Symantec Intelligence

# Symantec Intelligence Report: February 2013

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 through February 2013.

## Report highlights

- Spam – 65.9 percent (an increase of 1.8 percentage points since January): page 2
- Phishing – One in 466.3 emails identified as phishing (an increase of 0.018 percentage points since January): page 4
- Malware – One in 408.2 emails contained malware (a decrease of 0.11 percentage points since January): page 5
- Malicious websites – 1,530 websites blocked per day (a decrease of 32.2 percent since January): page 6

## Introduction

In the past month we‘ve discovered of the earliest known variant of the Stuxnet worm, as well as combat the Bamital botnet, which was successfully shut down through a joint Symantec/Microsoft collaboration.

Up until last month the earliest known variant of Stuxnet was 1.001, created in 2009. Last month, we discovered the earliest known version of the Stuxnet worm, Stuxnet 0.5, which stems from 2007. Stuxnet 0.5 allows us further insight into the history and evolution of Stuxnet.

Stuxnet 0.5 differs in form from other known variants as it is based on a different programming platform. Stuxnet 0.5 is partly based the same platform as W32.Flamer, whereas 1.x versions were based on the Tilded platform. It is also different in that Stuxnet 0.5's only method of replication is through infection of Siemens Step 7 project files. When a removable drive is inserted in an infected drive, Stuxnet 0.5 will infect any Step 7 project archives with .s7p or .zip file name extensions on the drive.

Stuxnet 0.5 takes control of valves attached to centrifuges, opening and closing the valves at intervals, compromising the integrity of the system as a whole. Version 0.5 works by fingerprinting target computers to determine if it is in the right location before activating the payload. Stuxnet 0.5 also collects instrument readings when the centrifuges are running as normal and, when it is making its attack, displays those readings to the controllers in order to mask its activities. Stuxnet 0.5 differs in that it was designed to attack the centrifuges' valve system as opposed to 1.x variants which sought to disrupt the operation of frequency converters used to control the speed of the centrifuges.

In other news, Symantec, in partnership with Microsoft, shut down a botnet controlling hundreds of thousands of computers. Bamital, a botnet which in the last two years has compromised more than eight million computers, operated by hijacking search engine results and redirecting to servers controlled by attackers. Analysis of a single Bamital command and control (C&C) sever over a six week period in 2011 revealed over 1.8 million unique IP addresses communicating with the server. The botnet servers have now been shut down, and users of infected computers will be informed of their infection when attempting to search the Internet.

Bamital is an example of click fraud, a highly lucrative endeavor where by attackers aim to distort the numbers of clicks on an advertisement or visits to a specific website. Redirecting internet users to corrupt third party vendors or selling internet traffic through fictitious users, attackers seek to make financial gain from advertising expenditure.

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.

**Darragh Cotter, Associate Information Developer**
symantec_intelligence@symantec.com

@symantec, @symanteccloud, @nortononline, @threatintel

## 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 February, the global ratio of spam in email traffic rose by 1.8 percentage point since January, to 65.9 percent (1 in 1.52 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.

### Global Spam Categories

The most common category of spam in February is related to the Sex/Dating category, with 78.13 percent.

| Category Name | February 2013 | January 2013 |
|---|---:|---:|
| Sex/Dating | 78.13% | 71.65% |
| Pharma | 14.20% | 14.87% |
| Jobs | 3.75% | 0.55% |
| Watches | 1.06% | 7.29% |
| Software | 1.04% | 1.52% |
| Casino | 0.79% | 3.50% |
| Malware | 0.47% | 0.12% |
| 419/scam/lotto | 0.06% | 0.05% |
| Newsletters | 0.04% | 0.04% |
| Degrees | 0.01% | 0.01% |

### Spam URL Distribution based on Top Level Domain Name

The proportion of spam exploiting URLs in the .com top-level domain decreased in February, as highlighted in the table below. This is in line with a slight increase in all other top-level domains this month.

| TLD | February 2013 | January 2013 |
|---|---:|---:|
| com | 51.33% | 54.36% |
| ru | 13.14% | 12.34% |
| info | 9.34% | 8.92% |
| net | 6.88% | 5.85% |

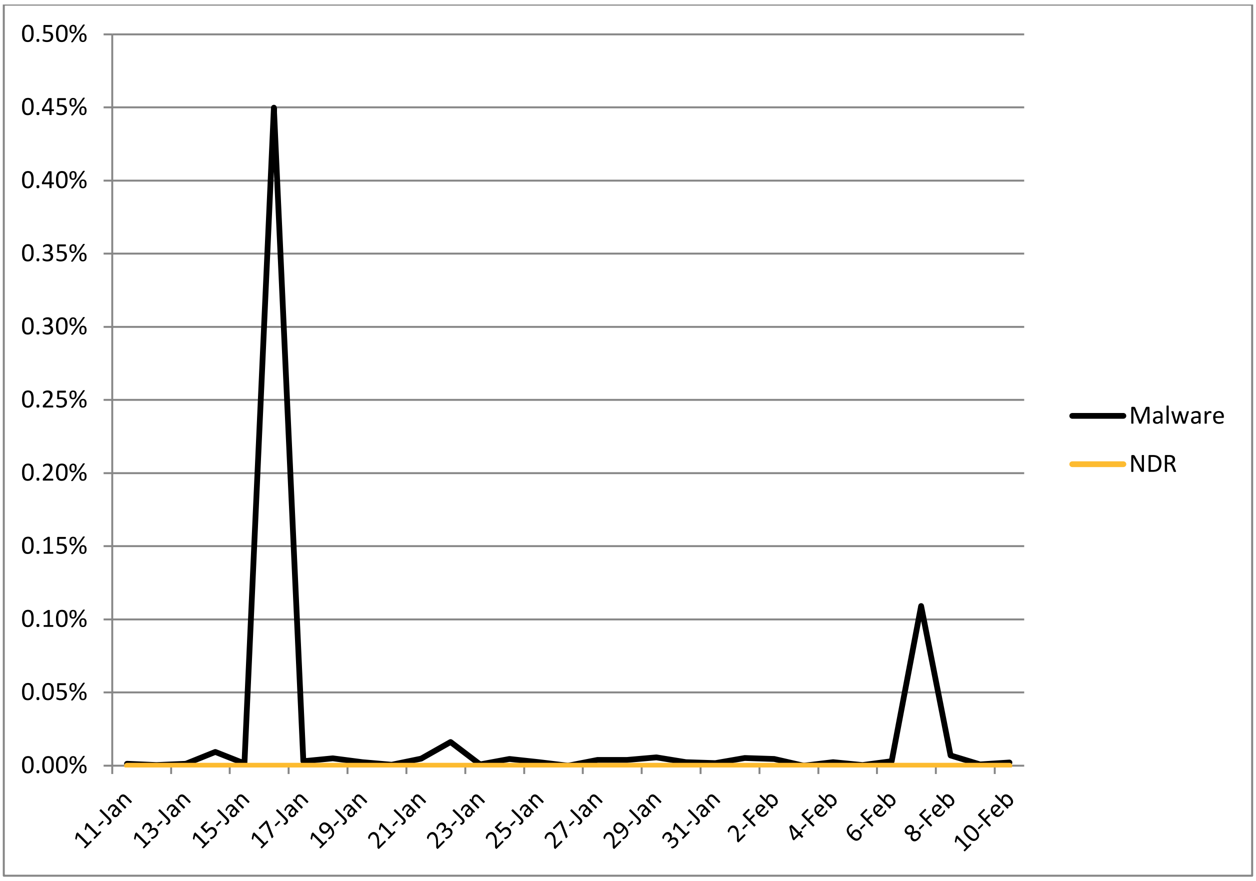
### Average Spam Message Size

In February, the proportion of spam emails that were 5Kb in size or less increased by 10.92 percentage points. Furthermore, the proportion of spam messages that were greater than 10Kb in size increased by 1.03 percent, as can be seen in the following table.

| Message Size | February 2013 | January 2013 |
|---|---|---|
| 0Kb – 5Kb | 57.73% | 46.81% |
| 5Kb – 10Kb | 27.03% | 38.98% |
| >10Kb | 15.24% | 14.21% |

### Spam Attack Vectors

February highlights the decrease 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.

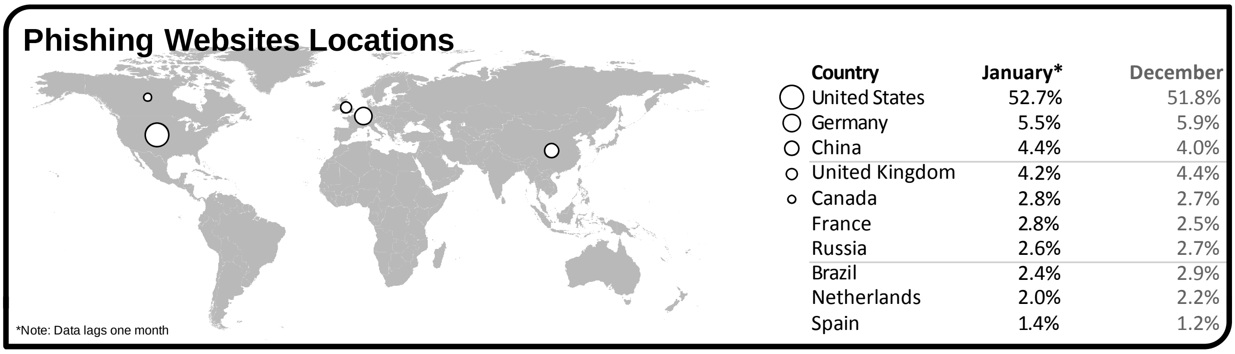
# Phishing Analysis

In February, the global phishing rate increased by 0.018 percentage points, taking the global average rate to one in 466.3 emails (0.214 percent) that comprised some form of phishing attack.

## Analysis of Phishing Websites

The overall phishing increased by about 19 percent this month. Unique domains increased by about 8 percent as compared to the previous month. Phishing websites that used automated toolkits increased by 33 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) increased by about 28 percent. Webhosting services comprised of 5 percent of all phishing, an increase of 55 percent from the previous month.  The number of non-English phishing sites decreased by 56 percent. Among non-English phishing sites, Portuguese, French and German were highest in January.

## Geographic Location of Phishing Websites



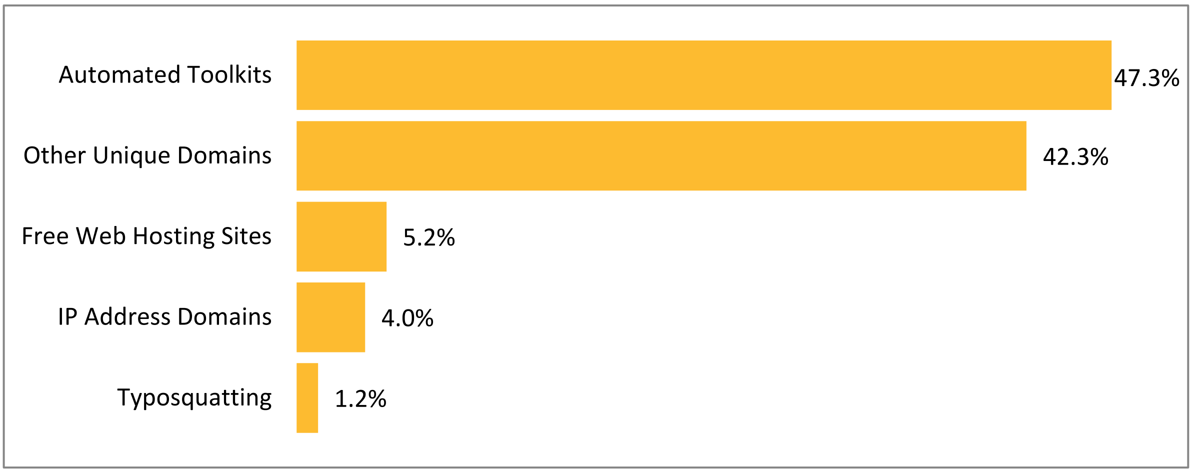
Phishing Websites Locations

| Country | January* | December |
|---|---|---|
| ○ United States | 52.7% | 51.8% |
| ○ Germany | 5.5% | 5.9% |
| ○ China | 4.4% | 4.0% |
| ○ United Kingdom | 4.2% | 4.4% |
| ○ Canada | 2.8% | 2.7% |
| France | 2.8% | 2.5% |
| Russia | 2.6% | 2.7% |
| Brazil | 2.4% | 2.9% |
| Netherlands | 2.0% | 2.2% |
| Spain | 1.4% | 1.2% |

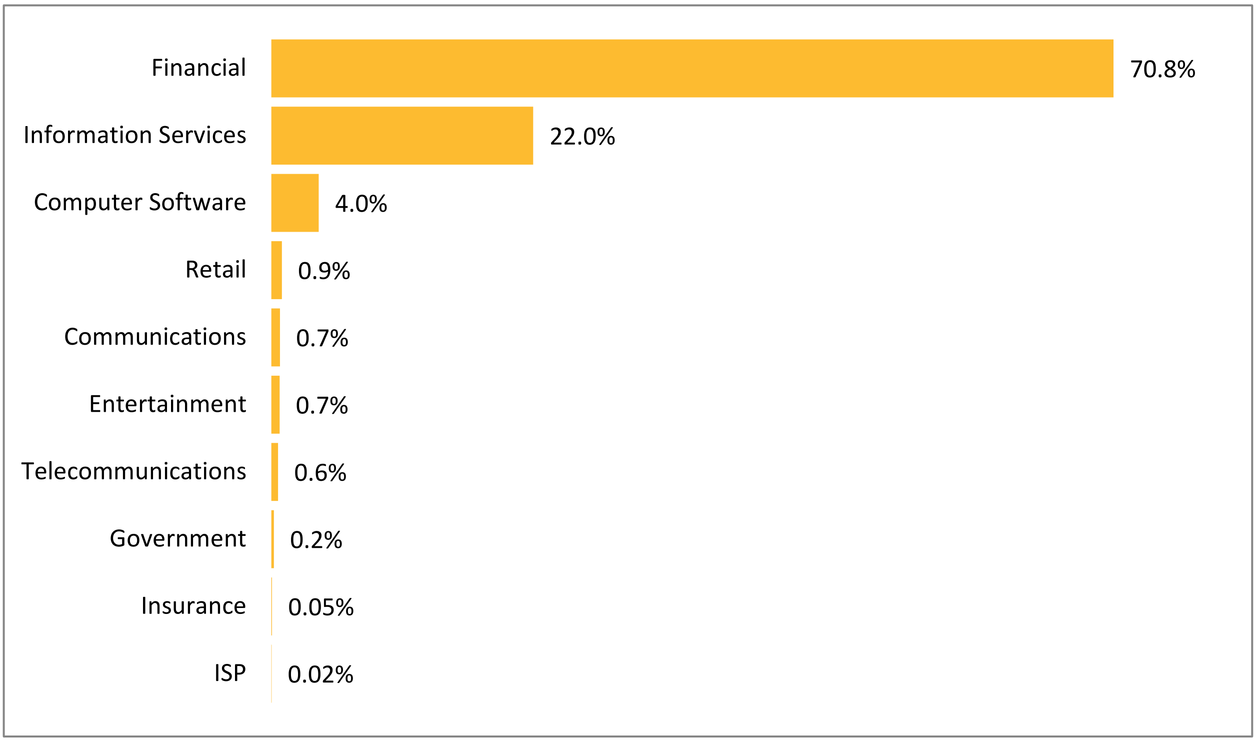
*Note: Data lags one month

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 408.2 emails (0.25 percent) in February, a decrease of 0.11 percentage points since January.

In February, 23.0 percent of email-borne malware contained links to malicious websites, 10.5 percentage points lower than January.

### 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 18.7 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 1.1 percent of all email-borne malware blocked in February.

| Malware Name | % Malware |
|---|---:|
| Suspicious.JIT.a-SH | 38.14% |
| Exploit/Link-Inducement-18d5-SH | 4.14% |
| Trojan.Gen-SH | 4.01% |
| Exploit/Link-82c6 | 3.75% |
| HTML/JS-Encrypted.gen | 2.09% |
| Trojan.Gen | 1.80% |
| Exploit/Link-d6b1 | 1.66% |
| Trojan.Malscript | 1.54% |
| W32/Exploit-Archive.Gen-SH | 1.50% |
| Exploit/SpoofBBB | 1.48% |

The top-ten list of most frequently blocked malware accounted for approximately 60.1 percent of all email-borne malware blocked in February.

### Web-based Malware Threats

In February, Symantec Intelligence identified an average of 1,530 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 32.2 percent since January. 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 37.2 percent of all malicious domains blocked were new in February; a decrease of 2.3 percentage points compared with January. Additionally, 11.5 percent of all Web-based malware blocked was new in February; a decrease of 0.5 percentage points since January.

### 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-ups, 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.

## 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[1] | % Malware |
|---|---|
| W32.Sality.AE | 7.35% |
| W32.Ramnit!html | 6.87% |
| W32.Ramnit.B | 5.86% |
| W32.Ramnit.B!inf | 4.29% |
| W32.Downadup.B | 4.00% |
| W32.Almanahe.B!inf | 2.27% |
| W32.Virut.CF | 2.19% |
| W32.SillyFDC.BDP!lnk | 1.44% |
| Trojan.ADH | 1.17% |
| W32.Chir.B@mm(html) | 1.16% |

For much of 2012 and 2013, variants of W32.Sality.AE[2] and W32.Ramnit[3] had been the most prevalent malicious threats blocked at the endpoint. Variants of W32.Ramnit accounted for approximately 17.4 percent of all malware blocked at the endpoint in February, compared with 8.2 percent for all variants of W32.Sality.

Approximately 40.7 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.

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

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

[3] *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.

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.