Symantec Intelligence Report: January 2012

Spammers seek to take advantage of New Year holidays and events.

Welcome to the January edition of the Symantec Intelligence report which, 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 report includes data from December 2011 and January 2012.

Report highlights

- Spam – 69.0 percent (an increase of 1.3 percentage points since December 2011): page 5
- Phishing – One in 370.0 emails identified as phishing (an increase of 0.06 percentage points since December 2011): page 7
- Malware – One in 295.0 emails contained malware (a decrease of 0.02 percentage points since December 2011): page 9
- Malicious Web sites – 2,102 Web sites blocked per day (a decrease of 77.4 percent since December 2011): page 11
- Spammers continue to take advantage of holidays and events: page 2
- Best Practices for Enterprises and Users: page 14

Introduction

As this is the first edition of the Symantec Intelligence report for 2012, I would like to take this opportunity to wish you a very happy and malware-free New Year. As you will see from the main topic of this report, The New Year is an opportune time for spammers to take advantage of one of the major notable dates in the calendar.

In the most recent examples, cited in this report, spammers have taken advantage of compromised Web sites in order to redirect people to their own spam Web sites. The compromised Web sites are used to host a PHP redirect script, frequently containing a reference to New Year in the name of the file, as an element of the social engineering used to lure the recipient into clicking on the link. Other notable events coming-up in 2012 are likely to become more exploited in spam, phishing and malware as the year draws on, including the Chinese New Year, St. Valentine's Day in February and the London Olympics in June.

In December, global spam levels reached 67.7 percent, 2.8 percentage points lower than the November figure of 70.5 percent. However, spam activity increased by 1.3 percentage points in January, gradually returning to similar levels as November 2011, which was lower than the average in 2011. There have been a number of pressures on spammers throughout 2011 and as a result they are now using more targeted approaches and continue to exploit social media as alternatives to email.

I hope you enjoy reading this month's edition of the report, and please feel free to contact me directly with any comments or feedback.

Paul Wood, Senior Intelligence Analyst
paul_wood@symantec.com
@paulowoody

Report analysis

Spammers continue to take advantage of holidays and events

Beginning on New Year's Eve, January 1, 2012 and continuing earlier into the days following, Symantec Intelligence identified spammers taking advantage of the New Year anniversary, seemingly to entice users into clicking on spam links contained in the email messages.

Further investigation revealed that spammers were compromising legitimate Web servers, leaving the main Web site content intact (to avoid or delay detection) and simply adding a simple PHP script, typically named "HappyNewYear.php", "new-year-link.php" or "new-year.link.php". These scripts simply redirect to a spam pharmaceutical Web site.

Analysis of one of the messages we saw using these links makes the spammers' motives clearer, as can be seen in figure 1, below.
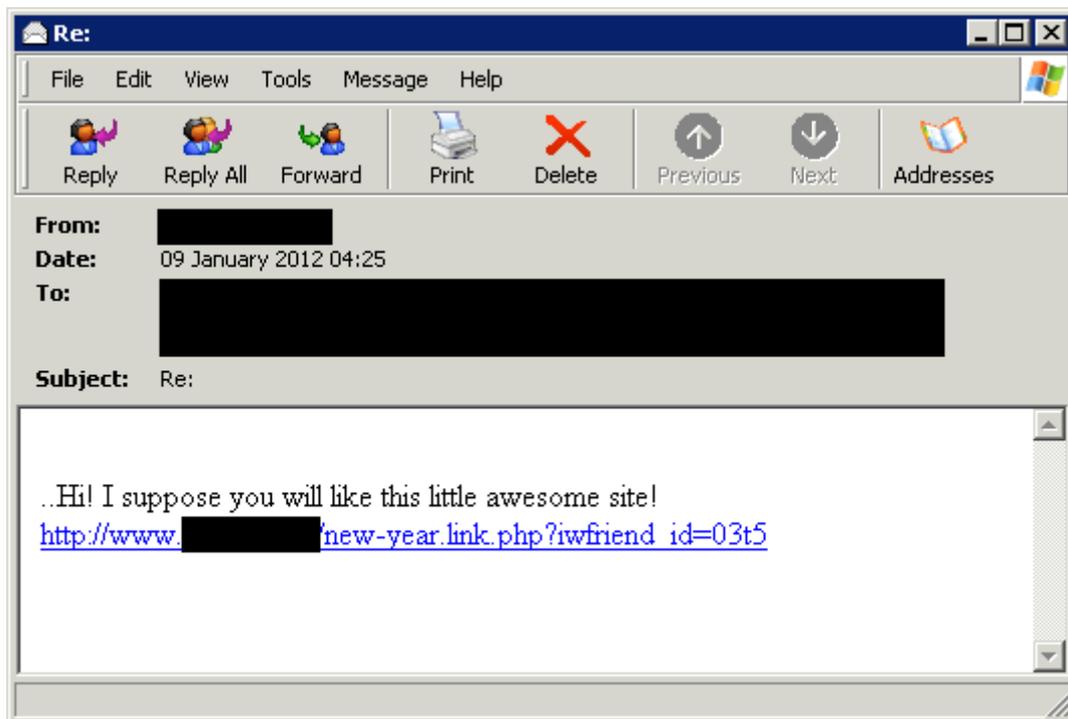

Figure 1: Example spam email containing New Year reference in spam URL

The message uses social engineering techniques to try to entice the recipient to open the link. The `friend_id` parameter in the URL could perhaps suggest that the destination is some kind of social networking Web site.

In addition, around New Year, many Web sites and blogs publish various "top ten" lists of the past year, their predictions for the coming year, so a URL containing the phrase "new year" may seem more relevant and topical, and may increase the likelihood of it being opened.

However, this is just the social engineering element, and the URL redirects (through a compromised machine) to a familiar spammer "My Canadian Pharmacy" Web site, as can be seen in figure 2, below.

Figure 2: Example spam Web site redirected from New Year spam URL

Symantec Intelligence has seen over 10,000 unique domain names compromised with this "new year link" redirect script. It is likely that files called "new-year-link.php" or similar are likely to indicate that the Web server has been compromised; perhaps serving as a timely reminder to ensure all servers are properly patched and updated.

This is just the latest example of spammers using holidays and current events to try to make their mails more appealing. In the run-up to Christmas in 2011, spammers spoofed a number of legitimate retailers, offering Christmas special offers and deals on a variety of products (typically counterfeit watches and drugs). As we've separately covered in the Symantec Intelligence Report and in some of our blogs, 419 or advance fee fraud scammers are also skilled at using notable holidays, anniversaries and current events to their advantage, for example, there was an increase in the number of scams relating to the devastating earthquake in Japan last year, and the "Arab spring" movement, as well as many others.

January 23 also sees the start of Chinese New Year (also referred to as "Spring Festival") celebrations. With celebrations continuing for several days, it is the most important traditional Chinese holiday, and is also celebrated in many countries and territories with significant Chinese populations. The huge interest in this event (to celebrate the "Year of the Dragon") means that spammers and malware authors are likely to try to exploit this annual festivity. Symantec Intelligence also expects to see spammers taking advantage of the fast-approaching Valentine's Day. It is likely that pharmaceutical spammers will take advantage of the day's romantic connotations, typically to promote their erectile dysfunction drugs, while malware authors are likely to use the popular idea of having a secret admirer to lure victims into unwittingly installing malware.

Following Valentine's Day, we also expect to see plenty of spam and malware taking advantage of the upcoming UEFA Euro 2012 football tournament, jointly hosted by Ukraine and Poland. Once UEFA Euro 2012 is over, it's not long until the Summer Olympics in London. Indeed we have already seen many references to the games in 419 or advance fee fraud messages. These messages have included attachments such as "London 2012 Olympic Games.doc", "LONDON 2012 OLYMPIC GAMES RAFFLE PROGRAM.doc", "LONDON OLYMPICS LOTTERY WINNER!.doc," to name but a few examples, such as the one shown in figure 3, below.
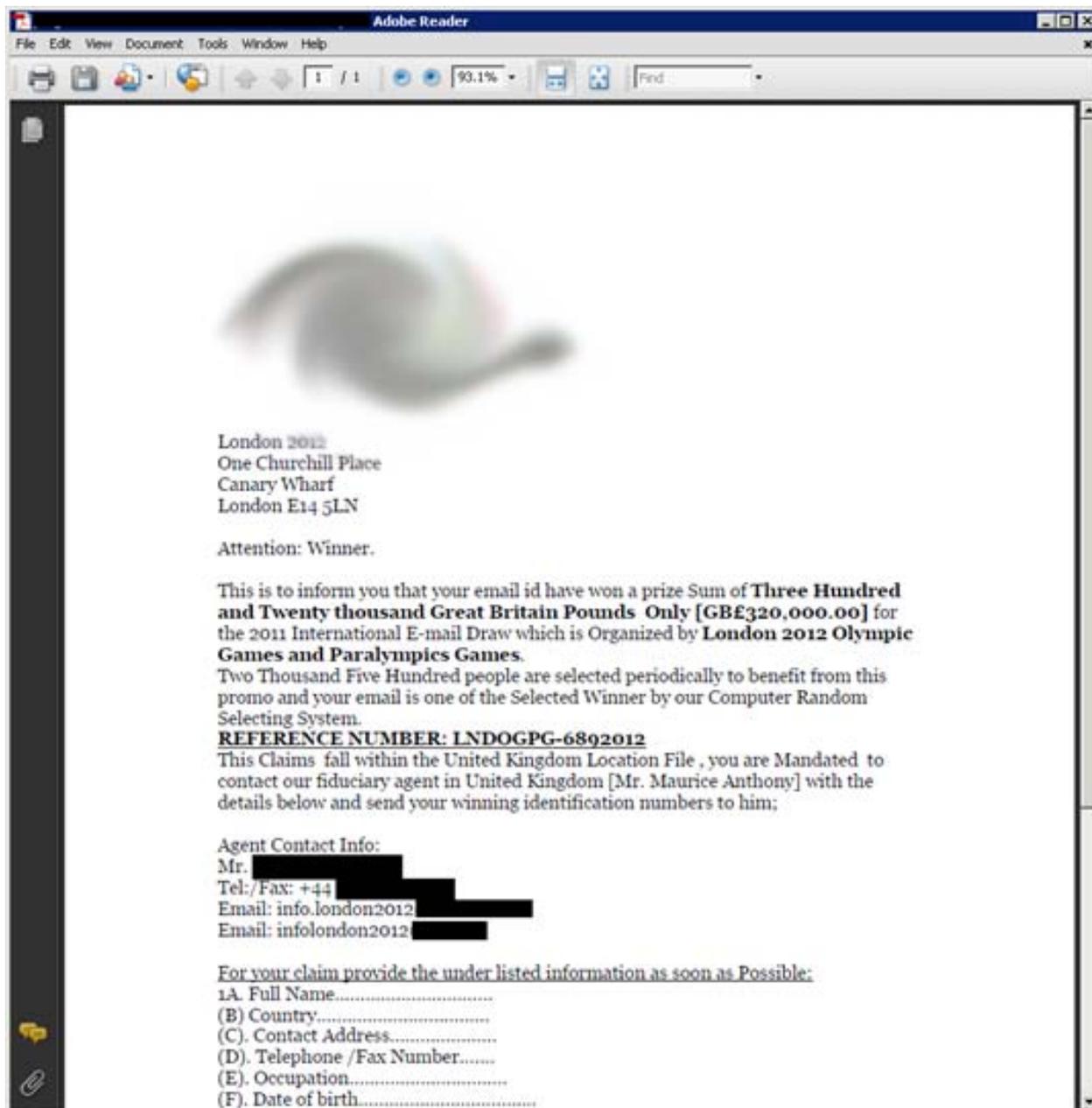
London 2012
One Churchill Place
Canary Wharf
London E14 5LN

Attention: Winner.

This is to inform you that your email id have won a prize Sum of **Three Hundred and Twenty thousand Great Britain Pounds Only [GB£320,000.00]** for the 2011 International E-mail Draw which is Organized by **London 2012 Olympic Games and Paralympics Games**.
Two Thousand Five Hundred people are selected periodically to benefit from this promo and your email is one of the Selected Winner by our Computer Random Selecting System.
REFERENCE NUMBER: LNDOGPG-6892012
This Claims fall within the United Kingdom Location File , you are Mandated to contact our fiduciary agent in United Kingdom [Mr. Maurice Anthony] with the details below and send your winning identification numbers to him;

Agent Contact Info:
Mr.
Tel:/Fax: +44
Email: info.london2012
Email: infolondon2012

For your claim provide the under listed information as soon as Possible:
1A. Full Name...............................
(B) Country...............................
(C). Contact Address......................
(D). Telephone /Fax Number........
(E). Occupation...........................
(F). Date of birth........................

Figure 3: Example 419 spam referencing a major sporting event

By relating their mails to widely-celebrated holidays and current events with global interest, spammers and malware authors can (at first glance at least) make their messages more interesting, and increase the chance of recipients visiting spam Web sites or becoming infected.

Therefore, as major events draw closer, such as notably St. Valentine's Day and the London Olympic Games, the social engineering employed by spammers will almost certainly be adapted to take advantage of people's interest in these events. We expect there to be an increase not only in spam activity relating to these events, but also in scams and 419 frauds as well. With legitimate Web servers being exploited in many of these latest attacks, it is especially important to remain vigilant and ensure that businesses adhere to a best practice for patching and maintaining Web and other potentially vulnerable servers.

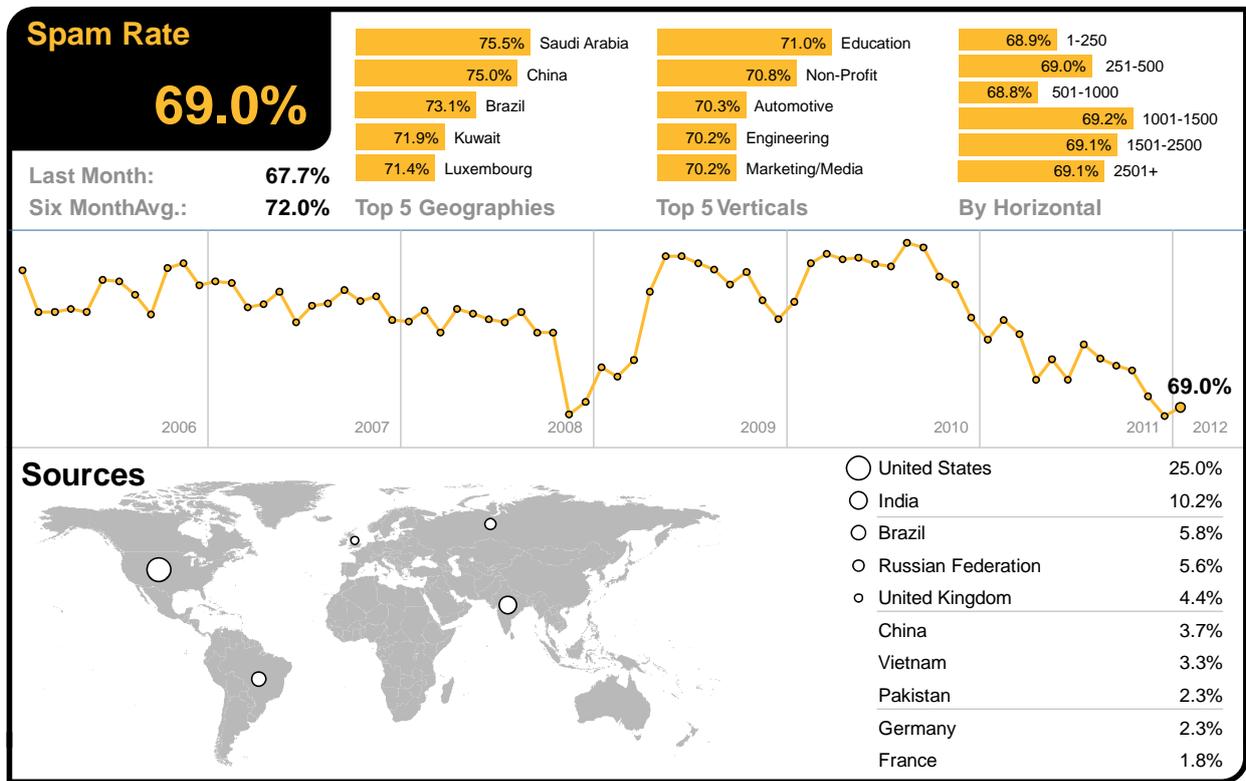✓Symantec.

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 from over 8 billion email messages and over 1 billion Web requests, which are processed per day across 15 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 January 2012, the global ratio of spam in email traffic rose by 1.3 percentage points since December 2011, to 69.0 percent (1 in 1.45 emails). This follows a more noticeable drop in December when spam fell by 2.8 percentage points to 67.7 percent. Consequently, this recent increase means that spam has almost returned to the same level as in November 2011.

Spam Rate		
69.0%		

| Last Month: | **67.7%** |
| Six MonthAvg.: | **72.0%** |

Top 5 Geographies	
75.5%	Saudi Arabia
75.0%	China
73.1%	Brazil
71.9%	Kuwait
71.4%	Luxembourg

Top 5 Verticals	
71.0%	Education
70.8%	Non-Profit
70.3%	Automotive
70.2%	Engineering
70.2%	Marketing/Media

By Horizontal	
68.9%	1-250
69.0%	251-500
68.8%	501-1000
69.2%	1001-1500
69.1%	1501-2500
69.1%	2501+

69.0% (2012)

Sources

United States	25.0%
India	10.2%
Brazil	5.8%
Russian Federation	5.6%
United Kingdom	4.4%
China	3.7%
Vietnam	3.3%
Pakistan	2.3%
Germany	2.3%
France	1.8%

January 2012

As the global spam rate increased, Saudi Arabia became the most spammed geography in January; with a spam rate of 75.5 percent and China was the second most-spammed with 75.0 percent of email traffic blocked as spam.

In the US, 69.0 percent of email was spam and 68.7 percent in Canada. The spam level in the UK was 69.3 percent. In The Netherlands, spam accounted for 70.7 percent of email traffic, 68.2 percent in Germany, 69.1 percent in Denmark and 68.6 percent in Australia. In Hong Kong, 67.5 percent of email was blocked as spam and 66.7 percent in Singapore, compared with 65.6 percent in Japan. Spam accounted for 69.5 percent of email traffic in South Africa and 73.1 percent in Brazil.

✓ Symantec.

Moreover, the Education sector became the most spammed industry sector in January, with a spam rate of 71.0 percent. The spam rate for the Chemical & Pharmaceutical sector was 69.0 percent, compared with 68.7 percent for IT Services, 68.4 percent for Retail, 68.9 percent for Public Sector and 68.2 percent for Finance.

The spam rate for small to medium-sized businesses (1-250) was 68.9%, compared with 69.1% for large enterprises (2500+).

Global Spam Categories

The most common category of spam in January was pharmaceutical related, but the second most common was related to watches/jewelry spam. Examples of many of these subjects can be found in the subject line analysis, below.

Category Name	January 2012	November 2011
Pharmaceutical	38.0%	32.5%
Watches/Jewelry	27.5%	19.5%
Adult/Sex/Dating	22.5%	12.5%
Weight Loss	3.5%	8.0%
Unsolicited Newsletters	2.5%	17.5%
Casino/Gambling	2.0%	2.0%
Unknown/Other	1.5%	4.0%
Software	0.5%	2.0%
Scams/Fraud/419	0.5%	1.5%
Degrees/Diplomas	0.5%	<0.5%
Jobs/Recruitments	0.5%	<0.5%
Malware	<0.5%	<0.5%
Phishing	<0.5%	<0.5%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com and .info top-level domains increased in January, as highlighted in the table below.

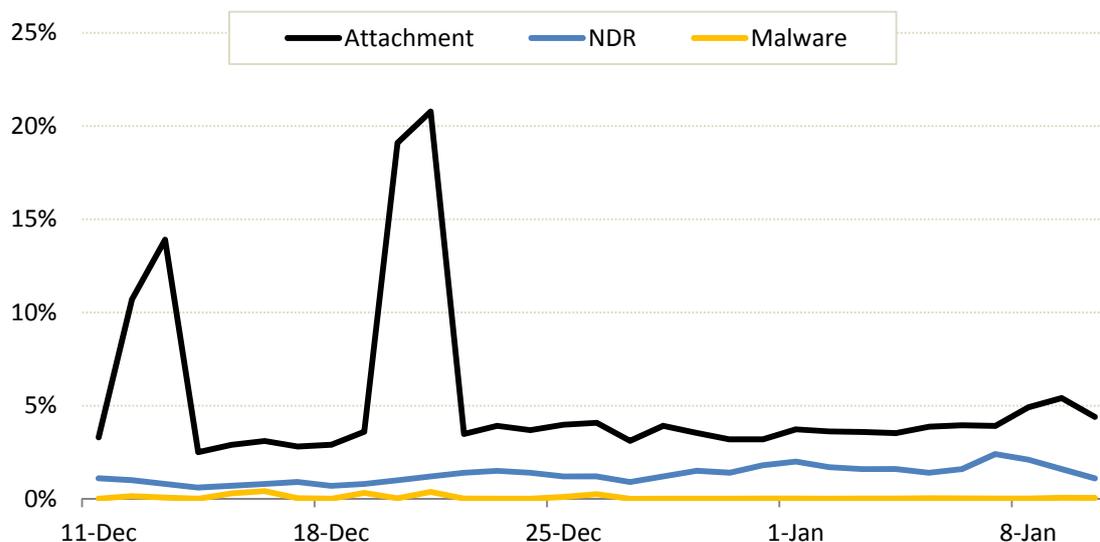| TLD	January 2012	November 2011
.com	57.8%	55.1%
.ru	9.4%	9.4%
.info	6.9%	N/A
.org	6.6%	7.4%

Average Spam Message Size

In January, the proportion of spam emails that was 5Kb in size or less decreased; however, the proportion of spam messages that were greater than 10Kb in size increased, as can be seen in the following table.

Message Size	January 2012	November 2011
0Kb – 5Kb	55.7%	57.8%
5Kb – 10Kb	30.5%	31.2%
>10Kb	13.8%	11.0%

✓Symantec.™

Spam Attack Vectors

The proportion of spam that contained a malicious attachment or link was much less than was observed during the previous month, with only two major spikes of spam activity during the first half of the period. The frequency of attacks has diminished significantly since the end of December 2011. Many of these larger attachments were related to generic polymorphic malware variants, as discussed in many previous[1] Symantec Intelligence reports.
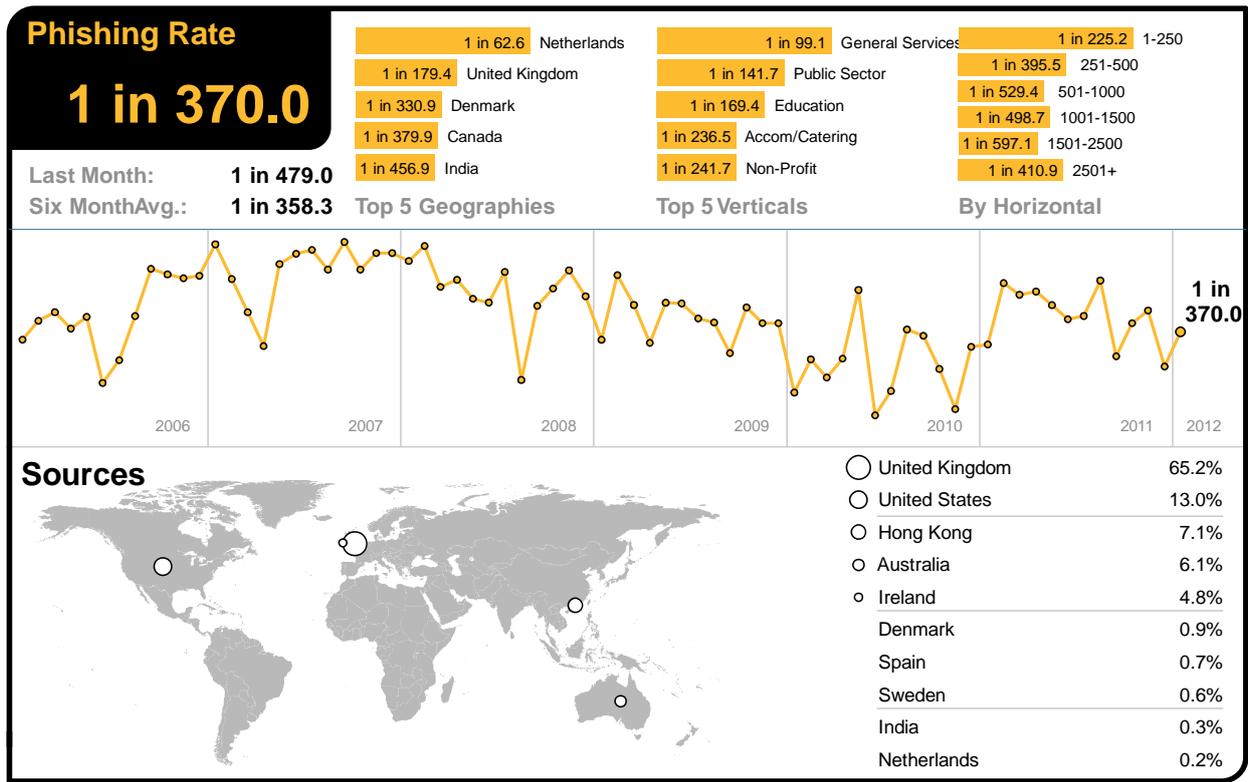

In January, the number of spam emails resulting in NDRs (spam related non-delivery reports), has been consistently stable and low, suggesting the attackers may be using valid email distribution lists to conduct these attacks, and using more targeted approaches. NDR spam is often as a result of widespread dictionary attacks during spam campaigns, where spammers make use of databases of first and last names and combine them to generate random email addresses. This low-level of activity is indicative of spammers that are seeking to maintain their distribution lists in order to minimize bounce-backs; IP addresses are more likely to appear on anti-spam block-lists if they become associated with a high volume of invalid recipient emails.

✓Symantec™

Phishing Analysis

In January, the global phishing rate increased by 0.06 percentage points, taking the average to one in 370.0 emails (0.27 percent) that comprised some form of phishing attack.

Phishing Rate		
1 in 370.0		

1 in 62.6 Netherlands	
1 in 179.4 United Kingdom	
1 in 330.9 Denmark	
1 in 379.9 Canada	
1 in 456.9 India	

1 in 99.1 General Services	
1 in 141.7 Public Sector	
1 in 169.4 Education	
1 in 236.5 Accom/Catering	
1 in 241.7 Non-Profit	

1 in 225.2 1-250	
1 in 395.5 251-500	
1 in 529.4 501-1000	
1 in 498.7 1001-1500	
1 in 597.1 1501-2500	
1 in 410.9 2501+	

Last Month:	**1 in 479.0**
Six MonthAvg.:	**1 in 358.3**

Top 5 Geographies   Top 5 Verticals   By Horizontal

2006   2007   2008   2009   2010   2011   2012

1 in 370.0

Sources

◯ United Kingdom	65.2%
◯ United States	13.0%
◯ Hong Kong	7.1%
◯ Australia	6.1%
◯ Ireland	4.8%
Denmark	0.9%
Spain	0.7%
Sweden	0.6%
India	0.3%
Netherlands	0.2%

January 2012

The Netherlands became the country most targeted for phishing attacks in January, with one in 62.6 emails identified as phishing. The UK was the second most targeted country, with one in 179.4 emails identified as phishing attacks.

Phishing levels for the US were one in 1,145 and one in 379.9 for Canada. In Germany phishing levels were one in 797.6, one in 330.9 in Denmark. In Australia, phishing activity accounted for one in 542.2 emails and one in 942.9 in Hong Kong; for Japan it was one in 5,692 and one in 1,156 for Singapore. In Brazil one in 1,007 emails was blocked as phishing.

The Public Sector remained the most targeted by phishing activity in January, with one in 99.1 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 838.0 and one in 647.8 for the IT Services sector, one in 529.4 for Retail, one in 169.4 for Education and one in 253.7 for Finance.

Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 225.2 emails, compared with one in 410.9 for large enterprises (2500+).
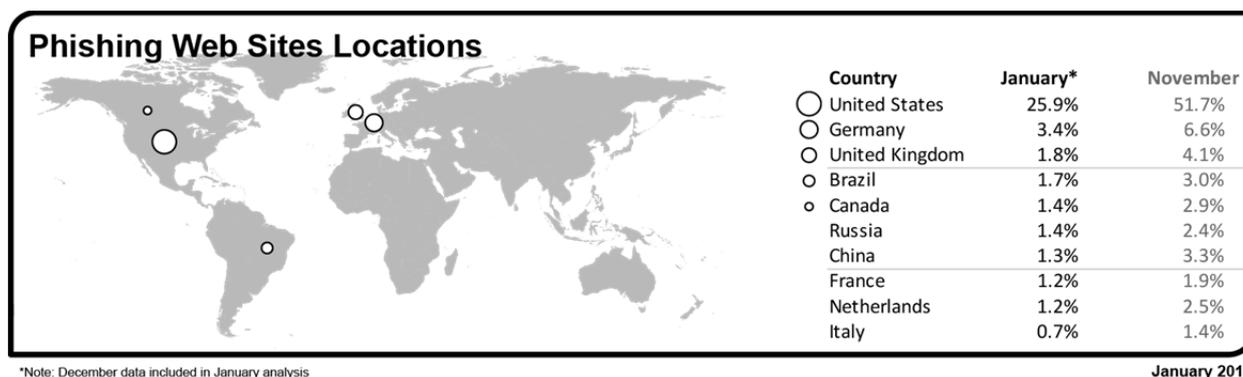
Analysis of Phishing Web sites

The number of phishing Web sites decreased by 18.2 percent in January. The number of phishing Web sites created by automated toolkits decreased by approximately 41.4 percent, accounting for approximately 42.6 percent of phishing Web sites, including attacks against well-known social networking Web sites and social networking apps.

The number of unique phishing domains increased by 15.9 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), increased by 78.0 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 5.9 percent of all phishing Web sites, an increase of 21.2 percent from the previous month. The number of non-English phishing Web sites increased by 41.5 percent.

Of the non-English phishing Web sites Portuguese, Italian, French and Spanish were among the highest in January.
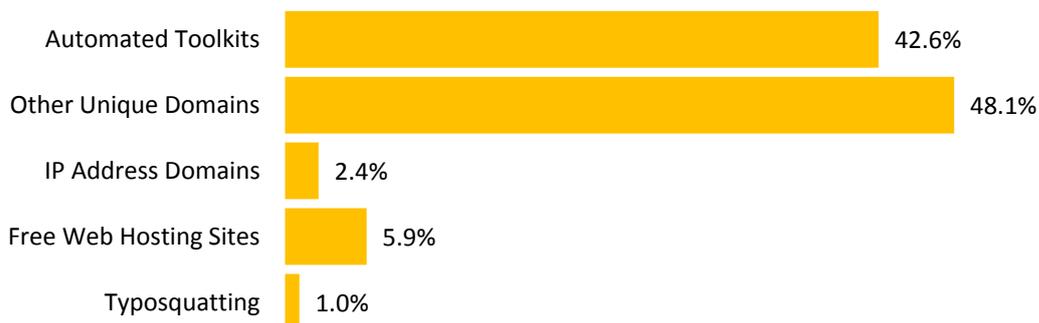
✓Symantec.™
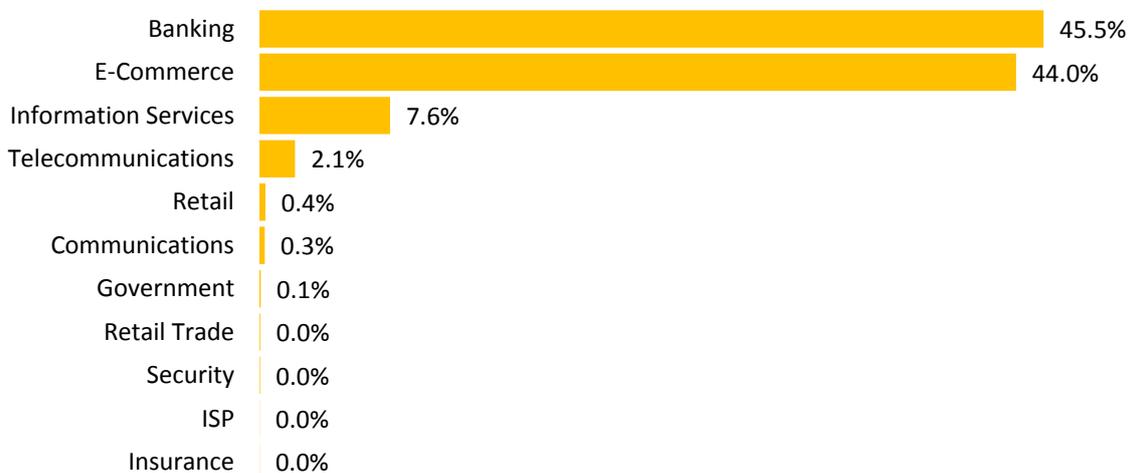
Geographic Location of Phishing Web Sites

Phishing Web Sites Locations

Country	January*	November
United States	25.9%	51.7%
Germany	3.4%	6.6%
United Kingdom	1.8%	4.1%
Brazil	1.7%	3.0%
Canada	1.4%	2.9%
Russia	1.4%	2.4%
China	1.3%	3.3%
France	1.2%	1.9%
Netherlands	1.2%	2.5%
Italy	0.7%	1.4%

*Note: December data included in January analysis

January 2011

Tactics of Phishing Distribution

Automated Toolkits	42.6%
Other Unique Domains	48.1%
IP Address Domains	2.4%
Free Web Hosting Sites	5.9%
Typosquatting	1.0%

Organizations Spoofed in Phishing Attacks, by Industry

Banking	45.5%
E-Commerce	44.0%
Information Services	7.6%
Telecommunications	2.1%
Retail	0.4%
Communications	0.3%
Government	0.1%
Retail Trade	0.0%
Security	0.0%
ISP	0.0%
Insurance	0.0%

Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 295.0 emails (0.33 percent) in January, a decrease of 0.02 percentage points since December 2011.

In January, 29.0 percent of email-borne malware contained links to malicious Web sites, unchanged since December 2011.

Virus Rate			
1 in 295.0			

Top 5 Geographies	Top 5 Verticals	By Horizontal
1 in 61.4 Netherlands	1 in 90.2 Public Sector	1 in 277.3 1-250
1 in 169.1 United Kingdom	1 in 138.3 Education	1 in 294.8 251-500
1 in 205.4 Luxembourg	1 in 203.8 Non-Profit	1 in 349.1 501-1000
1 in 278.0 India	1 in 229.9 Marketing/Media	1 in 325.6 1001-1500
1 in 285.4 Canada	1 in 236.7 Finance	1 in 393.8 1501-2500
		1 in 281.5 2501+

Last Month: 1 in 278.6
Six MonthAvg.: 1 in 242.9

2006   2007   2008   2009   2010   2011   2012

1 in 295.0

Sources

◯	United States	47.1%
◯	United Kingdom	36.1%
◯	India	3.0%
○	Australia	2.3%
○	Netherlands	1.8%
	Ireland	1.8%
	Sweden	1.5%
	Hong Kong	0.9%
	France	0.9%
	Canada	0.6%

January 2012

The Netherlands was besieged with the highest ratio of malicious emails in January, with one in 61.4 emails identified as malicious. The UK had the second highest rate, with one in 169.1 emails identified as malicious.

In South Africa, one in 305.9 emails was blocked as malicious. The virus rate for email-borne malware in the US was one in 592.5 and one in 285.4 in Canada. In Germany virus activity reached one in 471.7 and one in 318.1 in Denmark. In Australia, one in 327.9 emails was malicious. For Japan the rate was one in 1,573, compared with one in 482.9 in Singapore. In Brazil, one in 681.7 emails in contained malicious content.

With one in 90.2 emails being blocked as malicious, the Public Sector remained the most targeted industry in January. The virus rate for the Chemical & Pharmaceutical sector reached one in 381.3 and one in 399.4 for the IT Services sector; one in 407.1 for Retail, one in 138.3for Education and one in 236.7 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 277.3 emails, compared with one in 281.5 for large enterprises (2500+).

✓Symantec.™

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for January, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 28.7 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware, such as Bredolab, Zeus and SpyEye, accounted for 22.0 percent of all email-borne malware blocked in January; equivalent to 76.8 percent of all generic malware blocked.

Malware Name	% Malware
Exploit/SpoofBBB	7.31%
Exploit/Link-generic-ee68	6.71%
Suspicious.JIT.a	4.36%
VBS/Generic	4.20%
Exploit/LinkAliasPostcard-4733	2.79%
Trojan.Bredolab	2.10%
Trojan.Bredolab!eml-3a2a	1.58%
HeurAuto-14d6	1.55%
W32/Zbot-gen-c30b-54b2	1.47%
Link-Trojan.IFrame.QZ-544e	1.42%

The top ten list of most frequently blocked malware accounted for approximately 33.5% of all email-borne malware blocked in January.

Web-based Malware Threats

In January, Symantec Intelligence identified an average of 2,102 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 77.4 percent since December 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 39.9 percent of all malicious domains blocked were new in January; a decrease of 4.8 percentage points compared with December 2011. Additionally, 15.2 percent of all Web-based malware blocked was new in January; an increase of 0.7 percentage points since December 2011.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware	26/day
New sites with web viruses	2,076/day
Total	**2,102/day**

January 2012

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

Web Policy Risks from Inappropriate Use

The most common trigger for policy-based filtering applied by Symantec Web Security.cloud for its business clients was for the "Advertisements & Popups" category, which accounted for 32.4 percent of blocked Web activity in January. Web-based advertisements pose a potential risk though the use of "malvertisements," or malicious

advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless Web site.

The second most frequently blocked traffic was categorized as Social Networking, accounting for 19.4 percent of URL-based filtering activity blocked, equivalent to approximately one in every 5 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 11.0 percent of URL-based filtering blocks in January. Streaming media is increasingly popular when there are major sporting events or high profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This rate is equivalent to one in every 9 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	32.4%	JS:Trojan.Script.DR	25.3%	PUP:JS.Script.C	21.4%
Social Networking	19.4%	Trojan.JS.WPress.A	18.2%	PUP:MyWebSearch.EC	14.1%
Streaming Media	11.0%	Gen:Variant.Graftor.8369	5.2%	PUP:9231	11.9%
Computing and Internet	4.5%	Trojan.Maljava	3.5%	PUP:Clkpotato!gen3	10.6%
Search	4.0%	Trojan.Script.475646	3.1%	PUP:Generic.183433	9.3%
Chat	3.1%	Trojan.ADH.2	2.4%	PUP:Generic.62006	5.3%
Hosting Sites	2.9%	Trojan.Gen.2	2.0%	PUP:Relevant.BH	3.4%
Games	2.7%	JS.AddedIframe	1.9%	PUP:Generic.183457	2.3%
Peer-To-Peer	2.3%	Trojan.Malscript!html	1.8%	PUP:Generic.391406	1.9%
News	2.0%	Trojan.Script.12023	1.7%	PUP:Generic.376539	1.5%

January 2012

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[2]	% Malware
WS.Trojan.H	26.52%
W32.Sality.AE	6.09%
W32.Ramnit!html	5.88%
W32.Ramnit.B!inf	5.75%
W32.Ramnit.B	5.18%
W32.Downadup.B	2.63%
W32.Virut.CF	1.65%
W32.Almanahe.B!inf	1.63%
Trojan.ADH.2	1.50%
W32.SillyFDC	1.40%

---

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

✓Symantec™

The most frequently blocked malware for the last month was WS.Trojan.H[3]. WS.Trojan.H is generic cloud-based heuristic detection for files that posses characteristics of an as yet unclassified threat. Files detected by this heuristic are deemed by Symantec to pose a risk to users and are therefore blocked from accessing the computer.

For much of 2011, variants of W32.Sality.AE[4] and W32.Ramnit[5] had been the most prevalent malicious threat blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 17.0% of all malware blocked at the endpoint in January, compared with 6.8% for all variants of W32.Sality.

Ramnit has also recently been implicated in the theft of identities from major social networking Web sites. It was reported that many of these stolen credentials used to distribute malicious links via the profile pages of the affected users, heightening the risk for those users who shared the same password for several online accounts, potentially providing the attackers with a springboard into corporate networks.

Approximately 13.5 percent of the most frequently blocked malware last month was identified and blocked using generic detection. 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's 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.

---

[3] *http://www.symantec.com/security_response/writeup.jsp?docid=2011-102713-4647-99*

[4] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*

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

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 Web 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:

   o Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;

   o Browser protection for protection against obfuscated Web-based attacks;

   o Consider cloud-based malware prevention to provide proactive protection against unknown threats;

   o 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;

   o Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;

   o Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;

   o 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:**
    o 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;
    o 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;
    o Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
    o Isolate infected computers to prevent the risk of further infection within the organization;
    o If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
    o Perform a forensic analysis on any infected computers and restore those using trusted media.

12. **Educate users on the changed threat landscape:**
    o 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;
    o Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
    o Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
    o 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;
    o 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;
    o Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
    o Only download software (if allowed) from corporate shares or directly from the vendors Web site;
    o 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 Consumers

1. **Protect yourself**: Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

   o Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;

   o Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;

   o Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;

   o Browser protection to protect against obfuscated Web-based attacks;

   o 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.

   o 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.

   o 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 Web sites sharing pornography, gambling and stolen software.

   o 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.

   o 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.

   o 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.

   o 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.

   o 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 via social networks) as it may be harvested and used in malicious activities such as targeted attacks and phishing scams.

   o Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

✓Symantec™

- 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.