MessageLabs® | Now part of Symantec

MessageLabs Intelligence: Q2/June 2009
"Cutwail's bounce-back; Instant messages can lead to instant malware"

Welcome to the Q2/June edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for June 2009 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Report Highlights

- Spam – 90.4% in June (unchanged since May)
- Viruses – One in 269.4 emails in June contained malware (an increase of 0.06% since May)
- Phishing – One in 280.4 emails comprised a phishing attack (unchanged since May)
- Malicious websites – 1,919 new sites blocked per day (an increase of 67.0 % since May)
- 58.8% of all web-based malware intercepted was new in June, an increase of 24.6% since May
- The Cutwail Botnet bounces back
- The power of botnets – 83.2% of all spam was sent via botnets in June
- Image spam continues, accounting for 8-10% of all spam in June
- Instant Messaging malware increases – 1 in 78 IM-based hyperlinks point to malicious websites
- HITECH Act puts pressure on healthcare sector

Report Analysis

Cutwail's bounce-back: Harnessing the power of botnets

One of the largest and most actve botnets responsible for spam activity, the Cutwail botnet, experienced several hours of downtime on the morning of June 5, 2009, following the shutdown of California-based ISP Pricewert LLC (also known as 3FN and APS Telecom) by the U.S. Federal Trade Commission earlier that week. Malware from the Cutwail botnet, also known as Pandex, was first identified in January 2007.

botnet	% of spam	spam/day	spam/min	spam/bot /min	estimated botnet size	top 3 countries of infection
Cutwail	45.8%	74,115,721,081	51,469,251	257	1400k - 2100k	Brazil (14%), RepKorea (14%), USA (10%)
Rustock	4.5%	7,231,588,803	5,021,937	97	640k - 960k	Brazil (12%), India (10%), Turkey (9%)
Grum	6.0%	9,624,703,890	6,683,822	76	600k - 900k	Russia (27%), Ukraine (11%), Brazil (8%)
Donbot	3.2%	5,150,182,696	3,576,516	62	360k - 540k	Brazil (12%), India (12%), Turkey (8%)
Bagle	1.7%	2,716,295,255	1,886,316	53	300k - 450k	Brazil (14%), USA (9%), Argentina (8%)
Xarvester	0.2%	285,121,953	198,001	41	30k - 50k	Poland (11%), Brazil (11%), Turkey (7%)
Mega-D	9.3%	15,043,613,046	10,446,954	560	460k - 700k	Brazil (17%), India (7%), Turkey (7%)
Gheg	1.4%	2,216,672,839	1,539,356	69	170k - 250k	Turkey (24%), Vietnam (17%), India (10%)
Asprox	0.2%	382,667,732	265,741	146	11k - 17k	Brazil (25%), Argentina (9%), Poland (8%)
Darkmailer	0.1%	93,954,453	65,246	590	1k	USA (22%), France (16%), RepKorea (11%)
Unclassified Botnets	10.5%	17,012,784,584	11,814,434	93	860k - 1300k	Brazil (14%), USA (6%), India (5%)

Figure 1: Table of top active botnets (June 2009)

© Symantec 2009

With between 1.5 and 2 million active bots, Cutwail was perhaps the largest botnet in history at its peak. Before the November 2008 shutdown of ISP McColo, Cutwail was linked to approximately 25% of all spam. By the end of May 2009 it was responsible for 35% of all spam. The Acai berry spam runs, which MessageLabs Intelligence reported on in May, have been among its larger spam runs.

At the time of writing, the Cutwail botnet had managed to recover to approximately one third of its original capacity, while still limping from the impact of this latest ISP shutdown, it wasn't as badly affected as Srizbi, a rival botnet that was devastated by the closure of McColo, another ISP, in November 2008. The fact that the botnet was able to recover after only a few hours highlights the progress that spammers have made since November's McColo shutdown. Clearly, spammers have learned the importance of having a backup for their command and control channels.

Pricewert allegedly engaged in the deployment of botnets and the distribution of illegal, malicious and harmful content such as spam and child exploitation images.

Cutwail	Without doubt the biggest botnet around. Since March it has doubled in size and output per bot
Rustock	Still sending in bursts, when active this botnet shows the scale of its spamming ability. Frequently goes through periods of zero activity.
Grum	Still patchy in output, has become more active in recent months
Donbot	One of the top botnets, but less active recently than it has been previously
Bagle	Smaller than the really big botnets, but consitent in output and still growing
Xarvester	Earlier in the year, one of the major botnets. In recent months it has drastically reduced in size and output
Mega-D	At the start of the year, the top botnet, it has been steadily declining in size since then. Still one of the hardest working botnets in terms of spam per bot per minute
Gheg	A smaller botnet, but with consistent output
Asprox	Patchy output, has recently started working its bots harder to increase output
Darkmailer	A very small botnet, but has managed to get attention by the sheer volume of spam it sends per bot per minute

Descriptions of major botnets most active during June 2009

Spam from botnets accounted for around 83.2% of all spam in June. Much of the remainder is sent from compromised mail servers and webmail accounts. Some of the smaller botnets can also control the sending of spam through webmail accounts in such a way as to make it appear as though there is a real person behind the use of each webmail account.

As reported in previous MessageLabs Intelligence reports, many such webmail accounts are established in an automated fashion, using CAPTCHA-breaking tools to bypass the visual or audio puzzles that are found on the signup pages of websites. This deters registration by automated software programs. As an alternative approach, there are also businesses that specialize in providing real people to break CAPTCHA manually on a 24-hour basis. Often advertised as a data processing job, each worker can be expected to receive approximately two to three dollars per 1,000 accounts created which are then sold to the spammers for around $30 to $40.

Image spam continues unabated

Image spam, blamed for the significant rise in spam activity in May, has become even more sustained during June, now accounting for between 8 and 10% of all spam intercepted. Attached to spam messages, rather than being hosted remotely and included using HTML images, some of these more recent examples include background noise patterns that have been generated automatically.

Figure 2: Image spam including background noise patterns

Almost certainly sent from a botnet, the emails often contain no hyperlinks. The spammers' website names are frequently included in the content of the images.

Instant Messenger threats rising

At the end of 2008, MessageLabs Intelligence research indicated that 1 in 200 (0.50%) hyperlinks shared over public instant messaging (IM) applications were identified as malicious, i.e. the website harbored some form of malware designed to perform a drive-by attack on a vulnerable web browser or browser plug-in. In June, the same research was conducted again and highlighted that the threat has increased. Approximately 1 in 405 (0.25%) IMs were found to contain a hyperlink of some form (excluding disclaimers and other legal requirements appropriate to some organizations), of which 1 in 78 (1.28%) were linked to websites that hosted malicious content; an increase of 0.78%. Based on these figures, MessageLabs Intelligence predicts that 1 in 80 IM users may expect to receive a malicious IM each month.

Investment in Healthcare IT

By August 17, 2009, the deadline imposed by the Health Information Technology for Economic and Clinical Health (HITECH) Act, the US Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) will synchronize their respective regulations and issue interim final regulations.The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 and imposes notification requirements in the event of security breaches related to protected health information (PHI).

As millions of government dollars are currently being invested in the digitization and protection of personal health records, medicine and technology are more intersected than ever. Organizations across the healthcare sector are feeling the pressure to comply with regulations such as the HITECH Act and rightfully so.

MessageLabs Intelligence has detected a growing need to safeguard against threats targeting the Healthcare sector. From the charts below, it can be seen that spam destined for the healthcare sector has risen in recent months and levels may be predicted to rise to 90 percent before the end of 2009. Email-borne malware attacks have more than doubled since the start of 2009.

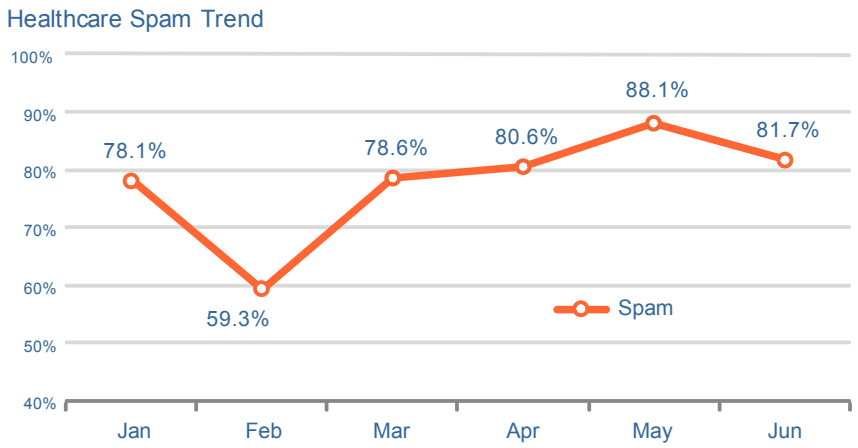


Figure 3: Healthcare Spam Trend

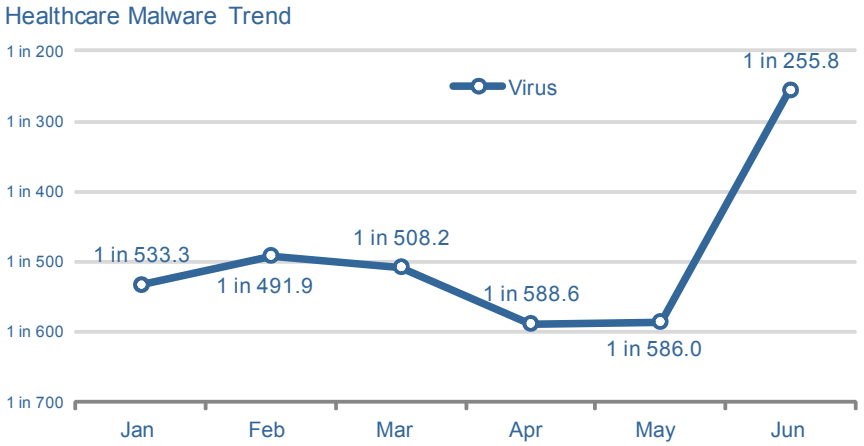
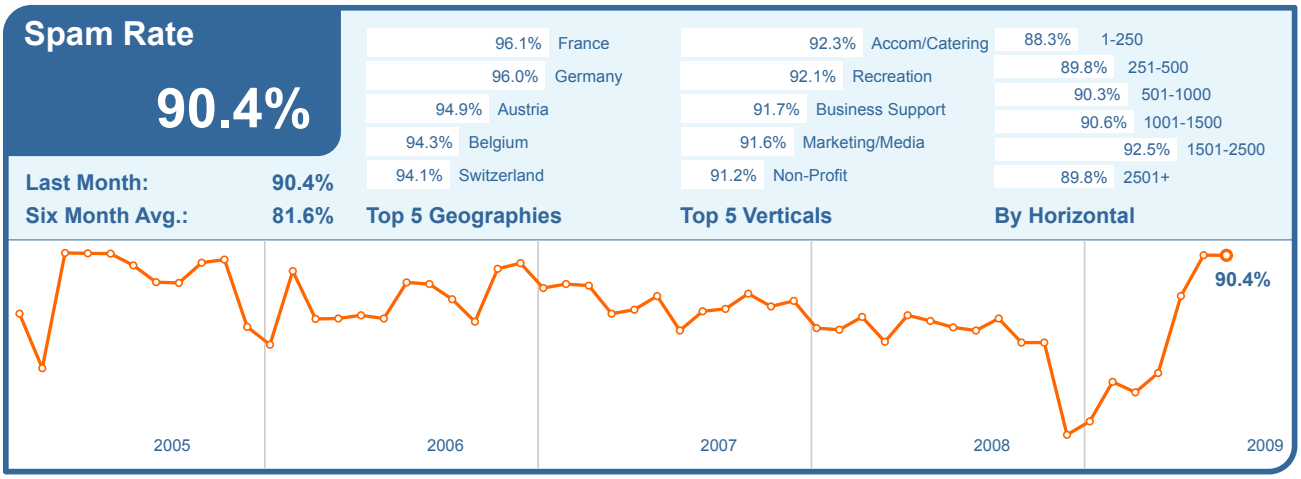


Figure 4: Healthcare Malware Trend

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 June 2009, the global ratio of spam in email traffic was unchanged from the previous month at 90.4% (1 in 1.1 emails).

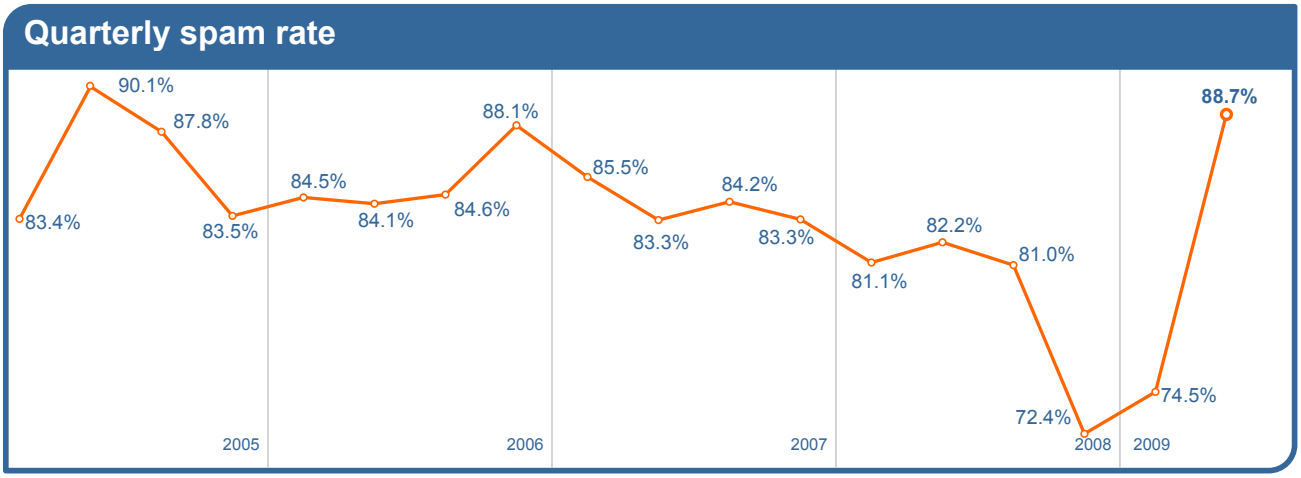


June 2009

Spam levels in France rose by 8.6% in June, positioning it as the most spammed country with levels of 96.1% of all email. Spam levels in the US declined to 78.4% and 72.2% in Canada, but increased to 90.3% in the UK. In Germany the spam rate reached 96.0% and 93.9% in the Netherlands. Spam levels in Australia decreased to 88.8% and 67.1% in Japan.

In June, the most spammed industry sector with a spam rate of 92.3% was the Accomodation and Catering sector. Spam levels reached 90.3% for the Education sector, and 88.6% for the Chemical & Pharmaceutical sector; 90.2% for Retail, 90.8% for Public Sector and 87.5% for Finance.

Quarterly Review: From the chart below it can be seen that spam levels for Q2 2009 averaged 88.7%, compared with 74.5% for Q1 2009.

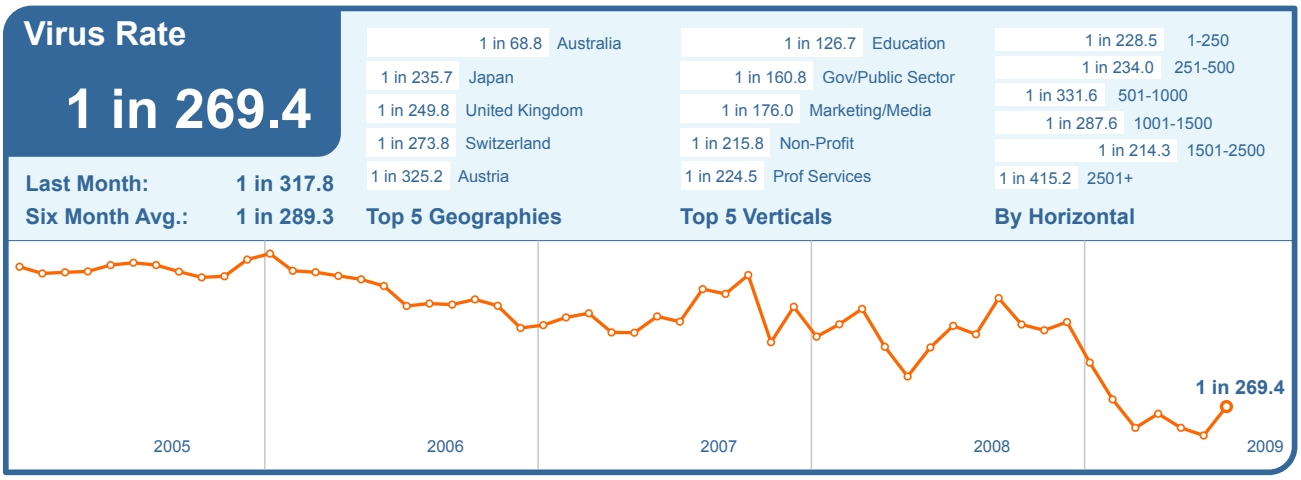


June 2009

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 269.4 emails (0.37%) in June, an increase of 0.06% since May.

This slight increase was owing in part to a burst of email-based malware attacks spoofing well-known, reputable international freight carriers, purporting to be a notification that a parcel delivery was unable to be made. The intention is to dupe a victim into opening a malicious attachment masquerading as an invoice for the non-existent parcel.

In June, 10.4% of email-borne malware contained links to malicious sites, an increase of 3.4% since May. Spoofed postcard mails were responsible for 66.5% of malicious links in June.

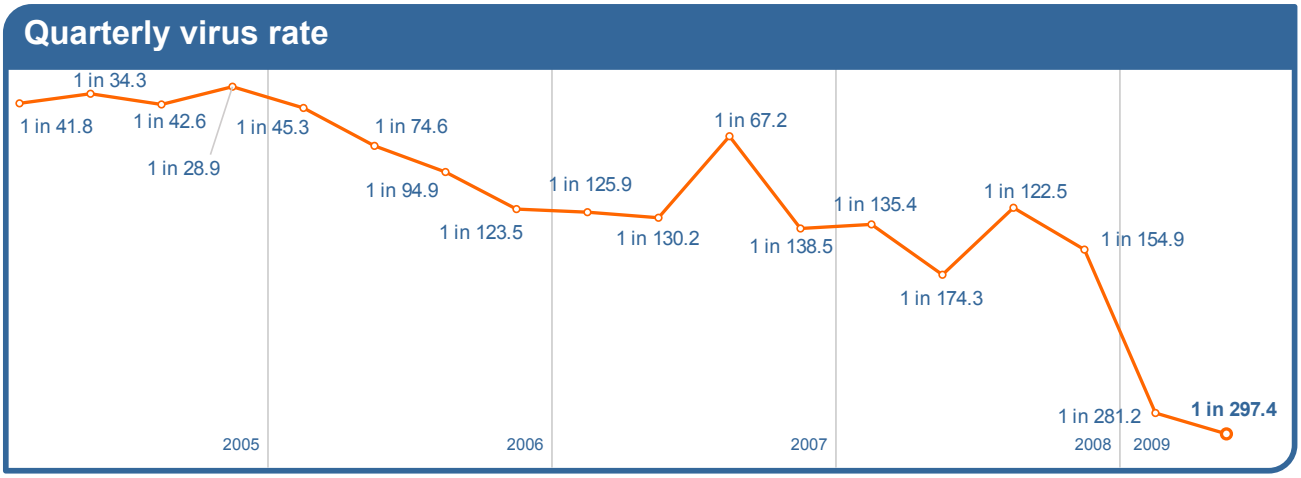


June 2009

Virus activity in Australia rose by 1.29% to 1 in 68.8 emails, placing it at the top of the table in June. Virus levels for the US were 1 in 371.7 and 1 in 423.7 for Canada. In Germany virus levels were 1 in 444.0 and for the Netherlands reached 1 in 644.5. In Hong Kong virus activity was 1 in 354.7 and in Japan it reached 1 in 235.7.

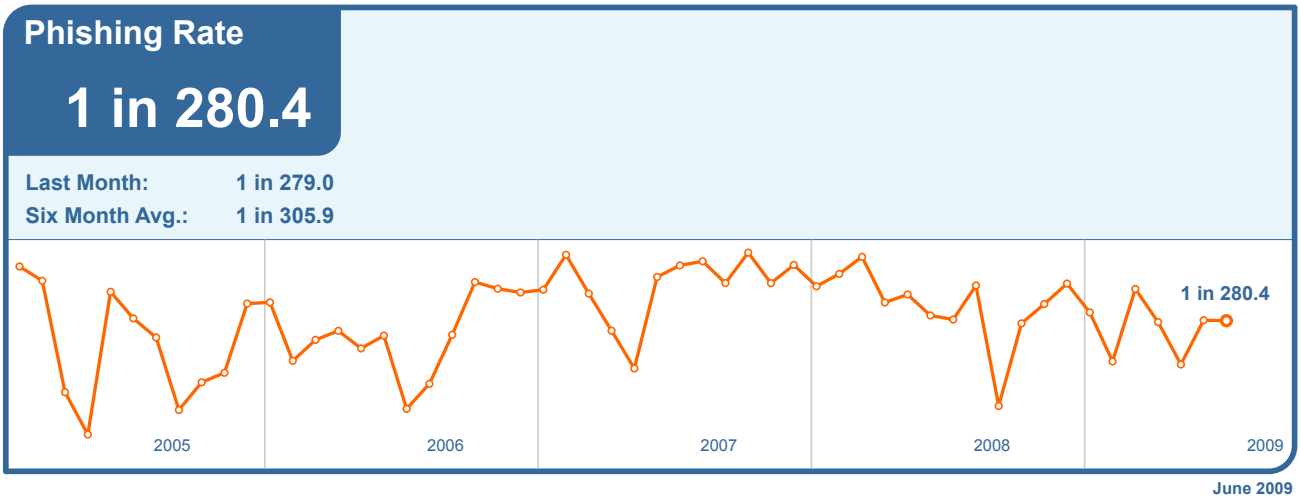
Virus activity in the Education sector fell by 0.10%, but retained its place at the top of the table with 1 in 126.7 emails being infected. Virus levels for the IT Services sector were 1 in 358.0, 1 in 493.6 for Retail and 1 in 259.1 for Finance.

Quarterly Review: From the chart below it can be seen that virus levels for Q2 2009 averaged 1 in 297.4 emails identified as malicious, compared with 1 in 281.2 in Q1 2009.



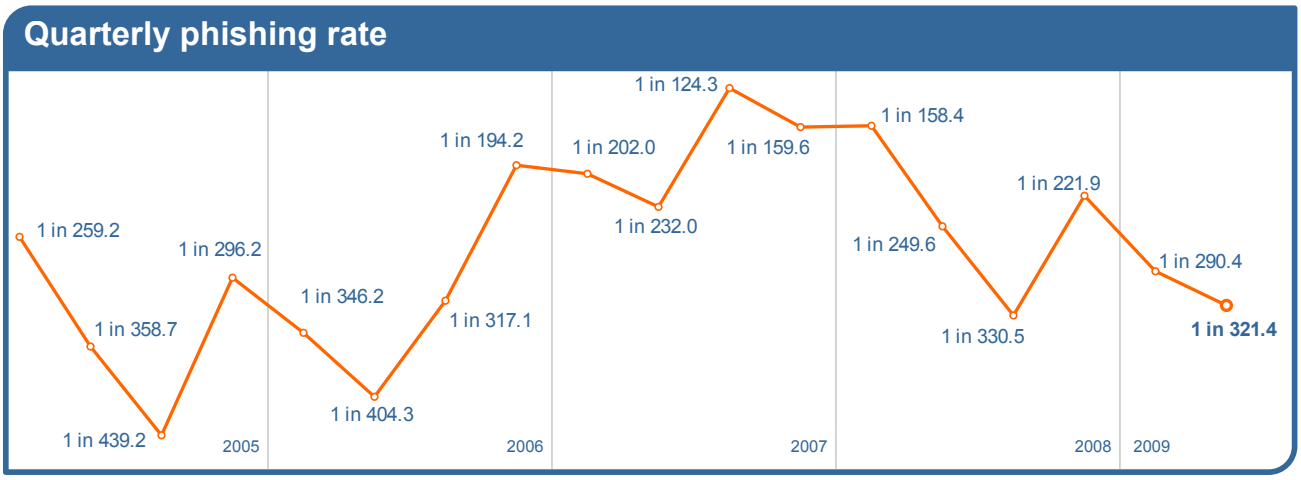
June 2009

Phishing: June saw almost no change in the level of phishing attacks compared with May. One in 280.4 (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 number of phishing emails had increased by 6.4% to 96.1% of all email-borne malware and phishing threats intercepted in June.



Phishing activity continues to come in waves, often focusing on financial institutions in a particular geography, before moving onto another target. More phishing activity can be linked to the increased availability of phishing kits and the use of compromised, legitimate domains used to host the phishing sites.

Quarterly Review: From the chart below it can be seen that phishing levels for Q2 2009 were 1 in 321.4, compared with 1 in 290.4 for Q1 2009.



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, up by 0.2% since May, to 61.6% in June.

Analysis of web security activity shows that 58.8% of all web-based malware intercepted was new in June, an increase of 24.6% since May. MessageLabs Intelligence also identified an average of 1,919 new sites per day harboring malware and other potentially unwanted programs such as spyware and adware; an increase of 67.0% since May.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	61.6%	Infostealer.Gampass	23.4%	PUP:WebToolbar.Win32.MyWebSea...	60.9%
Streaming Media	11.1%	Generic Dropper.eb	8.4%	PUP:SAHAgent	7.9%
Downloads	4.5%	Trojan-Downloader.JS.Gumblar.a	4.4%	PUP:WebToolbar.Win32.Zango.ca	4.0%
Games	3.7%	Trojan.Fakeavalert	3.7%	PUP:RemoteAdmin.Win32.WinVNC.1102	3.6%
Blogs & Forums	2.5%	Trojan Horse	2.6%	PUP:PSWTool.Win32.WinPassViewer.q	2.2%
Chat	2.0%	Trojan.JS.Agent.xz	2.3%	PUP:WebToolbar.Win32.Zango.cb	2.0%
Adult/Sexually Explicit	1.8%	Obfuscated Script.f	2.1%	PUP:NetTool.Win32.Portscan.c	1.8%
Peer-to-Peer	1.5%	Bloodhound.DirActCOM	2.1%	PUP:RemoteAdmin.Win32.WinVNC.c	1.0%
Computing & Internet	1.3%	Trojan.JS.Agent.ahc	1.7%	PUP:PSWTool.Win32.Messen.ct	1.0%
Personals & Dating	1.3%	Trojan-Downloader.JS.Iframe.aqu	1.6%	PUP:AdTool.Win32.MyWebSearch.br	1.0%

June 2009

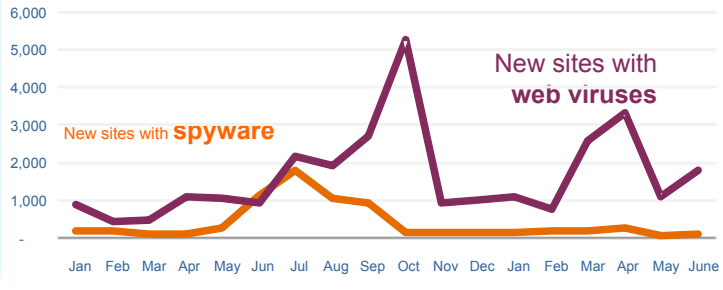
The "Unclassified" category (not listed above) identifies new and previously uncategorized sites, accounted for 0.6% of blocks in June. While these sites can be used for disreputable purposes, such as hosting phishing and spam sites, they may also be new sites and domains set up by legitimate organizations 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 June compared with the equivalent number of web-based malware sites blocked each day.

Web Security Services (Version 2.0) Activity:

New Malware Sites per Day

New sites with **spyware**	123/day
New sites with **web viruses**	1,796/day
Total	**1,919/day**

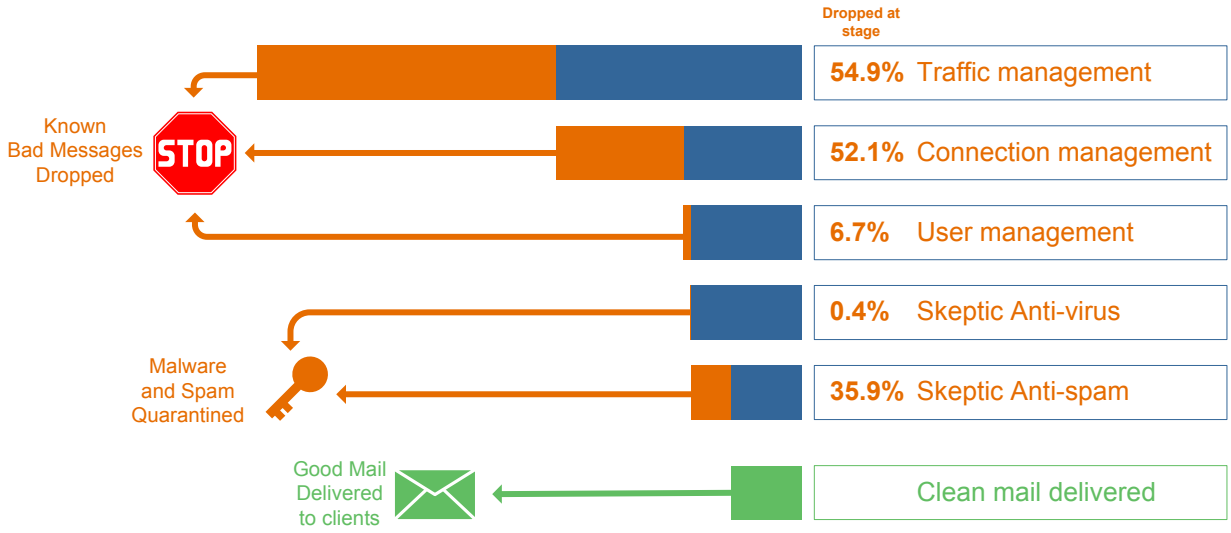


June 2009

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 June, MessageLabs services processed an average of 6.44 billion SMTP connections per day, of which 54.9% 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 June, an average of 52.1% 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 June, 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.