Symantec Intelligence Report: January 2013

Welcome to the January edition of the Symantec Intelligence report, which provides the latest analysis of cyber security threats, trends, and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The data used to compile the analysis for this report includes data from December 2012 through January 2013.

Report highlights

- Spam – 64.1 percent (a decrease of 6.5 percentage points since December): page 2
- Phishing – One in 508.6 emails identified as phishing (a decrease of 0.068 percentage points since December): page 3
- Malware – One in 400 emails contained malware (a decrease of 0.11 percentage points since December): page 3
- Malicious websites – 2,256 websites blocked per day (an increase of 196.1 percent since December): page 5

Introduction

In this month's report, we find that the email malware rate has dropped significantly since December, where only one in 400 emails containing a virus in January. This is the lowest virus rate we've seen since 2009. It could indicate that email virus distributors took a break after the holiday season, or that they have continued to migrate away from email as a choice for malicious payload delivery. We'll watch this trend carefully to see if it continues to drop off.

In other news this month, Valentine's Day spam is in full swing. Such spam generally arrives as an ecard during this time of year, preying upon a potential victim's curiosity about a potential secret admirer—a situation where a legitimate email would likely arrive unsolicited in the first place. Unfortunately many such emails around this time of year do not lead to unexpected romance, but rather fake bargains, phishing attempts, or malicious code. More details on these scams can be found here.

Finally, this month Symantec and Microsoft partnered to take down a notorious botnet: Bamital. The primary purpose of this botnet has been to generate ad revenue by hijacking search engine results, redirecting them to a C&C server hosting ads of the attacker's choosing. Symantec has been tracking this botnet since 2009, and has successfully shut down the all known components of used to operate the botnet. Security Response has released a whitepaper, providing a detailed overview of the botnet, which is available for download here.

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.

Ben Nahorney, Cyber Security Threat Analyst
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.

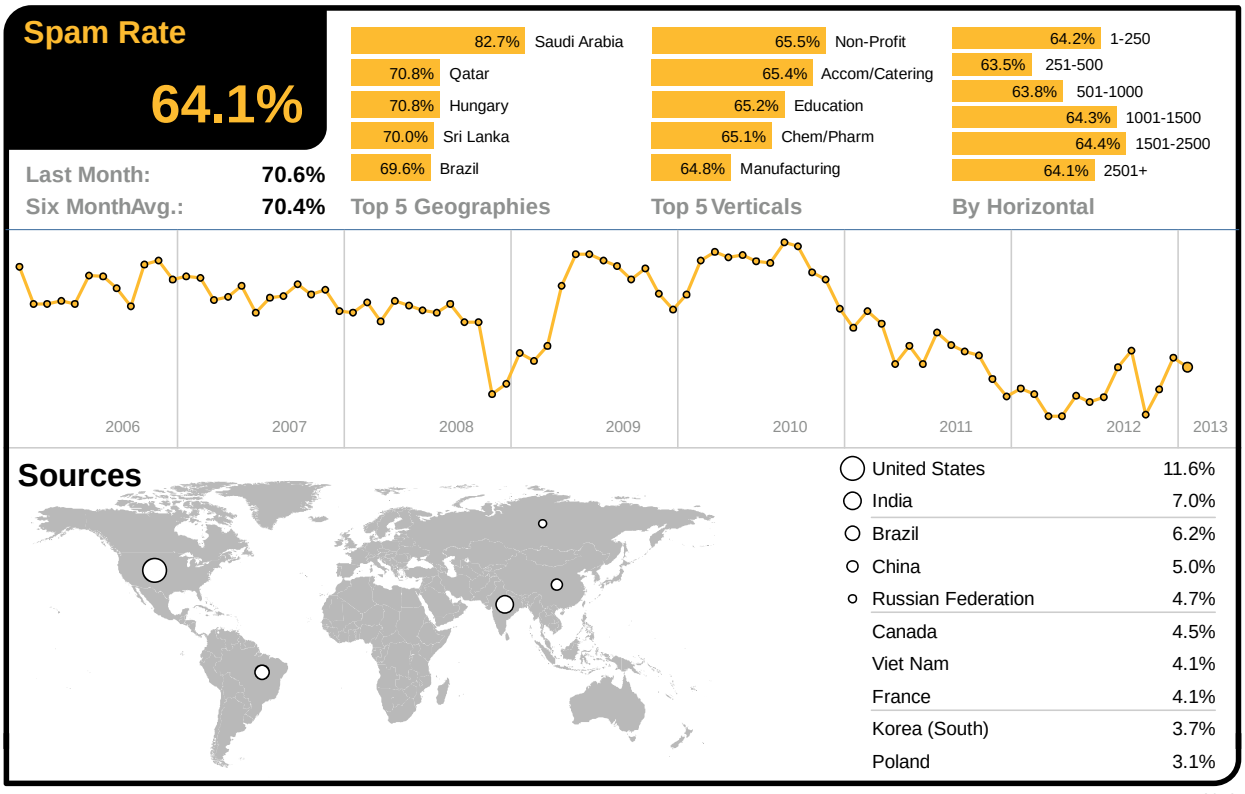
In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

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 January, the global ratio of spam in email traffic fell by 6.5 percentage points since December, to 64.1 percent (1 in 1.56 emails). This follows the continuing trend of global spam levels diminishing gradually since the latter part of 2011.



January 2013

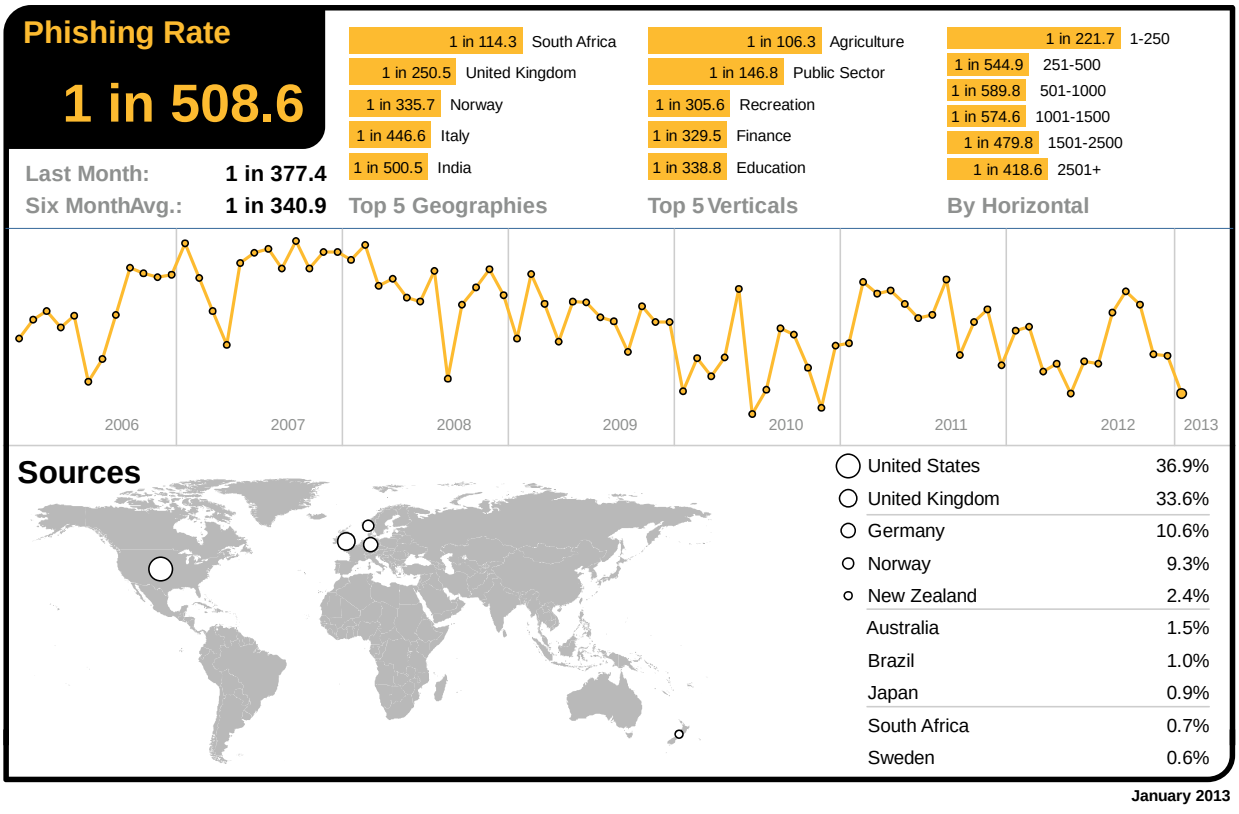
Global Spam Categories

The most common category of spam in January is related to the Sex/Dating category, with 71.65 percent.

Category Name	January 2013	December 2012
Sex/Dating	71.65%	82.62%
Pharma	14.87%	9.04%
Watches	7.29%	4.49%
Casino	3.50%	0.04%
Software	1.52%	1.22%
Jobs	0.55%	1.45%
Mobile	0.24%	0.14%
419/scam/lotto	0.05%	0.06%
Newsletters	0.04%	0.75%
Degrees	0.01%	0.02%

Phishing Analysis

In January, the global phishing rate decreased by 0.068 percentage points, taking the global average rate to one in 508.6 emails (0.197 percent) that comprised some form of phishing attack.



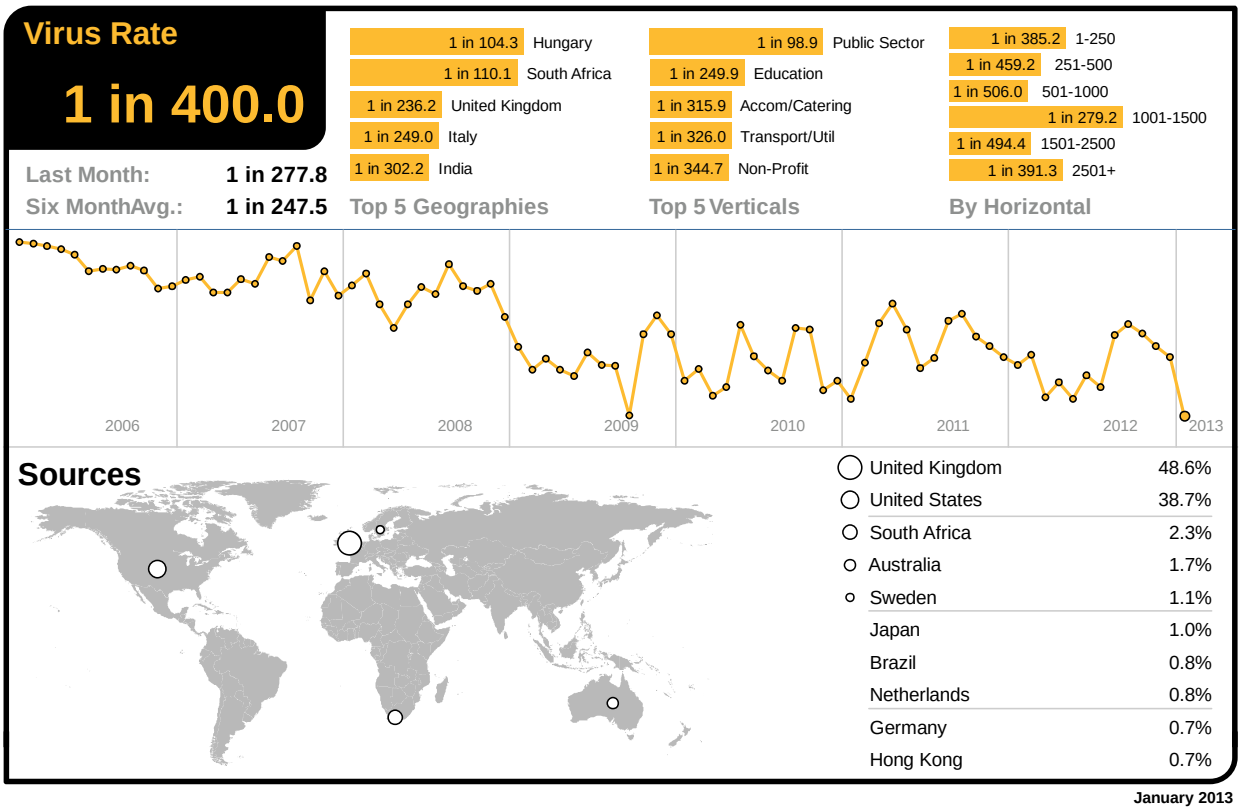
January 2013

Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 400 emails (0.25 percent) in January, a decrease of 0.11 percentage points since December.

In January, 33.5 percent of email-borne malware contained links to malicious websites, 6.3 percentage points higher than December.



January 2013

Frequently Blocked Email-borne Malware

The table below shows the most frequently blocked email-borne malware for January, many of which relate to generic variants of malicious attachments and malicious hyperlinks distributed in emails. Approximately 30.9 percent of all email-borne malware was identified and blocked using generic detection.

Malware identified generically as aggressive strains of polymorphic malware accounted for 0.2 percent of all email-borne malware blocked in January.

Malware Name	% Malware
Suspicious.JIT.a-SH	32.90%
Exploit/Link-generic-ee68	8.89%
Link-Trojan.Generic.KDZ.2843-1cc7	6.00%
W32/NewMalware-Generic	5.30%
Exploit/LinkAliasPostcard-bc46	5.11%
Exploit/OutlookDate	3.80%
Exploit/SpoofBBB	3.72%
Exploit/Link-b288	2.13%
W32/Generic.dam	1.26%
Trojan.Gen-SH	1.25%

The top-ten list of most frequently blocked malware accounted for approximately 70.4 percent of all email-borne malware blocked in January.

Symantec™

Web-based Malware Threats

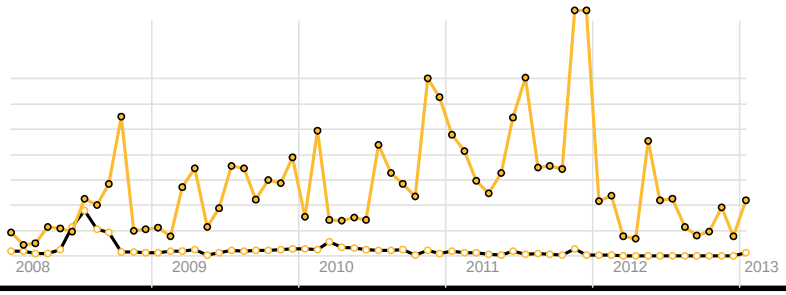
In January, Symantec Intelligence identified an average of 2,256 websites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 196.1 percent since December. This reflects the rate at which websites are being compromised or created for the purpose 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 39.1 percent of all malicious domains blocked were new in January; a decrease of 0.5 percentage points compared with December. Additionally, 11 percent of all Web-based malware blocked was new in January; a decrease of 0.9 percentage points since December.

Web Security Services Activity:

New Malware Sites per Day

New sites with spyware	141/day
New sites with web viruses	2,115/day
Total	**2,256/day**



The chart above shows the increase in the number of new spyware and adware websites blocked each day on average during January 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-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.

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Social Networking	34.1%	Gen:Heur.ManBat.1	11.4%	Gen:Adware.MPlug.1	63.4%
Advertisement and Popups	27.6%	Trojan.HTML.Agent.II	10.2%	Application:Android/Counterclank. A	6.0%
Streaming Media	6.7%	W32.Generic-5204-0118	5.1%	Adware.GoonSquad	5.7%
Computing and Internet	3.9%	JS:Trojan.JS.Iframe.AM	4.2%	Adware:Android/AirPush. A	4.0%
Chat	2.8%	Trojan.Malscript	3.9%	Adware.JS.Agent.F	3.2%
Peer-To-Peer	2.7%	Trojan.Iframe.BMY	3.3%	Adware:Android/Ropin. A	2.1%
Hosting Sites	2.6%	JS:Trojan.Script.AKB	3.1%	Adware.Clkpotato!gen3	1.9%
Shopping	2.0%	Trojan.JS.Agent.GHF	3.0%	Adware:W32/Baidu.gen!B	1.8%
Games	1.9%	Trojan.Maljava	2.6%	Gen:Application.Heur.cmKfbiBPZXoO	1.7%
News	1.7%	Suspicious.JIT.a	2.6%	Gen:Application.Heur.cmKfbWuUv3fO	0.7%

January 2013

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

Symantec™

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	7.52%
W32.Ramnit!html	7.03%
W32.Ramnit.B	5.57%
W32.Ramnit.B!inf	4.97%
W32.Downadup.B	4.24%
W32.Almanahe.B!inf	2.42%
W32.Virut.CF	2.31%
W32.SillyFDC.BDP!lnk	2.05%
W32.Chir.B@mm(html)	1.24%
W32.SillyFDC	0.99%

For much of 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 17.9% of all malware blocked at the endpoint in January, compared with 8.3 percent for all variants of W32.Sality.

Approximately 40.8 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.