



MessageLabs Intelligence: May 2009

“Reputable sources are cyber criminals favored resources; spammers work by US clocks”

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

Report Highlights

- Spam – 90.4% in May (an increase of 5.1% since April)
- Viruses – One in 317.8 emails in May contained malware (a decrease of 0.01% since April)
- Phishing – One in 404.7 emails comprised a phishing attack (an increase of 0.11% since April)
- Malicious websites – 1,149 new sites blocked per day (a decrease of 67.7% since April)
- Spammers continue to abuse reputable domains and web-based malware more likely to be found on older domains
- Geographic location determines at what time of day you receive spam
- “Russian” spam squarely rooted in Cutwail botnet

Report Analysis

Reputable domains fall under the spotlight for spammers as they capitalize on free services

MessageLabs Intelligence recorded a further rise in spam levels between April and May 2009 of 5.1%. Much of this increase is attributed to spam with very little content other than a subject line and a valid hyperlink, such as in the typical examples below:

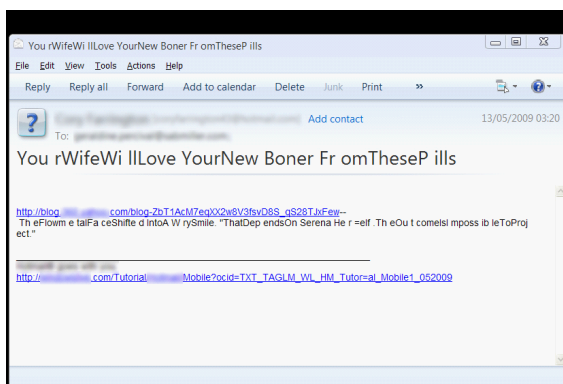


Figure 1

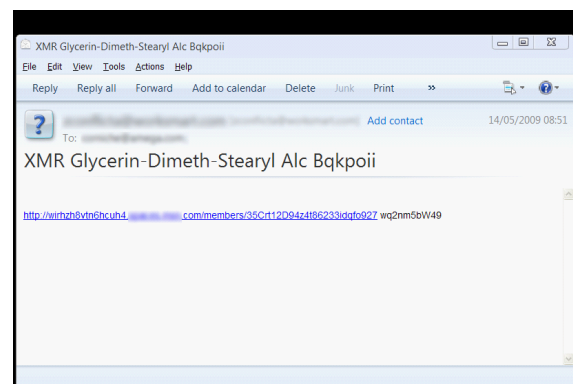


Figure 2

In each case, the hyperlink pointed to a different active profile on one of a number of major social networking environments. These profiles appear to have been created using random names, perhaps with automated CAPTCHA-breaking tools. Spammers may be using this method as they recognize that the days are numbered for the traditional approach to CAPTCHAs¹, as some major sites are already investigating alternatives to the swirling letters and numbers. In some cases photographic images are now being used with which the user must be able to analyze or interact, in such a way that would be very challenging for a computer program.

The benefit to the spammers of using such accounts is that the emails are sent from valid accounts on major free-webmail hosting providers, which in turn means that the headers were correct for the domains from which each message originated. The emails were not being spoofed, as was often the case for these types of domains in the past. Techniques to check the validity of these headers are ineffective as anti-spam countermeasures, as all they will establish is that the sender is genuine and not spoofed or sent from a botnet.

The hyperlink in Figure 2 on the previous page opens the below example (Figure 3) for the profile account created on the social networking environment.

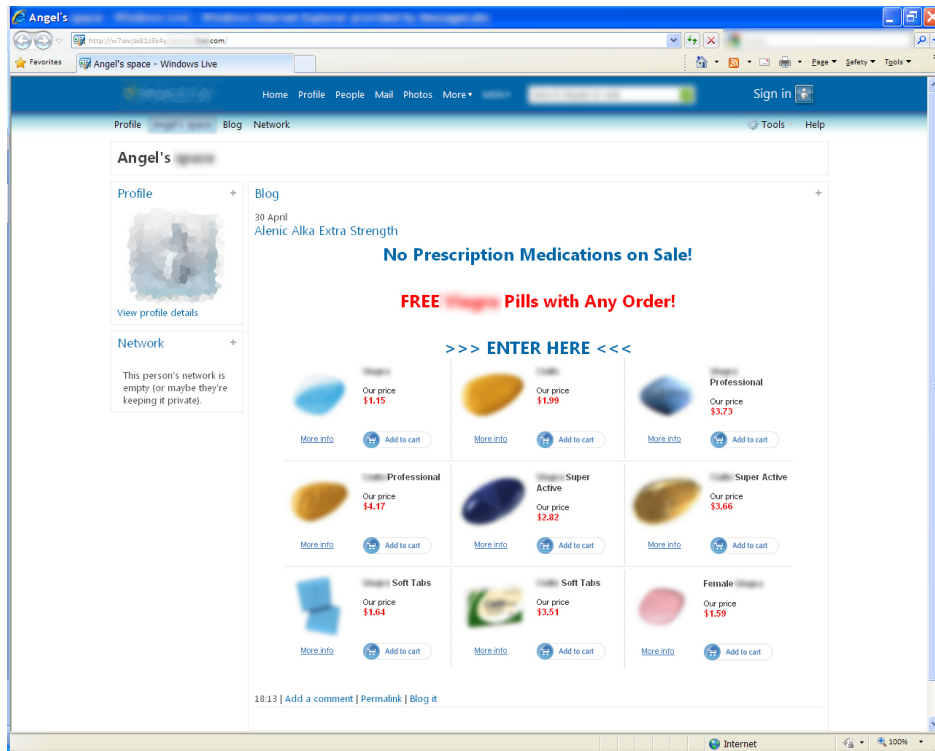


Figure 3

In the main part of the profile page is an image file, which is used to present the main advertisement for the pharmaceuticals being offered. The properties of this image reveal that it is actually being hosted on a .cn (China) domain, located elsewhere:

```
</a>
```

This domain in turn acts as a proxy service, redirecting the link in order to obfuscate the true location of the image file, as can be seen from the trace below (Figure 4), which follows the route a web browser would take in order to download and present the image on the screen.

1 Completely Automated Public Turing test to tell Computers and Humans Apart

```

C:\>net -S -U "MSIE/8.0" http://[redacted].cn
--2009-05-14 13:55:08-- http://[redacted].cn/
Resolving [redacted].cn...
Connecting to [redacted].cn|:80... connected.
HTTP request sent, awaiting response...
HTTP/1.1 302 Moved Temporarily
Server: nginx/0.6.35
Date: Thu, 14 May 2009 12:55:08 GMT
Content-Type: text/html
Content-Length: 161
Connection: keep-alive
Location: http://[redacted].com/
Location: http://[redacted].com/[following]
--2009-05-14 13:55:09-- http://[redacted].com/
Resolving [redacted].com...
Connecting to [redacted].com|:80... connected.
HTTP request sent, awaiting response...
HTTP/1.1 200 OK
Server: nginx/0.6.34
Date: Thu, 14 May 2009 12:55:09 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/4.4.9
Set-Cookie: USID=21408b141cf4396dd1c084f3528efac9; expires=Sat, 14 Jul 2012 22:41:49 GMT; path=/
Set-Cookie: aid-deleted; expires=Wed, 14 May 2009 12:55:08 GMT; path=/
Set-Cookie: said-deleted; expires=Wed, 14 May 2009 12:55:08 GMT; path=/
Set-Cookie: LastVisit=2009-05-14+16X3A55X3A09; expires=Fri, 14 May 2010 12:55:09 GMT; path=/
length: unspecified [text/html]
Saving to: 'index.html'

[ <=> ] 88,500 211K/s in 0.4s
2009-05-14 13:55:09 (211 KB/s) - "index.html" saved [88500]

```

Figure 4

In some cases there were also formatting and coding errors contained within the HTML code behind the short email messages that would not be obvious to the recipient viewing the message, but were only visible when viewing the source code to the HTML email.

Spam for breakfast, lunch or dinner?

Research into when you can expect to receive spam, depending on your geographic location, has been conducted by MessageLabs Intelligence. Traced over a seven day period, analysis highlights that if you are located in the US, spam activity peaks at between 9 – 10 a.m. local time, and trails off to much lower levels overnight. Europeans are likely to receive a steady stream of spam throughout their day, while users in the Asia-Pacific region are likely to start their day with an inbox already full of spam, with only small amounts trickling in after this point until the evening.

In the charts below (Figure 5,6,7), the time of day is adjusted for the local time zone of the recipient, and shows the spam levels as they fluctuate throughout the day, in each region.

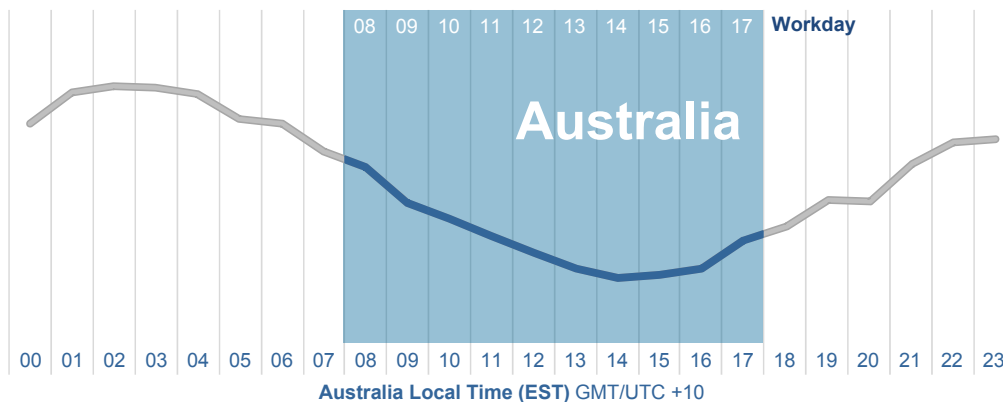


Figure 5: Hourly volume of spam received for Australian Sydney-based recipients

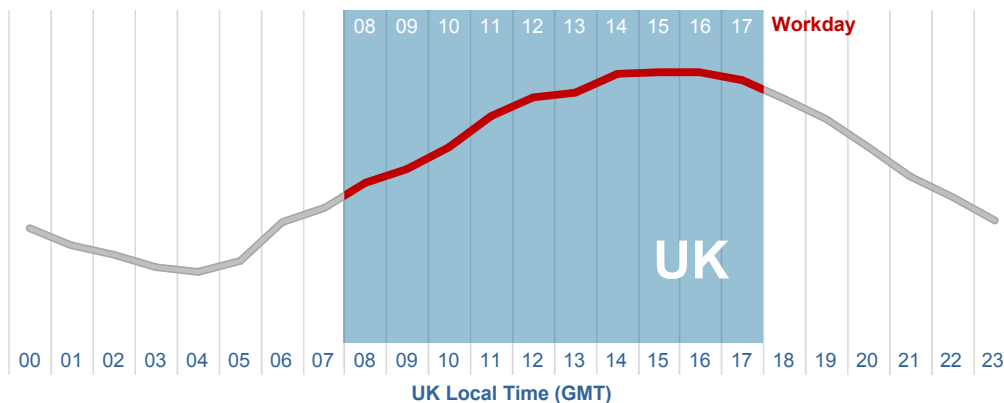


Figure 6: Hourly volume of spam received for UK recipients

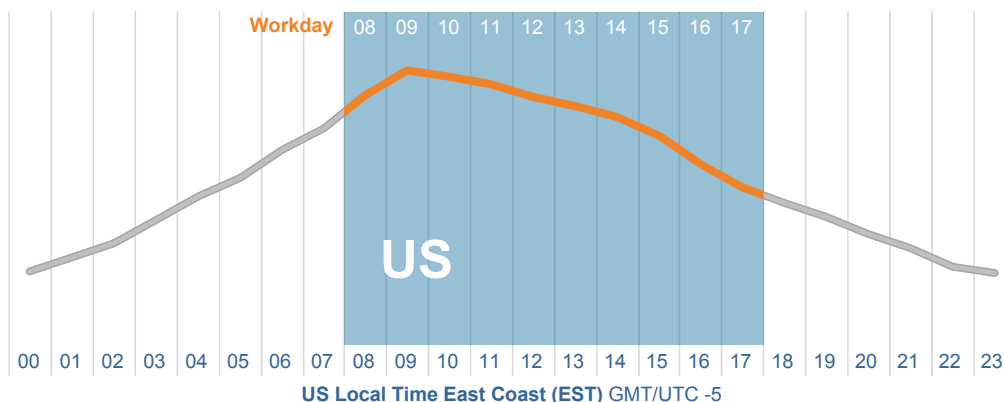


Figure 7: Hourly volume of spam received for US East Coast recipients

This profile suggests that spammers are predominately active during the US working day, and may be indicative of the fact that the most active spammers are based in the US (according to Spamhaus ROKSO²). It may also be considered that this time of day is when the spammers' largest target audience are online and more likely to respond.

Further analysis reveals that the source of this spam (based on the originating IP address of the sender) is very much more evenly distributed across the three main regions:

- 34.8% of spam originates from the Americas (21.4% from South America, 13.4% from North America);
- 31.6% from Europe;
- 27.8% from Asia

The majority (around 57.6%) of spam was sent from known botnets, and these botnets are more or less evenly distributed around the world. Analysis of the spam sent from each botnet reveals that Donbot is currently the most active botnet and is responsible for around 18.2% of all spam and is most active in Asia. However, Rustock (16.1% of spam), and Bagle (6.3% of spam), the second and fourth most active respectively, are heavily based in the Americas with very little activity in Asia. Cutwail, currently the third most active botnet with a large presence in EMEA, South America and APJ, was responsible for 8.6% of all spam. Xarvester was responsible for 1.9% of the spam, and is found mainly in South America, US and India.

2 Spamhaus Register of Known Spam Operations (<http://www.spamhaus.org/rokso>)

Much of the remainder (around 42.4%) of spam originated from smaller, or unclassified botnets and included spam sent from accounts created on major webmail hosting providers (often created using CAPTCHA-breaking tools). This type of spam emanates mainly from the US, as this is the location of many of the mainstream free webmail and application service providers being abused by the spammers and cybercriminals.

Understandably, across all regions, spam levels drop significantly on Sundays. For all countries examined (except Japan), spam levels drop mid-week, with peak activity periods being Mondays and Fridays.

Web-based malware more likely to be found on older domains

The common assumption that most web-based malware resides on less reputable websites, perhaps touting adult content, was called into question when MessageLabs Intelligence identified that cybercriminals appear to be more likely to hide malicious content on older domains that have been well-established, but perhaps compromised or malware being hosted in breach of their terms of use. The latter being typical of domains connected with social networking environments, providing mainly user-generated content.

MessageLabs Intelligence data³ from the week of 5 May 2009 revealed that:

- 84.6% of website domains blocked for hosting malicious content are well-established domains that are over a year old
- 15.4% of domains blocked are domains that are less than a year old
- 10.2% are domains that are less than a month old
- and 3.1% are domains that are less than a week old

Older domains are almost certainly more likely to be well-established and more reputable, and the likelihood that they are legitimate sites that have been compromised in some way is increased.

Domains that are only a week old or less and implicated in hosting malware are more likely to be temporary sites set up with the sole purpose of distributing malware or spam, such as in the numerous domains that exist solely to distribute rogue anti-spyware or anti-malware products.

Very new sites are often found to be used by affiliates, in order to redirect visitors to another site. This helps to ensure that they receive payment for any click-thrus that their sites generate, but sometimes they will include drive-by attacks, using hidden HTML IFRAME exploits, for example.

The number of new websites harboring malicious content identified daily fell from 3,561 in April, to 1,149 in May. Although the number of new sites may have declined in May, the nature of the threat has shifted towards older domains being used to host malware. Legitimate sites are more likely to be trusted and are more valuable to the criminals if compromised through SQL injection attacks, for example.

This highlights a trend that cybercriminals are now favoring well-established domains for hosting malware, as the number of blocks against sites already identified as hosting malicious content continues to grow. This pattern is very similar to the way that spammers abuse the services of well-known online webmail and social networking environments to host spam content and evade detection.

Businesses therefore need to ensure they take the necessary precautions to block the latest wave of malicious attacks.

³ NB: These figures are cumulative; for example, 10.2% of sites less than a month old includes 3.1% of sites less than a week old.

Russian language “ransom-style” spam and obfuscation

In late April, in a rather bizarre new twist on image spam, MessageLabs Intelligence identified a small volume of what at first glance appeared to be “ransom-style” spam messages, reminiscent of traditional ransom messages constructed from individual letters cut out of newspapers. The image appeared to have been made up from the Russian character set, taken from different font styles.

Although the subject isn’t very menacing, translating to “how to attract customers,” it also included an email contact as well as a telephone and ICQ contact number. ICQ is a legitimate instant messaging service favored by many Eastern European and Russian cybercriminals and spammers.

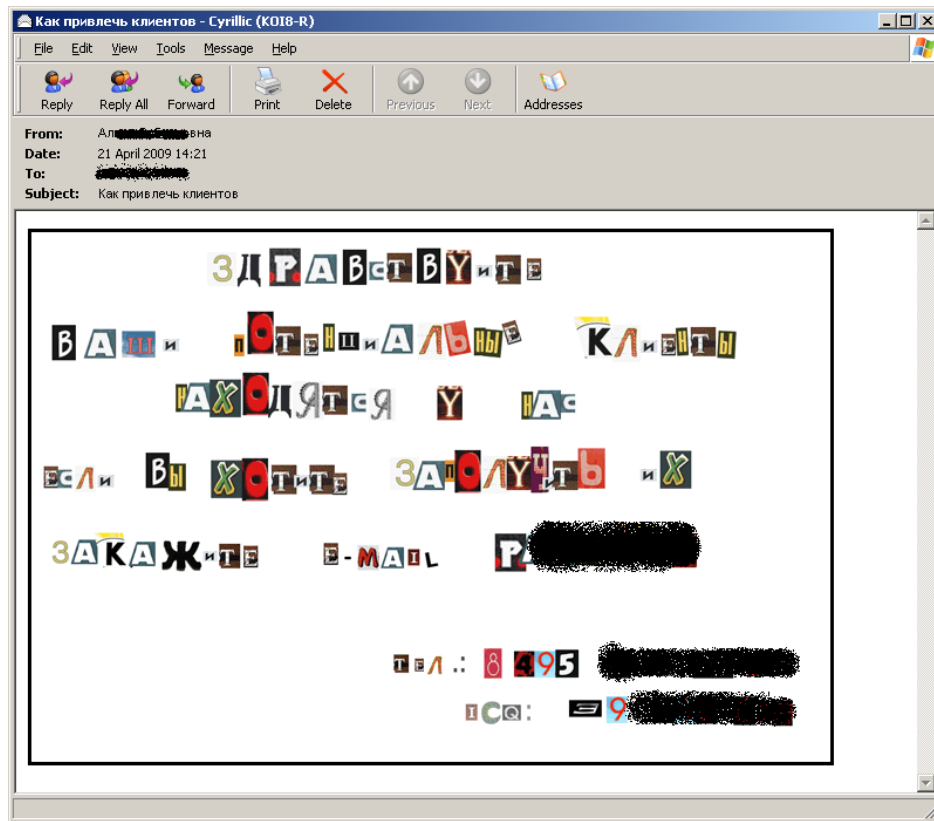


Figure 8

The translation for the message in Figure 8 is as follows:

Hi,

we know your target audience,
If you want to get to them
order email distribution from us
Phone XXX
ICQ XXX

The use of the Russian language character set has risen in some more recent spam runs, most notably where the subjects are using a Russian character set to hide the English language content, such as in the following example, when viewing the text source of the email message:

Subject: =?koi8-r?B?QmVpbmcd2VhbHROesBpcyBhYm91dCBiZWluzYBoZWfSdGh5IJYgbGVh?=
=?koi8-r?B?cm4gaG93Lg==?=

Each character set includes the 26-letter Roman alphabet, which in turn is being used by the spammers to hide the true meaning behind the message. When decoded, the subject is displayed as follows and can be seen in the screenshot of the original email below (Figure 9):

Subject: Real manliness is renewable at any age √ make sure yourself.

The unnecessary use of another character set to encode the English language subject is purely to hide the true content of the subject of the message, and a technique sometimes used by spammers to avoid content filters.

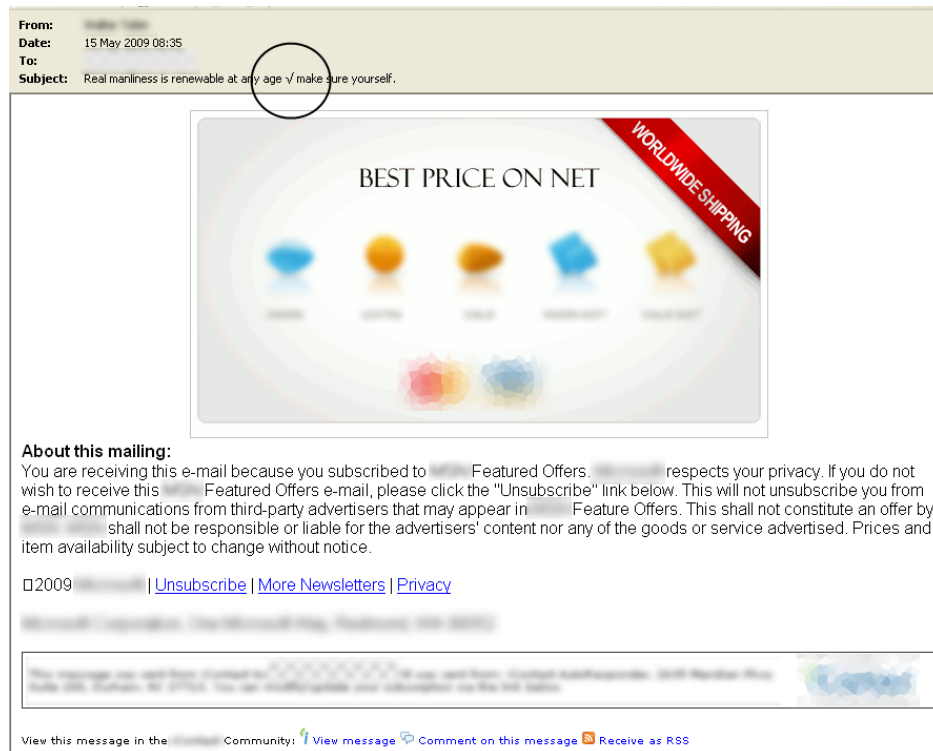


Figure 9

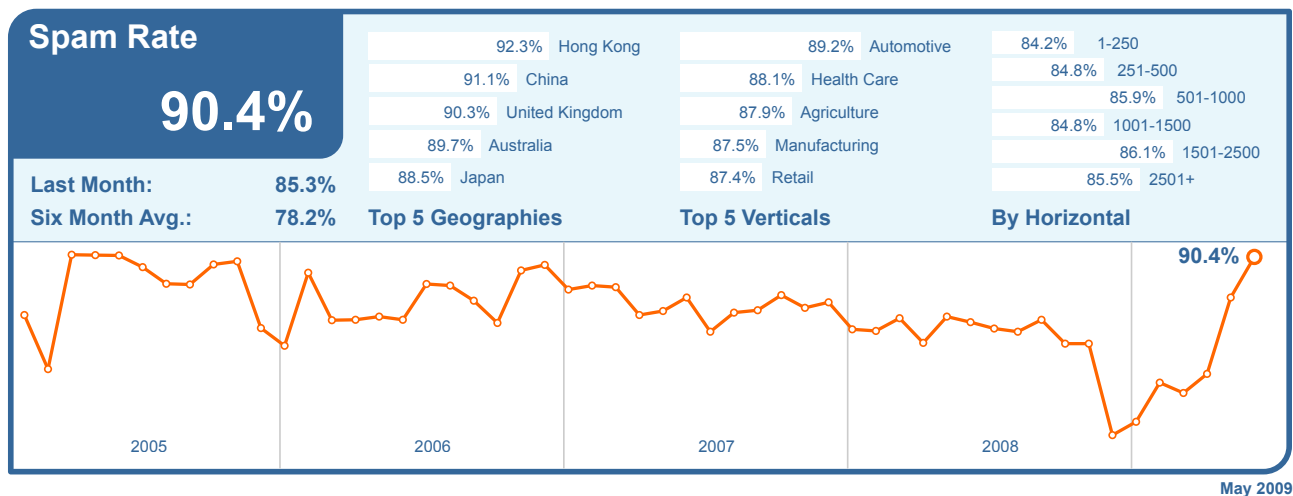
The use of the square-root character (√) is perhaps interesting and doesn't appear to have been used in spam messages in this way before.

This practice seems to have become more popular in recent weeks, and now appears in up to 2% of spam, all of which has been sent from the Cutwail botnet.

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 May 2009, the global ratio of spam in email traffic from new and previously unknown bad sources, was 90.4% (1 in 1.11 emails), an increase of 5.1% since April.

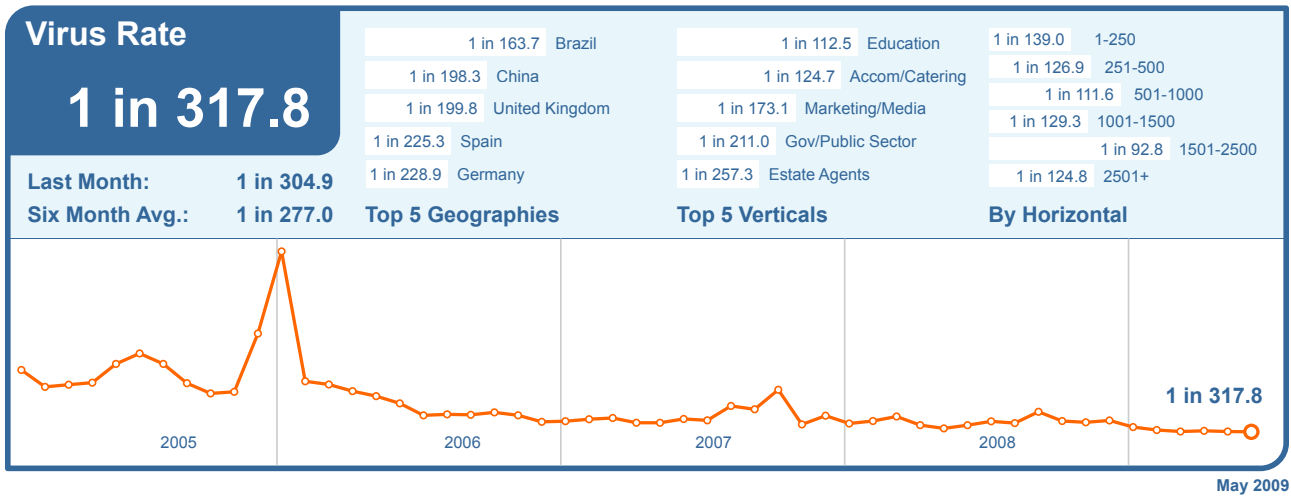


Spam levels in Hong Kong rose by 2.4% in May, placing it at the top of the table as the most spammed country, with levels at 92.3% of all email. Spam levels in the UK fell to 90.3%, in the US rose to 86.6% and 85.2% in Canada. Germany's spam rate reached 84.8% and spam reached 82.4% in the Netherlands. Spam levels in Australia were 89.7%, 91.1% in China and 88.5% in Japan.

In May, the most spammed industry sector with a spam rate of 89.2% was the Automotive sector. Spam levels reached 85.4% 88.1% for the Healthcare sector, and 87.9% for the Agricultural sector; and 87.5% for Manufacturing and 87.4% for Retail.

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 317.8 emails (0.31%) in May, a decrease of 0.01% since April.

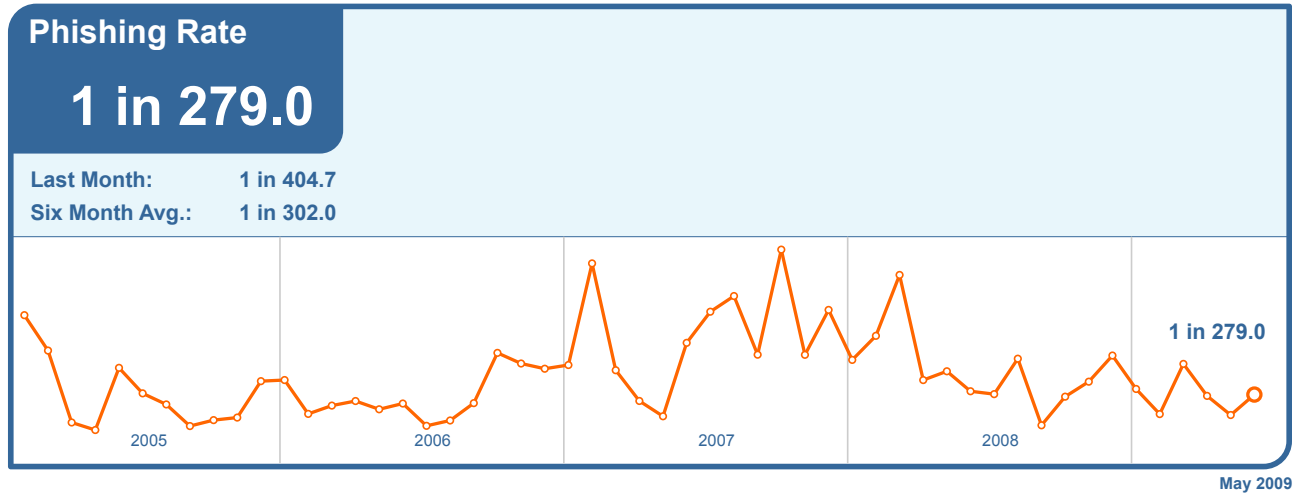
In May, 7.0% of email-borne malware contained links to malicious sites, a decrease of 6.3% since April. Spoofed postcard mails were responsible for 59.1% of malicious links in May.



Virus activity in Brazil rose by 0.05% to 1 in 163.7 emails, placing it at the top of the table in May. Virus levels in the UK rose to 1 in 199.8, in the US rose to 1 in 473.4 and 1 in 262.1 in Canada. Germany's virus rate reached 1 in 228.9 and the virus rate reached 1 in 766.0 in the Netherlands. Virus levels in Australia were 1 in 602.8, 1 in 198.3 in China and 1 in 1,852 in Japan.

Virus activity in the Education sector rose by 0.04% and remains positioned as the most targeted vertical with 1 in 112.5 emails being infected. Virus levels for the IT Services sector were 1 in 249.1, 1 in 433.5 for Retail, 1 in 466.9 for Finance and 1 in 211.0 for the Public Sector.

Phishing: May saw an increase of 0.11% in the proportion of phishing attacks compared with April. One in 279.7 (0.36%) emails comprised some form of phishing attack. When judged as a proportion of all email-borne threats such as viruses and Trojans, the proportion of phishing attacks had remained unchanged at 89.7% of all email-borne malware and phishing threats intercepted in May.



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 0.2% since April, to 61.4% in May.

Analysis of web security activity shows that 34.2% of all web-based malware intercepted was new in May. MessageLabs Intelligence also identified an average of 1,149 new sites per day harboring malware and other potentially unwanted programs such as spyware and adware; a decrease of 67.7% since April.

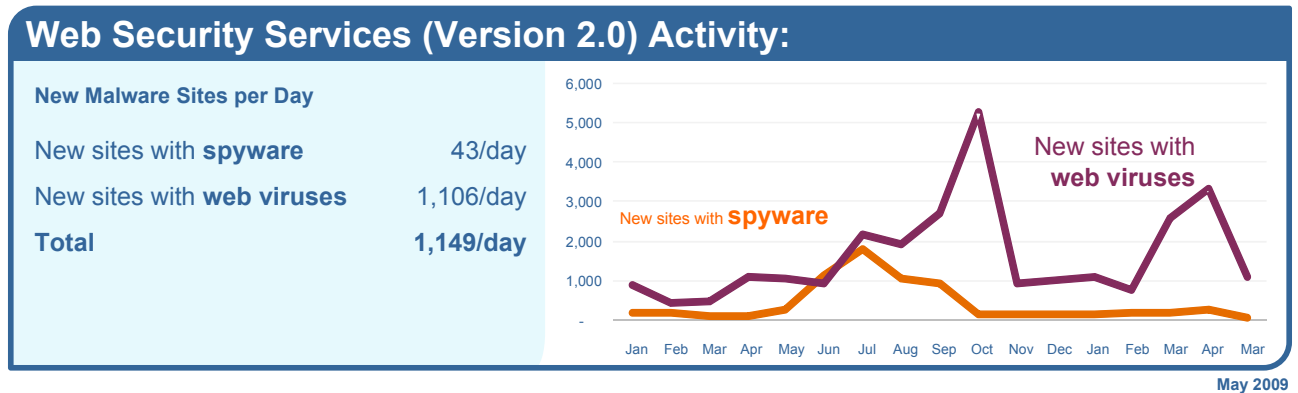
Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	61.4%	Backdoor.Win32.VB.iqo	5.0%	PUP:WebToolbar.Win32.MyWebSearc...	43.0%
Streaming Media	9.9%	New virus	4.7%	PUP:ZangoSA	18.2%
Games	5.6%	Trojan-Downloader.HTML.Agent.ij	3.2%	PUP:AdWare.Win32.SearchPage	8.0%
Downloads	4.2%	Trojan-Downloader.JS.Iframe.aqu	3.0%	PUP:RemoteAdmin.Win32.WinVNC...	3.3%
Blogs & Forums	2.5%	JS/Tenia.d	2.7%	PUP:SAHAgent	2.8%
Adult/Sexually Explicit	2.0%	Trojan-Downloader.JS.Iframe.auk	2.5%	PUP:BDSearch	2.8%
Chat	1.8%	Trojan.JS.Agent.abf	2.4%	PUP:WebToolbar.Win32.Zango.ca	2.5%
Personals & Dating	1.7%	HTML/FakeAV	2.3%	PUP:RemoteAdmin.Win32.WinVNC.n	2.5%
Computing & Internet	1.3%	Exploit-CVE2009-0553	2.1%	PUP:WebToolbar.Win32.MyWebSea...	2.2%
Infrastructure	1.0%	Trojan-Spy.HTML.Fraud.gen	1.90%	PUP:Server-FTP.Win32.Tftp.500	2.2%

May 2009

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.

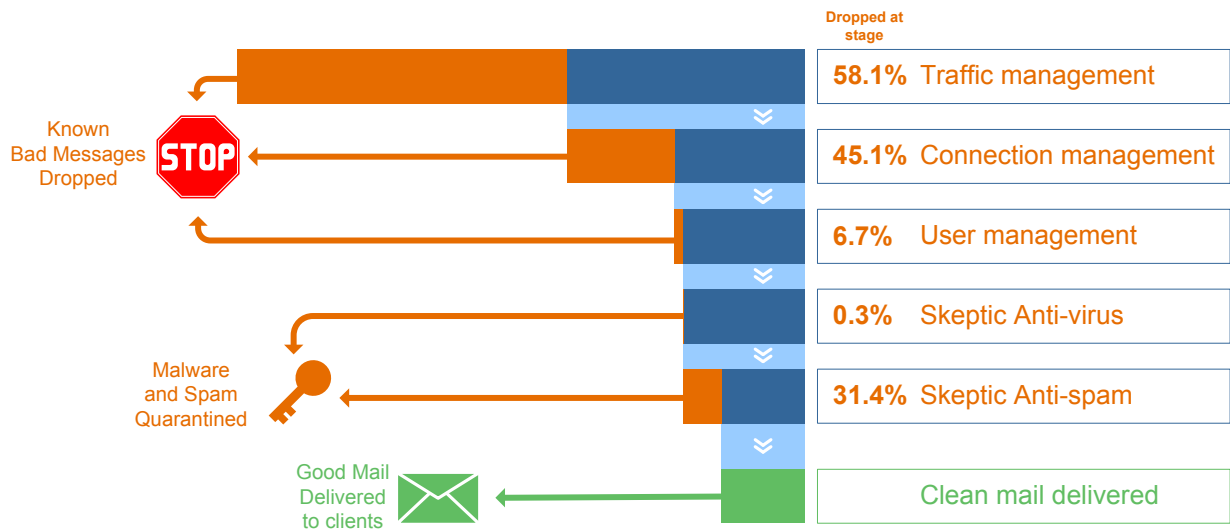
The chart below shows the increase in the number of new spyware and adware sites blocked each day on average during May compared with the equivalent number of web-based malware sites blocked each day.



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 May, MessageLabs services processed an average of 3.54 billion SMTP connections per day, of which 58.1% 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 May, an average of 45.1% 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 May, an average of 6.7% 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 19,000 clients in more than 86 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 © 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.