Symantec Intelligence Report: September 2011

Social Engineering Attacks Soar as Polymorphic Malware Rate Peaks at 72% of Email Malware in September; Cyber Criminals Ambush Popular Blogging Platform to Push Pills

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

Report highlights

Introduction

A deluge of malicious email-borne malware has left a clear mark on the threat landscape for September. Approximately 72% of all email-borne malware in September could be characterized as aggressive strains of generic polymorphic malware, first identified in the July[1] Symantec Intelligence Report. In July, this rate was 23.7%, falling slightly to 18.5% in August before soaring to 72% in September. This unprecedented high-water mark underlines the nature by which cyber criminals have escalated their assault on businesses in 2011, fully exploiting the weaknesses of more traditional security countermeasures.

The social engineering behind many of these attacks has also accelerated, with the adoption of a variety of new techniques such as pretending to be an email from a smart printer/scanner being forwarded by a colleague in the same organization. Many of these attacks continue to impersonate a variety of well-known, international parcel delivery services. The idea of an office printer sending malware is perhaps an unlikely one, as printers and scanners were not actually used in these attacks, but perhaps this sense of security is all that is required for such a socially engineered attack to succeed in the future.

Moreover, although spam levels remained fairly stable during September, spammers have identified vulnerabilities in certain older versions of the popular WordPress blogging software used on a large number of Web sites across the Internet. The exploitation of these vulnerabilities to serve the spammers' interests functions as a stark reminder for the

[1] *http://www.symanteccloud.com/mlireport/symcint_2011_07_july_final-en.pdf*

Symantec™

need to ensure software is up-to-date with latest patches and releases. It is important to note that blogs hosted by WordPress.com seem to be unaffected by these compromises.

Finally, we also take an in-depth look at why JavaScript has become an enduring favorite in the arsenal of cyber criminals and spammers alike, and how it is being used on the front lines in the continuing war between the good and the bad guys.

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

Malicious emails masquerade as office printer messages

Some of the newest printers have scan-to-email ability, a feature that allows users to email scanned documents to a specified email address on demand. Symantec Intelligence has identified malware authors using social engineering tactics that take advantage of this, sending executables in a compressed ".zip" archive via email. The attachment contains an executable disguised as a scanned document from a printer, as shown in the example in figure 1, below.

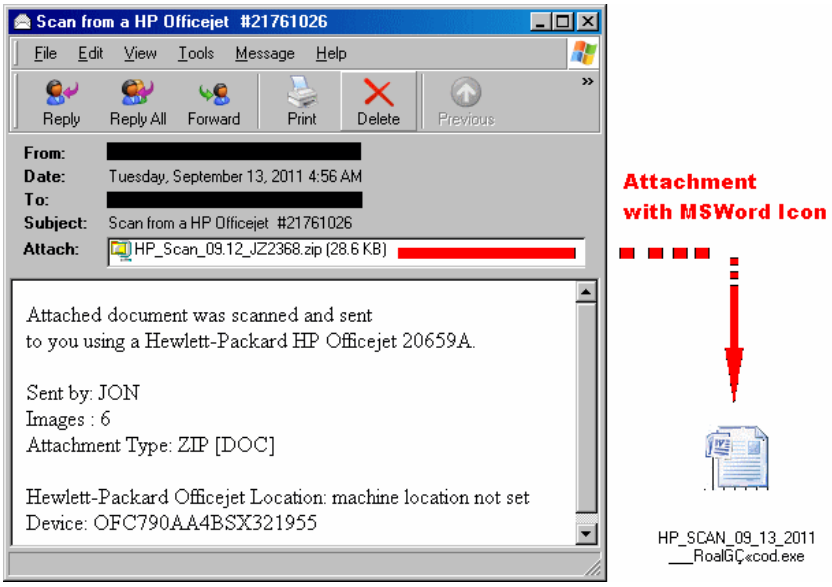


Figure 1: Example of malicious email masquerading as a scanned document sent from an office printer

In each case the sender domain was spoofed to match the recipient domain, sometimes appearing as though forwarded to the recipient by a colleague at the same organization, implying that this email originated internally.

To be clear, office printers and scanners will not send malware-laden files, and many are unlikely to be able to send scanned documents as ".zip" file attachments. No printer or scanner hardware was involved in the distribution process, and in general, users should always be careful when opening email attachments, especially from an unknown sender.

Some examples are shown in figure 2, below.

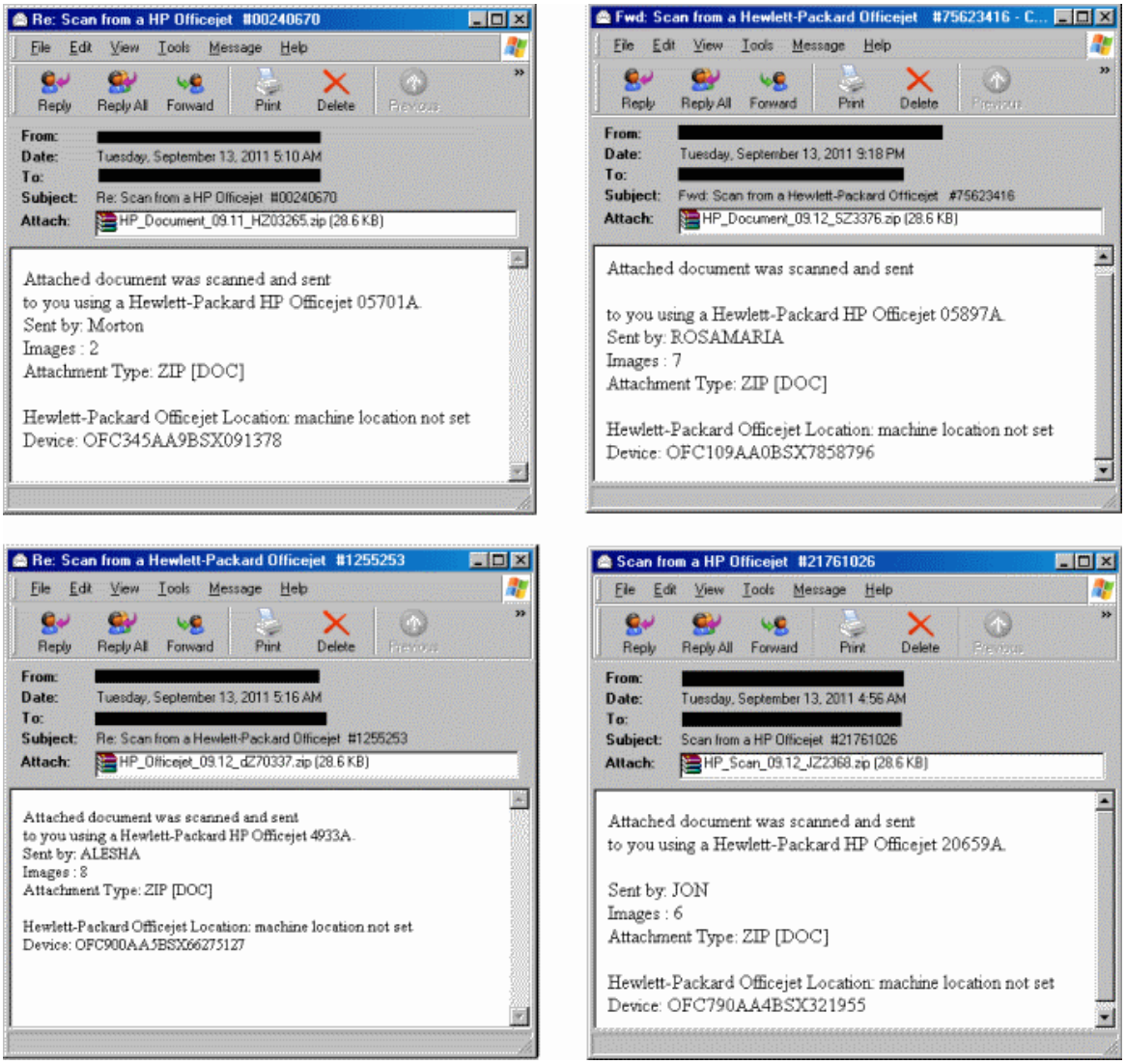


Figure 2: Examples of malicious emails spoofing smart office printer/scanners

In figure 3, Symantec Intelligence gathered some interesting statistics from observing these emails during a 24-hour period beginning 13 September 2011.

Subjects	Frequency	Unique Attachments
Scan from a **[printer name A]** #{6-8 random digits}	742	1,393
Scan from a **[printer name B]** #{6-8 random digits}	41	779

Figure 3: Table showing the frequency and number of different attachments spoofing a printer

In these examples, the attacker has also changed the file extension of the archived file in such a way as to display a ".doc" extension when viewed using certain archiving tools, as shown in figure 4, below.

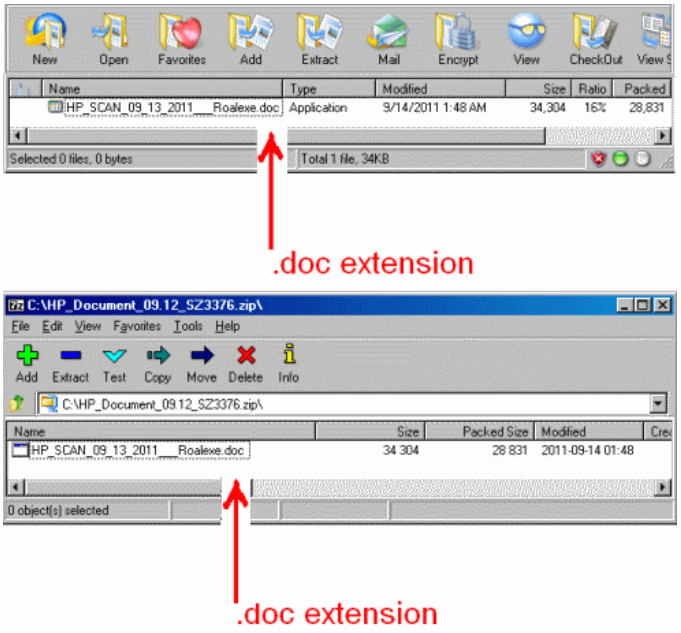


Figure 4: Example of ".zip" archive incorrectly displaying contents with ".doc" extension

The actual file name stored in the ".zip" archive is comprised of a "cod.exe" extension, but this is incorrectly displayed by some archiving tools because of a special hidden character (hex code 0xAB, highlighted below), which precedes the "cod.exe" part of the file name. This will result in the file being incorrectly displayed with "exe.doc" appended in the archive viewer.

In addition to the above examples, we have also seen the following example, which was the same strain of malware distributed using a number of different subjects and two different filenames; in one case a supposed document and another as a photograph, shown in figure 5, below.

File Name	Frequency
Document_NR727875272_Coll=d4=c7=abcod.exe	410
photo_W71765413082011_Coll=d4=c7=abgpj.exe	149

Figure 5: Table showing the frequency of another example

As before, the file name ending with "cod.exe" will be incorrectly displayed using some ".zip" archive viewing tools as "exe.doc" and similarly, "gpj.exe" will display as "exe.jpg."

In figure 6, below are some examples of other interesting subject lines that were also used to distribute this particular malware run during the same 24-hour period, beginning 13 September.

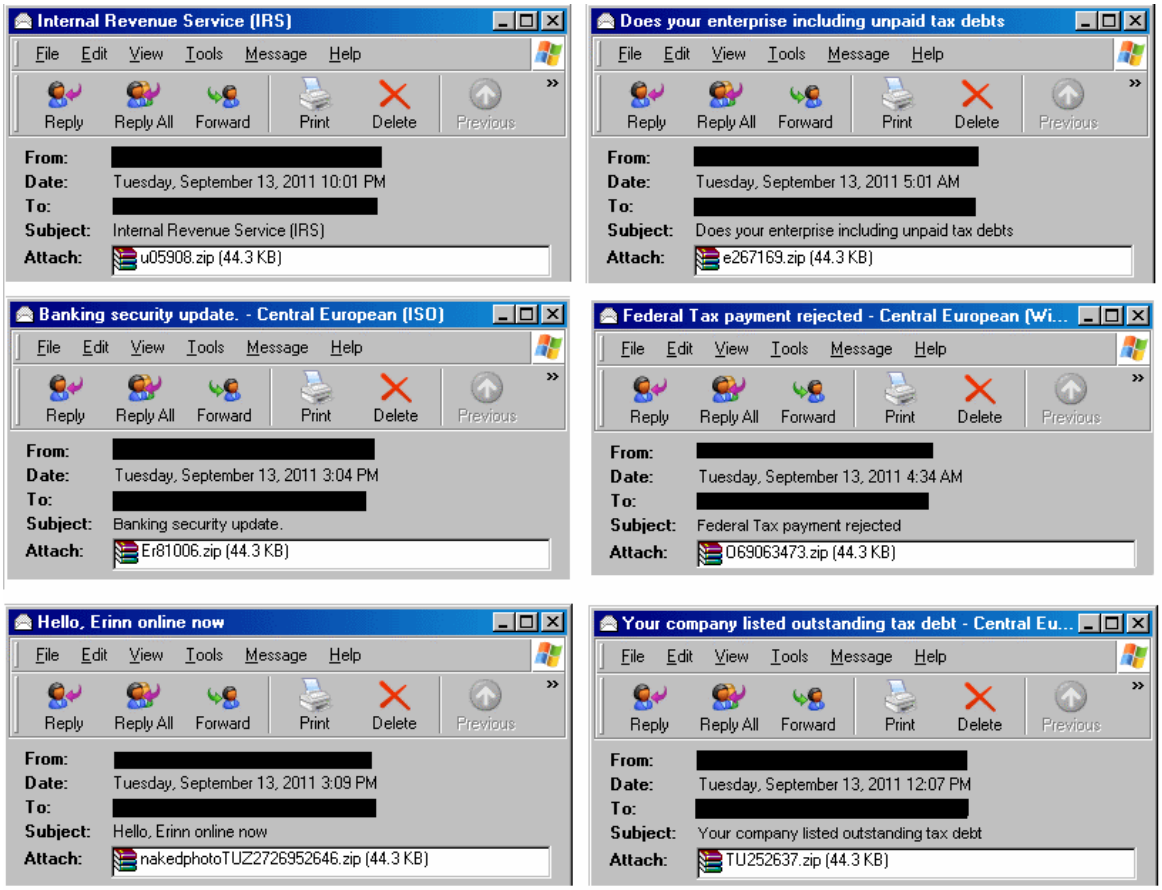


Figure 6: Examples of other social engineering subjects used to spread the same malware

Some Other Interesting Subjects	Frequency
Pornographic mail	85
Company Contract doc	40
Tax debt notification	34
Revenue (IRS) Department	25
Printer Scanned doc	21
domain suspension mail	9
pornographic picture	3

Figure 7: 24-hour snapshot showing variety of subject frequencies in use to distribute malware

It is evident from the variety shown in these examples that the attackers are trying a wide number of different possible social engineering strategies in order to trick the recipient into opening the malicious attachment.

This article was contributed by Bhaskar Krishnappa, Malware Analyst, Symantec

Spammers exploit WordPress vulnerability to promote pharmaceutical spam Web sites

In the Symantec Intelligence blog we've covered how spammers like to conceal their actual spam sites through elaborate chains of redirects, often involving hacked or compromised sites, URL shortening sites, obfuscation techniques, or combinations of all of these.

We've recently seen spammers exploiting a vulnerability in WordPress, the popular open-source blogging software running on thousands of servers worldwide. Spammers are using the WordPress platform to compromise a Web server, placing a file deep within the WordPress directory structure, presumably in an attempt to avoid (or at least delay) detection. The buried file is a simple HTML page, usually containing text like "Page loading" which is briefly shown before a HTTP “meta refresh” is used to redirect users to the spammer's "Canadian Health&Care Mall" Web site, as shown in figure 8:

```
<meta http-equiv="refresh" content="0; url=http://[new address to redirect]" />
```

Note that blogs hosted by WordPress.com seem to be unaffected by these vulnerabilities, it is only older versions of the software downloaded from WordPress.org that appear vulnerable. Symantec Intelligence has not yet been able to identify the specific versions affected, but will continue to update this information via the Symantec Intelligence blog[2].

Spam emails containing links to these compromised Web sites are also being spammed out.

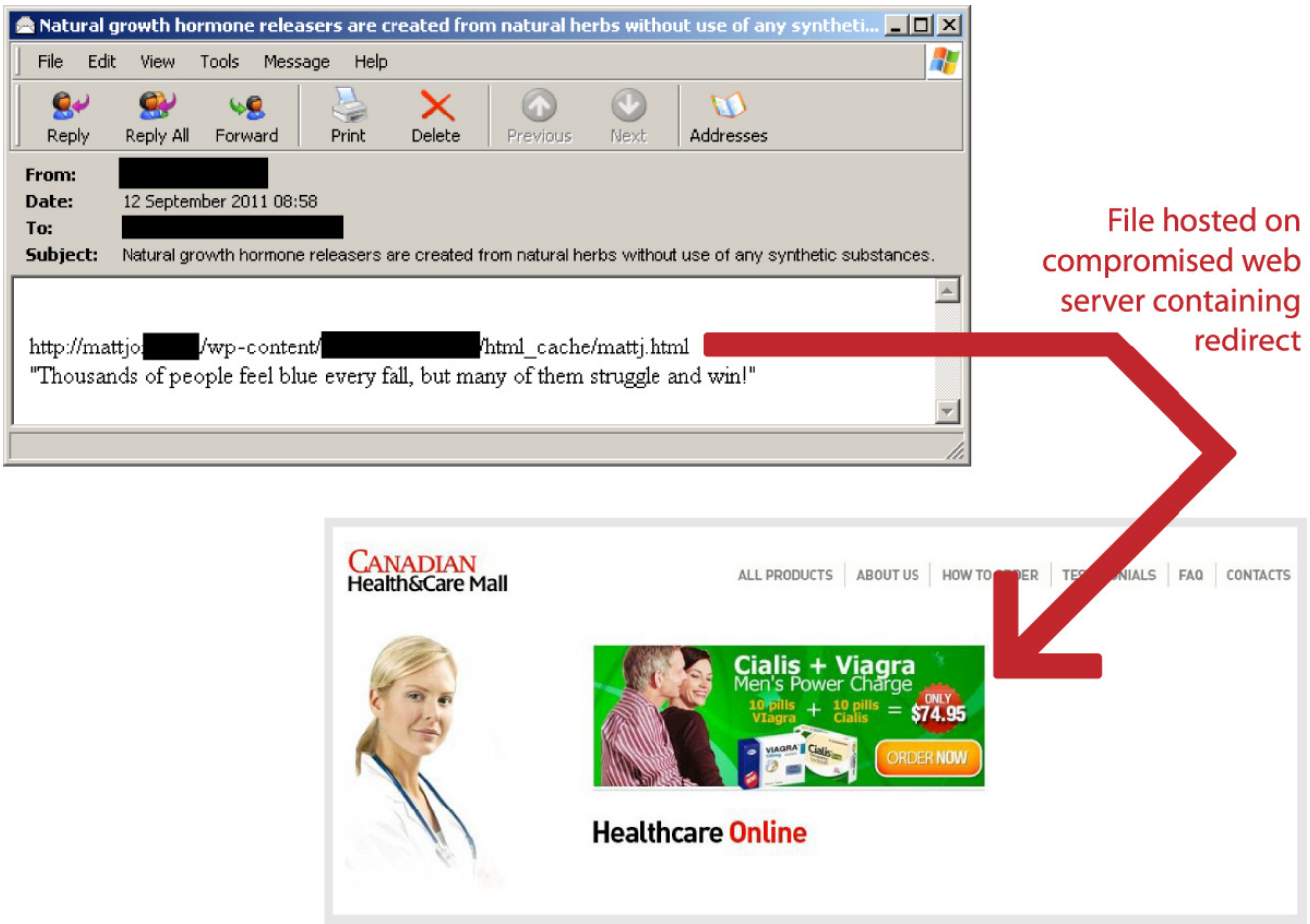


Figure 8: Pharmacy Web site linked from spam email via a compromised blog

In some cases, the file placed on compromised servers is named as the first few characters of the compromised domain name, with a ".html" extension. In the above example, the compromised domain name started with "mattjo", and the file placed on the server is called "mattj.html".

[2] *http://www.symantec.com/connect/symantec-blogs/symantec-intelligence*

Later compromises used a randomly generated file name instead. Over a 48-hour period, we saw several thousand unique domains being compromised in this way. It is likely that the only common factor is that these domains were all using a vulnerable version of the blogging platform. A carefully crafted search engine query is perhaps all that is needed by the attackers as a prelude to compromising these Web sites.

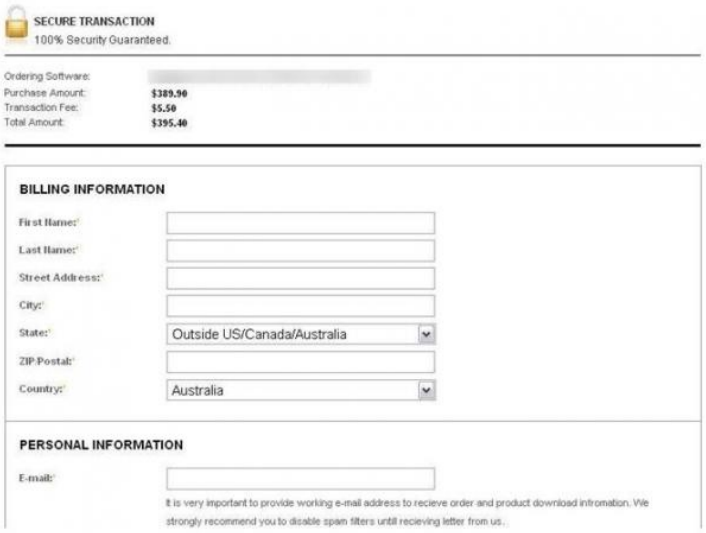
This serves as a good reminder of the need to keep all software up-to-date with latest patches and releases. Recent versions of WordPress (2.7 and higher) can be updated semi-automatically as described in this WordPress support article[3].

This article was contributed by Nicholas Johnston, Senior Engineer, Symantec

Fake Offers with Fake Trust Seals

Phishers are constantly looking for new ideas in their efforts of tricking end users. Symantec Intelligence identified a phishing site that utilized a number of new tricks. The phishing site masqueraded as a well-known software company and claimed to offer associated software products at discounted rates. The phishing page highlighted these fake offers as “summer offerings” and stated that customers could save 80% on their purchases. Users were prompted to enter their billing information, personal information, and credit card details to complete their purchases.

The personal information that was requested consisted of the user’s email address and phone number, as shown in figure 9. The credit card details that were asked for were the card number, CVV code, and card expiration date. If any users had fallen victim to the phishing site, the phishers would have successfully stolen their confidential information for financial gain.



[3] *http://codex.wordpress.org/Updating_WordPress#Automatic_Update*

Figure 9: Phishing Web site

Although these fake offers were used as the bait, it wasn't the only trick being offered up by the phishing site. There were further tactics employed in the hope of luring a greater number of end users. The phishing site was hosted on a newly registered domain name, and this new domain name was indexed in several popular search engines and had a very high page ranking. Phishers achieved the boosted page ranking by using common search keywords for the products within the domain name. For example, the domain would look like "common-search-keywords.com". Thus, if a user searched with these keywords in a search engine, they could end up with the phishing site as a high-ranked result.

The phishers' ploys didn't end there. The phishing page also contained fake trust seals at the bottom of the page. A legitimate trust seal is a seal provided to Web pages by a third party, typically a software security company, to certify that the Web site in question is genuine. Clicking on a trust seal will pop up a window provided by the third party, which contains details of the site name and the encryption data used to secure the site.

How did phishers overcome this security measure? They used fake trust seals that spoofed two major companies, which when clicked, popped up a window that referenced a fake site. The URL of the fake site utilized sub-domain randomization. Below is the format of the URL:

http://www.[*software security company*].com.[*fake domain*].com

With a quick glance at the URL, it would seem that the trust seal is linked to an appropriate third party, but it's not. If we read the complete URL for the pop-up window, we can see that it's a fake site. The best practice for identifying a legitimate trust seal is to click on the seal and read the complete URL of the pop-up window. The pop-up window should have a padlock icon, 'https', or a green address bar.

This article originally appeared as a blog[4] post by Mathew Maniyara, on 5 September 2011

Spammers and malware authors making increasing use of obfuscated JavaScript

JavaScript is a rich and dynamic programming language, becoming increasingly popular for developing richer, more interactive web applications, which more closely mirror their desktop counterparts in functionality and responsiveness.

However, it's not just Web developers who are increasingly using JavaScript. Spammers and malware authors are increasingly using obfuscated JavaScript to conceal where they are redirecting users, and in some cases, also to conceal entire Web pages.

For spammers, hosting simple JavaScript obfuscation pages on free hosting sites can increase the lifetime of that site before the site operator realizes the page is being used as part of malicious activity. JavaScript is popularly used for redirecting visitors of a compromised Web site to the spammers landing page.

[4] *http://www.symantec.com/connect/blogs/fake-offers-fake-trust-seals*

While some of these techniques have been common in malware distribution for some time, spammers are also increasingly using them.

Simple redirecting

JavaScript, through the Web browser and document interface DOM (Document Object Model) makes it possible to redirect a user from one site to another. This has long been a favored technique of spam and malware authors, creating ever longer and more complex "chains" of redirects (i.e. one redirect redirecting to another redirect and so on, before ultimately leading to the destination site).

Obfuscating techniques allow the destination URL or Web site address to be concealed to such an extent that when the Web page's HTML source is viewed, the URL is not visible.

A very simple technique is to replace some characters of the destination address with escaped characters. This notation is usually used for representing special characters, or including quotation marks inside a quoted string. For example:

```
location.href=unescape('%68%74%74%70%3a%2f')+'\u002f\u0077\u0077'+'w.smswi'+'fe.c'+'\u006f\u006d'+''
```

This snippet of code combines URI-style escaping, where each character is represented as a percent symbol (%) followed by its hex representation, and JavaScript string escaping (**\u** followed by the Unicode codepoint value of a character). When executed, this code will redirect the browser to *http://www.smswife.com*.

This is a simple technique, but probably enough to bypass many naïve checks in some more basic security countermeasures.

Another similar technique doesn't directly redirect the user; instead, JavaScript code updates the document, adding text to it, for example:

```
document.write(unescape("%3c%68%74%6d%6c%3e%3c%...."))
```

This particular code promotes a get-rich-quick site, which it then loads within a HTML frame:

```
<html><head><title>CityVille Secrets - Get Your Exclusive Secrets Guide Today!</title></head><frameset
border="0" framespacing="0" frameborder="0" rows="100%,*"><frame name="mainone" marginwidth="0"
marginheight="0" src="http://ca748bqp27uuhz67qf1tpaz19f.hop.clickbank.net/"></frameset></html>
```

Making use of the Eval function call

JavaScript is a dynamic language and contains an "eval()" function. This allows JavaScript code to be evaluated (i.e. executed or run) during runtime. This is a powerful feature but can also be abused. Spammers and malware authors often build up huge strings of JavaScript code, usually by iterating through vast strings or arrays containing characters encoded in a primitive way. These huge strings are then evaluated, making it harder to analyze the code.

Here's an example of this technique:

```
sblrvyn="" + "h" + "t" + "t" + "p" + ":" + "/" + "/" + "v" + "i" + "p" + "-" + "m" + "e" + "d" + "s" + "2" +
"4" + "." + "c" + "o" + "m" + "/";

document.write('<script>xlkfgizslh="p" + "a" + "r" + "e" + "n" + "t" + "." + "l" + "o" + "c" + "a" + "t" +
"i" + "o" + "n" + "." + "href=" + "sblrvyn"; eval(xlkfgizslh);<\/scr');

document.write('ipt>');
```

The "sblrvyn" variable gets the text string of "http://vip-meds24.com/" assigned to it. The code then writes more JavaScript to the page. This JavaScript assigns "`parent.location.href=sblrvyn`" to a variable called "xlkfgizslh". Note that "sblrvyn" contains the URL to redirect to.

Finally, the JavaScript evaluates the contents of the "xlkfgizslh" variable, causing the Web browser's JavaScript engine to run the code and redirect the user to the desired Web site.

Advanced obfuscation

In some cases, JavaScript is used to obfuscate an entire web page, rather than just conceal or hide a redirect. This is more common for malware, where malware authors want to conceal the many exploits hosted on such obfuscated pages.

A common technique is to store the entire page's obfuscated content in a single HTML "div" element. This "div" element is often hidden using CSS (Cascading Style Sheets), so a user viewing the web page won't see a long list of seemingly random characters. For example, a Web page might contain this HTML:

```
<div id="ReferenceError"><div style="display:none;">504c364c602c413

... ]</div></div>
```

Note: We haven't included all the obfuscated data here, as it's around 89,000 bytes long.

The obfuscation works by representing each character in the actual page as a number. These numbers are separated or delimited by the letter "c" - so 504, 364, 602 and 413 represents the first few characters in this example. Note that the "div" element finishes with a “]”.

The code to de-obfuscate this replaces all occurrences of the letter "c" inside the "div" with a comma, and add a “[” to the beginning. The string now resembles “[504, 364, 602, 413]”, which is evaluated as a JavaScript array using the “eval()” function as described earlier. Each element of the array (i.e. each number in the list) is then being divided by the number “7” and the result used as an index into a look-up table. This look-up table returns the actual desired character, which is then appended to a string, building up yet more JavaScript code to evaluate.

In this case, the code writes more JavaScript to the page, which attempts many exploits including exploits for Java, PDFs (with different exploits tailored to different versions of PDF viewing software), Flash and other software.

JavaScript's rich and dynamic nature combined with the DOM interface to Web browsers (and Web pages) allows spammers and malware authors lots of potential for obfuscation and thus concealing the real nature of the Web page.

This article was contributed by Nicholas Johnston, Senior Engineer, Symantec

Global Trends & Content Analysis

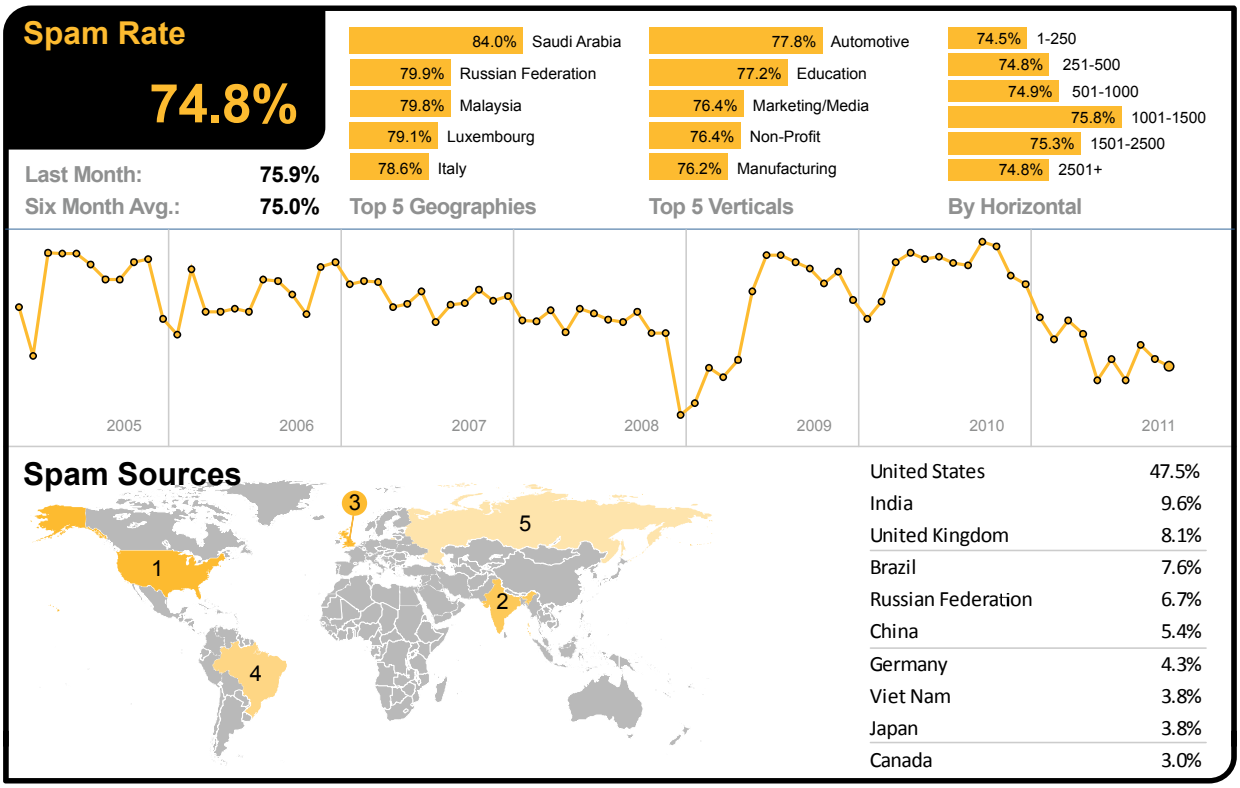
Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud 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 September 2011, the global ratio of spam in email traffic declined to 74.8 percent (1 in 1.34 emails), a decrease of 1.1 percentage points when compared with August 2011.



September 2011

As the global spam level remained relatively unchanged in September 2011, Saudi Arabia remained the most spammed geography; with a spam rate of 84.0 percent and Russia became the second most-spammed. The largest increase in spam in China was attributed to the IT Services sector (89.3 percent of email blocked as spam).

In the US, 74.5 percent of email was spam and 74.1 percent in Canada. The spam level in the UK was 75.5 percent. In The Netherlands, spam accounted for 76.4 percent of email traffic, 75.5 percent in Germany, 75.2 percent in Denmark and 73.3 percent in Australia. In Hong Kong, 73.9 percent of email was blocked as spam and 72.6 percent in Singapore, compared with 71.6 percent in Japan. Spam accounted for 74.3 percent of email traffic in South Africa and 77.1 percent in Brazil.

Symantec™

In September, the Automotive industry sector remained as the most spammed industry sector, with a spam rate of 77.8 percent. The spam level for the Education sector was 77.2 percent and 74.6 percent for the Chemical & Pharmaceutical sector, 74.4 percent for IT Services, 74.3 percent for Retail, 74.5 percent for Public Sector and 74.3 percent for Finance.

Global Spam Categories

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

Category Name	September 2011	August 2011
Pharmaceutical	52.5%	40.0%
Casino/Gambling	16.0%	7.0%
Unsolicited Newsletters	14.5%	11.5%
Watches/Jewelry	7.5%	17.5%
Unknown/Other	4.0%	2.5%
Adult/Sex/Dating	3.5%	19.0%
Weight Loss	1.5%	<0.5%
Jobs/Recruitments	1.0%	1.0%
Software	0.5%	0.5%
Scams/Fraud/419	<0.5%	0.5%
Degrees/Diplomas	<0.5%	1.5%

Spam Subject Line Analysis

In the latest analysis, adult-related dating spam accounted for fewer of the most common spam subject lines in September, with the most frequent being associated with a surge in generic polymorphic malware, spoofing the identity of an international delivery service. Pharmaceutical related subjects are also becoming increasingly more common.

Rank	September 2011 Total Spam: Top Subject Lines	No. of Days	August 2011 Total Spam: Top Subject Lines	No. of Days
1	UPS notification	6	(blank subject line)	31
2	Uniform traffic ticket	4	ED-Meds-Antidepressants-And-Pain Relief-Meds-8O%-OFF	31
3	You have notifications pending	22	Buy Advanced Penis Enlargement Pill now, it is selling fast.	31
4	SALE OFF: Pharmacy store!	2	Made of the most potent clinically proven natural herbs.	31
5	(blank subject line)	31	Permanently increases length and width of your erection. Advanced Penis Enlargement Pill.	31
6	Re: Windows 7, Office 2010, Adobe CS5 …	12	Advanced Penis Enlargement Pill. Permanently increases length and width of your erection.	31
7	Sarah Sent You A Message	11	my hot pics :)	23
8	Ed-Meds-Antidepressants-And-Pain Relief-Meds-8O%-OFF	25	found you :)	23
9	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 …	9	new pics for you..	24
10	Fw: Windows 7, Office 2010, Adobe CS5 …	9	im online now	23

Spam URL TLD Distribution

The proportion of spam exploiting URLs in the .info top-level domain fell by 7.9 percentage points in September, with the largest increase relating to spam URLs in the .com TLD.

TLD	September	August	Change (% points)
.com	59.5%	57.6%	+1.9
.info	10.5%	18.4%	-7.9
.ru	8.1%	7.1%	+1.0
.net	5.8%	5.8%	0

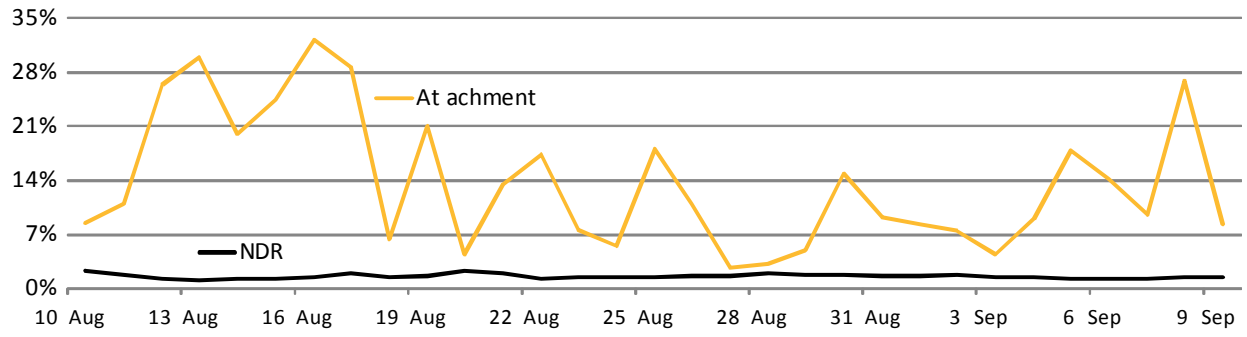
Average Spam Message Size

In September, almost half of all spam was 5Kb in size or less, however, spam with a larger file size, including attachments increased by 11.2 percentage points compared with August. This was a result of a rise in the number of generic polymorphic malware variants in circulation during September.

Message Size	September	August	Change (% points)
0Kb – 5Kb	48.1%	49.7%	-1.6
5Kb – 10Kb	25.6%	35.2%	-9.6
>10Kb	26.2%	15.0%	+11.2

Spam Attack Vectors

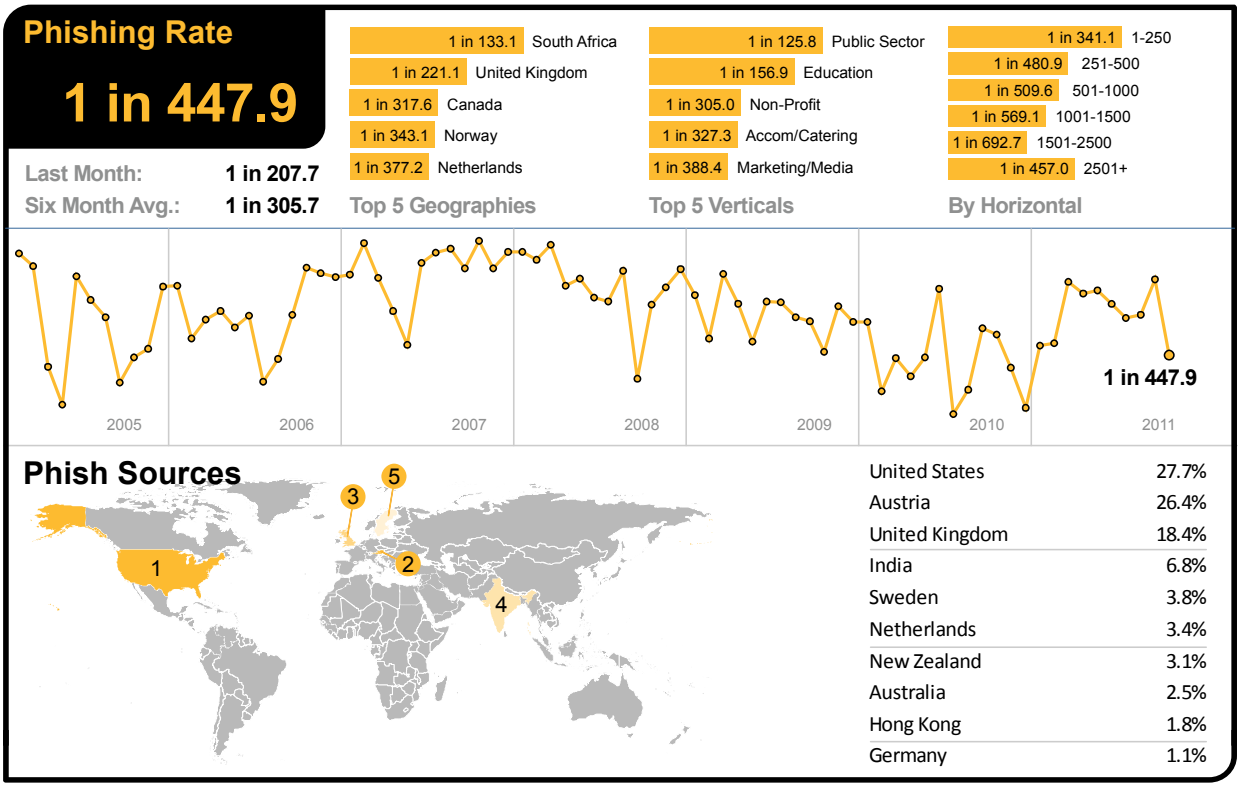
It can be seen in the chart below that from the end of August, a series of major spikes in attachment spam occurred approximately every two days. These attachments were connected to a rise in volume of generic polymorphic malware variants, as discussed at the beginning of this report. Furthermore, these attacks did not result in a surge in NDR spam (spam related non-delivery reports), which would be expected following a widespread dictionary attack, suggesting the attackers may be using valid email distribution lists to conduct these attacks. It may also be that they are perhaps doing a better job of maintaining their distribution lists in order to minimize bounce-backs, since IP addresses are more likely to appear on block-lists if they generate a high volume of invalid recipient emails.



Symantec™

Phishing Analysis

In September, phishing email activity diminished by 0.26 percentage points since August 2011; one in 447.9 emails (0.223 percent) comprised some form of phishing attack.



September 2011

Phishing attacks in South Africa increased once more position the country as the most targeted geography for phishing in September, with one in 133.1 emails identified as phishing. The UK remained the second most targeted country, with one in 221.1 emails identified as phishing attacks.

Phishing levels for the US were one in 985.9 and one in 317.6 for Canada. In Germany phishing levels were one in 1,125, one in 1,071 in Denmark and one in 377.2 in The Netherlands. In Australia, phishing activity accounted for one in 740.0 emails and one in 1,882 in Hong Kong; for Japan it was one in 12,812 and one in 1,958 for Singapore. In Brazil one in 439.0 emails was blocked as phishing.

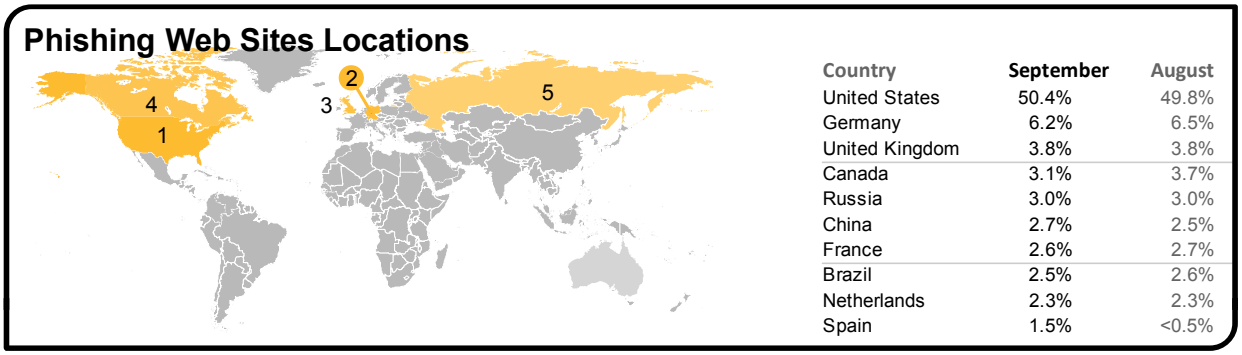
The Public Sector remained the most targeted by phishing activity in September, with one in 125.8 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector reached one in 797.3 and one in 754.6 for the IT Services sector, one in 664.5 for Retail, one in 156.9 for Education and one in 388.6 for Finance.

Analysis of Phishing Web sites

The number of phishing Web sites decreased by 12.2 percent in September. The number of phishing Web sites created by automated toolkits decreased by approximately 38.6 percent. The number of unique phishing URLs also decreased by 2.6 percent and phishing Web sites using IP addresses in place of domain names (for example, http://255.255.255.255), decreased by 16.9 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 6 percent of all phishing Web sites, a decrease of 32.7 percent from the previous month. The number of non-English phishing sites saw a decrease of 14.1 percent.

The most common non-English languages identified in phishing Web sites during September included Portuguese, French, Italian and Spanish.

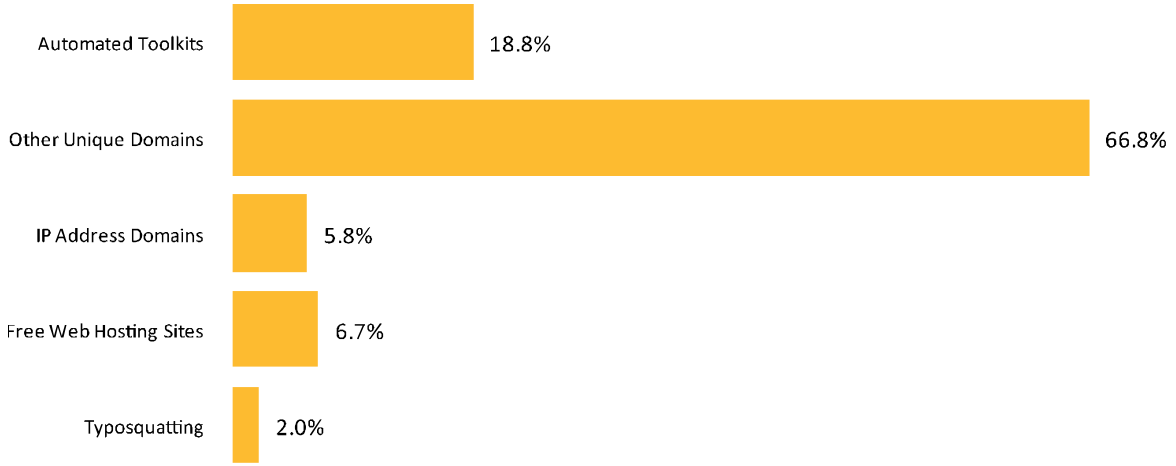
Geographic Location of Phishing Web Sites



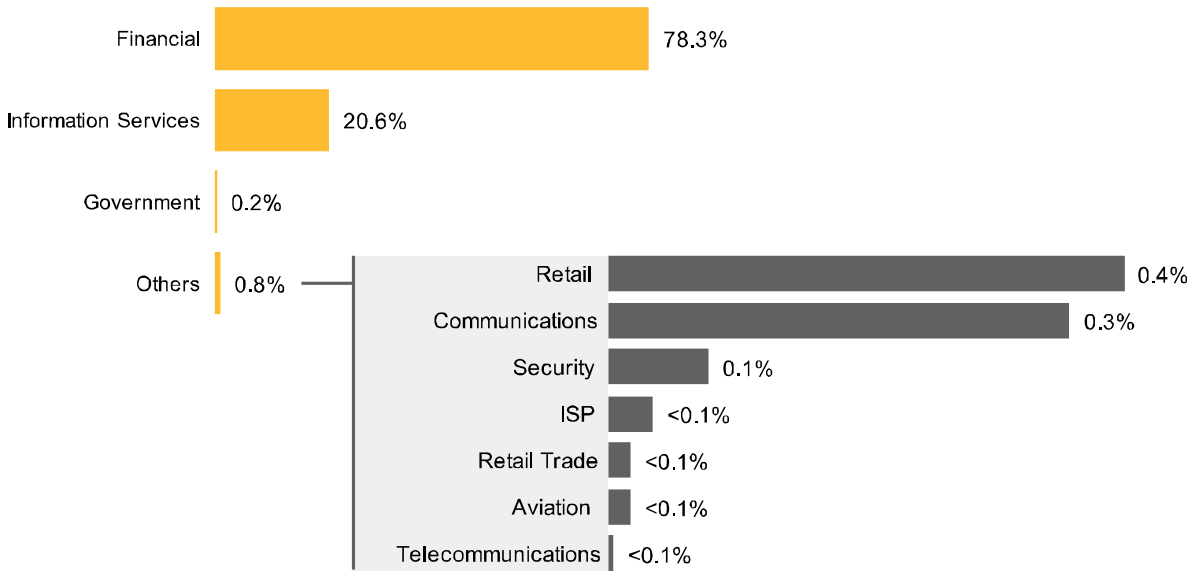
Country	September	August
United States	50.4%	49.8%
Germany	6.2%	6.5%
United Kingdom	3.8%	3.8%
Canada	3.1%	3.7%
Russia	3.0%	3.0%
China	2.7%	2.5%
France	2.6%	2.7%
Brazil	2.5%	2.6%
Netherlands	2.3%	2.3%
Spain	1.5%	<0.5%

September 2011

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry Sector



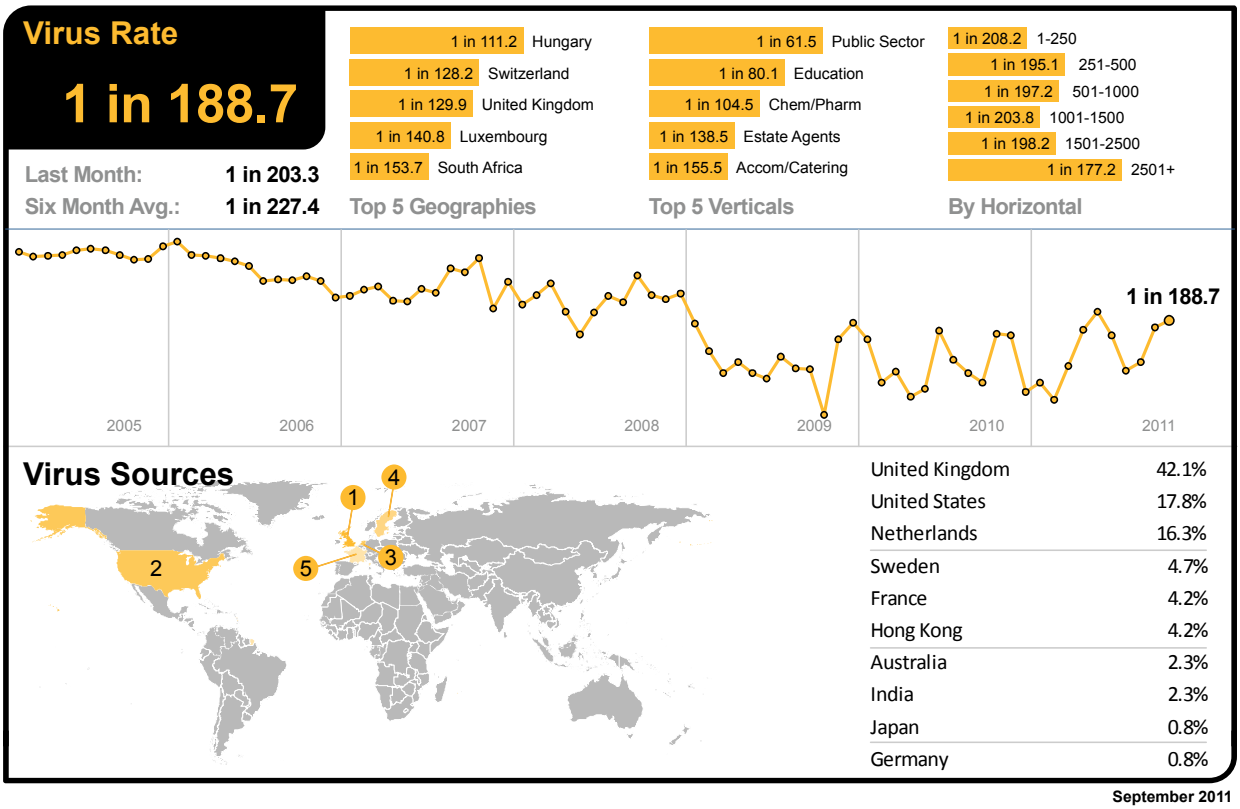
Symantec™

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 188.7 emails (0.53 percent) in September, an increase of 0.04 percentage points since August 2011.

In September, 16.5 percent of email-borne malware contained links to malicious Web sites, a decrease of 20.5 percentage points since August 2011. Emails that contained generic polymorphic malware variants accounted for 72.0 percent of all email-borne malware in September, compared with 18.5 percent in August; many included attached ZIP files that contained the generic malware.



Email-borne malware attacks in Hungary climbed to one in 111.2 emails, positioning the country at the top of the table with the highest ratio of malicious emails in September. Switzerland was the second most geography under fire in September, with one in 128.2 emails was identified as malicious in September.

In the UK one in 129.9 emails was blocked as malicious, and virus levels for email-borne malware reached one in 224.8 in the US and one in 164.8 in Canada. In Germany virus activity reached one in 197.9, one in 488.8 in Denmark and in The Netherlands one in 174.9. In Australia, one in 341.5 emails were malicious and one in 215.6 in Hong Kong; for Japan it was one in 658.3, compared with one in 307.2 in Singapore. In Brazil, one in 363.5 emails in contained malicious content.

With one in 61.5 emails being blocked as malicious, the Public Sector remained the most targeted industry in September. Virus levels for the Chemical & Pharmaceutical sector were one in 104.5 and one in 192.2 for the IT Services sector; one in 276.1 for Retail, one in 80.1 for Education and one in 240.9 for Finance.

The table below shows the most frequently blocked email-borne malware for September, many of which take advantage of malicious attachments. Overall, 72.0 percent of email-borne malware was associated with variants of generic polymorphic malware, including Bredolab, Sasfis, SpyEye and Zeus variants.

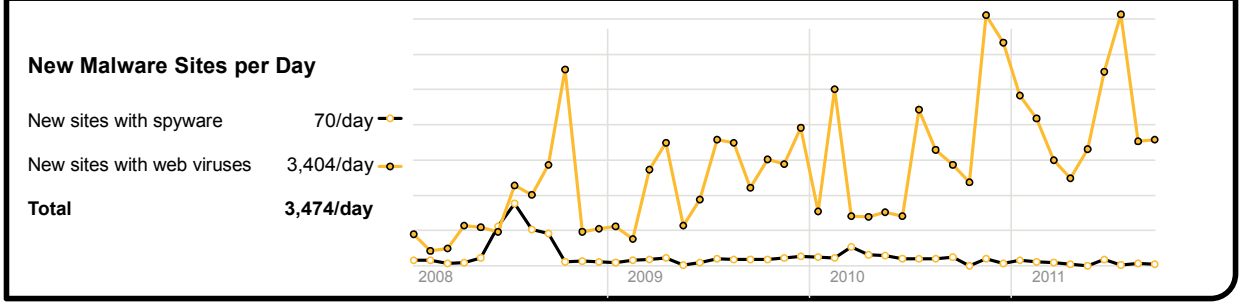
Malware Name	% Malware
Gen:Trojan.Heur.FU.bqW@amtJU@oi	5.1%
Gen:Trojan.Heur.BDT.bqW@b8J!Mvci	4.2%
Gen:Trojan.Heur.BDT.bqW@bS6mfcai	4.1%
Exploit/Link-generic-ee68	3.8%
Gen:Trojan.Heur.FU.bqW@a8Y5GDei	3.6%
Gen:Trojan.Heur.BDT.bqW@bC6h06ii	3.4%
Trojan.Zbot	3.1%
Gen:Trojan.Heur.FU.bqW@aiZha1gi	3.0%
Gen:Trojan.Heur.FU.bqW@a4wN11gi	2.9%
Gen:Trojan.Heur.FU.bqW@a0jG0qpi	2.8%

Web-based Malware Threats

In September, Symantec Intelligence identified an average of 3,473 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 1.0 percent since August 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 44.6 percent of all malicious domains blocked were new in September; an increase of 10.0 percentage points compared with August 2011. Additionally, 14.5 percent of all Web-based malware blocked was new in September; a decrease of 2.9 percentage points since the previous month.

Web Security Services Activity:



The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during September 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 41.0 percent of blocked Web activity in September. 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 17.7 percent of URL-based filtering activity blocked, equivalent to approximately one in every six Web sites blocked. Many organizations allow access to social networking Web sites, but facilitate access logging so that usage patterns can be tracked and in

some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Activity related to Streaming Media policies resulted in 8.8 percent of URL-based filtering blocks in September. 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 11 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement & Popups	41.0%	VBS/Generic	42.3%	PUP:9231	37.9%
Social Networking	17.7%	Trojan:GIF/GIFrame.gen!A	24.4%	PUP:W32/CnsMin.S	19.6%
Streaming Media	8.8%	Trojan.Gen	2.8%	PUP:Generic.62006	8.6%
Chat	4.7%	W32.Downadup	2.6%	PUP:Generic.188886	5.3%
Computing & Internet	3.9%	W32.Downadup.B	2.4%	PUP:Generic.183433	3.4%
Peer-To-Peer	2.4%	Gen:Variant.Kazy.34674	2.2%	PUP:WinPump.A	2.8%
Gambling	1.9%	Trojan.Gen.2	1.9%	PUP:Generic.188088	2.7%
Games	1.8%	Bloodhound.Flash.7	1.7%	PUP:Keylogger	1.9%
Hosting Sites	1.7%	New Unclassified Trojan	1.2%	PUP:Heur.xq1@RihoWSii	1.9%
Search	1.6%	Gen:Variant.Kazy.32829	1.0%	PUP:Generic.183172	1.8%
News	1.6%				

September 2011

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

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

Malware Name[5]	% Malware
W32.Sality.AE	7.8%
W32.Ramnit!html	7.1%
W32.Ramnit.B!inf	6.2%
Trojan.Bamital	6.1%
W32.Downadup.B	3.9%
W32.SillyFDC.BDP!lnk	3.1%
Trojan.ADH.2	2.8%
Trojan.ADH	2.5%
W32.Virut.CF	2.4%
W32.Almanahe.B!inf	2.2%

The most frequently blocked malware for the last month was W32.Sality.AE[6], a virus that spreads by infecting executable files and attempts to download potentially malicious files from the Internet. For the first time since the end of 2010, Sality overtook Ramnit to become the most prevalent malware blocked at the endpoint. For much of 2010, W32.Sality.AE had been the most prevalent malicious threat blocked at the endpoint.

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

[6] *http://www.symantec.com/connect/blogs/sality-whitepaper*

W32.Ramnit!html is a generic detection for .HTML files infected by W32.Ramnit[7], a worm that spreads through removable drives and by infecting executable files. Variants of the Ramnit worm accounted for 13.5 percent of all malicious software blocked by endpoint protection technology in September.

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. Approximately 20.8 percent of the most frequently blocked malware last month was identified and blocked using generic detection.

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

Best Practice Guidelines for Enterprises

1. **Employ defense-in-depth strategies**: Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.
2. **Monitor for network threat, vulnerabilities and brand abuse.** Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious site reporting.
3. **Antivirus on endpoints is not enough:** On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:
    - Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
    - Browser protection for protection against obfuscated Web-based attacks;
    - Consider cloud-based malware prevention to provide proactive protection against unknown threats;
    - File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
    - Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
    - Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
    - Device control settings that prevent and limit the types of USB devices to be used.
4. **Use encryption to protect sensitive data:** Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.
5. **Use Data Loss Prevention to help prevent data breaches:** Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.
6. **Implement a removable media policy**. Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.
7. **Update your security countermeasures frequently and rapidly:** With more than 286M variants of malware detected by Symantec in 2010, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.
8. **Be aggressive on your updating and patching:** Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.
9. **Enforce an effective password policy**. Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

10. **Restrict email attachments:** Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.
11. **Ensure that you have infection and incident response procedures in place:**
    - Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
    - Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
    - Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
    - Isolate infected computers to prevent the risk of further infection within the organization;
    - If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
    - Perform a forensic analysis on any infected computers and restore those using trusted media.
12. **Educate users on the changed threat landscape:**
    - Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
    - Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
    - Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
    - Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;
    - Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
    - Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
    - Only download software (if allowed) from corporate shares or directly from the vendors Web site;
    - If users see a warning indicating that they are “infected” after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.

Best Practice Guidelines for Users and Consumers

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

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

About Symantec.cloud Intelligence

Symantec.cloud Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud Intelligence publishes a range of information on global security threats based on live data feeds from more than 15 data centers around the world scanning billions of messages and Web pages each week. Team Skeptic™ comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of Web pages, email and IM messages they monitor each day on behalf of 31,000 clients in more than 100 countries. More information is available at www.messagelabs.com/intelligence.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

Symantec™