May 2011 Intelligence Report

For the First Time, Spammers Establish Their Own Fake URL-Shortening Services; Spam Rate Rises by 2.9%

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

Report highlights

- Spam – 75.8% in May (an increase of 2.9 percentage points since April 2011)
- Viruses – One in 222.3 emails in May contained malware (a decrease of 0.14 percentage points since April 2011)
- Phishing – One in 286.7 emails comprised a phishing attack (a decrease of 0.06 percentage points since April 2011)
- Malicious web sites – 3,170 web sites blocked per day (an increase of 30.4% since April 2011)
- 36.8% of all malicious domains blocked were new in May (an increase of 3.8 percentage points since April 2011)
- 24.6% of all web-based malware blocked was new in May (an increase of 2.1 percentage points since April 2011)
- For the First Time, Spammers establish their own fake URL-shortening services

Report analysis

Spammers establish their own fake URL-shortening services

URL shortening services—which allow long, unwieldy URLs, or links, to be converted into much shorter URLs have experienced growth in popularity with the advent of length-restricted micro-blogging services and social media status updates. Unfortunately, these services are very useful to spammers as they are simple, relatively anonymous and easy to automate by nature which makes them rife for abuse. In 2010, MessageLabs Intelligence published its security predictions[1] for 2011, which included the likelihood of more sophisticated attacks using URL-shortening services either by a criminal enterprise gaining control of a legitimate URL-shortening service or by one of these groups creating a service which appears legitimate, and operates in a legitimate manner, before being turned to malicious use.

This month, MessageLabs Intelligence uncovered evidence of spammers establishing their own fake URL-shortening services for the first time. Shortened links created on these fake URL-shortening sites are not included directly in spam messages; instead, the spam emails contain shortened URLs created on legitimate URL-shortening sites. Rather than leading directly to the spammer's final Web site, these links actually point to a shortened URL on the spammer's fake URL-shortening Web site, which in turn redirects to the spammer's final Web site. This process is shown in figure 5, below.

MessageLabs Intelligence research has identified several similar fake URL-shortening Web sites associated with the same spammers, each behaving in the same way. All the sites use .ru (Russian) domain names, and many are hosted in Russia and Ukraine.

To make things more interesting, the domains were registered several months before they were used, potentially as a means to evade detection by legitimate URL-shortening services since the age of the domain may be used as an indicator of legitimacy making it more difficult for the genuine shortening services to identify potential abuse.

[1] https://www-secure.symantec.com/connect/blogs/2011-trends-cybercriminals-usurp-url-shortening-services

The MessageLabs Intelligence team has been monitoring how spammers abuse URL-shortening services for several years, and have observed spammers using a wide range of these services, often creating thousands of links in a very short period of time on a single site. Using the aforementioned method of establishing their own Web sites, spammers also often create elaborate "chains" where one short URL points to another URL from a different URL-shortening site. This is sometimes repeated more than ten times before arriving at the spammer's site. Figure 1, below, shows the trend over time of legitimate URL-shortening services being used in spam emails. Following an increase at the end of 2010, the use has recently declined as spammers switched to spamming via social media, as reported in the April MessageLabs Intelligence report. However, in recent weeks, the practice appears to be returning to spam emails, contributing to the recent rise in spam levels.

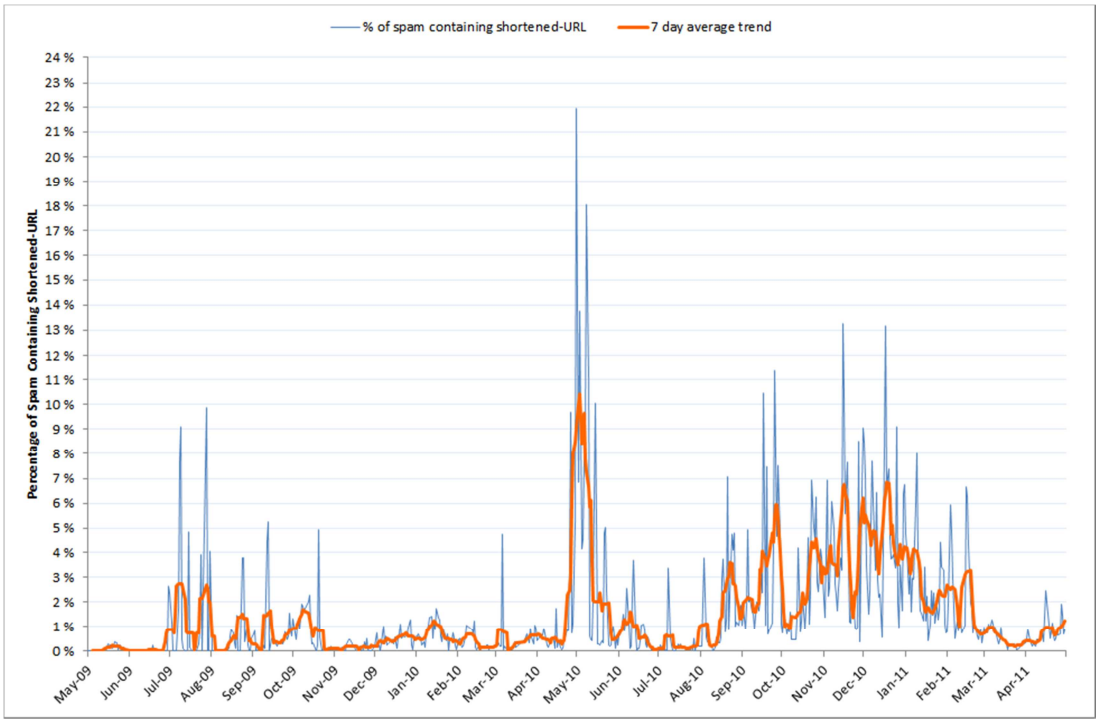


Figure 1: Chart showing percentage of spam that contains a shortened URL over time

Continual research and monitoring

As part of its research, MessageLabs Intelligence tracks many URL-shortening sites, discovering new ones every day. During this process, we identified some particularly interesting new URL-shortening sites. These sites don't have public interfaces, are not found in search results and do not appear on any micro-blogging services. Therefore, they are unlikely to be private URL-shortening services created by some organizations (who prefer to use their own, rather than rely on external sites).

Spammer-owned and operated sites?

Many URL-shortening sites use common wordplays and abbreviations in their domain names, but these sites don't. They use a consistent pattern. There are no references to the sites in search engine results, and we have only seen them used in spam. This strongly suggests that these sites are actually run by spammers themselves.

Even more suspiciously, the sites have another crucial difference to normal URL-shortening sites. The ID, which identifies the URL or link to which it redirects, is mostly ignored. After changing characters or the length of the ID, the URL still redirects to the same spam URL.

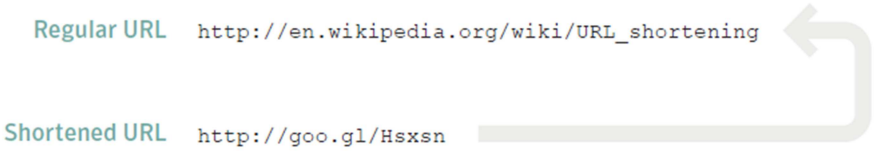


Figure 2: Example of a legitimate shortened URL; the ID in the short URL uniquely identifies the target Web site

Site appearance

The main pages of these URL-shortening sites are simply "holding" or "coming soon" pages, as shown in figure 3:

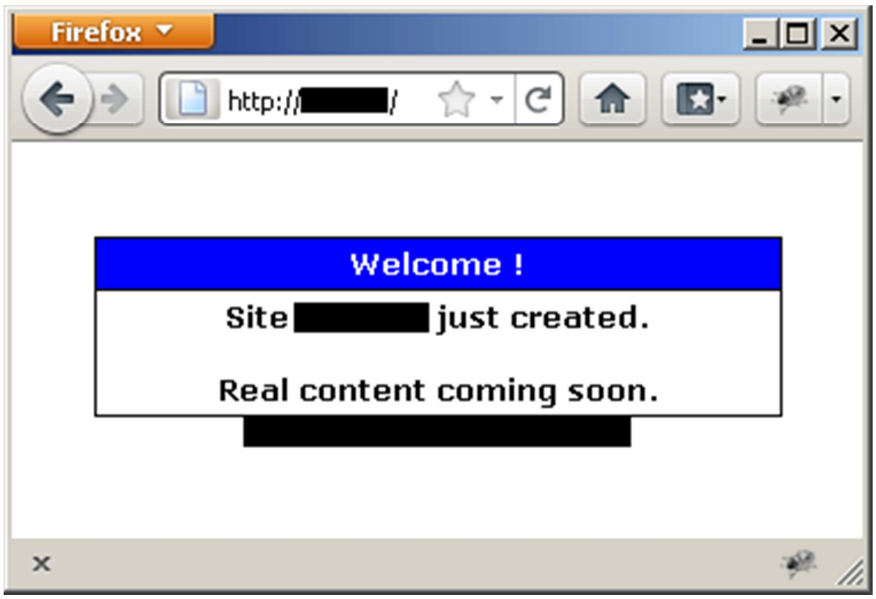


Figure 3: Web site landing page for apparent spammer short URL domain

As previously mentioned, there are no links to any page where a short URL can be created, and there are no details about the service. This page itself is generated by legitimate Web hosting "control panel" software. Despite this message, the site is being actively used as a URL-shortening service, redirecting visitors to spam Web sites.

Putting it together

Interestingly, these spammer URL-shortening sites are not used directly in spam messages. Instead, they are used as intermediate points or "stepping stones" between (usually) a link to a public URL-shortening service, and the spammer's site.

A sample spam message contains a URL pointing to a normal, public URL-shortening service, as can be seen in figure 4, below.

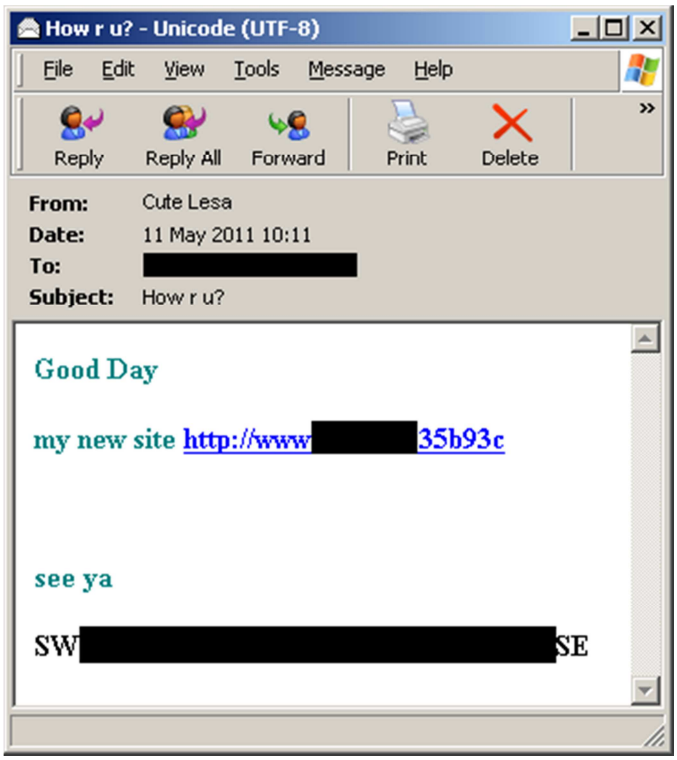


Figure 4: Sample email containing genuine shortened URL

Anyone following this link is first taken to a public URL-shortening site, which redirects to the spammer's URL-shortening service, and then finally on to the spammer's Web site, as shown in figure 5, below.

Figure 5: Process involved in redirecting users through spam emails and URL-shortening services

This particular spammer is promoting a rather strange mismatch of pirated software (including Symantec products), pharmaceutical products and hardcore adult content, as shown in the example in figure 6, below.

Figure 6: Final Web site landing page involved in the redirection process

These URL-shortening services don't work in the same way as legitimate ones; interestingly, any ID passed to the spammer's redirect service will redirect to the same spam Web site. This suggests that spammers are at this stage using this technique to "dress-up" their spam and give the appearance and functionality of a genuine URL-shortening service. The ability to use any seemingly genuine ID to redirect to the same Web site means that they don't have to go to the trouble of generating genuine IDs and with a low level of re-use, may help to better evade traditional anti-spam filters. With legitimate URL-shortening services attempting to tackle abuse more seriously, spammers seem to be experimenting with ways to establish their own services to better avoid disruption.

We expect spammers to continue abusing URL-shortening services, particularly with the continual flow of new URL-shortening services being created. Symantec MessageLabs Email AntiSpam.cloud customers benefit from our

proprietary technology to effectively block URL-shortening spam, while still allowing messages using URL-shortening for legitimate purposes.

By Nick Johnston, Senior Software Engineer, Symantec

Blog: Are You At Risk of a Targeted Attack? Lifting the Lid on Who Was Targeted in 2010

Targeted attacks are bespoke pieces of malware that are sent to email addresses that appear to have been specifically selected by the attacker. In this way, they differ from the rest of email malware that are sent in large numbers without apparent regard to the recipient. Approximately one in every 208 emails contained malware in March 2011, rising to one in 168 in April; however, only one in every 5,000 (0.02%) of malware-containing emails can be classified as targeted. Although these attacks are quite rare, MessageLabs Intelligence identified an increase of 60.4% in the average number of daily attacks between 2010 and 2009.

Since April 2008, almost a third of all targeted attacks have been sent to the public sector (32.4%), followed by companies in the manufacturing sector (15.9%), financial companies (8.0%), IT Services (6.1%) and educational organizations (predominantly universities) (4.6%). Compared with 2009, the number of targeted attacks is increasing as is the number of companies attacked. Additionally there was a 17.4% increase in the number of attacked customers in 2010 over 2009 and a 31.4% increase in the number of distinct attacks. Moreover, there was a clear increase in the number of attacks directed against the most frequently targeted organizations; targeted attacks appear to be becoming more common, but also more highly targeted.

Most of the recipients of targeted attacks could be identified from their Internet footprint. For example, 34% of recipients were senior managers and 24%of recipients were individuals with managerial responsibilities. Only 4% were of low seniority; many of these are personal assistants to senior managers. Interestingly, 19% of recipients are not identifiable through public Internet searches, yet the attackers know their identity possibly by way of successful attacks elsewhere.

For more information, please visit the MessageLabs Intelligence blog at:
https://www-secure.symantec.com/connect/blogs/are-you-risk-targeted-attacks-lifting-lid-who-was-being-targeted-2010

Blog: Rise in ZIP File Attachments in Spam Emails Lead to Bredolab Malware

On March 26, MessageLabs Intelligence tracked a large increase in the amount of data traffic hitting its spam traps, despite the overall volume of spam emails continuing to decline in the wake of the recent Rustock botnet takedown. Further analysis revealed that the Cutwail botnet had begun sending more emails than usual with ZIP file attachments, meaning the average size of each mail was much larger than normal. These mails are all variations on the same familiar subject, a package could not be delivered and the recipient would need to open the attachment to print out and take to their depot to collect it.

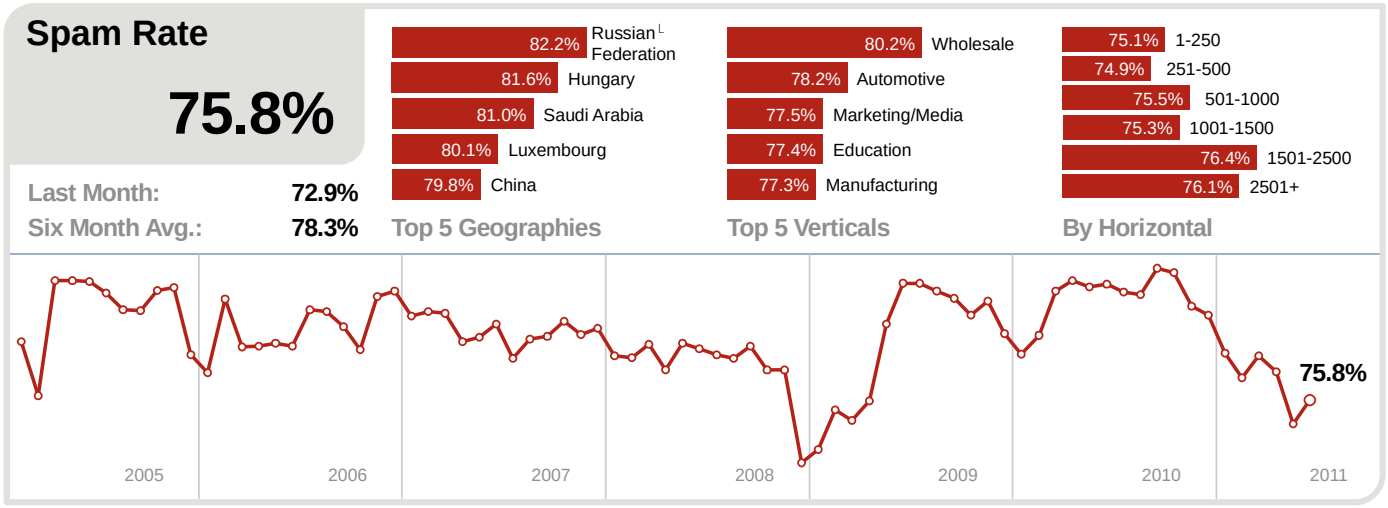
Inside the ZIP file attachment is an executable file, which if run, will infect the users' machine. The malicious files are all variants of the Bredolab malware. Once on the system, the Bredolab family of malware allows the attacker to take control of the machine and download other software to it, including malware and fake, rogue security software. Most likely the infected machine would become part of a botnet and used to spread the infection to others.

For more information, please visit the MessageLabs Intelligence blog at:
https://www-secure.symantec.com/connect/blogs/rise-zip-file-attachments-spam-emails-lead-bredolab-malware

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 May 2011, the global ratio of spam in email traffic increased by 2.9 percentage points since April 2011 to 75.8% (1 in 1.32 emails) partly as a result of the increased level of activity around shortened URL redirects. However, it was also expected to rise again following the Rustock botnet takedown in March.



May 2011

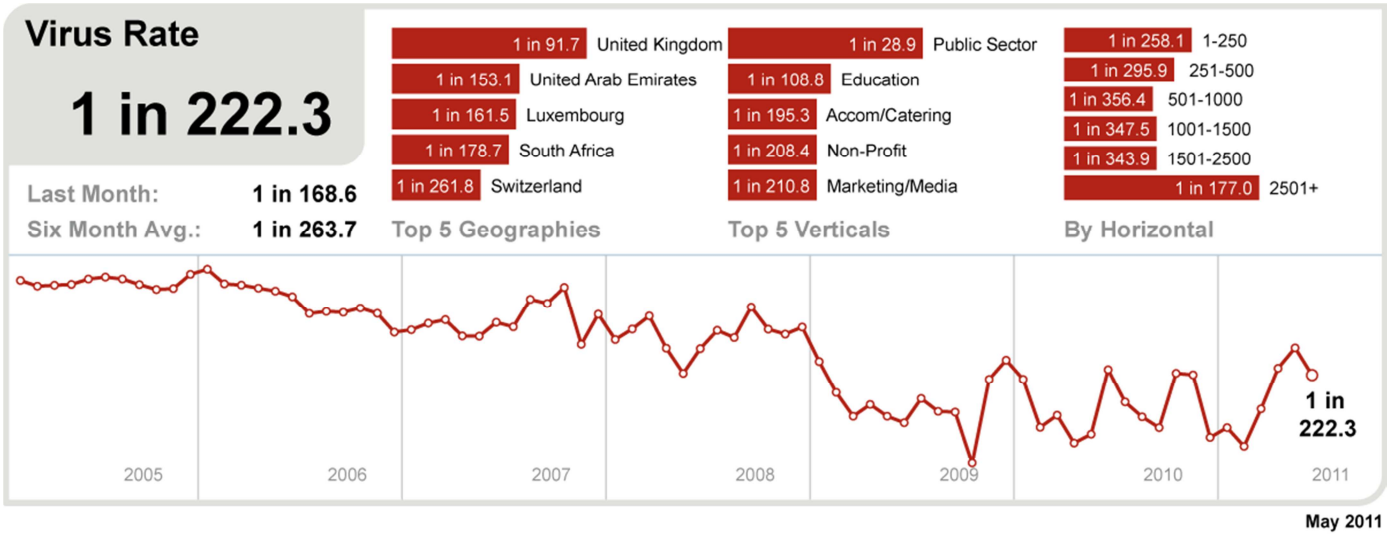
As the overall spam level climbed in May 2011, Russia became the most spammed geography, with a spam rate of 82.2%.

In the US, 76.4% of email was spam and 75.3% in Canada. The spam level in the UK was 75.4%. In The Netherlands, spam accounted for 77.5% of email traffic, 75.5% in Germany, 75.1% in Denmark and 73.9% in Australia. In Hong Kong, 75.2% of email was blocked as spam and 74.0% in Singapore, compared with 72.3% in Japan. Spam accounted for 75.9% of email traffic in South Africa and 74.8% in Brazil.

In May, the Wholesale industry sector became the most spammed sector, with a spam rate of 80.2%. Spam levels for the Education sector reached 77.4% and 76.0% for the Chemical & Pharmaceutical sector; 75.4% for IT Services, 75.4% for Retail, 74.5% for Public Sector and 74.7% for Finance.

Symantec MessageLabs Email AntiVirus.cloud: The global ratio of email-borne viruses in email traffic was one in 222.3 emails (0.450%) in May, a decrease of 0.143 percentage points since April 2011.

In May, 30.0% of email-borne malware contained links to malicious Web sites, an increase of 16.9 percentage points since April 2011. A large number of emails containing variants of Bredolab- related malware, accounted for 16.3% of all email-borne malware, compared with 55.1% in the previous month. These variants were commonly attached as ZIP files, rather than hyperlinks, and as the volume of these attacks diminishes, the proportion of attacks using hyperlinks increased.



May 2011

The UK had the highest ratio of malicious emails in May, as one in 91.7 emails was blocked as malicious in May. A large number of variants of Bredolab malware continued to be observed in a number of countries during May, as highlighted in the table below.

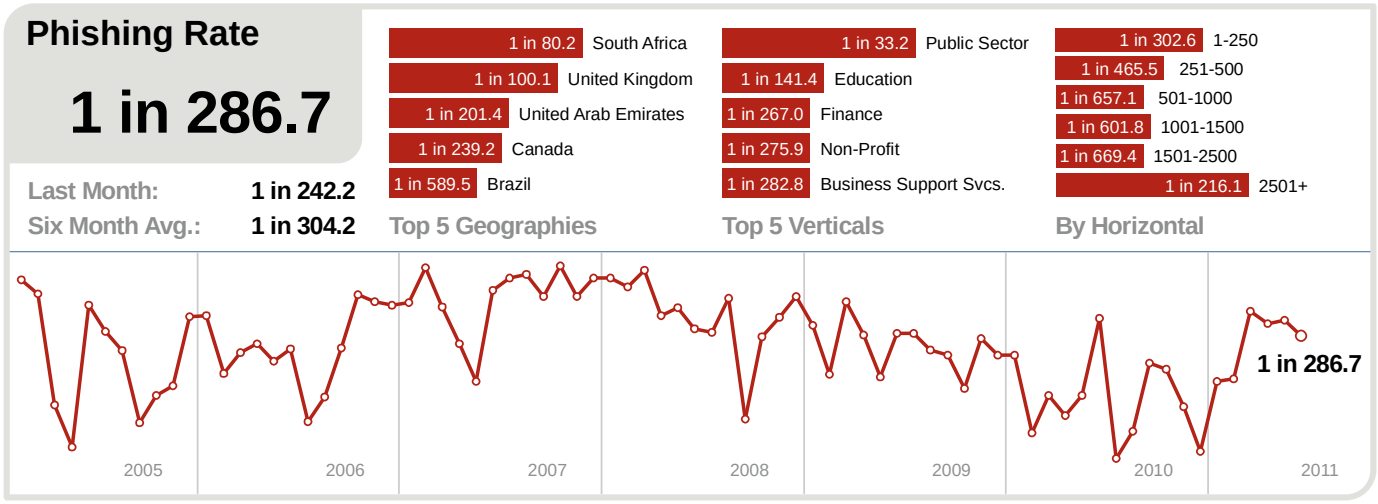
In the US, virus levels for email-borne malware were 1 in 540.3 and 1 in 334.5 for Canada. In Germany virus activity reached 1 in 435.9, 1 in 1,197 in Denmark and in The Netherlands 1 in 330.1. In Australia, 1 in 513.5 emails were malicious and 1 in 377.2 in Hong Kong; for Japan it was 1 in 1,164, compared with 1 in 706.7 in Singapore. In South Africa, 1 in 178.7 emails and 1 in 378.3 emails in Brazil contained malicious content.

With 1 in 28.9 emails being blocked as malicious, the Public Sector remained the most targeted industry in May. Virus levels for the Chemical & Pharmaceutical sector were 1 in 305.9 and 1 in 367.9 for the IT Services sector; 1 in 377.7 for Retail, 1 in 108.8 for Education and 1 in 313.5 for Finance.

The table below shows the most frequently blocked email-borne malware for May, many of which take advantage of malicious hyperlinks. Overall, 55.1% of email-borne malware was associated with Bredolab, Sasfis, SpyEye and Zeus variants, a trend initially reported in the MessageLabs Intelligence Report for February 2011.

Malware	% Malware
Gen:Variant.Bredo.21	6.79%
Trojan.Bredolab!eml	5.15%
W32/NewMalware!836b	4.64%
W32/NewMalware!8103	3.09%
W32/NewMalware-Generic-7ba5	2.38%
HeurAuto-bb01	2.36%
W32/Generic-6bfd	2.30%
Exploit/FakeAttach	1.60%
W32/Packed.Generic-1d11-bd36	1.47%
Exploit/FakeAttach-844a	1.39%

Phishing Analysis: In May, phishing activity decreased by 0.06 percentage points since April 2011; one in 286.7 emails (0.349%) comprised some form of phishing attack.



May 2011

South Africa remained the most targeted geography for phishing emails in May, with 1 in 80.2 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.

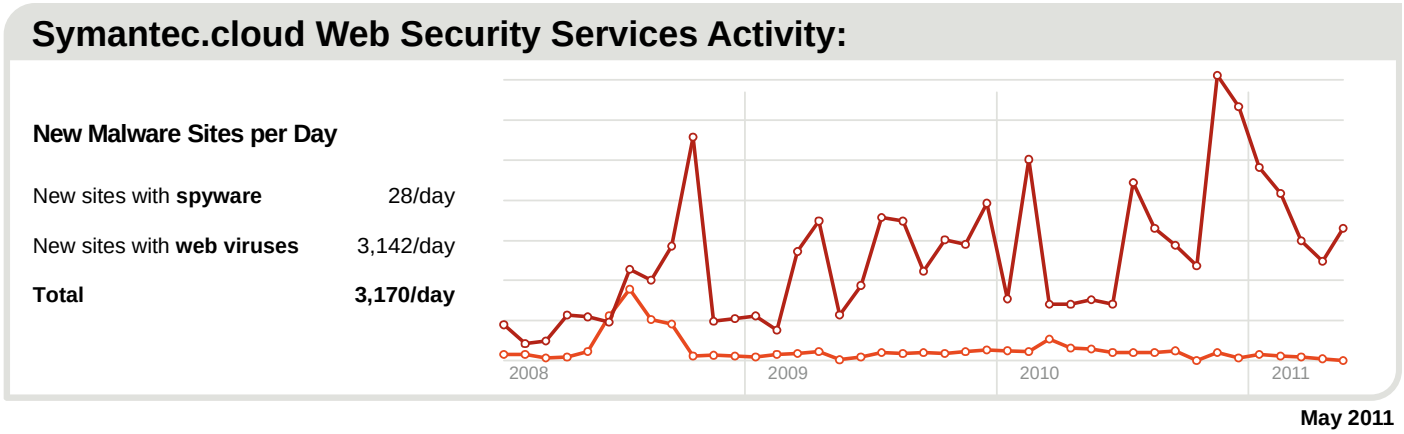
In the UK, phishing accounted for 1 in 100.1 emails. Phishing levels for the US were 1 in 1,227 and 1 in 239.2 for Canada. In Germany phishing levels were 1 in 1,540, 1 in 2662 in Denmark and 1 in 780.9 in The Netherlands. In Australia, phishing activity accounted for 1 in 1,022 emails and 1 in 2,235 in Hong Kong; for Japan it was 1 in 10,735 and 1 in 2,111 for Singapore. In Brazil, 1 in 589.5 emails were blocked as phishing attacks.

The Public Sector remained the most targeted by phishing activity in May, with 1 in 33.2 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 982.8 and 1 in 738.9 for the IT Services sector; 1 in 537.0 for Retail, 1 in 141.4 for Education and 1 in 267.0 for Finance.

Symantec MessageLabs Web Security.cloud: In May, MessageLabs Intelligence identified an average of 3,142 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 30.4% since April 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 is in circulation for a longer period of time 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 36.8% of all malicious domains blocked were new in May; an increase of 3.8 percentage points compared with April 2011. Additionally, 24.6% of all Web-based malware blocked was new in May; an increase of 2.1 percentage points since the previous month.

Symantec.cloud Web Security Services Activity:



May 2011

Symantec.cloud

The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during May 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 45.9% of blocked Web activity in May. The second most frequently blocked traffic was categorized as Social Networking, and accounted for 16.2% of URL-based filtering activity blocked, equivalent to one in every 6.2 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.

Activity related to Streaming Media policies resulted in 8.8% of URL-based filtering blocks in May. 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. This rate is equivalent to one in every 11.3 Web sites blocked.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	45.9%	Trojan:GIF/GIFrame.gen!A	26.5%	PUP:W32/CnsMin.S	17.4%
Social Networking	16.2%	Trojan:HTML/GIFrame.gen!B	22.2%	PUP:Generic.9001	14.0%
Streaming Media	8.8%	Exploit/Link-JavaScript-4cda	6.0%	PUP:Clickpotato!gen	13.1%
Chat	4.0%	Infostealer.Gampass	5.0%	PUP:Generic.167772	12.8%
Computing and Internet	3.4%	Exploit/Link-JavaScript-3f9f	4.7%	PUP:Generic.62006	7.5%
Peer-To-Peer	2.8%	Downloader.MisleadApp	3.3%	PUP:9231	5.5%
Games	2.5%	Trojan.Patchep!inf	1.7%	PUP:SMShoax.K	4.9%
Hosting Sites	1.6%	Gen:Variant.Kazy.11241	1.6%	PUP:.Generic.357550	2.5%
News	1.5%	Trojan.Gen	1.6%	PUP:Generic.168911	2.5%
Search	1.4%	W32.Almanahe.B	0.9%	PUP:Perfect	1.7%

May 2011

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[2]	% Malware
W32.Ramnit!html	7.83%
W32.Sality.AE	6.54%
W32.Ramnit.B!inf	5.90%
Trojan.Bamital	5.08%
W32.Downadup.B	3.96%
Trojan.FakeAV	2.82%
Trojan.ADH.2	2.59%
Trojan.ByteVerify	2.29%
W32.SillyFDC	2.22%
Trojan.ADH	2.14%
*Generic Detection**	19.7%

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

The most frequently blocked malware for the last month was W32.Ramnit!html. This is a generic detection for .HTML files infected by W32.Ramnit[3], a worm that spreads through removable drives and by infecting executable files. The worm spreads by encrypting and then appending itself to files with .DLL, .EXE and .HTM extensions. Variants of the Ramnit worm accounted for 14.0% of all malicious software blocked by endpoint protection technology in May.

For much of 2010, W32.Sality.AE had been the most prevalent malicious threat blocked at the endpoint; however, for the first time in twelve months, it fell to second place in the chart.

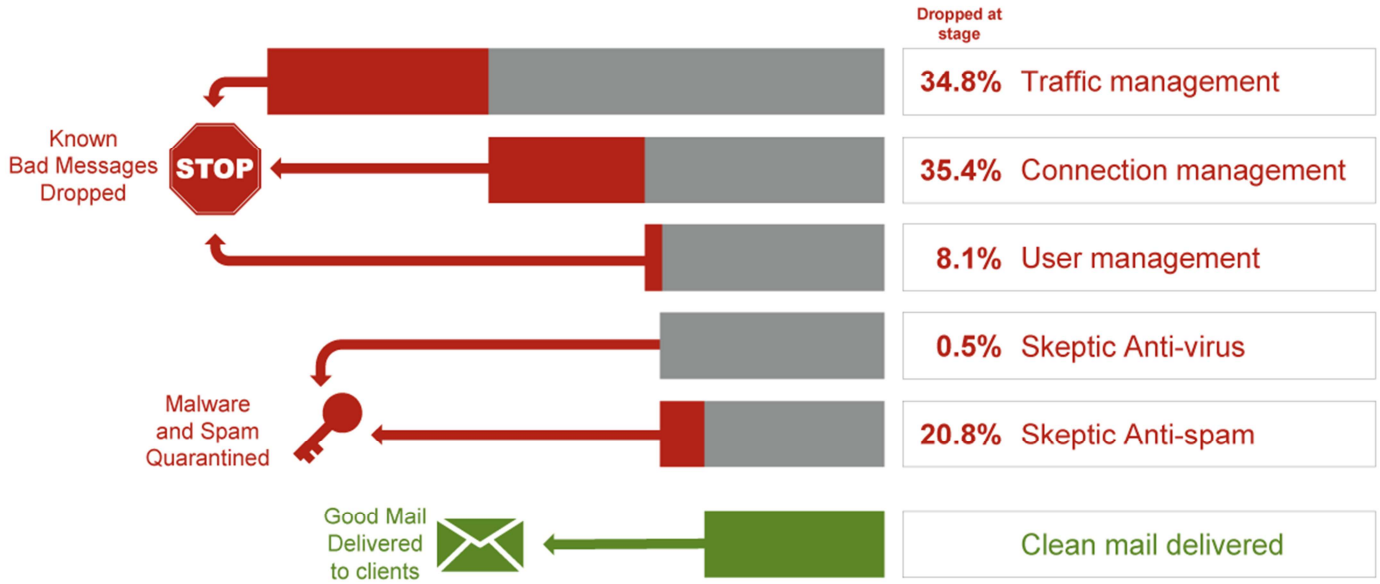
***** *Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic 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 19.7% of the most frequently blocked malware last month was identified and blocked using generic detection.

[3] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99&tabid=2*

Traffic Management

Traffic Management continues to reduce the overall message volume through techniques operating at the protocol level. Unwanted senders are identified and connections to the mail server are slowed down using features embedded in the TCP protocol. Incoming volumes of known spam are significantly slowed, while ensuring legitimate email is expedited.



In May, MessageLabs services processed an average of 1.1 Billion SMTP connections per day, of which 34.8% 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 May, an average of 35.4% of inbound messages was intercepted from botnets and other known malicious sources and rejected as a consequence.

User Management

User Management uses Registered User Address Validation techniques to reduce the overall volume of emails for registered domains, by discarding connections for which the recipient addresses are identified as invalid or non-existent. In May, an average of 8.1% 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 15 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.

Symantec.cloud™