Symantec Intelligence

Symantec Intelligence Report: June 2011

Three-quarters of spam send from botnets in June, and three months on, Rustock botnet remains dormant as Cutwail becomes most active; Pharmaceutical spam in decline as new Wiki- pharmacy brand emerges

Welcome to the June edition of the Symantec Intelligence report, which for the first time combines the best research and analysis from the Symantec.cloud MessageLabs Intelligence Report and the Symantec State of Spam & Phishing Report. The new integrated report, the Symantec Intelligence Report, provides the latest analysis of cyber security threats, trends and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The data used to compile the analysis for this combined report includes data from May and June 2011.

Report highlights

- Spam – 72.9% in June (a decrease of 2.9 percentage points since May 2011): page 11
- Phishing – One in 330.6 emails identified as phishing (a decrease of 0.05 percentage points since May 2011): page 14
- Malware – One in 300.7 emails in June contained malware (a decrease of 0.12 percentage points since May 2011): page 15
- Malicious Web sites – 5,415 Web sites blocked per day (an increase of 70.8% since May 2011): page 17
- 35.1% of all malicious domains blocked were new in June (a decrease of 1.7 percentage points since May 2011): page 17
- 20.3% of all Web-based malware blocked was new in June (a decrease of 4.3 percentage points since May 2011): page 17
- Review of Spam-sending botnets in June 2011: page 3
- Clicking to Watch Videos Leads to Pharmacy Spam: page 6
- Wiki for Everything, Even for Spam: page 7
- Phishers Return for Tax Returns: page 8
- Fake Donations Continue to Haunt Japan: page 9
- Spam Subject Line Analysis: page 12
- Best Practices for Enterprises and Users: page 19

Introduction from the editor

Since the shutdown of the Rustock botnet in March[1], spam volumes have never quite recovered as the volume of spam in global circulation each day continues to fluctuate, as shown in figure 1, below.

The overall impact has been that spam now accounts for 72.9% of email in June, returning to the same level as in April earlier this year. In June, 76.6% of this spam was being sent from botnets, compared with 83.1% in March. This marks a return to the same level of output as at the end of 2010. On average during 2010, 88.2% of spam was sent from botnets, falling to 77% by the end of the year. Despite these recent successes, botnets are still a dangerous force on the Internet and can be used for a variety of other purposes, from conducting distributed denial of service attacks (DDoS), carrying out fraudulent click-thrus on unsuspecting Web sites for financial gain, hosting illegal Web site content on infected computers (known as bots), harvesting personal data from infected users and installing spyware to track the activities of those users.

Global spam has generally been falling since the shutdown of the Spamit affiliate Web site in late September 2010, and the takedown of Rustock has accelerated this decline. Spamit was one of the main affiliate Web sites through which pharmaceutical spam was being promoted and pharmaceutical spam levels have fallen considerably in recent months. In the latest analysis, spam relating to pharmaceutical products has fallen to approximately 40% of all spam in June 2011. Pharmaceutical spam accounted for approximately 64.2% at the end of 2010.

[1] http://www.symantec.com/connect/blogs/has-rustock-botnet-ceased-spamming

Even though spam is currently at the lowest level it has been since the McColo takedown in November 2008, it is still a huge problem In March, following the disruption of Rustock, the largest spam-sending botnet, approximately 36.9 billion spam emails were in circulation each day during April. This number rose to 41.7 billion in May, before falling back to 39.2 billion in June.

A longer-term view shows that for the same period last year, spam accounted for 121.5 billion emails in global circulation each day, equivalent to 89.3% of email traffic in June 2010. Highlighting that over a twelve month period, a drop of 68.7% in volume resulted in a fall of only 16.4 percentage points in the overall global spam rate.

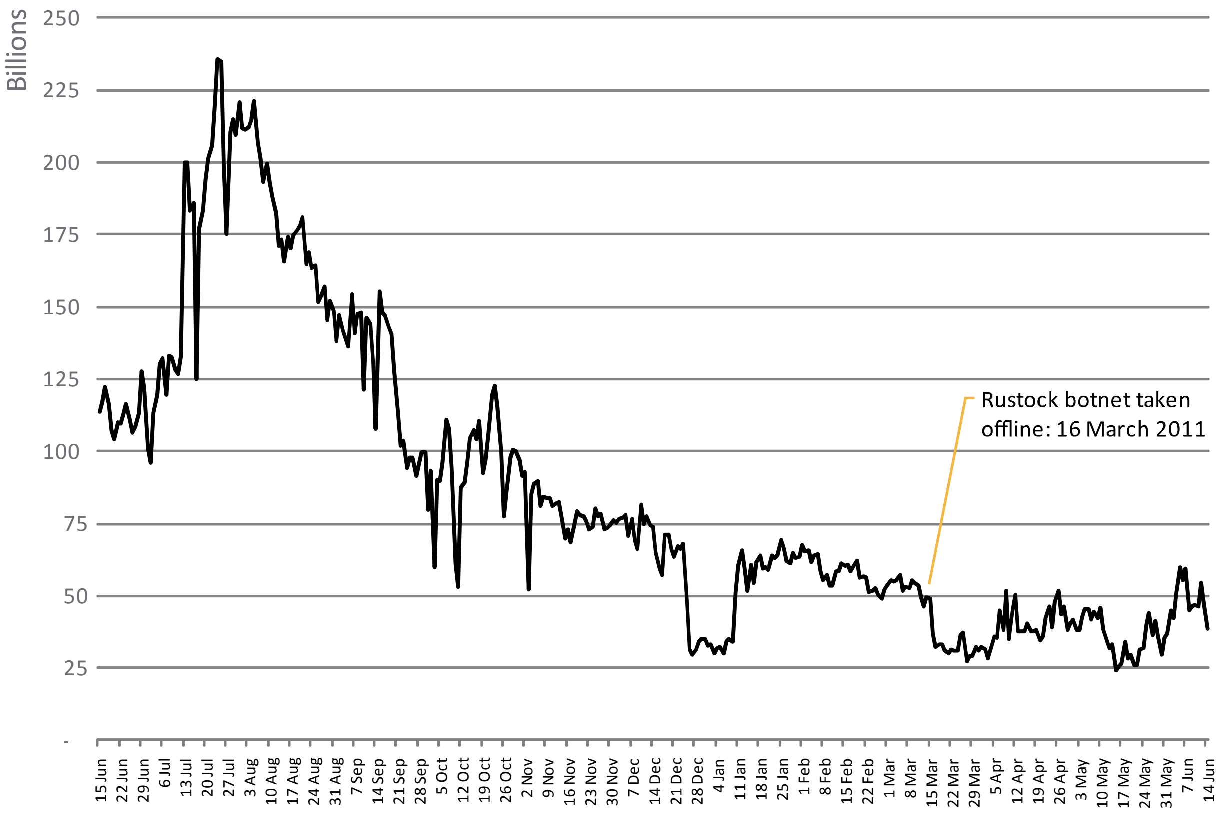


Figure 1 – Trend showing fluctuating global daily spam volume over twelve months

However, this does not mean that spammers are dead. This month's report highlights the changing nature of the spam-sending botnet landscape and online pharmacy spam using two different angles: a spoof of an online video sharing service and a new online pharmacy brand, perhaps seeking to exploit the popularity of the "wiki" name in a number of high-profile Web sites. Also, May spam subject line analysis shows that adult spam continue to flourish.

This month we reviewed the state of the spam-sending botnet landscape, and concluded that despite earlier predictions, Bagle has not taken over the role of Rustock following its shutdown; the main reason being that we could not find any relevant connection between spam campaigns sent by those two botnets. However, it did appear much more likely that Grum has taken over at least in part some of the previous Rustock activity. Several spam events occurred in which the two botnets were clearly interconnected.

I hope you enjoy reading this very first combined report, and please feel free to contact me directly with any comments or feedback as to what you like or dislike about this new format.

Paul Wood
Senior Intelligence Analyst, Symantec.cloud

paul_wood@symantec.com
@paulowoody

Report analysis

Review of spam-sending botnets in June 2011

There have certainly been some major changes in the world of botnet-spam in 2011, especially since the previous analysis from March[2], in which we reported the impact of a coordinated action led by Microsoft against the largest and most active spam-sending botnet, Rustock, which was taken offline as a result. Three months on, this takedown appears to have been completely effective and we have seen no spam whatsoever come from the former spamming giant since March 16th.

In figure 2, below, it can be seen that in June, 76.6% of spam was being sent from botnets; however, the global spam volume is still much lower than earlier in the year, following the disruption of the Rustock botnet. Moreover, global spam has generally been falling since the shutdown of the Spamit affiliate Web site in September 2010, and the takedown of Rustock has accelerated this decline. Even though spam is currently at the lowest level it has been since the McColo takedown in November 2008, it is still a huge problem, with an estimated 39.2 billion spam emails sent per day globally (which equates to approximately 72.9% of global email).

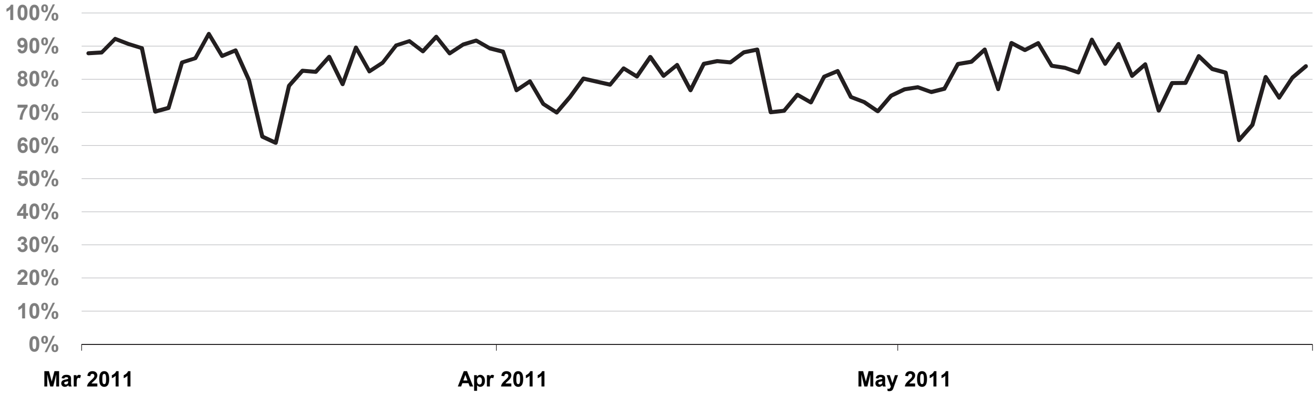


Figure 2 – Proportion of spam sent from botnets since March 2011

At that time, it appeared that as Rustock's dominance waned, Bagle was set to become its likely successor, as seen in figure 3, below; however, the Cutwail botnet emerged to become the current dominant force in June. Cutwail is an older, more established botnet, and has also been known for sending large volumes of email malware as well, particularly related to the Bredolab family of malware, which has been very active recently.

Pharmaceutical spam accounted for the vast majority of Rustock's output, and since Spamit ceased operating, Rustock had had periods where very little or even no spam was sent from its bots. However, these outages were always short-lived (the longest being less than 48 hours). So the rapid decline of Bagle's output since the end of April is still unexplained. Almost all of its spam related to pharmaceutical products, and potentially was one of the main contenders to take on the business following Rustock's demise.

The Symantec.cloud Intelligence team analyzed spam from both Rustock and Bagle since March 2011 and concluded that Bagle has not taken over the role of Rustock following its shutdown. The main reason for this conclusion is that we could not find any relevant connection between spam campaigns sent by those two botnets. On the contrary, looking in-depth at patterns obtained for the different spam features, their behaviors appeared to be very different; therefore there was no evidence that spam campaigns previously distributed by Rustock were being off-loaded to Bagle.

[2] http://www.symanteccloud.com/mlireport/MLI_2011_03_March_Final-EN.pdf

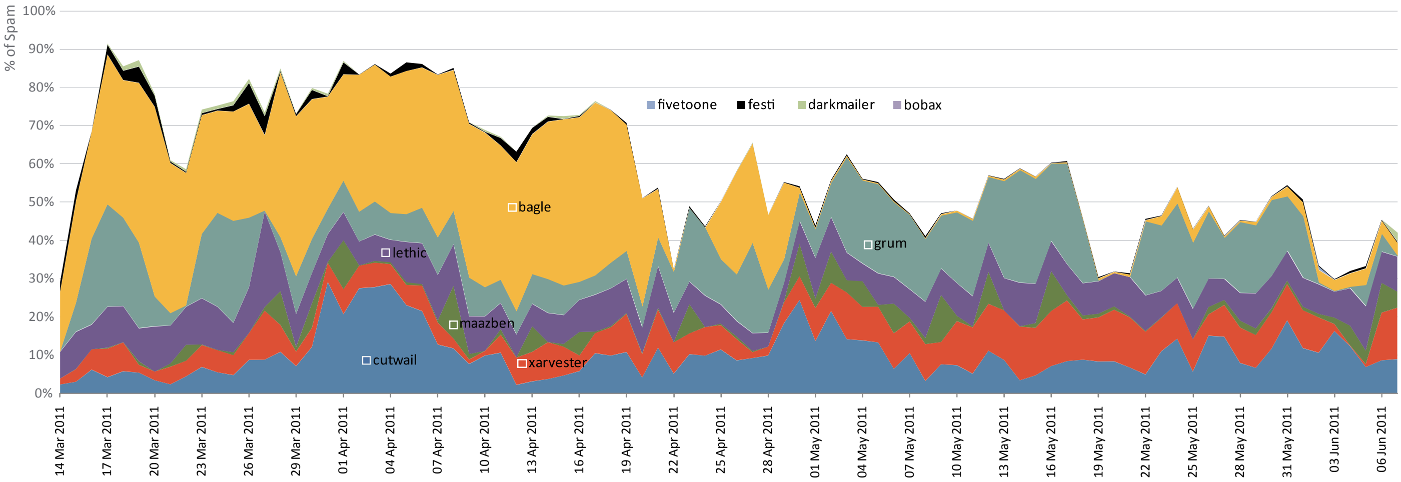


Figure 3 - Top ten spam-sending botnets (relative volumes) since March 2011

However, it did appear much more likely that Grum has taken over at least in part some of the previous Rustock activity. Several spam events occurred in which the two botnets were clearly interconnected, by at least the subject lines and the '*From:'* sender domains. Perhaps even more conclusively, we found that Grum had suddenly changed its character set from 'ISO-8859-1' to 'UTF-8' (the latter more often used by Rustock). This change occurred between March 10 and March 17, just a few hours after the Rustock takedown. Just prior to that, Rustock was also using UTF-8 to encode its spam; such a coincidence may appear to be quite unusual. Meanwhile, analysis of the '*Subject:'* lines used in spam messages, indicated that even though many botnets are involved in the distribution of pharmaceutical spam, Rustock, and subsequently Grum, were the only ones that were using the registered trademark ® symbol in their subject lines; perhaps another coincidence…

Furthermore, for each botnet, it seemed that the bot distribution of Grum was similar to that of Rustock, but with much fewer bots located in the ARIN region for the US, which could reflect the b107 operation undertaken by Microsoft and others in the US against the Rustock command and control servers.

On a Microsoft MSDN blog[3], Terry Zink recently claimed that Rustock may be back, but under a new name and has perhaps broken itself into smaller parts (or smaller botnets) to be less detectable. He claims also that Darkmailer looks a lot like Rustock, and it remains to be seen whether those claims can be verified independently. Certainly Darkmailer has increased its output in recent weeks and for the first time appears in the top-ten list of spam sending botnets for June.

Another long-standing botnet, Xarvester, has also increased its output since the demise of Rustock. Xarvester has been relatively quiet for a long time, but has recently come back to the fore to become the second most active spam-sending botnet in June, as shown in figure 4, below.

[3] http://blogs.msdn.com/b/tzink/archive/2011/05/23/has-anyone-stepped-in-to-fill-rustock-s-gap.aspx

Botnet	% of spam	spam/day	spam/min	Spam /bot /min	estimated botnet size	Country of Infection
Cutwail	16.1%	9,609,745,048	6,673,434	77	800k to 1200k	India (10%), Russia (9%), Brazil (8%)
Xarvester	6.7%	4,002,042,186	2,779,196	455	57k to 86k	United Kingdom (18%), France (13%), Italy (9%)
Maazben	3.1%	1,872,408,382	1,300,284	14	520k to 780k	Republic of Korea (14%), Russia (10%), India (10%)
Lethic	3.1%	1,824,416,511	1,266,956	45	230k to 340k	Republic of Korea (25%), Russia (15%), Ukraine (7%)
Grum	3.0%	1,801,605,428	1,251,115	140	200k to 290k	Russia (14%), India (14%), Ukraine (8%)
Bagle	2.7%	1,599,896,533	1,111,039	58	140k to 200k	India (15%), Russia (1%), Argentina (8%)
Fivetoone	2.3%	1,400,401,724	972,501	98	94k to 140k	Vietnam (20%), Brazil (12%), Indonesia (11%)
Festi	1.2%	691,992,804	480,551	166	25k to 37k	India (10%), Vietnam (10%), Brazil (9%)
Bobax	0.4%	254,229,254	176,548	24	80k to 120k	Ukraine (27%), India (18%), Russia (18%)
DarkMailer	0.5%	42,575,225	29,566	351	1k to 1.5k	France (27%), USA (16%), Germany (13%)
Other, smaller Botnets	0.5%	22,277,510	15,470	321	62k to 95k	
Unnamed Botnets	36.9%	21,962,912,697	15,252,023	196	660k to 990k	
Total Botnet Spam	**76.6%**	**45,084,503,302**	**31,308,683**	**162**		
Non-botnet spam	**23.4%**	**14,510,023,657**	**10,076,405**			
Grand Total		**59,594,526,959**	**41,385,088**			

Figure 4 – Most active spam-sending botnets in June 2011

As can seen from the chart in figure 5, below, with the demise of Rustock, the most common geographical sources of spam have also changed, for example, there is less spam being sent from the US than identified previously, with less than 2.8% of spam originating from the US, compared to 10.7% one year ago. This seems to have been largely due to the disruption of Rustock, which had most of its bots located in the US and since those bots were no longer active, the amount of spam from the country has dropped accordingly.

Country	% of Spam
Korea, Republic of (South Korea)	11.2%
Russian Federation	11.1%
India	8.7%
Ukraine	6.1%
Brazil	5.3%
Vietnam	2.9%
United States	2.8%
United Kingdom	2.4%
Taiwan	2.4%
Romania	2.3%

Figure 5 – Geographical distribution of spam-sending botnets in June 2011

Conversely, the amount of spam coming from compromised machines in the Republic of Korea (South Korea) has been approximately 3% for the past twelve months, but now accounts for over 11%. This seems to be mostly due to the increased output of the Maazben and Lethic botnets, which have a strong base in that region. Spam from Eastern Europe has been fairly consistent, with Russia and Ukraine being the top sources.

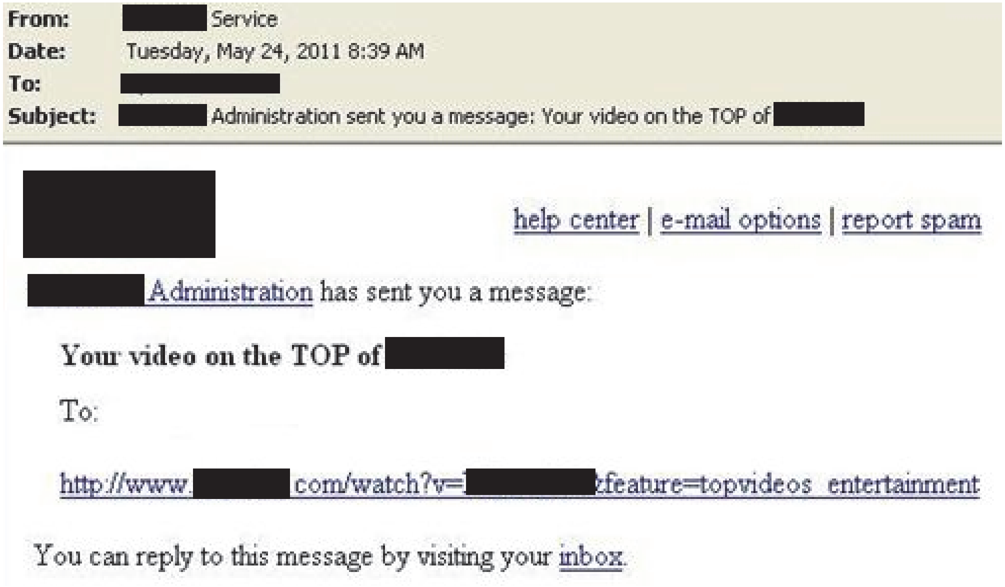
It is also interesting to note that with the recent increase in output from the Xarvester botnet, it is fairly unique in that the infected computers are almost exclusively based in Western European countries, including the UK and France.

Clicking to Watch Videos Leads to Pharmacy Spam

Spam messages promoting pharmaceutical products have been perhaps the most commonly seen spam attacks over the past several years. Pharmaceutical products are deceptively marketed through spam emails employing a variety of obfuscation techniques. Symantec saw an increase in pharmacy spam abusing well-known online video sharing site.

Sample From and Subject lines observed in this spam attack are below.

From: [REMOVED] Service <service@[REMOVED].com>
Subject: [REMOVED] Administration sent you a message: Your video on the TOP of [REMOVED]
Subject: [REMOVED] Service sent you a message: Best Unrated Videos To Watch
Subject: [REMOVED] Support sent you a message: Your video has been removed due to terms of use violation



From: [redacted] Service
Date: Tuesday, May 24, 2011 8:39 AM
To: [redacted]
Subject: [redacted] Administration sent you a message: Your video on the TOP of [redacted]

[redacted]

help center | e-mail options | report spam

[redacted] Administration has sent you a message:

Your video on the TOP of [redacted]

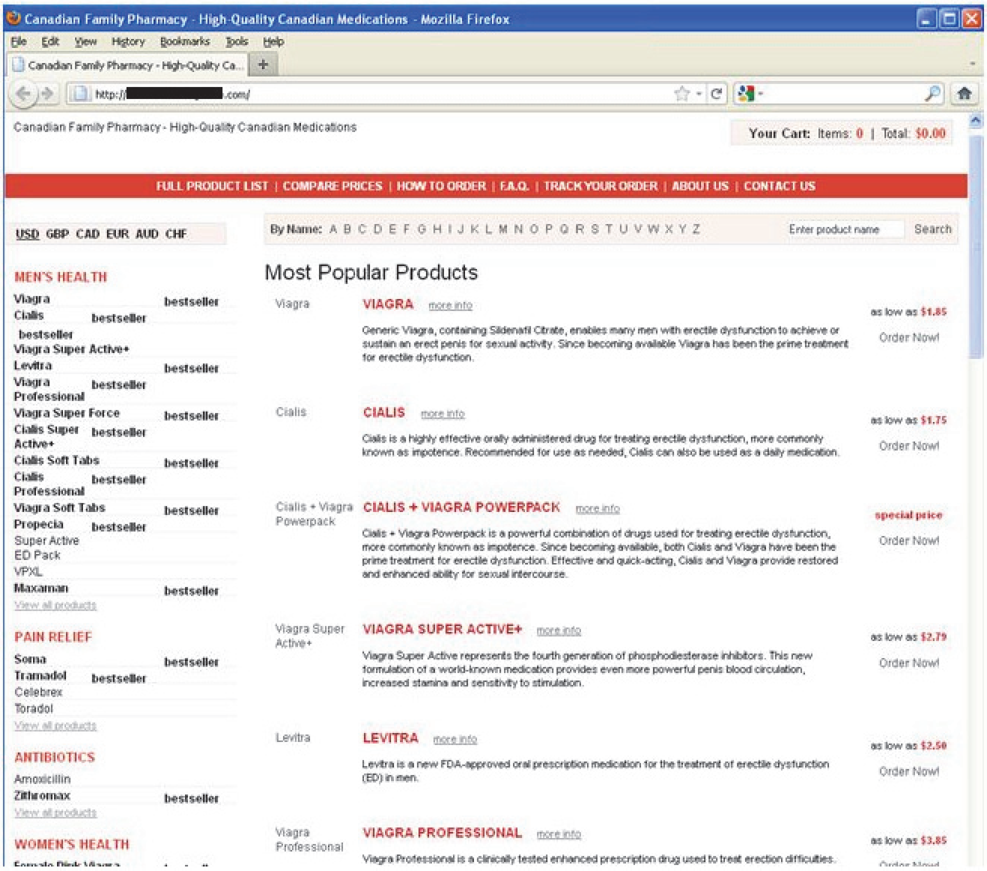
To:

http://www.[redacted]com/watch?v=[redacted]feature=topvideos_entertainment

You can reply to this message by visiting your inbox.

Figure 6 – Example of spam email purporting to contain hyperlink to video-sharing Web site

With these subject lines, the spammers have attempted to instill a sense of curiosity among the recipients. The spam messages either state that the recipient’s video features as a top video, such as in the example shown in figure 6 above, or that the recipient’s particular video has been removed due to a terms-of-use violation. The text, accompanied by URL links in the message body, as in most cases, is the call to action in this spam campaign. The included URLs which appear to link to the video sharing site are in fact spam URLs hosted on a hijacked domains. When clicked, all URLs redirect to a Canadian Family Pharmacy Web site as shown in figure 7 below, which was hosted on a recently created domain owned by the spammer. Some of these domains were found to be registered in Russia and France. The spammer, ironically, has placed a link to report spam which is just another redirect to the same pharmacy Web page.


Canadian Family Pharmacy - High-Quality Canadian Medications - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Canadian Family Pharmacy - High-Quality Ca...
http://[redacted].com/
Canadian Family Pharmacy - High-Quality Canadian Medications
Your Cart: Items: 0 | Total: $0.00
FULL PRODUCT LIST | COMPARE PRICES | HOW TO ORDER | F.A.Q. | TRACK YOUR ORDER | ABOUT US | CONTACT US
USD GBP CAD EUR AUD CHF
By Name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Enter product name
Search

MEN'S HEALTH

Viagra bestseller
Cialis bestseller
bestseller
Viagra Super Active+
Levitra bestseller
Viagra Professional bestseller
Viagra Super Force bestseller
Cialis Super Active+ bestseller
Cialis Soft Tabs bestseller
Cialis Professional bestseller
Viagra Soft Tabs bestseller
Propecia bestseller
Super Active ED Pack
VPXL
Maxaman bestseller
View all products

PAIN RELIEF

Soma bestseller
Tramadol bestseller
Celebrex
Toradol
View all products

ANTIBIOTICS

Amoxicillin
Zithromax bestseller
View all products

WOMEN'S HEALTH

Most Popular Products

Viagra — **VIAGRA** more info — as low as $1.85 — Order Now!

Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.

Cialis — **CIALIS** more info — as low as $1.75 — Order Now!

Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.

Cialis + Viagra Powerpack — **CIALIS + VIAGRA POWERPACK** more info — special price — Order Now!

Cialis + Viagra Powerpack is a powerful combination of drugs used for treating erectile dysfunction, more commonly known as impotence. Since becoming available, both Cialis and Viagra have been the prime treatment for erectile dysfunction. Effective and quick-acting, Cialis and Viagra provide restored and enhanced ability for sexual intercourse.

Viagra Super Active+ — **VIAGRA SUPER ACTIVE+** more info — as low as $2.79 — Order Now!

Viagra Super Active represents the fourth generation of phosphodiesterase inhibitors. This new formulation of a world-known medication provides even more powerful penis blood circulation, increased stamina and sensitivity to stimulation.

Levitra — **LEVITRA** more info — as low as $2.50 — Order Now!

Levitra is a new FDA-approved oral prescription medication for the treatment of erectile dysfunction (ED) in men.

Viagra Professional — **VIAGRA PROFESSIONAL** more info — as low as $3.85

Viagra Professional is a clinically tested enhanced prescription drug used to treat erection difficulties.

Figure 7 – Example of Canadian Family Pharmacy Web site linked from spam emails

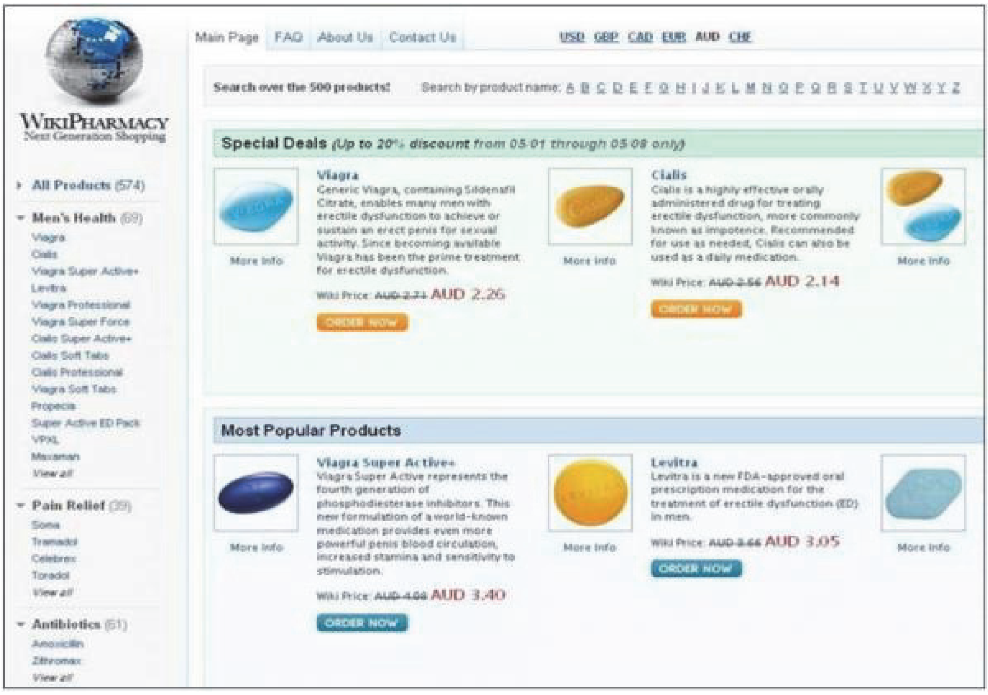
The IP addresses involved in these spam attacks are part of botnets and have been blacklisted for their past involvement in such spam campaigns. It is likely that these messages were sent using multiple botnets to distribute high-volume of spam.

Wiki for Everything, Even for Spam

Last month, Symantec Intelligence identified a new spam tactic being used, which introduced the "Wiki" name prefix for the promotion of fake pharmaceutical products relating to a new pharmacy brand, WikiPharmacy. The "*Subject:*" line in these attacks has a lot of randomization contained in the text. The "*From:*" header is either fake or a hijacked ISP account that gives a personalized appearance to the email.

Below are some subject lines that were observed in the spam samples:

Subject: wWIKIp
Subject: kWIKIx
Subject: yWIKIg
Subject: hWikiPharmacyl
Subject: oWikiPharmacyp
Subject: uWikiPharmacym



Special Deals *(Up to 20% discount from 05-01 through 05-08 only)*

Viagra
Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.

Wiki Price: ~~AUD 2.71~~ AUD 2.26

Cialis
Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.

Wiki Price: ~~AUD 2.66~~ AUD 2.14

Most Popular Products

Viagra Super Active+
Viagra Super Active represents the fourth generation of phosphodiesterase inhibitors. This new formulation of a world-known medication provides even more powerful penis blood circulation, increased stamina and sensitivity to stimulation.

Wiki Price: ~~AUD 4.00~~ AUD 3.40

Levitra
Levitra is a new FDA-approved oral prescription medication for the treatment of erectile dysfunction (ED) in men.

Wiki Price: ~~AUD 3.66~~ AUD 3.05

Figure 8 – Example of Wiki Pharmacy Web site linked from spam emails

In the example shown in figure 8 above, spammers are promoting pharmacy products at a discounted price using a wiki-style layout. The Web page appears to belong to the WikiPharmacy brand. The volume of spam in this latest attack is quite high. Needless to say is that the popularity of the wiki- name in a number of high-profile Web sites is being exploited here, and users must be very careful not to enter personal details on these fake sites.

Here are some of the URL patterns seen in these samples:

http://sucullu.[REMOVED].net/wiki14.html
http://cinar. [REMOVED].org.tr/wiki14.html
http://jmleml. [REMOVED]].com/wiki14.html
http:// [REMOVED].com.br/wiki15.html
http:// [REMOVED].com/wiki15.html
http://web164892.web23. [REMOVED].net/wiki15.html

A careful look at the “Subject” line is sufficient to identify this type of spam. Beware of prowling predators who are waiting to pounce on any opportunity. Please see the Best Practices section of the report for helpful tips in protecting your computer.

Phishers Return for Tax Returns

The Income Tax Department of India recently announced[4] that the last date for sending income tax returns for AY 2010-2011 has been extended to July 31, 2011. During 2010, phishers had plotted their phishing scams[5] based on the tax return deadline. As the deadline for tax returns of the current financial year approaches, phishers have returned with their stream of phishing sites.

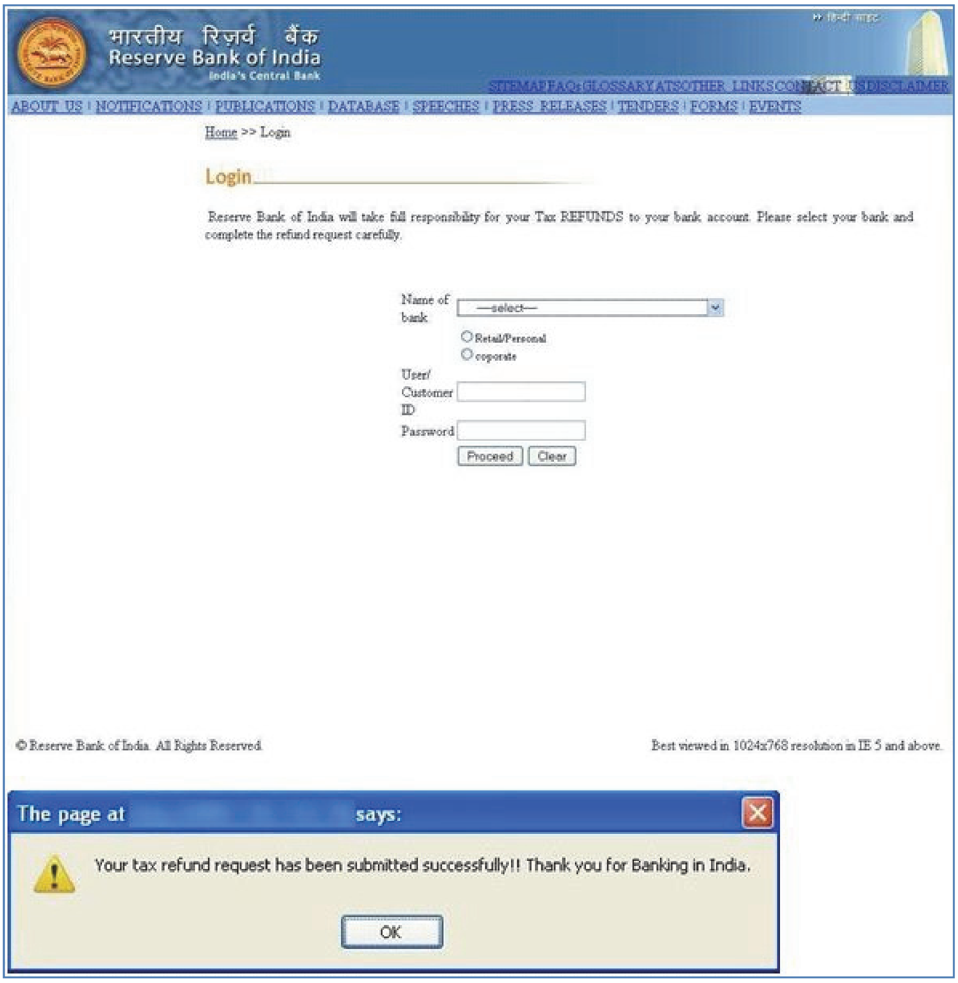
This time, phishers have spoofed the Reserve Bank of India’s Web site as a ploy for a tax refund scam. The phishing site attempts to lure users by stating that the bank would take full responsibility for depositing the tax refund to the user’s personal bank account. The user is prompted to select the name of the bank and enter their customer ID and password. There is a list of eight banks to choose from. In this way, phishers intend to steal the confidential

[4] https://incometaxindiaefiling.gov.in/portal/index.do

[5] http://www.symantec.com/connect/blogs/filing-deadline-extension-triggers-more-fake-offers-tax-refunds

information of customers of several banks from a single phishing site. The following page asked for credit/debit card number and PIN number. After these details are entered, the phishing site displays a message acknowledging that the request for the tax refund has been submitted successfully. The user is then redirected to the legitimate Web site of Reserve Bank of India. If users fall victim to the phishing site, phishers will have stolen their information for financial gain.

Symantec has been in contact with the Reserve Bank of India. The bank has stated that emails sent in its name to customers have been observed asking for bank account details. The Reserve Bank has clarified that it has not sent any such email and that the Reserve Bank (or any bank) never issues communication asking for bank account details for any purpose. The Reserve Bank has also appealed to members of public to not respond to such email and to not share their bank account details with anyone for any purpose.


भारतीय रिज़र्व बैंक
Reserve Bank of India
India's Central Bank
» हिन्दी साइट
SITEMAPFAQsGLOSSARYATSOTHER LINKSCONTACT USDISCLAIMER
ABOUT US | NOTIFICATIONS | PUBLICATIONS | DATABASE | SPEECHES | PRESS RELEASES | TENDERS | FORMS | EVENTS
Home >> Login

Login

Reserve Bank of India will take full responsibility for your Tax REFUNDS to your bank account. Please select your bank and complete the refund request carefully.

Name of bank —select—

○ Retail/Personal
○ coporate

User/ Customer ID

Password

Proceed Clear

© Reserve Bank of India. All Rights Reserved.

Best viewed in 1024x768 resolution in IE 5 and above.

The page at [redacted] says:

Your tax refund request has been submitted successfully!! Thank you for Banking in India.

OK

Figure 9 – Example of fake phishing Web site used in tax refund scams

The phishing site used a numbered IP domain (for example, domains like hxxp://255.255.255.255) hosted on servers based in St Louis, USA. The same IP was used for hosting phishing sites of several other Indian banks. The IP belongs to a Web site of a company that provides roofing for houses. The IP of the company's Web site was compromised to host the phishing sites.

Fake Donations Continue to Haunt Japan

A couple of months ago, Japan was hit by an earthquake of magnitude 9.0. The earthquake and tsunamis that followed caused severe calamity to the country. Phishers soon responded with their fake donation campaign[6] in the hopes of luring end users. Unfortunately, it seems that the phishers are continuing to use these fake donations as bait in a recent phishing attack we observed.

In a fake donation campaign, phishers spoof the Web sites of charitable organizations and banks and use those fake sites as bait. This time, they spoofed the German page of a popular payment gateway site with a bogus site that asked for user login credentials. The contents of the page (in German) translated to "Japan needs your helpage Support the relief efforts for the earthquake victims. Please donate now." The message was provided along with a map of Japan that highlighted two cities from the affected region. The first city shown was the one near Japan's nuclear power plant, Fukushima, and the second was the capital city, Tokyo. The map also showed the epicenter of the earthquake located undersea near the east coast of Japan.

Upon entering their credentials, users are redirected to the legitimate Web site where they continue their activity, unaware that they have provided their valuable login information to phishers. Because the login credentials in question are for a payment gateway site, the account is linked to users' money by means of credit cards or bank accounts. If the users have fell victim to the phishing site, phishers will have successfully stolen their personal information for financial gain. The phishing attack was carried out using a toolkit that utilized a single IP address, which resolved to four domain names and was hosted on servers based in France.

[6] http://www.symantec.com/connect/blogs/phishers-have-no-mercy-japan

Global Trends & Content Analysis

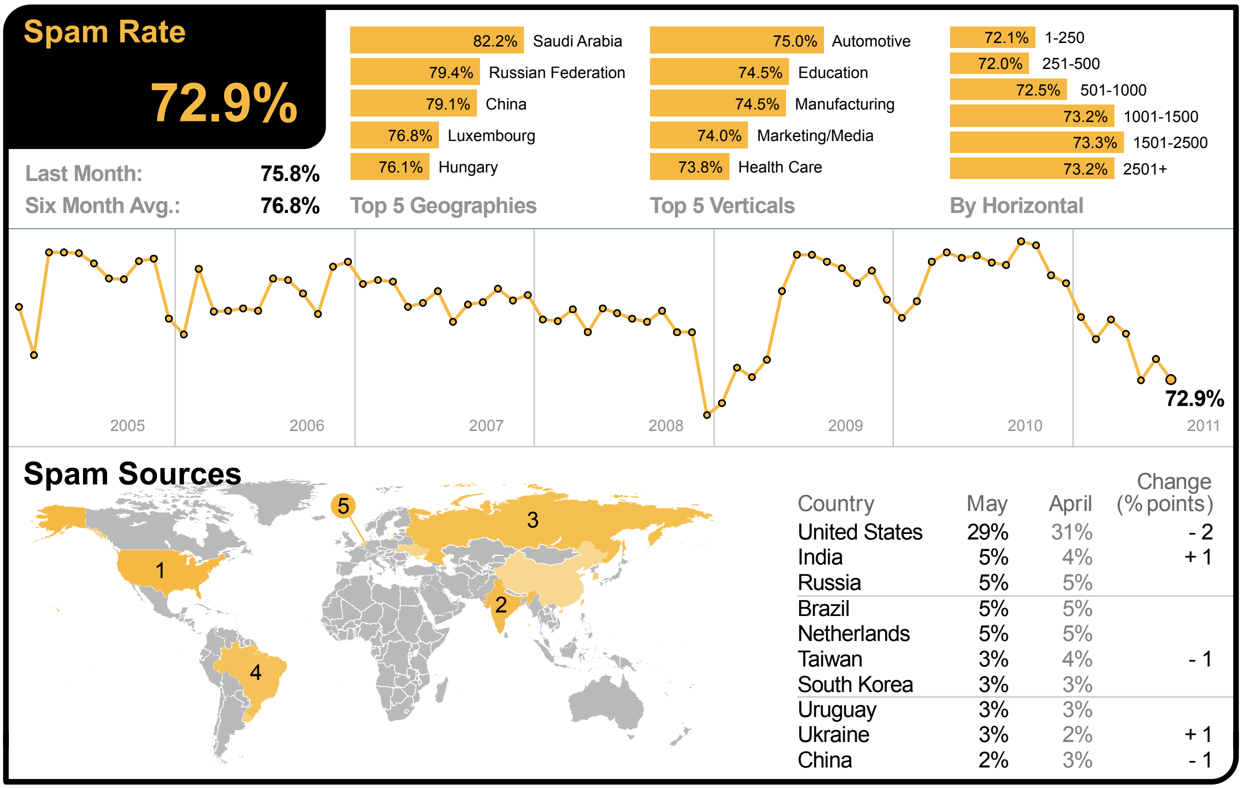
Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is also able to detect new and sophisticated targeted threats.

Data is collected in more than 86 countries from around the globe. Information is collected from over 8 billion email messages and over 1 billion Web requests which are processed per day across 16 data centers, including malicious code data which is collected from over 130 million systems in 86 countries worldwide. Symantec intelligence also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give the Symantec Intelligence analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. If there is a malicious attack about to hit, we know about it first. We block it; we keep it from affecting our customers.

Spam Analysis

In June 2011, the global ratio of spam in email traffic decreased by 2.9 percentage points since May 2011 to 72.9% (1 in 1.37 emails).



Top 5 Geographies	
82.2%	Saudi Arabia
79.4%	Russian Federation
79.1%	China
76.8%	Luxembourg
76.1%	Hungary

Top 5 Verticals	
75.0%	Automotive
74.5%	Education
74.5%	Manufacturing
74.0%	Marketing/Media
73.8%	Health Care

By Horizontal	
72.1%	1-250
72.0%	251-500
72.5%	501-1000
73.2%	1001-1500
73.3%	1501-2500
73.2%	2501+

Country	May	April	Change (% points)
United States	29%	31%	- 2
India	5%	4%	+ 1
Russia	5%	5%	
Brazil	5%	5%	
Netherlands	5%	5%	
Taiwan	3%	4%	- 1
South Korea	3%	3%	
Uruguay	3%	3%	
Ukraine	3%	2%	+ 1
China	2%	3%	- 1

June 2011

As the global spam level declined in June 2011, Saudi Arabia became the most spammed geography, with a spam rate of 82.2%, overtaking Russia, which moved into second position.

In the US, 73.7% of email was spam and 72.0% in Canada. The spam level in the UK was 72.6%. In The Netherlands, spam accounted for 73.0% of email traffic, 71.8% in Germany, 71.9% in Denmark and 70.4% in Australia. In Hong Kong, 72.2% of email was blocked as spam and 71.2% in Singapore, compared with 69.2% in Japan. Spam accounted for 72.3% of email traffic in South Africa and 73.4% in Brazil.

In June, the Automotive industry sector became the most spammed sector, with a spam rate of 75.0%. Spam levels for the Education sector reached 74.5% and 73.1% for the Chemical & Pharmaceutical sector; 72.7% for IT Services, 72.4% for Retail, 71.5% for Public Sector and 72.2% for Finance.

Global Spam Categories

Category Name	June 2011
Pharmaceutical	40.0%
Adult/Sex/Dating	19.0%
Watches/Jewelry	17.5%
Newsletters	11.5%
Casino/Gambling	7.0%
Unknown	2.5%
Degrees/Diplomas	1.5%
Weight Loss	1.0%

Spam Subject Line Analysis

In the latest analysis, adult-related spam took over the top spam subject line list. Online pharmacy spam subjects, which dominated the list last month, slipped with first one being seen in 16th place.

Rank	Total Spam: May 2011 Top Subject Lines	No. of Days	Total Spam: April 2011 Top Subject Lines	No. of Days
1	*Blank Subject line*	31	*Re: ru girl*	24
2	*Re: Windows 7, Office 2010, Adobe CS5 …*	16	*Blank Subject line*	30
3	*im online now*	31	*Re: Windows 7, Office 2010, Adobe CS5 …*	12
4	*my new pics :)*	31	*Save-80%-On-Viagra-Levitra-And-Cialis*	14
5	*drop me a line*	31	*Express Delivery system notification*	7
6	*r u online now?*	31	*Re:Hi*	29
7	*hi darling..*	31	*Re: sale wiagrow*	7
8	*new email*	31	*Do you have problem with ErectileDysfunction? ViagraCan help you and make sure it is a unique drug for treatingImpotence.*	16
9	*found you :)*	31	*BuyV!AGRA (SildenafilCitrate) Generic Tablets – Online Drugstore. ViagraCan help your ErectileDysfunction*	16
10	*my hot pics :)*	31	*Find Out How You Can Start Making $6487 a Month At HOME*	19

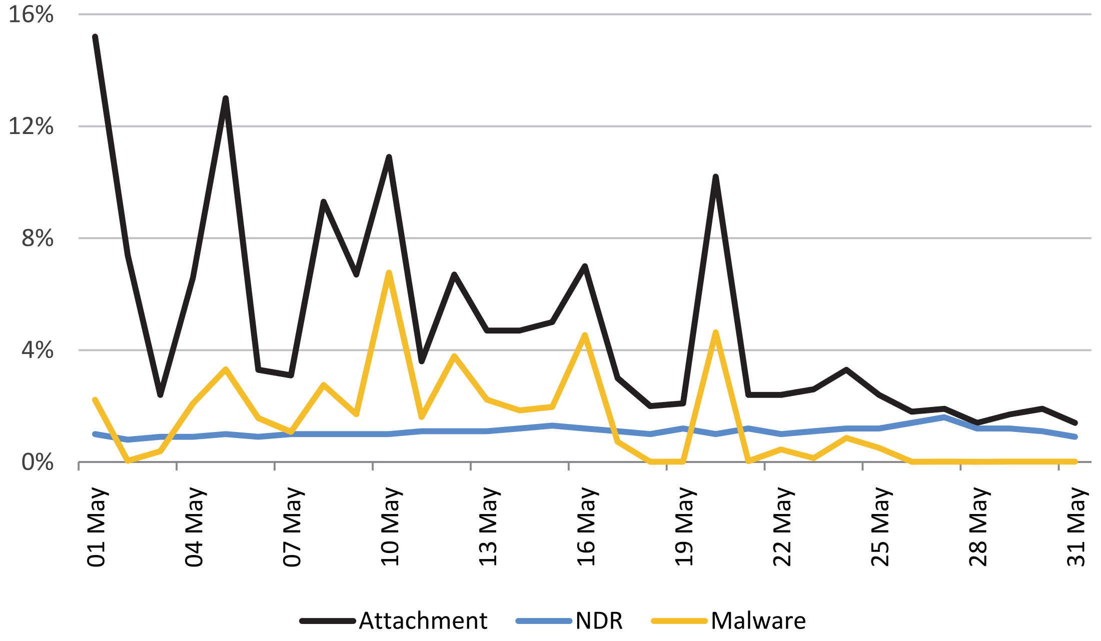
Spam URL TLD Distribution

TLD	May	April	Change (% points)
com	53.4%	55.0%	-1.6
ru	19.2%	10.1%	+9.1
info	14.9%	18.5%	-3.6
net	5.5%	6.9%	-1.4

Average Spam Message Size

Message Size	May	April	Change (% points)
0kb-5kb	62.33%	69.59%	-7.26
5kb-10kb	24.23%	16.18%	+8.05
10kb+	13.44%	14.23%	-0.79

Spam Attack Vectors



Phishing Analysis

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

Phishing Rate

1 in 330.6

Last Month:	1 in 286.7
Six Month Avg.:	1 in 289.7

Top 5 Geographies

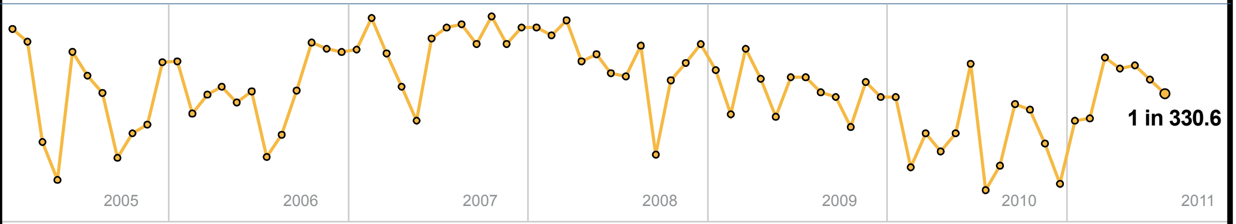
1 in 111.7	South Africa
1 in 130.2	United Kingdom
1 in 207.7	Canada
1 in 314.9	United Arab Emirates
1 in 320.1	Sweden

Top 5 Verticals

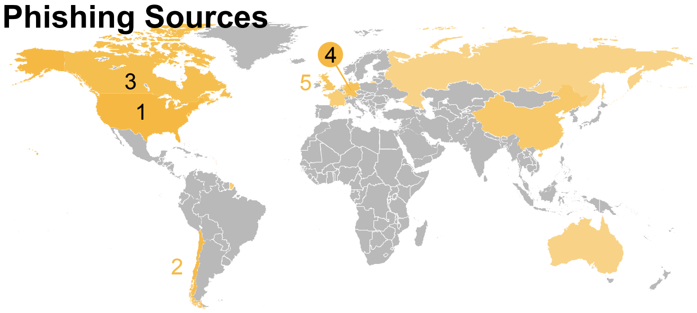
1 in 83.7	Public Sector
1 in 151.4	Education
1 in 160.8	Finance
1 in 311.5	Non-Profit
1 in 347.2	Accom/Catering

By Horizontal

1 in 322.6	1-250
1 in 490.1	251-500
1 in 689.3	501-1000
1 in 600.8	1001-1500
1 in 709.1	1501-2500
1 in 263.2	2501+



Phishing Sources



Country	May	April	Change (% points)
United States	44%	55%	-11
Chile	15%	unlisted	N/A
Canada	5%	5%	
Germany	5%	6%	-1
United Kingdom	4%	6%	-2
China	2%	unlisted	N/A
France	2%	3%	-1
Netherlands	2%	2%	
Russia	1%	2%	-1
Australia	1%	3%	-2

June 2011

South Africa remained the most targeted geography for phishing emails in June, with 1 in 111.7 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 130.2 emails. Phishing levels for the US were 1 in 1,270 and 1 in 207.7 for Canada. In Germany phishing levels were 1 in 1,375, 1 in 2,043 in Denmark and 1 in 543.7 in The Netherlands. In Australia, phishing activity accounted for 1 in 565.2 emails and 1 in 2,404 in Hong Kong; for Japan it was 1 in 11,179 and 1 in 2,456 for Singapore. In Brazil, 1 in 409.8 emails were blocked as phishing attacks.

The Public Sector remained the most targeted by phishing activity in June, with 1 in 83.7 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 897.3 and 1 in 798.3 for the IT Services sector; 1 in 663.2 for Retail, 1 in 151.4 for Education and 1 in 160.8 for Finance.

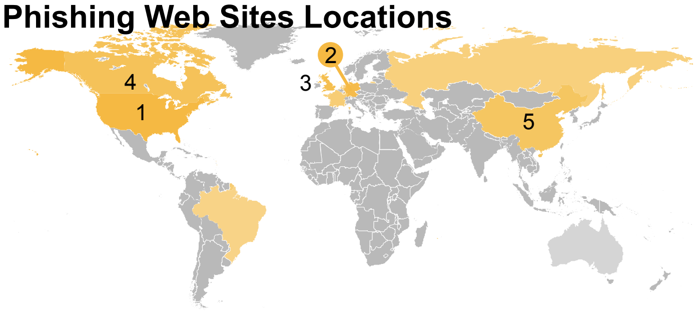
Analysis of Phishing Websites

The number of phishing Web sites increased by 6.67 percent this month, despite a small decline in the proportion of phishing emails blocked. Automated toolkits and unique domains increased as compared to the previous month. The number of phishing Web sites created by automated toolkits increased by 24.82 percent and the number of unique URLs increased slightly by 0.26 percent.

Phishing Web sites using IP addresses rather than domain names (e.g. domains like http://255.255.255.255) increased by 14.93 percent. Legitimate Web hosting services comprised 9 percent of all phishing, a decrease of 17.66 percent from the previous month. The number of non-English phishing sites saw an increase of 17.73 percent. Among non-English phishing sites, Portuguese, French, Italian and Spanish were the highest in May.

Geographic Location of Phishing Web Sites

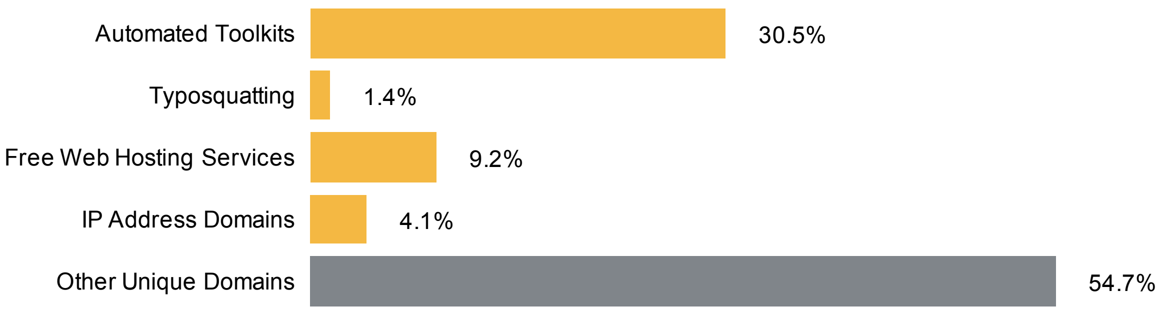
Phishing Web Sites Locations



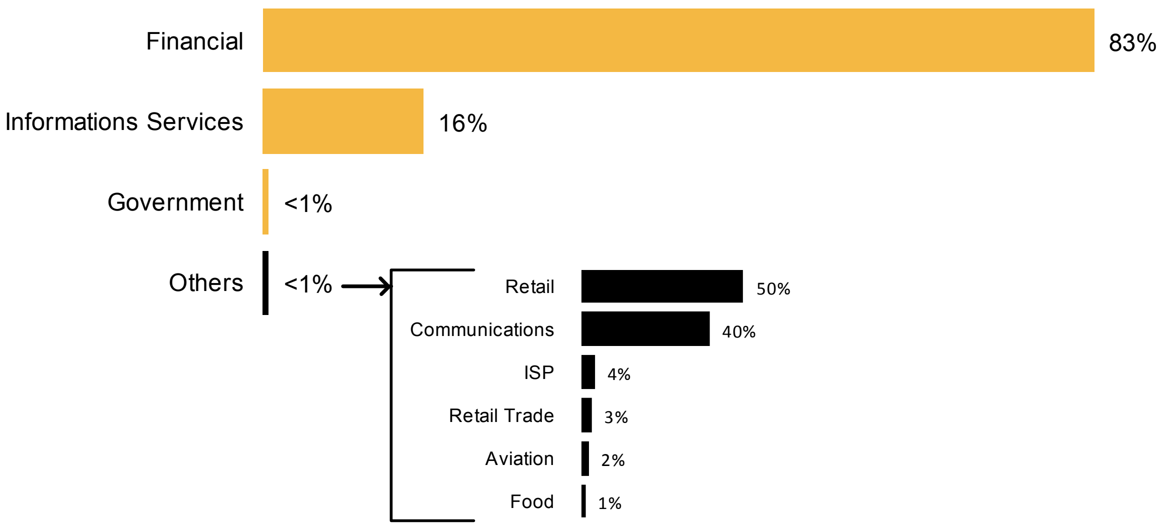
Country	May	April	Change (% points)
United States	51%	51%	
Germany	6%	7%	-1
United Kingdom	4%	5%	-1
Canada	4%	3%	1
China	3%	unlisted	N/A
Colombia	3%	2%	1
France	2%	3%	-1
Russia	2%	2%	
Netherlands	2%	3%	-1
Brazil	2%	2%	

June 2011

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry Sector

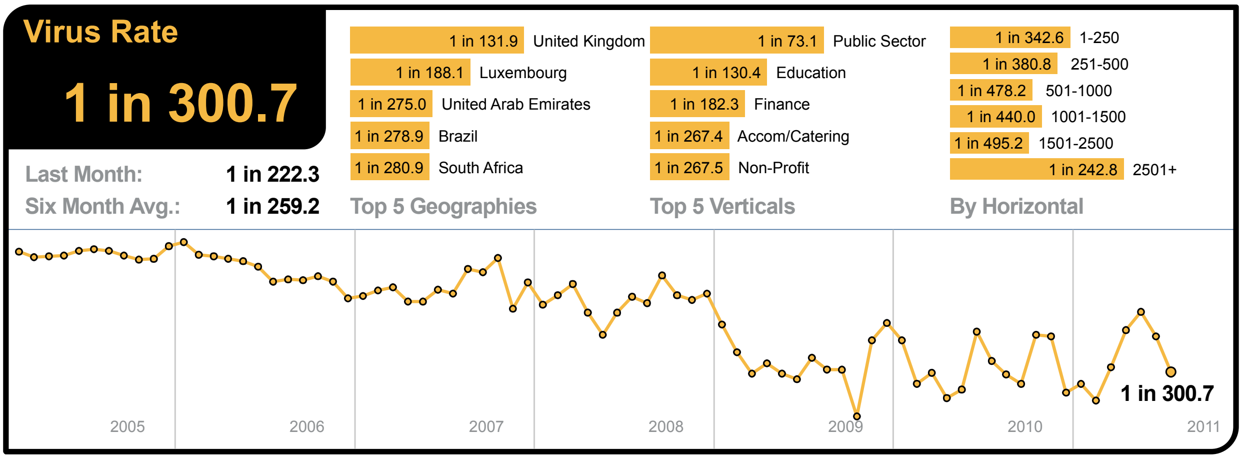


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 300.7 emails (0.333%) in June, a decrease of 0.117 percentage points since May 2011.

In June, 46.7% of email-borne malware contained links to malicious Web sites, an increase of 16.6 percentage points since May 2011. A large number of emails containing variants of Bredolab-related malware accounted for 12.3% of all email-borne malware. Many variants of which were commonly attached as ZIP files, rather than hyperlinks, and as the volume of these attacks diminished compared with the previous month, the relative proportion of attacks using hyperlinks increased.



June 2011

The UK remained the geography with the highest ratio of malicious emails in June, as one in 131.9 emails was blocked as malicious in June.

In the US, virus levels for email-borne malware were 1 in 805.2 and 1 in 297.7 for Canada. In Germany virus activity reached 1 in 721.0, 1 in 1,310 in Denmark and in The Netherlands 1 in 390.3. In Australia, 1 in 374.5 emails were malicious and 1 in 666.5 in Hong Kong; for Japan it was 1 in 2,114, compared with 1 in 946.7 in Singapore. In South Africa, 1 in 280.9 emails and 1 in 278.9 emails in Brazil contained malicious content.

With 1 in 73.1 emails being blocked as malicious, the Public Sector remained the most targeted industry in June. Virus levels for the Chemical & Pharmaceutical sector were 1 in 509.4 and 1 in 513.8 for the IT Services sector; 1 in 532.8 for Retail, 1 in 130.4 for Education and 1 in 182.3 for Finance.

The table below shows the most frequently blocked email-borne malware for June, many of which take advantage of malicious hyperlinks. Overall, 12.3% of email-borne malware was associated with Bredolab, Sasfis, SpyEye and Zeus variants.

Malware Name	% Malware
Exploit/SuspLink-d1f2	4.85%
Link-Trojan.Generic.5483393-4cac	2.89%
W32/NewMalware!836b	2.41%
W32/NewMalware!0575	2.39%
Exploit/Link-FakeAdobeReader-8069	2.32%
Trojan.Bredolab!eml-1f08	1.97%
Exploit/LinkAliasPostcard-d361	1.52%
W32/Packed.Generic-7946	1.46%
W32/Bredolab.gen!eml	1.36%
Exploit/FakeAttach-844a	1.39%

Web-based Malware Threats

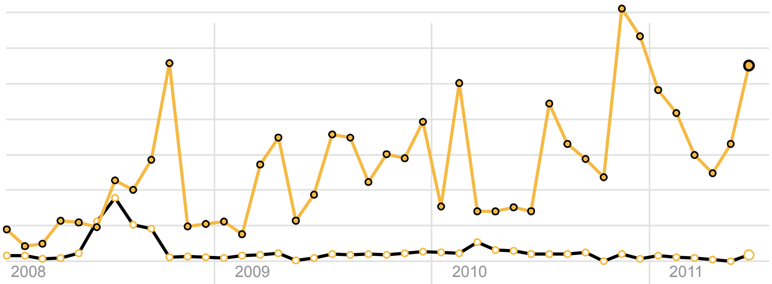
In June, MessageLabs Intelligence identified an average of 5,415 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 70.8% since May 2011. This reflects the rate at which Web sites are being compromised or created for the purpose of 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. The 70.8% rise marks a return to the highest rate since December 2010, as can be seen in the chart below; the rate had previously been diminishing during the first half of 2011.

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 35.1% of all malicious domains blocked were new in June; a decrease of 1.7 percentage points compared with May 2011. Additionally, 20.3% of all Web-based malware blocked was new in June; a decrease of 4.3 percentage points since the previous month.

Symantec.cloud Web Security Services Activity:

New Malware Sites per Day

New sites with **spyware**	196/day
New sites with **web viruses**	5,219/day
Total	**5,415/day**



June 2011

The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during June 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 45.0% of blocked Web activity in June. The second most frequently blocked traffic was categorized as Social Networking, and accounted for 15.8% of URL-based filtering activity blocked, equivalent to one in every 6.3 Web sites blocked.

Web Policy Risks from Inappropriate Use

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 8.6% of URL-based filtering blocks in June. 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 11.6 Web sites blocked.

Symantec.cloud Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	45.0%	Trojan:GIF/GIFrame.gen!A	21.1%	PUP:Zugo.C	63.5%
Social Networking	15.8%	Trojan:HTML/GIFrame.gen!B	19.2%	PUP:W32/CnsMin.S	7.3%
Streaming Media	8.6%	Packed.Generic.114	17.1%	PUP:Generic.171138	3.5%
Chat	3.8%	Infostealer.Gampass	7.0%	PUP:Zwunzi!gen3	3.2%
Peer-To-Peer	3.0%	Trojan.Generic.KD.232446	4.2%	PUP:Generic.168911	2.8%
Computing and Internet	2.9%	Exploit/Link-JavaScript-3f9f	2.9%	PUP:Clkpotato!gen2	2.4%
Search	2.0%	Trojan.Gen	2.2%	PUP:Generic.9001	1.9%
Games	2.0%	Trojan.Script.12023	2.1%	PUP:Generic.167772	1.9%
Hosting Sites	1.7%	W32.Almanahe.B	1.5%	PUP:Generic.175061	1.4%
Adult/Sexually Explicit	1.6%	Trojan.FakeAV	1.4%	PUP:Generic.178280	1.3%

June 2011

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers. 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 Web Security.cloud or Symantec Email AntiVirus.cloud.

Malware Name[7]	% Malware
W32.Ramnit!html	9.47%
W32.Sality.AE	8.49%
Trojan.Bamital	8.23%
W32.Ramnit.B!inf	7.59%
W32.DownadupageB	3.76%
W32.Virut.CF	2.70%
W32.Almanahe.B!inf	2.50%
W32.SillyFDC	1.99%
Trojan.ADH.2	1.91%
Trojan.ADH	1.90%
*Generic Detection**	*16.9%*

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[8], 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 17.4% of all malicious software blocked by endpoint protection technology in June.

For much of 2010, W32.Sality.AE had been the most prevalent malicious threat blocked at the endpoint; however, since May it has remained the second most prevalent malware blocked at the endpoint.

* *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 16.9% of the most frequently blocked malware last month was identified and blocked using generic detection.

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

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

Best Practice Guidelines for Enterprises

1. **Employ defense-in-depth strategies**: Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.

2. **Monitor for network threat, vulnerabilities and brand abuse.** Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious site reporting.

3. **Antivirus on endpoints is not enough:** On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including

   - Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
   - Browser protection for protection against obfuscated Web-based attacks;
   - Consider cloud-based malware prevention to provide proactive protection against unknown threats;
   - File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
   - Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
   - Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
   - Device control settings that prevent and limit the types of USB devices to be used.

4. **Use encryption to protect sensitive data:** Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

5. **Use Data Loss Prevention to help prevent data breaches:** Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.

6. **Implement a removable media policy**. Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

7. **Update your security countermeasures frequently and rapidly:** With more than 286M variants of malware detected by Symantec in 2010, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.

8. **Be aggressive on your updating and patching:** Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

9. **Enforce an effective password policy**. Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

10. **Restrict email attachments:** Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.

11. **Ensure that you have infection and incident response procedures in place**:
    - Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
    - Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
    - Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
    - Isolate infected computers to prevent the risk of further infection within the organization;
    - If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
    - Perform a forensic analysis on any infected computers and restore those using trusted media.

12. **Educate users on the changed threat landscape:**
    - Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
    - Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
    - Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
    - Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;
    - Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
    - Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
    - Only download software (if allowed) from corporate shares or directly from the vendors Web site;
    - If users see a warning indicating that they are “infected” after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.

Best Practice Guidelines for Users and Consumers

1. **Protect yourself**: Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:
   - Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;
   - Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
   - Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;
   - Browser protection to protect against obfuscated Web-based attacks;
   - Reputation-based tools that check the reputation and trust of a file and Web site before downloading; URL reputation and safety ratings for Web sites found through search engines.
2. **Keep up to date**: Keep virus definitions and security content updated at least daily if not hourly. By deploying the latest virus definitions, you can protect your computer against the latest viruses and malware known to be spreading in the wild. Update your operating system, Web browser, browser plug-ins, and applications to the latest updated versions using the automatic updating capability of your programs, if available. Running out-of-date versions can put you at risk from being exploited by Web-based attacks.
3. **Know what you are doing**: Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
   - Downloading “free” “cracked” or “pirated” versions of software can also contain malware or include social engineering attacks that include programs that try to trick you into thinking your computer is infected and getting you to pay money to have it removed.
   - Be careful which Web sites you visit on the Web. While malware can still come from mainstream Web sites, it can easily come from less reputable sites sharing pornography, gambling and stolen software.
   - Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.
4. **Use an effective password policy:** Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or Web sites. Use complex passwords (upper/lowercase and punctuation) or passphrases.
5. **Think before you click**: Never view, open, or execute any email attachment unless you expect it and trust the sender. Even from trusted users, be suspicious.
   - Be cautious when clicking on URLs in emails, social media programs even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using previews or plug-ins.
   - Do not click on links in social media applications with catchy titles or phrases even from friends. If you do click on the URL, you may end up “liking it” and sending it to all of your friends even by clicking anywhere on the page. Close or quit your browser instead.
   - Use a Web browser URL reputation solution that shows the reputation and safety rating of Web sites from searches. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
   - Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor’s Web site.
6. **Guard your personal data**: Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested and used in malicious activities such as targeted attacks, phishing scams.
   - Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.

About Symantec.cloud Intelligence

Symantec.cloud Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud 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. 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.

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.