center.html)
Subject: DHL Services. Please get your parcel NR.67554 (67554.zip)
Subject: UPS Delivery Problem Number 37678. (ups_invoice_nr28714.zip)

[1] http://www.symantec.com/connect/blogs/targeted-attacks-now-using-bredolab-malware

The Xarvester botnet also sends a lot of attachment-based spam. Approximately 3.1% of spam from Xarvester contains an attachment. This is almost exclusively Russian language spam with a .gif image attached.

More recently, however, other botnets are sending less than 1% of their spam with an attachment.

Waledac Botnet Revisited

As can be seen in figure 11, there have been some notable spikes of email-borne malware activity connected to the Waledac botnet. Waledac[2] is commonly believed to have descended from the now defunct Storm botnet, which first made its mark on the botnet landscape in January 2007, but declined during 2008 and disappeared altogether following the closure of McColo, the rogue California-based ISP in November 2008.

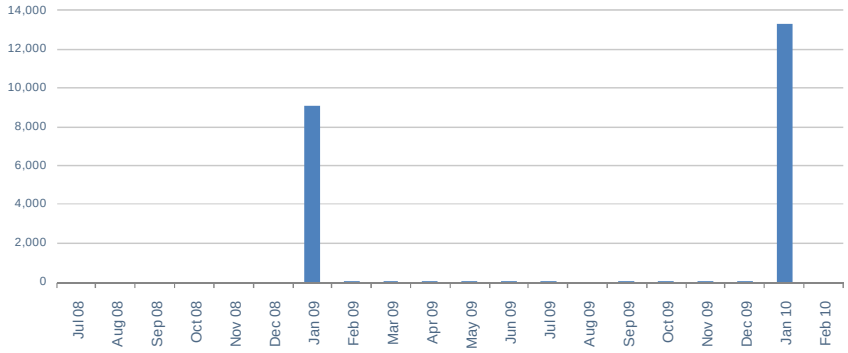


Figure 11 – Email interceptions of Waledac malware (18-months)

The first examples of Waledac malware were discovered in April 2008, and were delivered using similar techniques to the earlier Storm botnet malware (also known as Peacomm). The following year on 8 April 2009, computers infected with Downadup.C (also known as Conficker) were instructed to download two updated files through a peer-to-peer channel, one of these files was an update for the Downadup.C code, but the other was a copy of the Waledac malware. The Bredolab Trojan has also been known to drop Waledac malware on to computers under its control as well as other spam-sending botnet malware, including Rustock and Cutwail.

After an initial spike in January 2009, malware from Waledac had been relatively quiet, but another spike was observed in January 2010. Each spike accounted for less than 1% of all malware intercepted during the month.

Malicious emails connected to Waledac are not necessarily distributed by the botnet itself, but are sent by other botnets. In the typical example of the recent Waledac malware shown in figure 12, the email was sent from the Cutwail botnet.

2 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/W32_Waledac.pdf

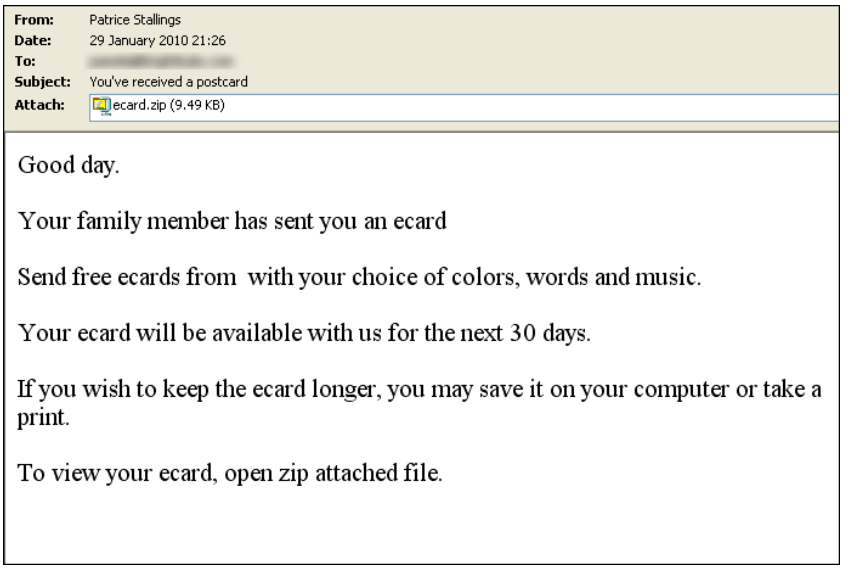


Figure 12 – Example of recent Waledac email-borne malware sent from Cutwail

Spammers using the Waledac botnet also seem to take great care to focus on major free webmail hosting services and using only email addresses that are actively in use by individuals. Waledac is adept at evading traditional dormant honeypot addresses.

On the 22 February 2009, in response to a complaint filed by Microsoft, a temporary restraining order was granted, resulting in 277 domain names believed to be associated with the Waledac botnet being taken offline[3].

Olympics-Themed Targeted Malware

As the 2010 Vancouver Olympic Games kicked-off, MessageLabs Intelligence prepared for a deluge of spam emails related to the event only to be surprised by relatively low volumes of Olympic-themed spam. Rather, what did emerge were some more sinister emails, as cyber criminals attempted to use the Olympics theme to distribute malware and launch a small number of specially targeted attacks.

One such example, as shown in figure 13, is an email with the subject, “Information and resources to help you travel during the Vancouver 2010 Winter Games. TravelSmart 2010.htm.”

[3] http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/02/24/cracking-down-on-botnets.aspx

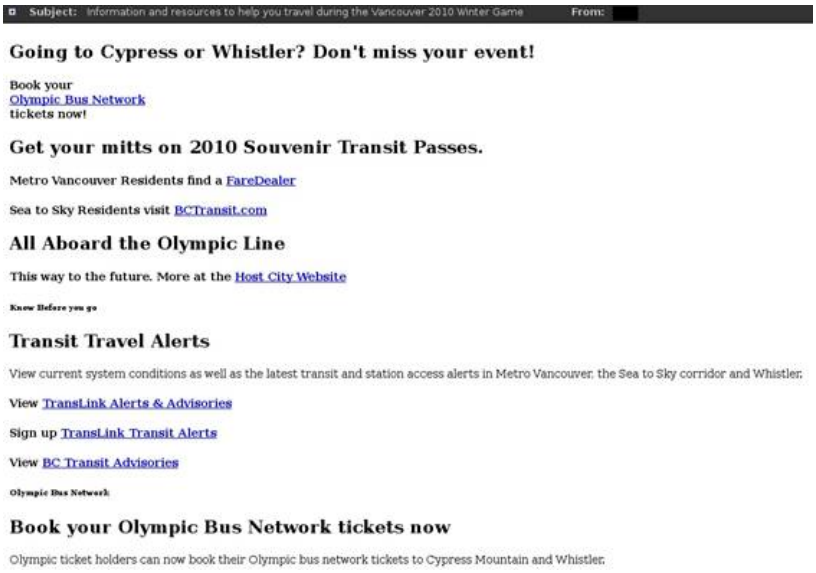


Figure 13 – An example of a malicious email containing a hidden IFRAME exploit

All of the hyperlinks contained within the email are legitimate links to genuine sites, however, a hidden HTML IFRAME tag, embedded in the email is being used to drop malware on to the recipient's computer.

MessageLabs Intelligence has also detected an Olympic-themed targeted attack, as seen in figure 14, with the subject, "How to make Olympics more interesting?"

Although the body of the email appears to be relatively simple, there was an attached presentation file, which attempts to deploy a hidden executable on to the recipient's computer through the exploitation of the CVE-2006-0022 vulnerability. This vulnerability allows an attacker to execute arbitrary code using a malformed record triggering memory corruption. In essence a chained attack, but since the initial outbreaks, the malicious executable has since been detected by many more antivirus vendors as "Spy-agent."

Figure 14 – Example of a recent Olympic-themed targeted attack

Although there were only three instances of this particular attack in February, by its nature it was not designed to be widespread. As a targeted attack it was intended to gain access to a small number of specific users' machines. If only one is successful, the damage to the victim could be substantial.

Update on Recent Gumblar Activity

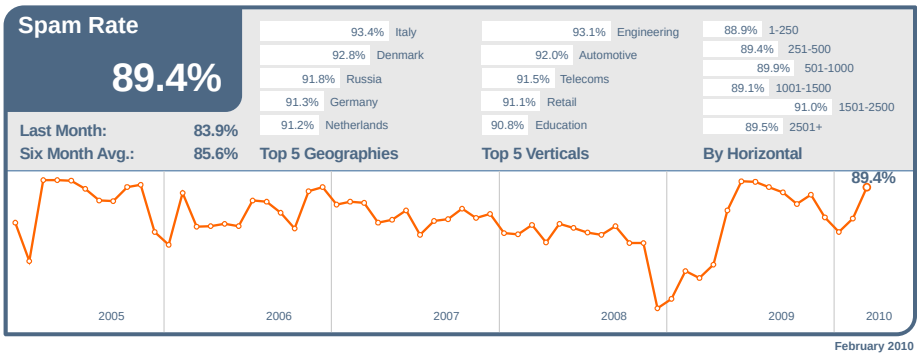
On the heels of having learned that Gumblar infected three Japanese websites late last year, MesageLabs Intelligence has tracked Gumblar's latest activity which has been heavy over the past few days, especially on January 17, when it represented 25% of all malicious blocks. Generally in January we have seen a small number of blocks each day: average blocks per day 46 (2.3% of malicious websites blocked).

For more information on this latest Gumblar activity, please visit the MessageLabs Intelligence blog at http://www.symantec.com/connect/blogs/gumblar-botnet-ramps-activity.

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 February 2010, the global ratio of spam in email traffic increased by 5.5% from the previous month to 89.4% (1 in 1.12 emails).



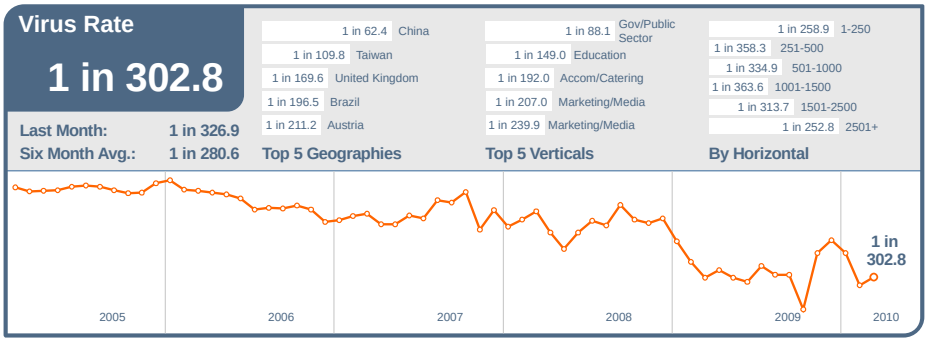
February 2010

The spam level in Italy reached 93.4% in February, positioning it as the most spammed country. In the US, 90.2% of email was spam and 88.0% in Canada. The spam level in the UK was 88.6%. In The Netherlands, spam activity accounted for 91.2% of email traffic, 91.3% in Germany and 89.5% in Australia. In Hong Kong, 90.6% of email was blocked as spam and 87.8% in Singapore, compared with 86.2% in Japan and 91.0% in China.

In February, the most spammed industry sector with a spam rate of 93.1% was the Engineering sector. Spam levels for the Education sector reached 90.8%, and 89.3% for the Chemical & Pharmaceutical sector; 89.8% for IT Services, 91.1% for Retail, 87.6% for Public Sector and 88.4% for Finance.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic was 1 in 302.8 emails (0.33%) in February, an increase of 0.02% since January.

In February, 30.5% of email-borne malware contained links to malicious websites, an increase of 17.3% since January.



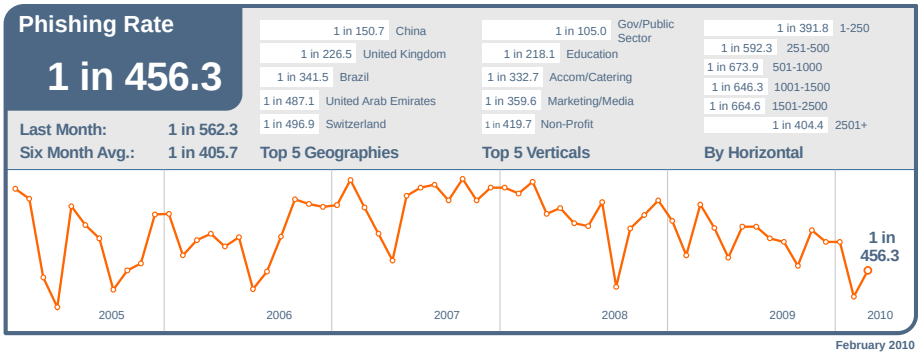
February 2010

Email-borne malware in China accounted for 1 in 62.4 emails, placing it at the top of the table in February. The virus level for the US was 1 in 488.6 and 1 in 364.8 for Canada. In Germany virus activity reached 1 in 275.8 and in The Netherlands was 1 in 616.3. In Australia, 1 in 315.1 emails were malicious and 1 in 272.2 in Hong Kong; for Japan it was 1 in 602.6, compared with 1 in 319.2 in Singapore.

In February, the Public Sector remained the most targeted industry with 1 in 88.1 emails being blocked as malicious. Virus levels for the Chemical & Pharmaceutical sector were 1 in 283.3 and 1 in 328.2 for the IT Services sector; 1 in 564.7 for Retail, 1 in 149.0 for Education and 1 in 350.4 for Finance.

VIRUSNAME	Total
Exploit/Fraud-AccUpdate	24.7%
W32/Prolaco-gen-4b33	6.0%
Trojan.Bredolab	5.3%
Trojan.Bredolab!eml	4.8%
Exploit/MimeBoundary003	3.7%
W32/Prolaco-gen	3.3%
Packed.Generic.265	2.8%
HeurAuto-fa70	2.4%
Packed.Win32.Krap.x	2.2%
Outlook/DateExploit	2.0%

Phishing: In February, phishing activity increased by 0.04%; 1 in 456.3 emails (0.22%) comprised some form of phishing attack. When judged as a proportion of all email-borne threats intercepted in February, including viruses and Trojans, the proportion of phishing emails rose by 5.1% to 56.1% of all email-borne malware and phishing threats combined.



February 2010

Phishing activity in China accounted for 1 in 150.7 emails, positioning it at the top of the table in February. Phishing levels for the US were 1 in 1,168 and 1 in 673.8 for Canada. In Germany phishing levels were 1 in 1,236 and 1 in 2,178 in The Netherlands. In Australia, phishing activity reached 1 in 502.2 and 1 in 865.7 in Hong Kong; for Japan it was 1 in 1,876 and 1 in 786.5 for Singapore.

The Public Sector remained at the top of the table with 1 in 105.0 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 599.1 and 1 in 780.9 for the IT Services sector; 1 in 1,019 for Retail, 1 in 218.1 for Education and 1 in 489.2 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 1.9% since January, to 54.4% in February. Blocking of online Computing & Internet sites increased by 0.49%, the largest rise in any category.

MessageLabs Intelligence identified an average of 4,998 websites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 184.0% since January. Further analysis also revealed that 41.6% of all malicious domains blocked were new in February; a decrease of 0.1% since January. Furthermore, 13.3% of all web-based malware blocked was new in February; an increase of 1.2% since the previous month.

Web Security Services (Version 2.0) Activity:

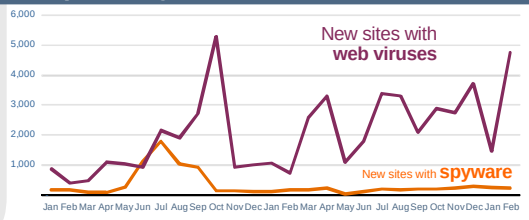
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	54.4%	New Unclassified Virus	51.22%	PUP:Server-FTP.Win32.Tftpd.274	77.7%
Streaming Media	9.0%	Trojan.Malscript.B	11.9%	PUP:WebToolbar.Win32.MyWebSear...	6.8%
Downloads	3.9%	Trojan.JS.Redirector.ar	10.6%	PUP:WebToolbar.Win32.Zango.dk	3.4%
Unclassified	3.6%	Bloodhound.DirActCOM	5.6%	PUP:NetTool.Win32.Proxy.g	1.2%
Chat	3.4%	Trojan.JS.Fraud.s	5.2%	PUP:AdWare.Win32.HotBar.da	1.1%
Games	3.1%	JS.SecurityToolFraud.B	3.1%	PUP:AdWare.Win32.Zwangi.hl	1.0%
Search Engines	3.0%	Trojan-Downloader.JS.Twetti.a	2.4%	PUP:Server-FTP.Win32.SFH.bc	0.9%
Blogs & Forums	2.9%	Trojan.JS.Iframe.hy	2.3%	PUP:AdWare.Win32.Shopper.l	0.6%
Computing & Internet	2.6%	Suspicious.MH690	1.3%	PUP:Server-FTP.Win32.SFH.cr	0.5%
Personals & Dating	2.6%	Packed.Win32.Katusha.e	1.2%	PUP:ZangoSearch	0.4%

February 2010

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

Web Security Services (Version 2.0) Activity:

New Malware Sites per Day	
New sites with **spyware**	255/day
New sites with **web viruses**	4,743/day
Total	**4,998/day**

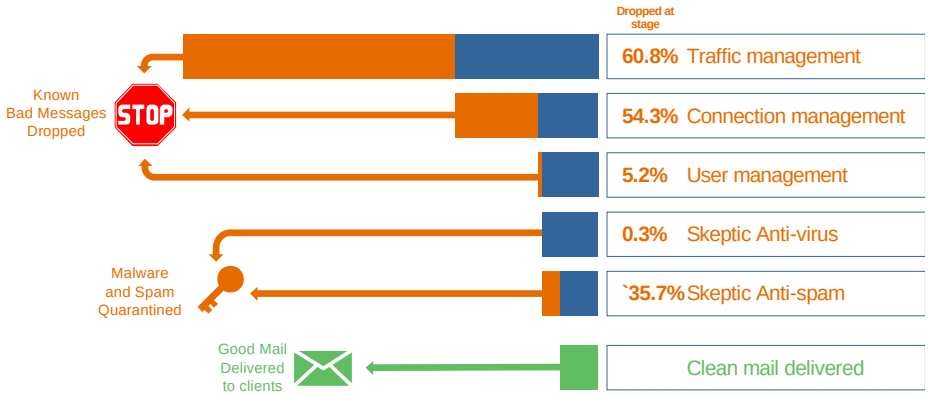


February 2010

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 February, MessageLabs services processed an average of 11.9 billion SMTP connections per day, of which 60.8% 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 February, an average of 54.3% 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 February, an average of 5.2% 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 29,000 clients in more than 100 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.