March 2011 Intelligence Report

Global Spam Drops by One Third as Rustock Botnet is Dismantled; MessageLabs Intelligence's First Review of Spam-sending Botnets in 2011

Welcome to the March edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for March 2011 to keep you informed regarding the ongoing fight against viruses, spam, spyware and other unwelcome content.

Report highlights

- Spam – 79.3% in March (a decrease of 2.0 percentage points since February 2011)
- Viruses – One in 208.9 emails in March contained malware (an increase of 0.13 percentage points since February 2011)
- Phishing – One in 252.5 emails comprised a phishing attack (a decrease of 0.07 percentage points since February 2011)
- Malicious websites – 2,973 web sites blocked per day (a decrease of 27.5% since February 2011)
- 37.0% of all malicious domains blocked were new in March (a decrease of 1.9 percentage points since February 2011)
- 24.5% of all web-based malware blocked was new in March (an increase of 4.2 percentage points since February 2011)
- Global spam volumes drop by one third, as Rustock botnet is dismantled
- First review of spam-sending botnets in 2011 identified Bagle as most active botnet as Rustock fell silent

Report analysis

Global Spam Drops as Rustock Botnet is Dismantled

On March 16, MessageLabs Intelligence posted a blog[1] reporting a drop in spam from the Rustock botnet that was consistent with reports from other organizations tracking spam output. The output fell dramatically and almost instantaneously, suggesting that the botnet was no longer sending any spam and that it had either been taken down or had entered a self-imposed exile, as it did in December 2010 as reported in the January 2011 MessageLabs Intelligence Report. It remains to be seen whether the criminals behind Rustock will be able to recover from this coordinated effort against what has become one of the most technically sophisticated botnets in recent years. Rustock has been a significant part of the botnet and malware landscape since January 2006, much longer than many of its contemporaries.

When the story initially broke on the KrebsonSecurity[2] blog, the reasons for the outage were unclear. The *Wall Street Journal*[3] later reported that Rustock had indeed been disrupted due to action against command and control hosts used by the Rustock botnet. The legal action was led by Microsoft, and involved a number of organizations including Pfizer, FireEye and others.

Reviewing the data in the days that followed, MessageLabs Intelligence identified that global spam volumes fell by 33.6% between March 15 and 17, comprising a sharp drop of 24.7% in global spam volumes between March 15 and 16, and a subsequent drop of 11.9% between March 16 and 17 as can be seen in figure 1, below.

[1] *http://www.symantec.com/connect/blogs/has-rustock-botnet-ceased-spamming*
[2] *http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/*
[3] *http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html*

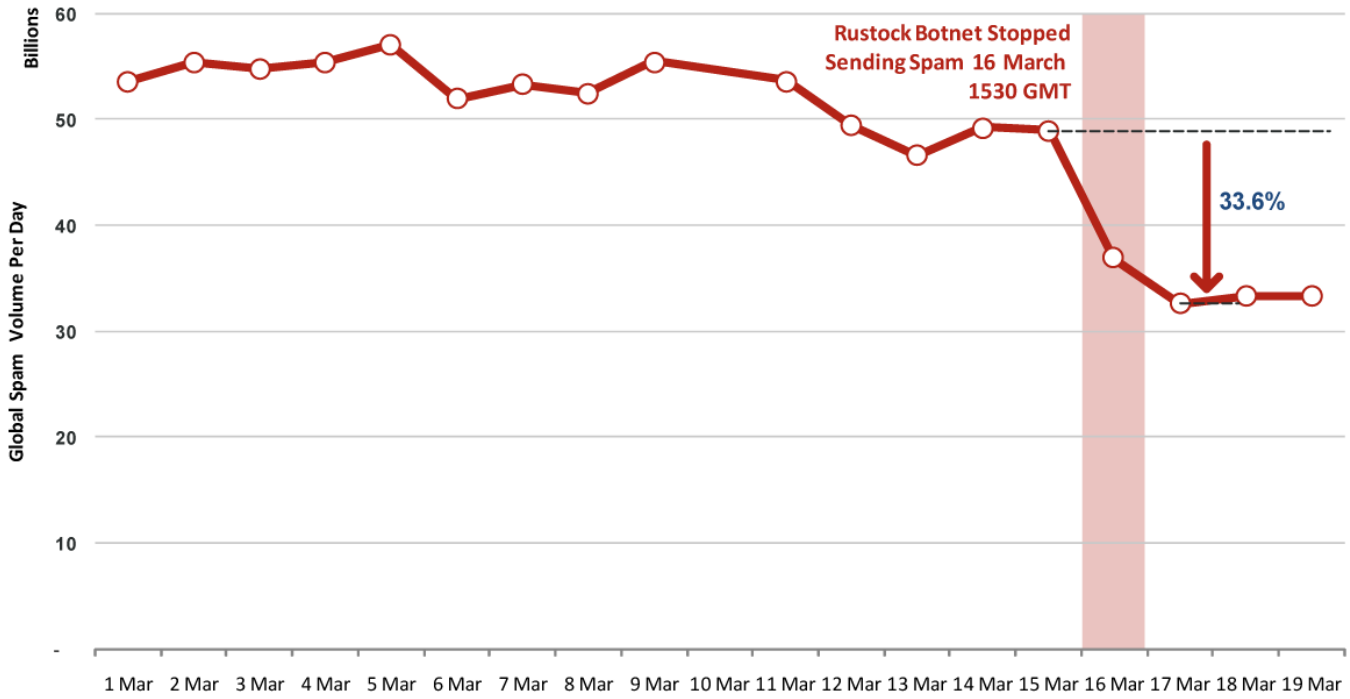


Figure 1 – Chart showing global daily spam volumes (billions per day)

In the days following the botnet takedown on March 16, spam accounted for approximately 33 billion emails per day, compared with an average of 52 billion per day in the previous week (commencing March 7).

A Review of Spam-sending Botnets in 2011

In March, 83.1% of global spam was sent from botnets, as shown in figure 2, below. This represents an increase of 6.1 percentage points compared with 77% at the end of 2010. On average during 2010, 88.2% of spam was sent from botnets. Botnets have been and remain a destructive resource for cyber criminals and through the years have become the spammers' air-supply, without which it would be very difficult for them to operate. In addition to anonymous spam-sending, many botnets can be used for a number of other purposes, such as launching distributed denial of service attacks, hosting illegal web site content on infected computers (known as bots), harvesting personal data from them and installing spyware to track the activities of their users.

In March, prior to its takedown, Rustock had been sending as much as 13.82 billion spam emails daily, accounting for an average of 28.5% of global spam sent from all botnets in March, as shown in figure 3. It is therefore no surprise that global spam volumes fell by approximately one third after the botnet ceased sending spam. By the end of 2010, Rustock had been responsible for as much as 47.5% of all spam, sending approximately 44.1 billion spam emails each day.

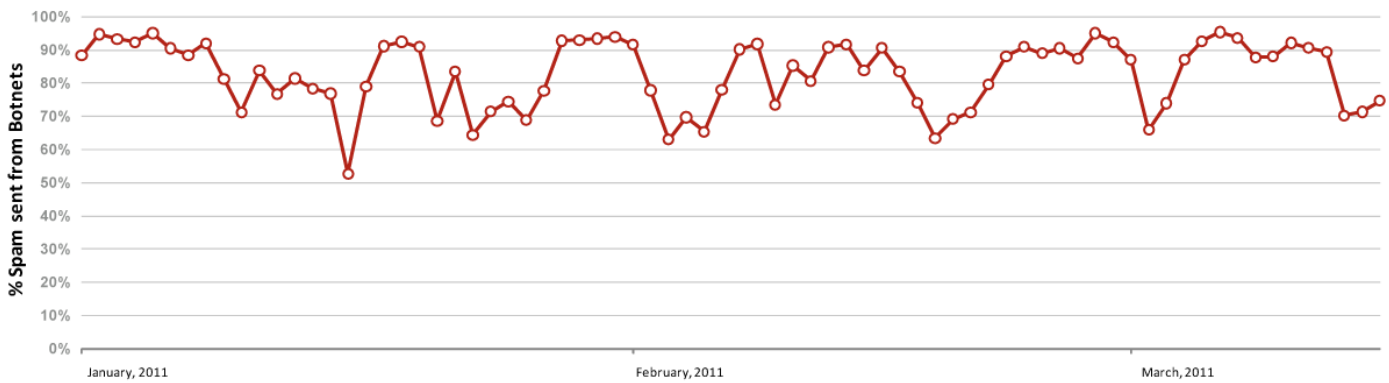


Figure 2 – Proportion of spam sent from botnets in 2011

In the wake of the notable Rustock takedown, other botnets have stepped up their activities to take advantage of the gap in the market that will likely be filled before long. MessageLabs Intelligence analyzed the spam traffic from the top ten major spam-sending botnets in March, including Rustock prior to the disruption of its activities reported above.

Botnet Name	% of Spam	Spam per Day	Spam per Bot per Minute	Estimated Botnet Size	Geographical Distribution
Rustock	28.5%	13.82 billion	117	470,000 to 690,000	USA (11%), India (9%), Russia (6%)
Bagle	17.2%	8.31 billion	176	180,000 to 280,000	Russia (22%), India (8%), Columbia (7%)
Festi	8.7%	4.20 billion	77	210,000 to 320,000	India (12%), Vietnam (11%), Indonesia (10%)
Cutwail	4.5%	2.17 billion	33	250,000 to 380,000	Indonesia (12%), India (11%), Vietnam (8%)
Lethic	4.1%	1.98 billion	43	180,000 to 270,000	Russia (12%), India (9%), Ukraine (5%)
Grum	3.4%	1.64 billion	111	56,000 to 84,000	Brazil (15%), India (11%), Russia (8%)
Xarvester	2.8%	1.36 billion	125	43,000 to 65,000	Spain (16%), UK (11%), France (10%)
Maazben	2.5%	1.20 billion	15	300,000 to 450,000	Brazil (18%), Russia (15%), India (8%)
Donbot	0.3%	149.58 million	148	4,000 to 6,000	Columbia (11%), India (10%), Italy (10%)
Gheg	0.1%	43.33 million	19	9,000 to 13,000	Indonesia (20%), Argentina (16%), India (13%)
Other, smaller Botnets	1.5%	47.44 million	11	250,000 to 380,000	-
Un-classified Botnets	9.6%	4.67 billion	69	270,000 to 400,000	-
Total Botnet Spam	**83.1%**	**39.61** billion	**79**	**2.22 million to 3.34 million**	**-**

Figure 3 – Table showing top spam-sending botnets in March 2011

Since the end of 2010, the Bagle botnet has been more active, sending approximately 8.31 billion spam emails each day, the majority of which linked to pharmaceutical products. While Bagle may not have as many bots under its control or have spikes of traffic as large and dominating as Rustock, its output has been more consistent. In the wake of Rustock's demise, Bagle has already taken over from Rustock as the most active spam-sending botnet in 2011.

In March, spam output from Bagle has been at its highest since 2009, when at its previous peak in October of that year it accounted for approximately 12.2% of global spam. Notably, Bagle did not appear in the top ten spam-sending botnets at the end of 2010, as reported in the MessageLabs Intelligence 2010 Annual Security Report.

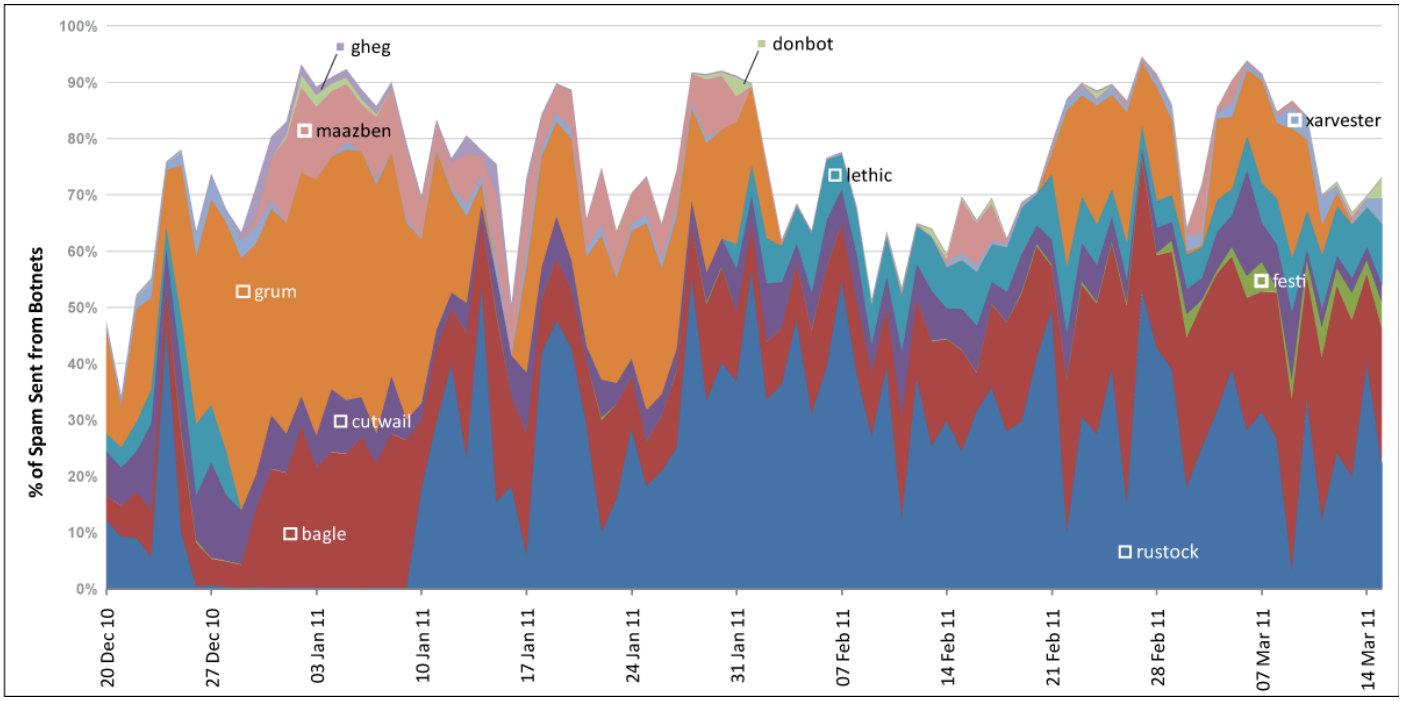


Figure 4 – Chart showing top spam-sending botnets in 2011

Analysis of the top countries of origin for spam-sending botnets is shown in figure 5. The Russian Federation is now the most frequent source of spam in March; perhaps in large part given that there are a large number of bots for Bagle, Lethic and Maazben located in this geography.

Country	% of Spam
Russian Federation	12.4%
India	8.8%
Brazil	5.9%
United States	4.5%
Ukraine	4.4%
Colombia	3.9%
Romania	3.8%
Argentina	2.8%
Vietnam	2.5%
Korea, Republic of	2.5%

Figure 5 – Table showing geographic sources for spam in March 2011

For the first time in over a year, the top ten spam-sending geographies did not include any countries from Europe.

Despite several takedown attempts in 2010, Cutwail remains among the top ten most active spam-sending botnets in March 2011. Additionally, the Mega-D botnet does not appear in the latest analysis; at the end of 2010 it accounted for as much as 2.3% of all botnet spam, but in March accounted for less than 0.1% of all botnet spam.

Finally, MessageLabs Intelligence identified an increase in spam containing a ZIP file archive attachment, as shown in figure 6, below. The increase was higher in February than in March, but in both cases it has been at its highest level this year. In 2010, it was much less common to see spam with files attached, and since June 2010 there have been approximately 3% of spam with file attachments of any type, with a peak of 11% for one day in September.

The larger file size associated with sending attachments in spam emails reduces the number of emails that the spammers are able to send and for this reason, compressed files, such as ZIPs are a way that spammers can reduce the file size of any attachment.

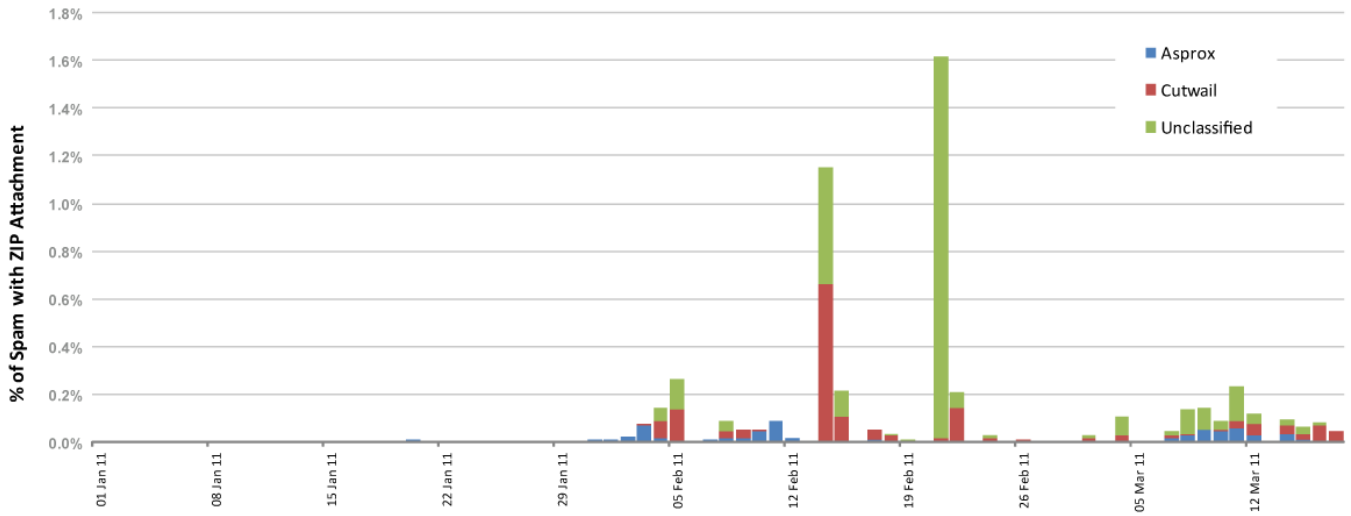


Figure 6 – Chart showing trend of spam comprising a ZIP archive file attachment

These latest spam emails were identified as originating from the Asprox, Cutwail and un-classified botnets. Un-classified botnets are either variants of existing botnets or wholly new botnets that are yet to be identified.

Blog: 419 Scammers Taking Advantage of Egypt's Revolution

When 419 scams started up, it had only been a few days since the resignation of Egypt's long-standing president, Hosni Mubarak, who resigned after intense political pressure following days of widespread protest across the country. As we've seen in the past, 419 or advance-fee fraud scammers (who typically promise large amounts of money, but demand up-front fees or payments first) were as quick to react to current events as they were in the aftermath of Haiti's devastating earthquake in January 2010, when 419 scammers impersonated the Red Cross, requesting donations. In this case, it was a 419 email written in German, claiming to be from the former Egyptian president's lawyer requesting the recipient's help to retrieve $2.5m of the president's funds, frozen in a Belgian bank account.

For more information, please visit the MessageLabs Intelligence blog at:
http://www.symantec.com/connect/blogs/419-scammers-taking-advantage-egypts-revolution

Blog: 419 Spammers Taking Advantage of Libyan Unrest

Similarly demonstrating how adept they were at using current events to their advantage, 419 scammers also sought to take advantage of the ongoing unrest in Libya. The email claimed to be written by someone connected to Libya's Senussi crown (overthrown by Muammar al-Gaddafi in his 1969 coup d'état), seeking assistance in transferring his money out of the country.

For more information, please visit the MessageLabs Intelligence blog at:
http://www.symantec.com/connect/blogs/419-spammers-taking-advantage-libyan-unrest

Blog: Spammers taking advantage of IDN with URL shortening services

Internationalized Domain Names (IDN) allow domain names to include Arabic, Chinese, Russian, Latin (with diacritics) and many other characters, like *寿司* and *한글*. It has been possible to include these characters in some domains for several years, but until last year, top-level domains (like *.ru* for Russia) were not internationalized like this. Several top-level domains now have internationalized versions, for example *.рф* for Russia.

MessageLabs Intelligence recently tracked a number of pharmacy spam emails (targeted at Germany, Austria and Switzerland), promoting erectile dysfunction medication. These spam emails included links to a popular URL shortening site which in turn redirected to a web site hosted under an IDN domain, which in turn redirects to the spammers' real web site.

For more information, please visit the MessageLabs Intelligence blog at:
http://www.symantec.com/connect/blogs/spammers-taking-advantage-idn-url-shortening-services

Blog: Welsh Language 419 Scam - No Language Is Safe!

For the first time, MessageLabs Intelligence tracked an otherwise atypical 419 scam email which was different only in that the email was written in Welsh. While we have seen 419 scam mails constructed in many different languages such as German and French, for example, this was the first time we had found one written in Welsh. Given that it would be unlikely that the 419 scammer can read and write Welsh fluently, it's more likely that the mail was translated from English using an automated language translation web site.

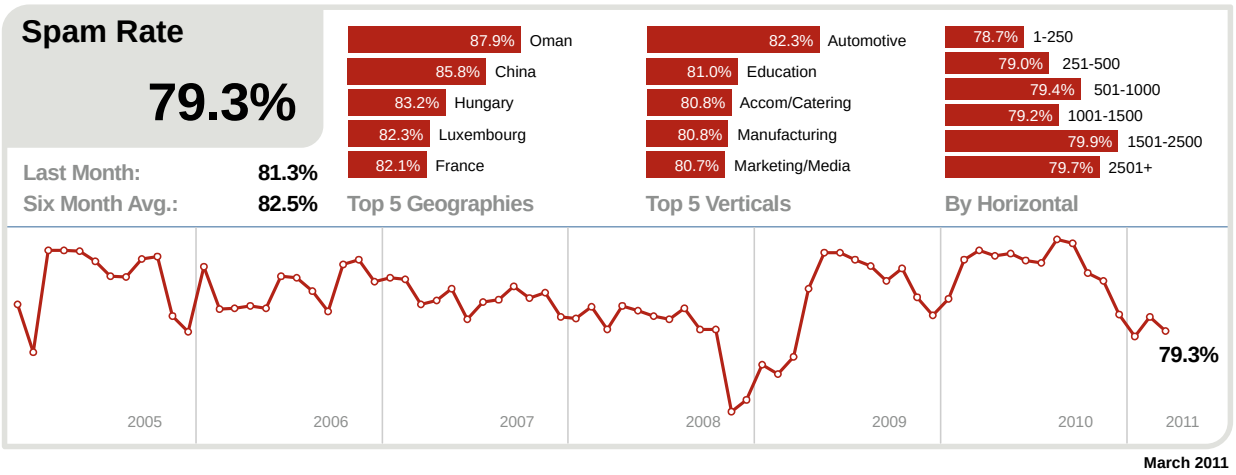
Further analysis revealed that the recipient in this case was actually based in Wales and that the names of the individuals mentioned in the email had also been tailored to match the name of the recipient; which may have been a tactic designed to catch the recipient off guard.

For more information, please visit the MessageLabs Intelligence blog at:
http://www.symantec.com/connect/blogs/welsh-language-419-scam-no-language-safe

Global Trends & Content Analysis

Symantec.cloud is focused on identifying, detecting and averting unwanted Internet threats such as viruses, spam, spyware and other inappropriate content. The intelligence collected from the billions of messages and millions of threats processed each day forms one of the most comprehensive and up-to-date knowledge bases of Internet threats in the world.

Symantec MessageLabs Email AntiSpam.cloud: In March 2011, the global ratio of spam in email traffic decreased by 2.0% percentage points since February 2011 to 79.3% (1 in 1.26 emails).



March 2011

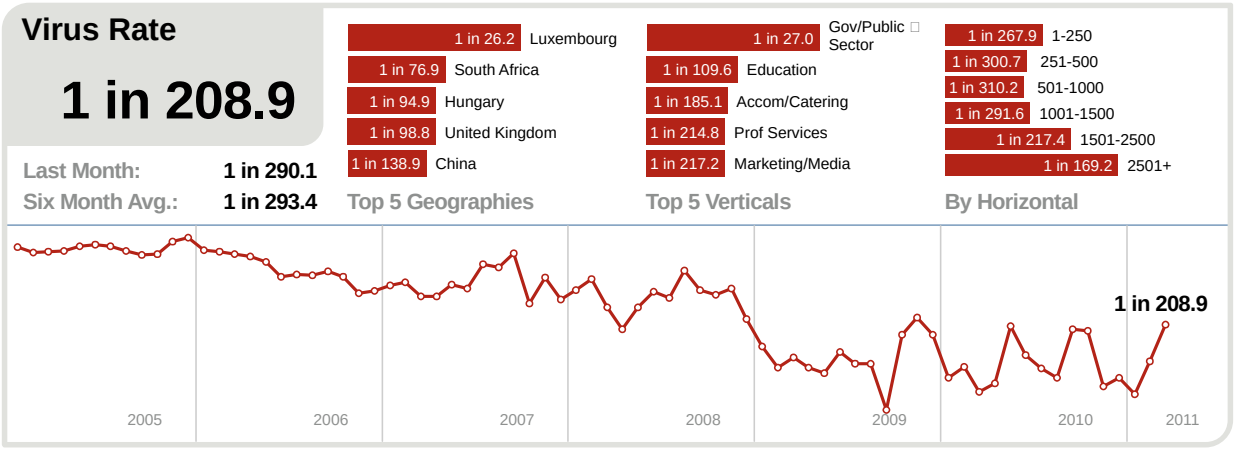
As the overall spam level decreased in March 2011, Oman became the most spammed geography, with a spam rate of 87.9%.

In the US, 79.6% of email was spam and 79.4% in Canada. The spam level in the UK was 79.1%. In The Netherlands, spam accounted for 80.2% of email traffic, 80.0% in Germany, 78.9% in Denmark and 78.8% in Australia. In Hong Kong, 80.6% of email was blocked as spam and 77.7% in Singapore, compared with 76.4% in Japan. Spam accounted for 79.5% of email traffic in South Africa.

In March, the Automotive industry remained the most spammed sector, with a spam rate of 82.3%. Spam levels for the Education sector reached 81.0% and 79.6% for the Chemical & Pharmaceutical sector; 79.8% for IT Services, 78.8% for Retail, 78.1% for Public Sector and 78.0% for Finance.

Symantec MessageLabs Email AntiVirus.cloud: The global ratio of email-borne viruses in email traffic was 1 in 208.9 emails (0.479%) in March, an increase of 0.134 percentage points since February 2011.

In March, 63.4% of email-borne malware contained links to malicious websites, a decrease of 0.1 percentage points since February 2011.



March 2011

Luxembourg became the most targeted geography as 1 in 26.2 emails were blocked as malicious in March. The sharp increase was a result of a large number of variants of Bredolab, Zeus and SpyEye malware, which was observed in a number of other countries, including South Africa.

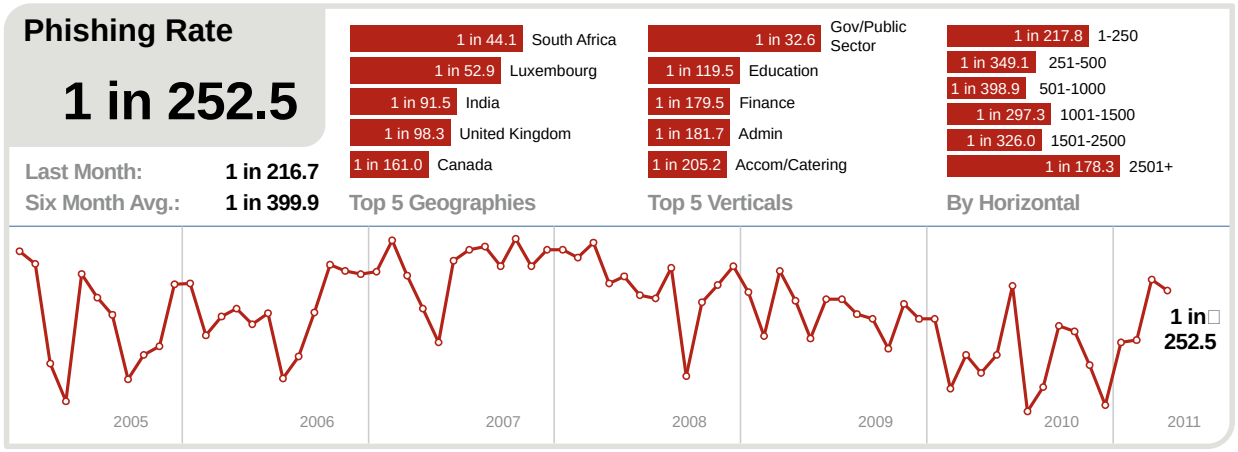
In the UK, 1 in 98.8 emails contained malware. In the US, virus levels for email-borne malware were 1 in 507.9 and 1 in 160.1 for Canada. In Germany virus activity reached 1 in 352.7, 1 in 916.8 in Denmark and in The Netherlands 1 in 467.1. In Australia, 1 in 261.0 emails were malicious and 1 in 357.3 in Hong Kong; for Japan it was 1 in 1,015, compared with 1 in 823.8 in Singapore. In South Africa, 1 in 76.9 emails contained malicious content.

With 1 in 27.0 emails being blocked as malicious, the Public Sector remained the most targeted industry in March. Virus levels for the Chemical & Pharmaceutical sector were 1 in 302.2 and 1 in 326.5 for the IT Services sector; 1 in 397.0 for Retail, 1 in 109.6 for Education and 1 in 318.9 for Finance.

The table below shows the most frequently blocked email-borne malware for March, many of which take advantage of malicious hyperlinks. In March, 35.3% of email-borne malware was associated with Bredolab, SpyEye and Zeus variants, a trend initially reported in the MessageLabs Intelligence Report for February 2011.

Malware	% Malware
Trojan.Bredolab!eml	24.0%
Exploit/SuspLink-7d87	17.1%
W32/Bredolab.gen!eml-19251	4.8%
Trojan.Bredolab	1.9%
Exploit/SuspLink.dam	1.8%
Exploit/SuspLink-6c7b	1.6%
W32/Bredolab.gen!eml	1.5%
W32/Bredolab!gen-ad91	1.4%
Exploit/LinkAliasPostcard-b354	0.8%
W32/Delf-Generic-ad9e	0.7%

Phishing Analysis: In March, phishing activity decreased by 0.065 percentage points since February 2011; 1 in 252.5 emails (0.396%) comprised some form of phishing attack



March 2011

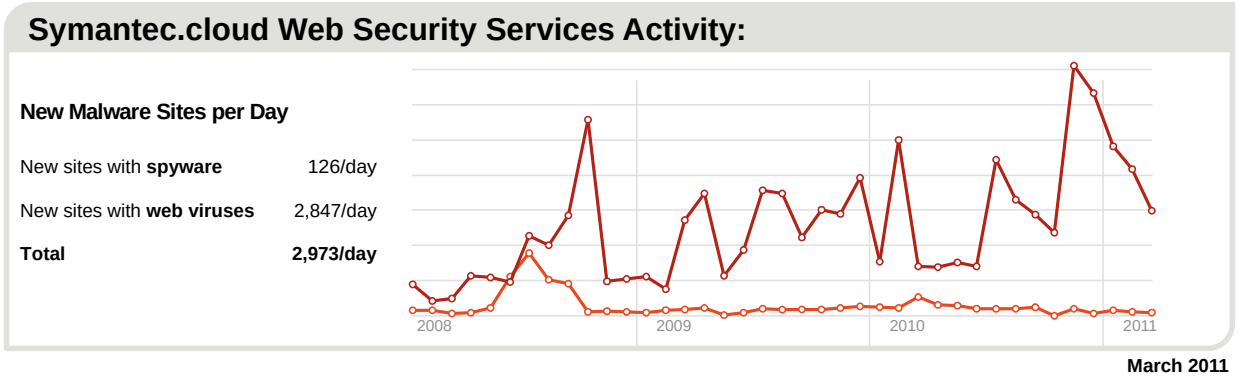
South Africa once again was the most targeted geography for phishing emails in March, with 1 in 44.1 emails identified as phishing attacks. South Africa suffers from a high level of phishing activity targeting many of its four major national banks, as well as other international financial institutions.

In the UK, phishing accounted for 1 in 98.3 emails. Phishing levels for the US were 1 in 535.5 and 1 in 161.0 for Canada. In Germany phishing levels were 1 in 549.6, 1 in 1,259 in Denmark and 1 in 585.7 in The Netherlands. In Australia, phishing activity accounted for 1 in 387.9 emails and 1 in 418.9 in Hong Kong; for Japan it was 1 in 1,724 and 1 in 1,033 for Singapore.

The Public Sector remained the most targeted by phishing activity in March, with 1 in 32.6 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 355.9 and 1 in 404.4 for the IT Services sector; 1 in 446.3 for Retail, 1 in 119.5 for Education and 1 in 179.5 for Finance.

Symantec MessageLabs Web Security.cloud: In March, MessageLabs Intelligence identified an average of 2,973 web sites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 27.5% since February 2011. This reflects the rate at which web sites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when web-based malware has been in circulation for longer to widen its potential spread and increase its longevity.

As detection for web-based malware increases, the number of new web sites blocked decreases and the proportion of new malware begins to rise, but initially on fewer web sites. Further analysis reveals that 37.0% of all malicious domains blocked were new in March; a decrease of 1.9 percentage points compared with February 2011. Additionally, 24.5% of all web-based malware blocked was new in March; an increase of 4.2 percentage points since the previous month.



March 2011

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

The most common trigger for policy-based filtering applied by Symantec MessageLabs Web Security.cloud for its business clients was for the “Advertisements & Popups” category, which accounted for 47.5% of blocked web activity in March. The second most frequently blocked traffic was categorized as Social Networking, and accounted for 14.0% of URL-based filtering activity blocked, equivalent to one in seven web sites blocked.

Many organizations allow access to social networking web sites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Symantec.cloud Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	47.5%	Exploit/Link-JavaScript-4cda	8.5%	PUP:W32/FunWeb.H	25.5%
Social Networking	14.0%	Exploit/Link-JavaScript-3f9f	7.5%	PUP:Zwunzi!gen1	16.1%
Streaming Media	9.0%	Downloader	6.5%	Spyware.9231	6.0%
Chat	4.2%	Trojan.Gen	6.4%	PUP:W32/FunWeb.J	4.9%
Computing and Internet	3.0%	Gen:Variant.Kazy.13334	5.1%	Application.Generic.9001	4.6%
Peer-To-Peer	2.1%	Packed.Gampass!gen1	3.2%	PUP:Generic.62006	4.2%
Search	2.0%	Gen:Variant.Dropper.26	3.1%	PUP:Generic.165137	3.6%
Games	1.9%	Trojan.Script.12023	2.9%	PUP:Clickpotato!gen	2.9%
News	1.7%	Gen:Variant.Buzy.1506	2.9%	Application.Generic.344399	2.4%
Spam URLs	1.4%	Trojan:GIF/GIFrame.gen!A	2.5%	PUP:W32/MyWebSearch.G	2.1%

March 2011

Activity related to Streaming Media policies resulted in 9.0% of URL-based filtering blocks in March. Streaming media is increasingly popular when there are major sporting events or high-profile international news stories, which often result in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes.

Symantec Endpoint Protection.cloud: The endpoint is often the last line of defense and analysis. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

The table below shows the malware most frequently blocked targeting endpoint devices for the last month. This includes data from endpoint devices protected by Symantec technology around the world, including data from clients which may not be using other layers of protection, such as Symantec MessageLabs Web Security.cloud or Symantec MessageLabs Email AntiVirus.cloud.

Malware[4]	% Malware
W32.Sality.AE	8.3%
Trojan.Gen*	7.7%
Trojan Horse	7.4%
W32.Ramnit!html	5.8%
Trojan.Gen.2*	4.9%
W32.Ramnit.B!inf	4.3%
Trojan.ADH.2	4.3%
Trojan.Bamital	4.3%
W32.Downadup.B	3.9%
Downloader*	3.5%

The most frequently blocked malware for the last month was the W32.Sality.AE virus. W32.Sality.AE is a virus that spreads by infecting executable files and attempts to download potentially malicious files from the Internet. The main goal of Sality.AE is to download and install additional malicious software on a victim’s computer. The virus also

[4] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*

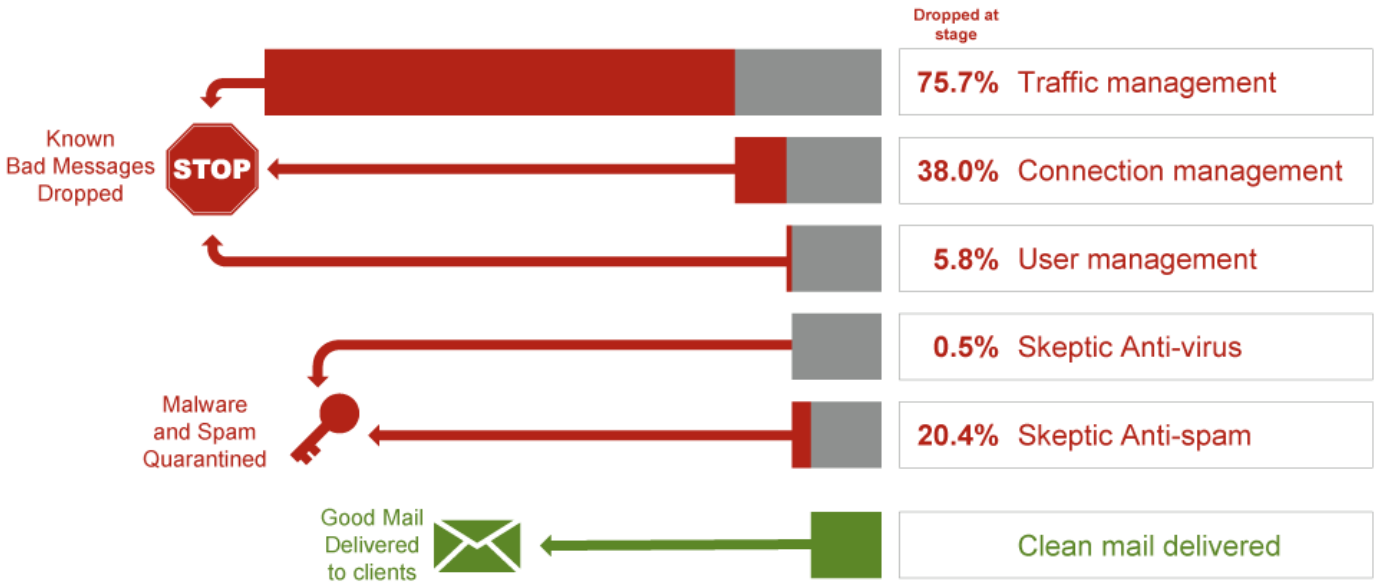
prevents access to various security-related domains, stops security-related services, and deletes security-related files. The virus also infects .EXE and .SCR files on a victim's local drive as well as on any writable network resource. It spreads by copying itself to attached removable drives.

*Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

By deploying techniques, such as heuristic analysis and generic detection, it is possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically. Approximately 15.7% of the most frequently blocked malware last month was identified and blocked in this way, using endpoint security protection.

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 2.7 billion SMTP connections per day, of which 75.7% 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 and operations. 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 38.0% 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 5.8% of inbound messages was identified as invalid by User Management.

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 31,000 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.