

MESSAGELABS INTELLIGENCE MARCH 2010

MessageLabs



The Nature of Cyber Espionage; Most Malicious File Types Identified and Encrypted Spam from Rustock

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

REPORT HIGHLIGHTS

- Spam – 90.7% in March (an increase of 1.4 percentage points since February)
- Viruses – One in 358.3 emails in March contained malware (a decrease of 0.05 percentage points since February)
- Phishing – One in 513.7 emails comprised a phishing attack (a decrease of 0.02 percentage points since February)
- Malicious websites – 1,919 websites blocked per day (a decrease of 61.6% since February)
- 39.9% of all malicious domains blocked were new in March (a decrease of 4.8 percentage points since February)
- 14.9% of all web-based malware blocked was new in March (an increase of 1.6 percentage points since February)
- The nature of industrial espionage and targeted attacks
- Understanding the most frequently targeted job roles in targeted attacks
- Death by a thousand cuts: Rustock botnet sends more encrypted spam

REPORT ANALYSIS

The nature of industrial espionage and targeted attacks

The ultimate aim of a targeted attack is to gain access to sensitive data or internal systems by targeting specific individuals or companies. They are sent in relatively small volumes compared with spam and phishing emails, for example, but are one of the most damaging email threats.

Any organization that possesses sensitive and valuable data can be an attractive target.

These messages are frequently business-related, or related to some newsworthy event, from a webmail account or with a spoofed 'From' address crafted to appeal to the target, and in some way gives the impression that the attachment contains important information, such as current affairs, meetings, legal documents, agreements or contracts.

The danger of targeted attacks is the stealth deployment of malicious code on the recipient's computer, often hidden within legitimate-looking documents such as .PDF, .DOC, .XLS and .PPT file types. The recipient only has to open the attachment and the computer is compromised.

MessageLabs Intelligence conducted an in-depth review of targeted malware in its 2009 Annual Security Report¹, which included analysis of the seniority of the recipients often targeted. In March 2010, we took a closer look at the origin of these types of messages to shed some light on the criminal operations behind them.

Figure 1 shows the source of targeted attacks based on the source IP address of the sending email server. Note that there are a high proportion of US-based addresses since many of these are webmail services hosted in the United States:

Country of Origin	Percentage of Targeted Attacks	Continent	Percentage of Targeted Attacks
United States	36.6%	N. America	36.8%
China	17.8%	Asia	32.8%
Romania	16.5%	Europe	30.3%
United Kingdom	10.7%	S. America	0.2%
Taiwan	10.0%		
Japan	3.2%		
Russian Federation	0.8%		
Cambodia	0.7%		
France	0.7%		
OTHER	3.0%		

Figure 1 – Source of targeted email attacks based on mail server location

Figure 2 below, is a visual representation of this same data, where the size of the plot is relative to the percentage of targeted malware sent from that location.

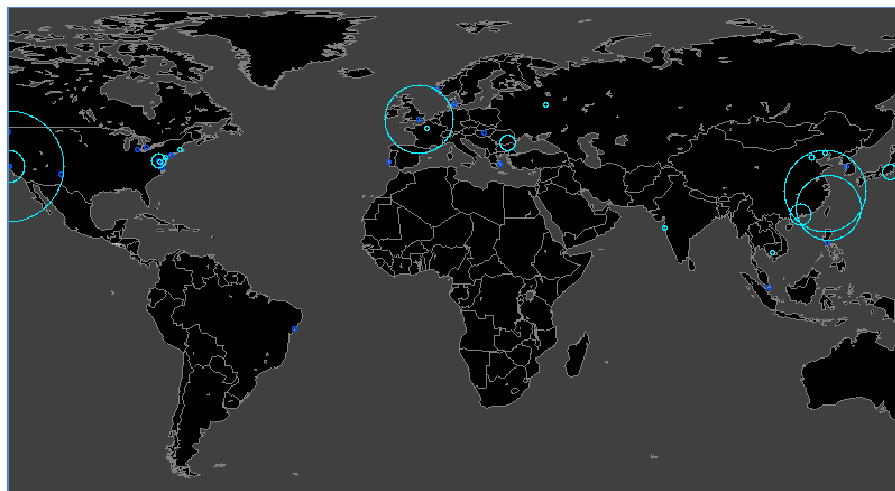


Figure 2 – Geographical plot of targeted email attack sources

¹ The report may be downloaded freely here: <http://www.message-labs.com/intelligence>

Since many webmail servers are located in the US, we then analyzed the headers of the messages and identified the true IP address of the sender. This provides the IP address of the computer that was used by the sender when the email was composed. A large proportion of targeted attacks are sent from legitimate webmail accounts, and therefore the IP address of the sending mail server is not a useful indicator of the true origin of the attack, as it will only identify the location of the email servers. Most webmail providers include the sender's IP address in the email headers, as can be seen in figure 3, below.

```

return-path: <[REDACTED]>
envelope-to: [REDACTED]
delivery-date: Thu, 18 Mar 2010 16:35:45 +0000
received:
from [REDACTED] for ([REDACTED]) by [REDACTED] with esmtp
+0000 ; Thu, 18 Mar 2010 16:35:43
from [REDACTED] for ([REDACTED]) by [REDACTED] with [REDACTED]
; Thu, 18 Mar 2010 09:35:40 -0700
message-id: <[REDACTED]>
content-type: multipart/alternative; boundary="_3dbb5e00-5357-49fb-a0c7-8c61a931f5f8_"
x-originating-ip: [REDACTED]
from: [REDACTED]
to: [REDACTED]
subject: [REDACTED] Foreign affairs policy - [REDACTED]
date: Thu, 18 Mar 2010 16:35:40 +0000
importance: Normal
mime-version: 1.0
x-originalarrivaltime: 18 Mar 2010 16:35:40.0094 (UTC) FILETIME=[0BB1EDE0:01CAC6B9]
    
```

Figure 3 – Example of email headers from legitimate webmail account

Different webmail providers include this IP address in a variety of ways that should be understood before extracting that information and identifying the country of origin. Unfortunately, one major webmail provider does not include this information at all, which makes it a favorite to use for some targeted attacks. This is perhaps deliberate so if the cyber criminals know, it will enable them to better cover their tracks.

Based on the analysis of the sender's IP address, rather than just the IP address of the email server, figure 4 shows the true source of many of these targeted attacks:

Country of Origin	Percentage of Targeted Attacks	Continent	Percentage of Targeted Attacks
China	28.2%	Asia	46.6%
Romania	21.1%	Europe	37.3%
United States	13.8%	N. America	13.8%
Taiwan	12.9%	Africa	2.4%
United Kingdom	12.0%		
Japan	4.0%		
Cameroon	2.2%		
Korea, Republic of	0.9%		
Russian Federation	0.9%		
OTHER	4.2%		

Figure 4 – Source of targeted email attacks based on sender location

Figure 5 below, is a visual representation of this data, where the size of the plot is relative to the percentage of targeted malware sent from that location, based on the location of the sender.

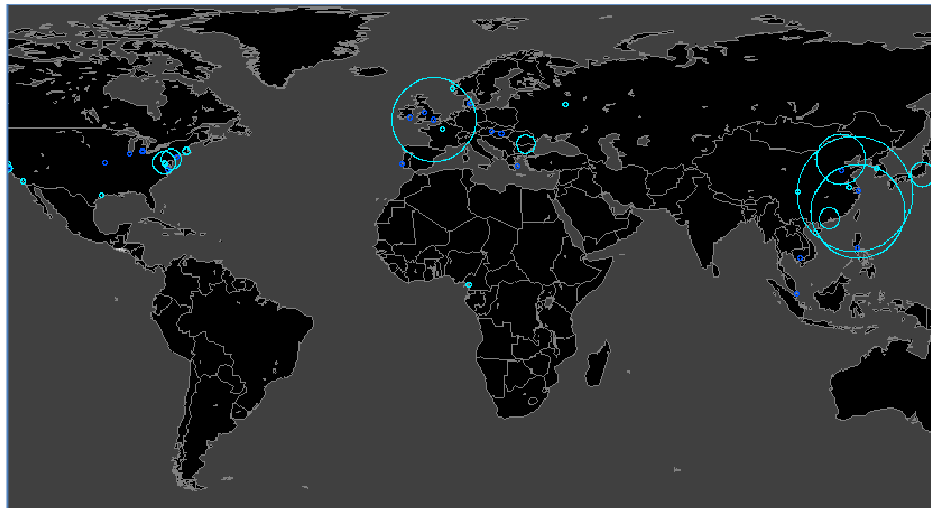


Figure 5 – Geographical plot of targeted attack sender locations

This closer analysis of the data reveals some interesting facts, notably; that more attacks originate from computers located in China, Romania and Cameroon than would first appear when looking solely at the mail server location alone. A comparison of the overall results from the first and second analysis is revealed in figure 6, below.

Continent	% of Attacks Based on Mail Server Location	% of Attacks Based on Sender Location	Difference
N. America	36.8%	13.8%	-23.0%
Europe	32.8%	37.3%	4.5%
Asia	30.3%	46.6%	16.3%
Africa		2.4%	
S. America	0.2%		

Figure 6 – Table showing variation between sender location and mail server locations

When considering the true location of the sender rather than the location of the email server, fewer attacks are actually sent from North America than it would at first seem.

More attacks are sent from addresses based in Europe, but a great deal more is actually sent from addresses in Asia. This shows that most of the attacks that seem to originate from webmail providers based in North America are actually being sent from other locations, including Asia, Europe and Africa.

When considering the mail server location, we find 17.8% come from China, but there seem to be a further 10.4% originating from China after further analysis of the sender location in webmail-based attacks (total 28.2% from China).

Similarly we find another 4.59% from Romania and 2.22% from Cameroon; these countries become more significant when analyzing the sender location, rather than considering the email server location alone.

The city of Shaoxing in China seems to be a major source, accounting for 21.3% of targeted attacks, as is Taipei (16.5%) in Taiwan, and London (14.8%) in the UK.

Understanding the most frequently targeted job roles in targeted attacks

Continuing the theme of targeted malware used in the commission of industrial espionage, bribery or blackmail and reflecting on the research in the MessageLabs Intelligence 2009 Annual Security Report, we reported that 60% of recipients were of a high or medium ranking seniority.

It was surprisingly straightforward to identify a great deal of information about the individuals being targeted; the Internet provided plenty of information on around 84% of the individuals in most targeted attacks. The top five most frequently targeted roles can be seen in figure 7.

Director	8.7%
Senior Official	7.3%
Vice President	4.4%
Manager	4.3%
Executive Director	2.9%

Figure 7 – the top five most frequently targeted job roles

Furthermore, the most frequently targeted individuals can be described in general terms in figure 8.

Expert: Asian Defense Policy	15.3%
Diplomatic Mission	15.2%
Expert: International Finance	7.9%
Asian Trade Policy	7.4%
Human Rights Activist	7.0%
Human Rights Researcher	5.7%
Academic	5.2%
Expert: Asian Foreign Policy	5.0%
European Musical Events Promoter	4.6%
European/Asian Trade Policy	4.1%
Expert: Asian Security	3.4%
Expert: Asian Economy	3.0%
Expert: Asian Policy	2.9%
Expert: International Relations	2.9%
Expert: Consumer Policy	2.9%
Executive: Asian Engineering Company	2.7%
Asian Banker	2.5%
Financial Analyst	2.4%

Figure 8 – the top five most frequently targeted individuals

Identifying the most common malicious file attachments in email-borne malware

When emails are passed through Skeptic™² they are automatically scrutinized and scored according to a variety of different factors. This score is tracked and recorded in the MessageLabs Intelligence data, from which we can analyze the results.

Based on the email file attachment data from March 2010, we collected the overall score of the email, including whether or not the file was encrypted. This analysis was focused on files and emails with files attached, and did not include emails that only contained hyperlinks or were without file attachments.

Starting with the most commonly seen file types, we ranked each file type by how frequently it was identified in malicious email traffic as a ratio of the total number of emails in which that file type appeared. This provided a measure of how likely a given file extension may be considered as more or less dangerous or malicious, when compared with other file types.

² For more information about Skeptic: <http://www.messagelabs.com/technology/skeptic>

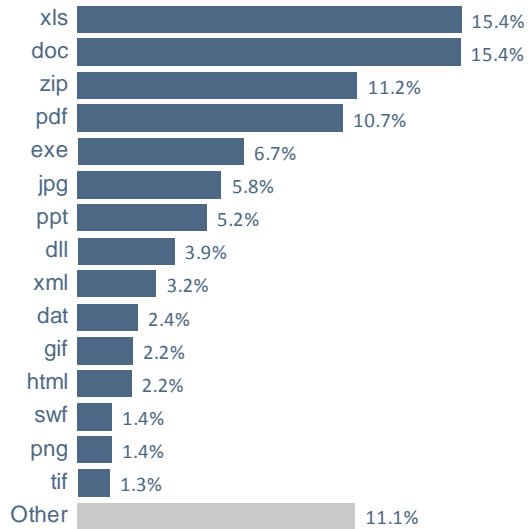


Figure 9 - most common file extensions seen in email traffic

As can be seen in figure 9, 15.4 % of files attached to emails in March were .XLS and .DOC file types, followed by 11.2% of attachments which were .ZIP files. The top four file types accounted for 50% of files attached to emails, and 17 file extensions accounted for 90% of files attached to emails.

It is worth noting that both .ZIP and .RAR file types could be unencrypted, or encrypted. There is more on this to follow, but first we identify the most compromised file attachment types, i.e. which files were blocked as malicious by Skeptic™. As seen in figure 9, the most compromised file extension identified was encrypted .RAR file types (a proprietary compressed archive format), which accounted for approximately 1 in 312 (0.32%) malicious files attached to emails. Although a relatively uncommon file type, it is compromised 96.8% of the time when attached to email.

Curiously, unencrypted .RAR files are rarely exploited and occur in 1.1% of mails. Therefore, they are more common than encrypted .RAR, but these are far less likely to be seen in a malicious email.

File type	% of files seen that are attached to malicious emails	% of files attached to emails
rar (encrypted)	96.8%	0.3%
sys	27.5%	0.3%
dll	22.5%	3.9%
tlb	19.2%	0.3%
bin	18.4%	0.9%
vbs	17.9%	0.2%
zip (encrypted)	17.5%	0.1%
exe	15.8%	6.7%
bat	13.0%	0.6%
com	12.4%	0.2%

Figure 9 - most dangerous email file attachments

A variety of other file extensions follow, but they are not compromised as often as encrypted .RAR files. For example, .ZIP files exhibit similar characteristics to .RAR files, where encrypted .ZIP files are much more likely to be attached to a malicious email, than plain .ZIP files.

The most commonly observed file extensions, including .XLS, .DOC, .ZIP and .PDF are least commonly exploited. Although there are a great number of malicious emails using these file types as attachments, there are far more that are not exploited.

Of course, .EXE is the main file extension that is expected to be most alarming when found attached to an email. Executable file types accounted for 6.6% of files attached to email in March, and 15% of the time they were found to be malicious.

Death by a thousand cuts - Rustock botnet sending more encrypted spam

In March, MessageLabs Intelligence observed that the Rustock botnet had been sending considerably more spam using TLS (Transport Layer Security). Approximately 77% of spam sent from the Rustock botnet used secure TLS connections, during March.

TLS is a popular way of sending email through an encrypted channel, rather than sending it in the clear like most emails are sent. MessageLabs Intelligence tracks the use of TLS to determine how much spam is sent over TLS, and which botnets are sending it. Not all mail servers force clients to use TLS, but it is frequently used for securing the communications channel between the client email sender and the email server to which the message is being delivered. It prevents eavesdropping of email traffic that would otherwise be sent in plain sight for anyone else on the network to see if they so wished, perhaps using network analysis tools.

However, TLS uses far more server resources and is much slower than a plain-text email; with TLS it takes time and resource to perform the necessary handshake where ciphers are negotiated and encryption keys exchanged and then to encrypt and decrypt the messages. There is a two-way conversation between the sending client computer and receiving email server, requiring both inbound and outbound traffic. In bandwidth terms, this outbound traffic frequently outweighs the size of the spam message itself and can significantly increase the workload being placed on corporate email servers.

With corporate email servers coming under more pressure to handle these expensive, but unnecessary TLS connections, it becomes a death by a thousand cuts – on its own the overhead of processing a single spam received with TLS may appear insignificant, but at large volumes, the overall impact can be enormous. The average additional inbound and outbound traffic due to TLS is an overhead of around one kilobyte. Many spam mails are often much lower than one kilobyte in size. Spam using TLS accounted for approximately 20 percent of all spam in March, peaking at approximately 35 percent of spam on March 10.

MessageLabs Boundary Encryption service allows clients to provide a secure and authenticated channel over which critical business email communications may be made. Furthermore, as the proportion of spam using TLS increases, the impact to MessageLabs clients will be zero, as the additional encryption overhead will be absorbed by the MessageLabs cloud infrastructure, and not by the client.

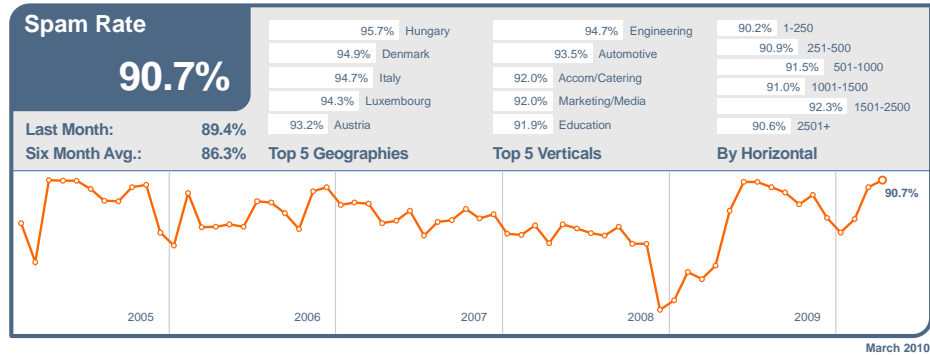
For more information on this growing trend, please read the full blog post at:

www.symantec.com/connect/blogs/death-thousand-cuts-rustock-botnet-sending-more-encrypted-spam.

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 March 2010, the global ratio of spam in email traffic increased by 1.5 percentage points since February to 90.7% (1 in 1.10 emails).

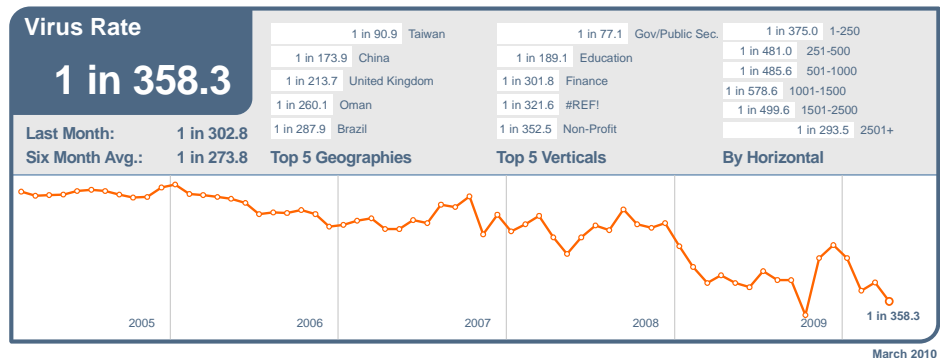


The spam level in Hungary rose to 95.7% of email traffic during March, making it the most spammed country. In the US, 91.1% of email was spam and 89.5% in Canada. The spam level in the UK was 90.1%. In The Netherlands, spam accounted for 93.0% of email traffic, 93.1% in Germany and 90.1% in Australia. In Hong Kong, 92.0% of email was blocked as spam and 88.3% in Singapore, compared with 87.5% in Japan and 92.4% in China.

In March, the most spammed industry sector with a spam rate of 94.7% was the Engineering sector. Spam levels for the Education sector reached 91.9% and 91.1% for the Chemical & Pharmaceutical sector; 91.6% for IT Services, 91.8% for Retail, 89.1% for Public Sector and 89.5% for Finance.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic was 1 in 358.3 emails (0.28%) in March, a decrease of 0.05 percentage points since February.

In March, 16.8% of email-borne malware contained links to malicious websites, a decrease of 13.7 percentage points since February.



In March, 1 in 90.9 emails destined for Taiwan was blocked as malicious, making the country the most targeted for email-borne malware. The virus levels for malware in email traffic in the US was 1 in 551.4 and 1 in 492.8 for Canada. In Germany virus activity reached 1 in 462.0

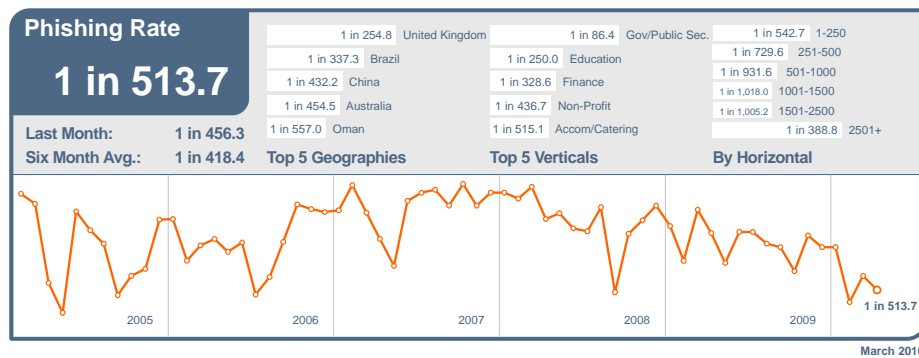
and in The Netherlands was 1 in 834.7. In Australia, 1 in 351.6 emails were malicious and 1 in 505.5 in Hong Kong; for Japan it was 1 in 1,063.3, compared with 1 in 504.1 in Singapore.

The Public Sector remained the most targeted industry in March, with 1 in 77.1 emails being blocked as malicious. Virus levels for the Chemical & Pharmaceutical sector were 1 in 642.9 and 1 in 510.9 for the IT Services sector; 1 in 728.6 for Retail, 1 in 189.1 for Education and 1 in 301.8 for Finance.

VIRUSNAME	Total
Trojan.Bredolab!eml	9.0%
Exploit/Fraud-AccUpdate	5.5%
Exploit/LinkAliasPostcard-2295	4.6%
W32/Prolaco-gen-4b33	4.1%
Trojan.Bredolab	3.5%
W32/NewMalware-Generic-e880-3269	3.4%
Exploit/MimeBoundary003	3.2%
Packed.Generic.265	3.2%
EML/Worm.MS.dam	2.6%
Trojan.Bredolab.dam	2.2%

Bredolab, a generic malware distribution botnet, accounted for 14.7% of all email-borne malware blocked in March. Bredolab has often been linked with other forms of malware and spyware, including fake security software and other botnet and identity fraud Trojans, such as Zeus, Waledac and Koobface. Bredolab is most frequently found in email-borne malware sent from the Cutwail botnet.

Phishing: In March, phishing activity decreased by 0.02 percentage points since February; 1 in 513.7 emails (0.19%) comprised some form of phishing attack. When judged as a proportion of all email-borne threats intercepted in March, including viruses and Trojans, the proportion of phishing emails rose by 8.4 percentage points to 64.6% of all email-borne malware and phishing threats combined.



The UK received the most phishing emails in March, with 1 in 254.8 emails comprising a phishing attack. Phishing levels for the US were 1 in 981.9 and 1 in 869.3 for Canada. In Germany phishing levels were 1 in 2,506 and 1 in 3,439 in The Netherlands. In Australia, phishing activity accounted for 1 in 454.5 emails and 1 in 3,569 in Hong Kong; for Japan it was 1 in 10,217 and 1 in 4,239 for Singapore.

The Public Sector continued at the top of the table with 1 in 86.4 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 1,403 and 1 in 1,386 for the IT Services sector; 1 in 1,160 for Retail, 1 in 250.0 for Education and 1 in 328.6 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 1.6 percentage points since February, to 52.8% in March.

The blocking of Unclassified websites increased by 0.82 percentage points, the largest rise in any category. The Unclassified category identifies new and previously uncategorized websites. While these websites 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. Customers are able to adopt a more flexible approach to how these websites are treated, since all content downloaded is scanned for malware by a unique combination of commercial anti-virus engines and Skeptic technology. This ensures that customers do not need to have a default block on these sites to maintain security, as may otherwise be the case.

Web Security Services (Version 2.0) Activity:

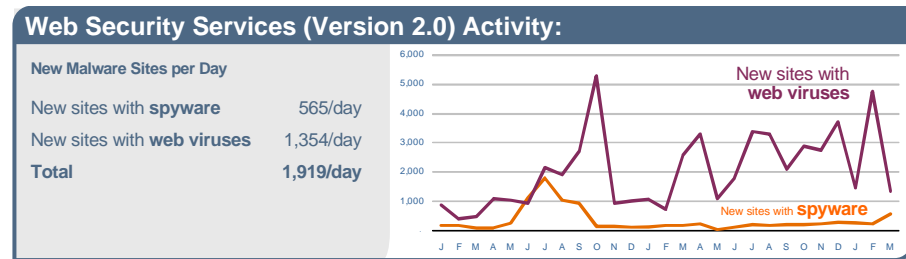
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	52.8%	Trojan-Downloader.JS.Gumblar.x	11.1%	PUP:NetTool.Win32.Proxy.g	79.8%
Streaming Media	9.5%	Trojan.ZbotIgen2	8.6%	PUP:WebToolbar.Win32.MyWebSea...	6.7%
Unclassified	4.4%	New Unclassified Trojan	6.4%	PUP:ZangoSearch	3.0%
Downloads	4.0%	Trojan.JS.Agent.bfy	4.7%	PUP:AdWare.Win32.Zwangi.ji	1.9%
Games	3.7%	Trojan-Downloader.JS.Gumblar.a	3.0%	PUP:AdWare.Win32.FunWeb.ar	1.4%
Search Engines	3.7%	Trojan-Clicker.JS.Iframe.ea	2.7%	PUP:AdWare.Win32.Zwangi.jo	0.9%
Personals & Dating	3.0%	Trojan.JS.Iframe.ik	2.5%	PUP:CWSIEFeats	0.5%
Blogs & Forums	2.7%	Trojan-Clicker.JS.Agent.ma	2.3%	PUP:NetTool.Win32.ProxySwitcher.d	0.4%
Computing & Internet	2.4%	New Unclassified Worm	2.1%	PUP:AdWare.Win32.Zwangi.m	0.3%
Adult/Sexually Explicit	2.1%	Exploit/Phishing-hmrc-ee11	2.1%	PUP:RiskTool.Win32.MBRFix.a	0.2%
Chat	1.9%				

March 2010

MessageLabs Intelligence identified an average of 1,919 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 61.6% since February, when the number of blocked malicious websites surged by 184%, but an increase of 9% since January.

Further analysis also reveals that 39.9% of all malicious domains blocked were new in March; a decrease of 4.8 percentage points since February. Additionally, 14.9% of all web-based malware blocked was new in March; an increase of 1.6 percentage points since the previous month.

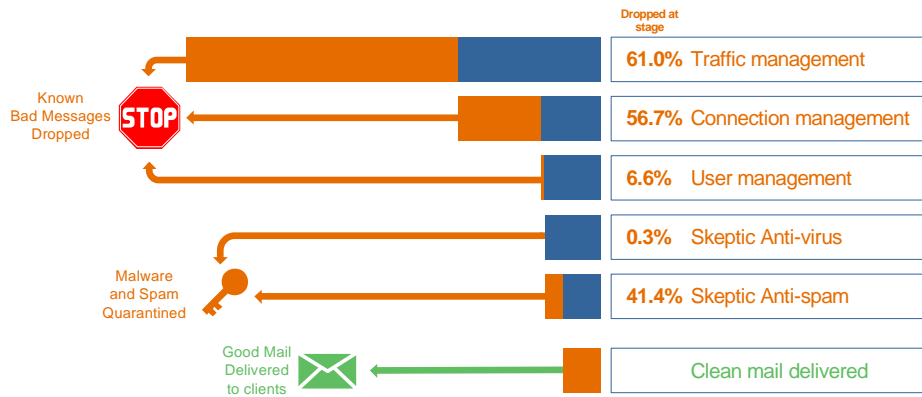
The chart below shows the increase in the number of new spyware and adware websites blocked each day on average during March compared with the equivalent number of web-based malware websites blocked each day.



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 March, MessageLabs services processed an average of 12.3 billion SMTP connections per day, of which 61.0% 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 March, an average of 56.7% 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 March, an average of 6.6% 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 30,000 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.

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.