Symantec

SYMANTEC INTELLIGENCE REPORT

JANUARY ⌖ 2014

CONTENTS

Executive Summary

Welcome to the January edition of the Symantec Intelligence report. Symantec Intelligence aims to provide the latest analysis of cyber security threats, trends, and insights concerning malware, spam, and other potentially harmful business risks.

A number of large data breaches were reported during the month of January. The largest new data breach included the exposure of 105.8 million identities in South Korea. (It's worth noting that many individuals in the country had more than one account exposed in this breach.) Another large data breach, previously reported as including 40 million identities, has since had its numbers adjusted upwards and is now estimated at 110 million identities exposed. These two breaches contribute significantly in bringing the total number of identities exposed to over 500 million for the last twelve months.

Targeted attacks are up to their highest level since August of last year, after what appears to be average-to-low attack numbers over the last four months. Manufacturing is the most targeted industry, making up 21.3 percent of attacks. The non-traditional services category, which includes hospitality, recreation, and repair, is a close second at 20.6 percent.

The number of vulnerabilities reported is also up in January after lower numbers reported in November and December of last year. However, at 555 vulnerabilities, this number is still well below October, which reported a high of 663 for the month.

In other news, spam and phishing rates are down slightly in January, while email virus rates are at their lowest levels since October of last year.

We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

Ben Nahorney, Cyber Security Threat Analyst

symantec_intelligence@symantec.com

BIG NUMBERS

Overall Email Phishing Rate:

HIGHER NUMBER = LOWER RISK

Nov	1 in 1,311
Dec	1 in 1,053
Jan	1 in 1,444

Overall Email Virus Rate:

HIGHER NUMBER = LOWER RISK

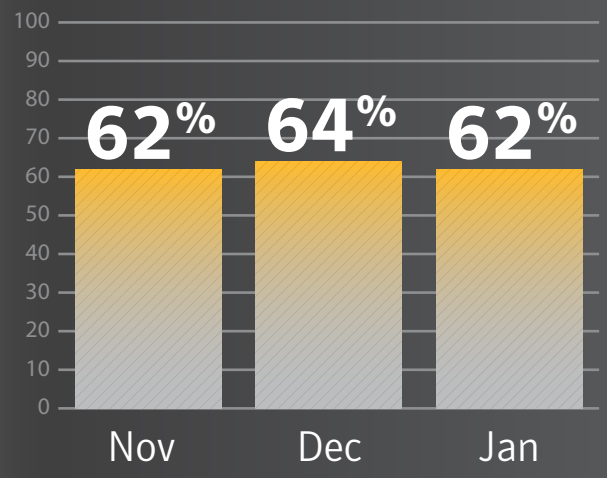
Nov	1 in 253
Dec	1 in 164
Jan	1 in 431

Mobile Vulnerabilities

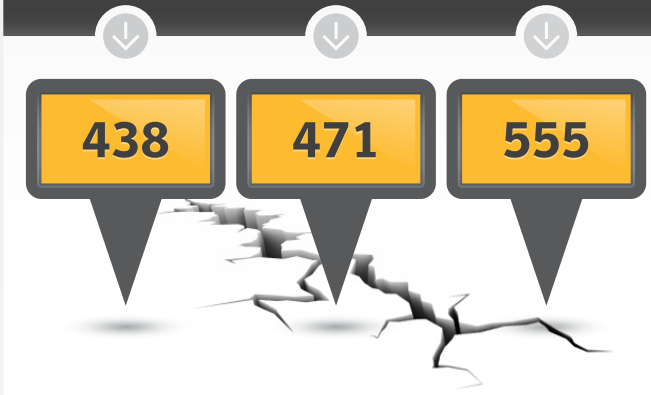
Nov	6
Dec	1
Jan	2

Estimated Global Email Spam Rate Per Day

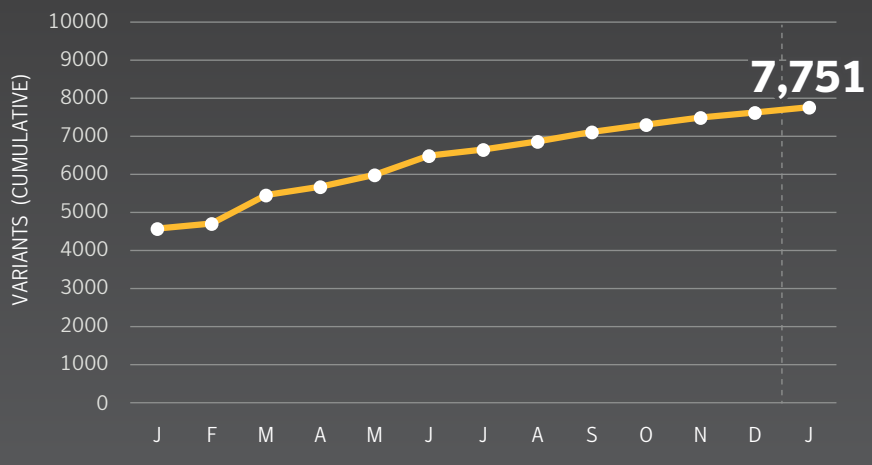
SPAM AS PERCENT OF ALL EMAIL

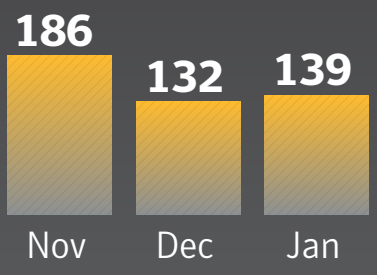


New Vulnerabilities



Mobile Malware Variants





Data Breaches

Number of Breaches (12 month period)

219

Number of Identities Exposed (12 month period)

501,516,310

TARGETED ATTACKS

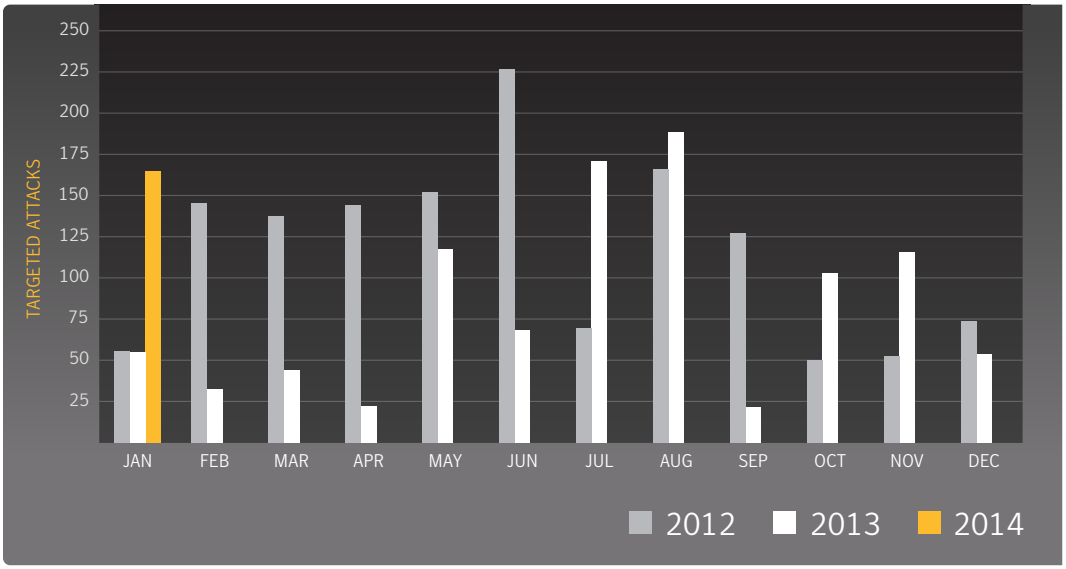
Targeted Attacks

At a Glance

- Targeted attacks were up in January, reaching their highest levels since August of 2013.
- Small companies of 250 employees or less were targeted in 39% of attacks, though organizations with 2500+ employees were targeted more often, based on first attacks.
- The .exe file type was the most common attachment, making up 24.7% of email-based targeted attacks that included file attachments.

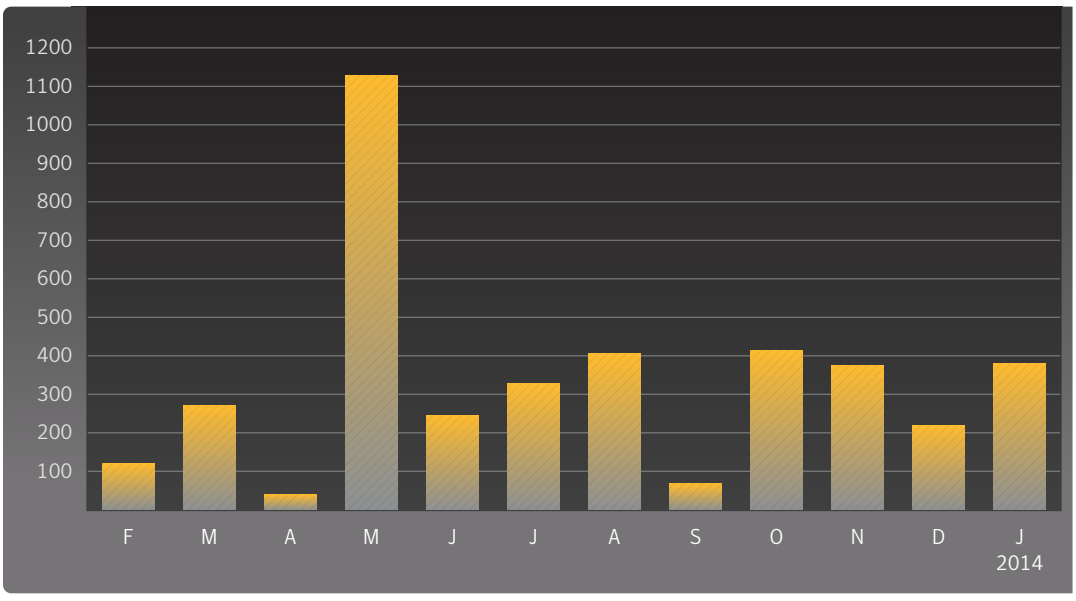
Targeted Attacks per Day

Source: Symantec



First Attacks Logged by Month

Source: Symantec



Attacks by Size of Targeted Organization

Source: Symantec

Company Size	Percent
1-250	38.9%
251-500	9.1%
501-1000	5.8%
1001-1500	3.4%
1501-2500	4.8%
2500+	37.9%

First Attacks Logged by Size

Source: Symantec

Company Size	Percent
1-250	29.2%
251-500	8.5%
501-1000	9.6%
1001-1500	6.0%
1501-2500	7.5%
2500+	39.1%

Top 10 Industries Attacked

Source: Symantec

Industry	Percent
Manufacturing	21.3%
Services - Non Traditional	20.6%
Finance, insurance & Real Estate	13.7%
Services - Professional	11.4%
Wholesale	11.0%
Transportation, communications, electric, gas & Sanitary Services	5.9%
Public Administration	4.2%
Retail	3.2%
Construction	2.2%
Mining	1.5%

The “Professional” services category includes services such as Legal, Accounting, Health, and Education. “Non-Traditional” services include Hospitality, Recreational, and Repair services.

File Extensions of Attachments

Source: Symantec

File Extension	Percent
.exe	24.7%
.doc	11.1%
.scr	8.4%
.au3	7.5%
.jpg	6.2%
.pdf	1.9%
.dat	1.5%
.com	0.4%
.rtf	0.4%
.zip	0.3%

SOCIAL MEDIA

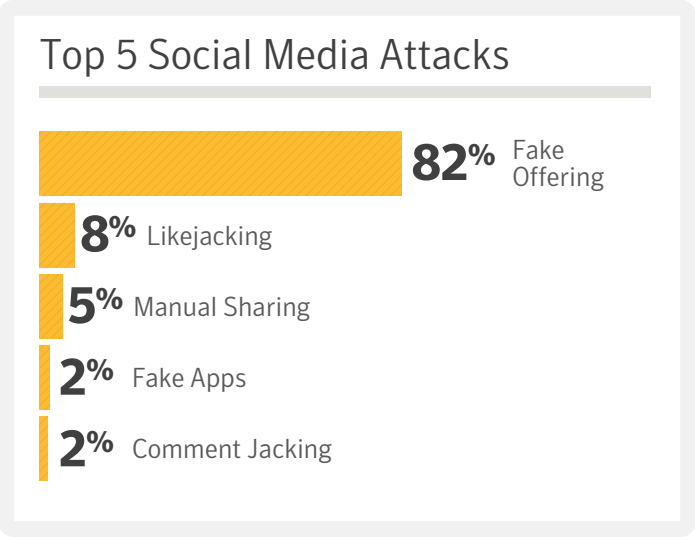
Social Media

At a Glance

- 82 percent of all social media attacks in January where fake offerings.
- Likejacking is the second-most common type of social media attack at 8 percent.

Top 5 Social Media Attacks

Source: Symantec



Methodology

Fake Offering. These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

Fake Plug-in Scams. Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.

Likejacking. Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

Fake Apps. Applications provided by attackers that appear to be legitimate apps; however, they contain a malicious payload. The attackers often take legitimate apps, bundle malware with them, and then re-release it as a free version of the app.

Manual Sharing Scams. These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

DATA BREACHES

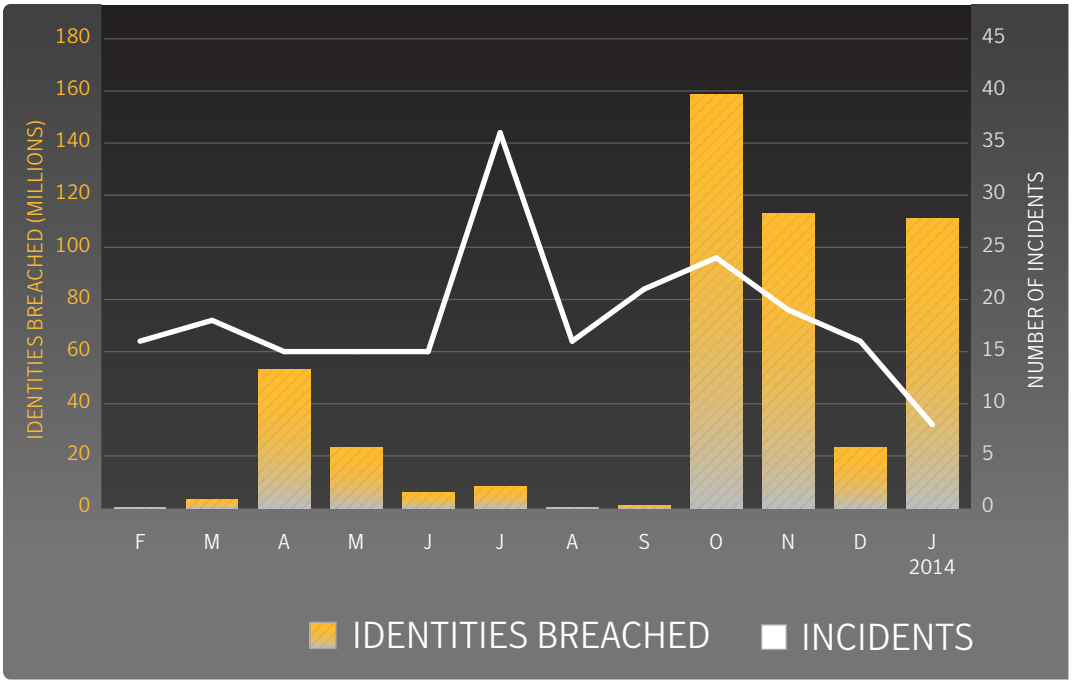
Data Breaches

At a Glance

- The largest data breach that was reported in January resulted in the exposure of 105.8 million identities.
- The reported number of identities exposed in a late-November data breach has since been adjusted upward. This breach is now estimated to have exposed 110 million identities.
- In the last 12 months, more than 500 million identities have been exposed.

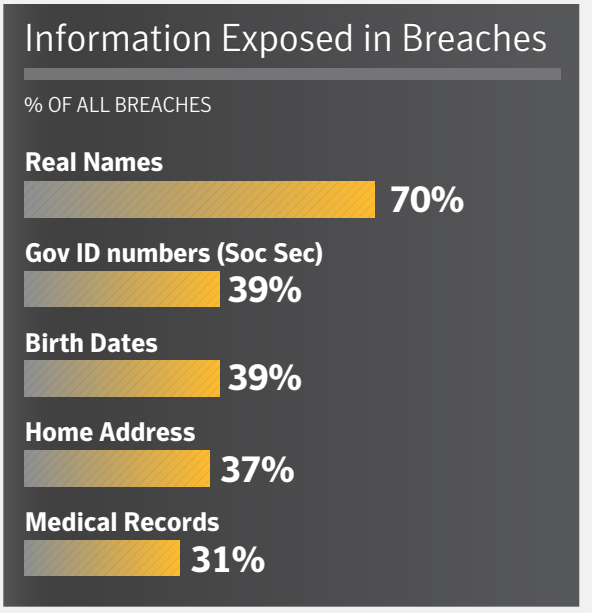
Twelve-Month Timeline of Data Breaches

Source: Symantec



Top 5 Types of Information Exposed

Source: Symantec



Methodology

This data is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model that measures the levels of threats, including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information.

In some cases a data breach is not publicly reported during the same month the incident occurred, or an adjustment is made in the number of identities reportedly exposed. In these cases, the data in the Norton CCI is updated. This causes fluctuations in the numbers reported for previous months when a new report is released.

Norton Cybercrime Index
http://us.norton.com/protect-yourself

MOBILE

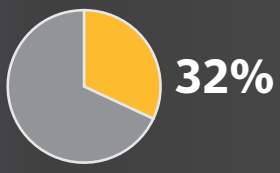
Mobile

At a Glance

- 32 percent of mobile malware discovered over the last 12 months tracks users.
- Traditional threats, such as back doors and downloaders are present in 14 percent of all mobile malware threats.
- Risks that collect data, such as device info and banking details, make up 15 percent of all risks.
- Three new mobile malware families were discovered in January, along with 139 new variants.

Mobile Malware by Type

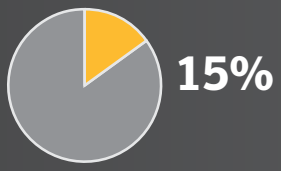
Source: Symantec



32%

Track User

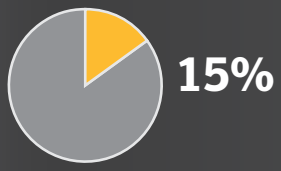
Risks that spy on the individual using the device, collecting SMS messages or phone call logs, tracking GPS coordinates, recording phone calls, or gathering pictures and video taken with the device.



15%

Collect Data

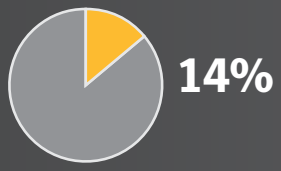
This includes the collection of both device- and user-specific data, such as device information, configuration data, or banking details.



15%

Send Content

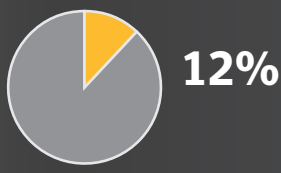
These risks will send text messages to premium SMS numbers, ultimately appearing on the bill of the device's owner. Other risks can be used to send spam messages.



14%

Traditional Threats

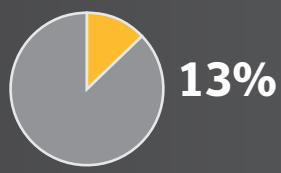
Threats that carry out traditional malware functions, such as back doors and downloaders.



12%

Adware/Annoyance

Mobile risks that display advertising or generally perform actions to disrupt the user.



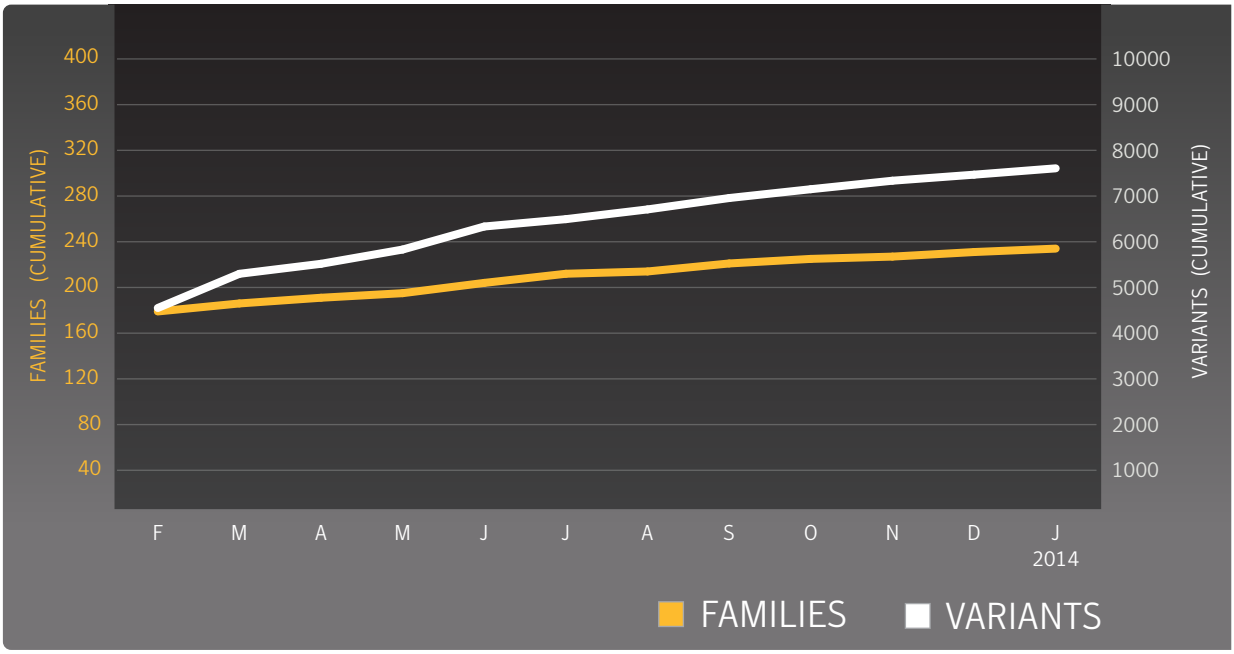
13%

Change Settings

These types of risks attempt to elevate privileges or simply modify various settings within the operating system.

Cumulative Mobile Android Malware

Source: Symantec



VULNERABILITIES

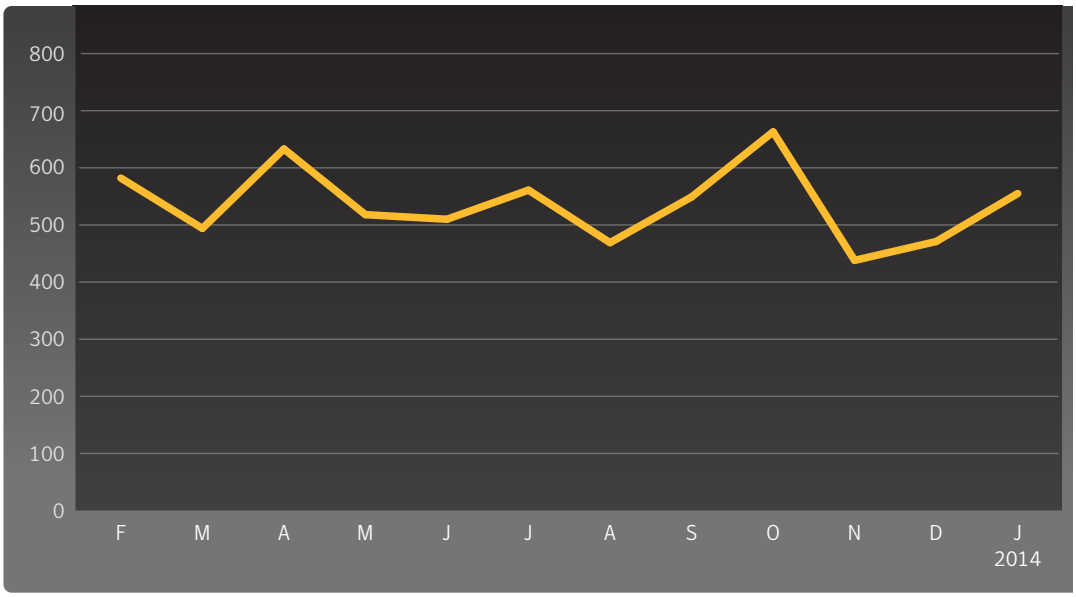
Vulnerabilities

At a Glance

- There were 555 new vulnerabilities discovered in January, bringing the total for the last 12 months to 6443. This is a 17 percent increase over the prior twelve month period.
- There were two vulnerabilities in mobile operating systems disclosed during the month of January.
- Google's Chrome browser continues to lead in reporting browser vulnerabilities, while Oracle's Java leads in reported plug-in vulnerabilities.

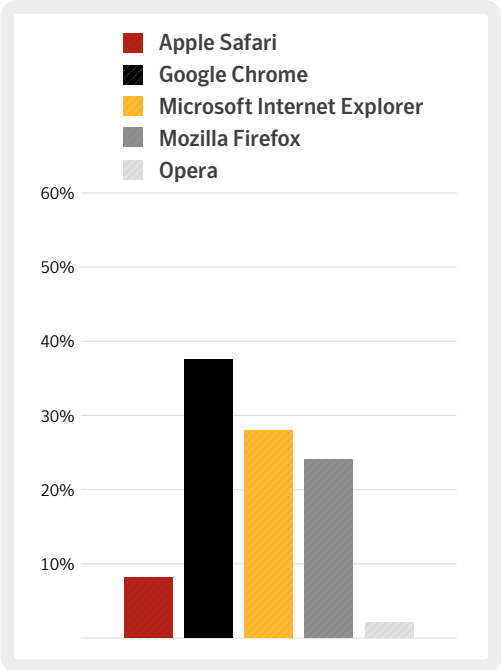
Total Vulnerabilities Disclosed by Month

Source: Symantec



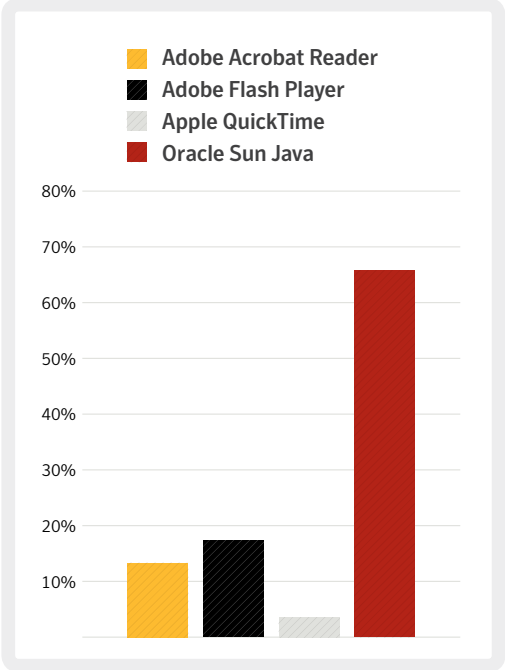
Browser Vulnerabilities

Source: Symantec



Plug-in Vulnerabilities

Source: Symantec



SPAM, PHISHING, & MALWARE

Spam

At a Glance

- The global spam rate decreased 1.9 percentage points in January to 62.1 percent, down from 64.0 percent in December.
- Mining was the most commonly targeted industry at 64.2 percent, followed by Manufacturing at 63.2 percent.
- The .com top-level domain (TLD) was again the most frequently used malicious TLD in January.
- Sex Dating spam is the most common category, at 75.2 percent. Pharmaceutical spam came in second at 20.1 percent.

Top 5 Activity for Spam Destination by Geography

Source: Symantec

Geography	Percent
Sri Lanka	74.7%
Israel	68.8%
Brazil	66.9%
South Africa	65.3%
Kuwait	64.8%

Top 5 Activity for Spam Destination by Industry

Source: Symantec

Industry	Percent
Mining	64.2%
Manufacturing	63.2%
Agriculture, forestry & fishing	62.9%
Services - Professional	62.1%
Construction	62.1%

Top 10 Sources of Spam

Source: Symantec

Source	Percent of All Spam
Canada	7.7%
Spain	6.8%
Russian Federation	6.4%
United States	5.9%
Finland	5.6%
Italy	5.0%
Argentina	4.2%
India	3.7%
Ukraine	3.2%
Romania	3.1%

Average Spam Message Size

Source: Symantec

Month*	0Kb – 5Kb	5Kb – 10Kb	>10Kb
Dec	28.4%	19.2%	52.3%
Nov	37.0%	24.7%	38.4%

*Data lags one month

Top 5 Activity for Spam Destination by Company Size

Source: Symantec

Company Size	Percent
1-250	62.0%
251-500	61.8%
501-1000	62.4%
1001-1500	62.2%
1501-2500	62.0%
2501+	62.3%

Spam by Category

Source: Symantec

Category	Percent
Sex/Dating	75.2%
Pharma	20.1%
Jobs	1.8%
Software	0.8%
Watches	0.8%

Spam URL Distribution Based on Top Level Domain Name

Source: Symantec

Month*	.com	.info	.ru	.biz
Dec	33.1%	13.7%	13.2%	10.3%
Nov	36.7%	12.4%	not listed	9.6%

*Data lags one month

Phishing

At a Glance

- The global phishing rate is down in January, comprising one in 1 in 1,444 email messages. In December this rate was one in 1 in 1,053.
- Financial themes continue to be the most frequent subject matter, with 67.5 percent of phishing scams containing this theme.
- The South Africa had the highest rate in January, where one in 530 emails was a phishing scam.
- The United States tops the list of sources of phishing emails, responsible for distributing 39.9 percent of phishing scams.
- Public Administration was the most targeted industry in January, with one in every 761 emails received in this industry being a phishing scam.

Top 10 Sources of Phishing

Source: Symantec

Source	Percent
United States	39.9%
Australia	27.1%
United Kingdom	24.3%
South Africa	2.4%
Netherlands	1.8%
Sweden	1.5%
Singapore	0.4%
Japan	0.3%
United Arab Emirates	0.3%
New Zealand	0.2%

Top 5 Activity for Phishing Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 1,122
251-500	1 in 1,130
501-1000	1 in 1,463
1001-1500	1 in 1,563
1501-2500	1 in 1,590
2501+	1 in 1,865

Top 5 Activity for Phishing Destination by Industry

Source: Symantec

Industry	Rate
Public Administration	1 in 761
Agriculture, forestry & fishing	1 in 874
Services - Professional	1 in 1,189
Transportation, communications, electric, gas & Sanitary Services	1 in 1,457.2
Construction	1 in 1,571.5

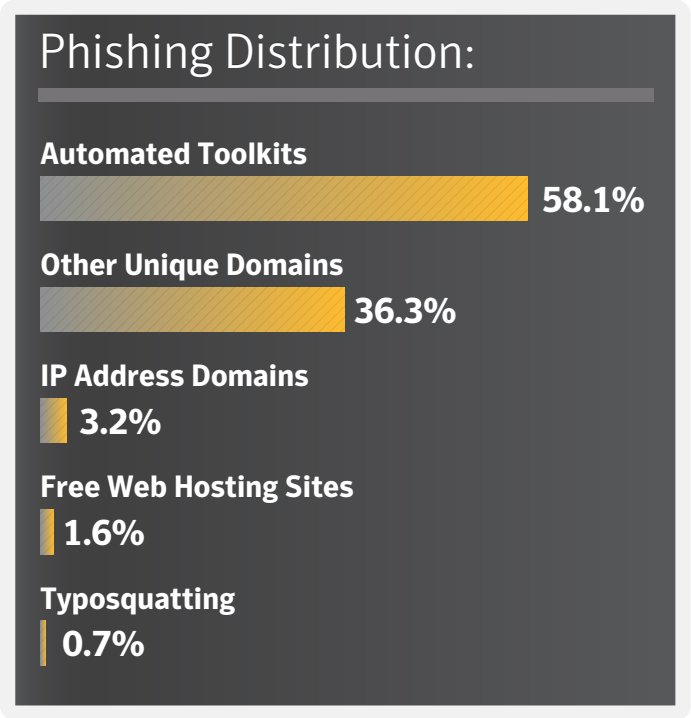
Top 5 Activity for Phishing Destination by Geography

Source: Symantec

Geography	Rate
South Africa	1 in 540
United Kingdom	1 in 731
Australia	1 in 821
Austria	1 in 1,183
New Zealand	1 in 1,215

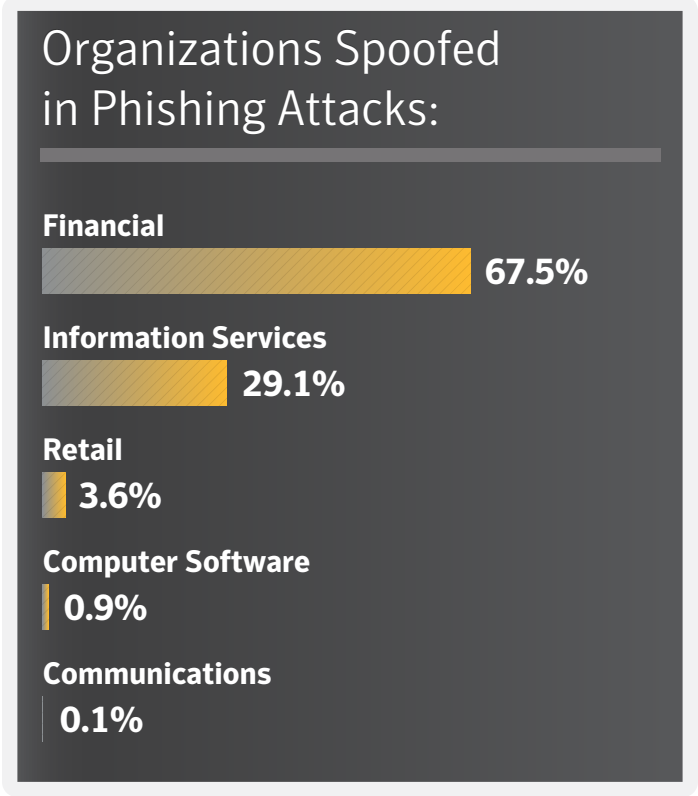
Phishing Distribution

Source: Symantec



Organizations Spoofed in Phishing Attacks

Source: Symantec



Malware

At a Glance

- The global average virus rate in January was one in 431 emails, compared to one in 164 in December.
- Hungary topped the list of geographies, with one in 217 emails containing a virus.
- The United States was the largest source of virus-laden emails, making up 66.5 percent of all email-based viruses.
- Organizations with 250-500 employees were the most targeted company size, where one and 383 emails contained a virus.

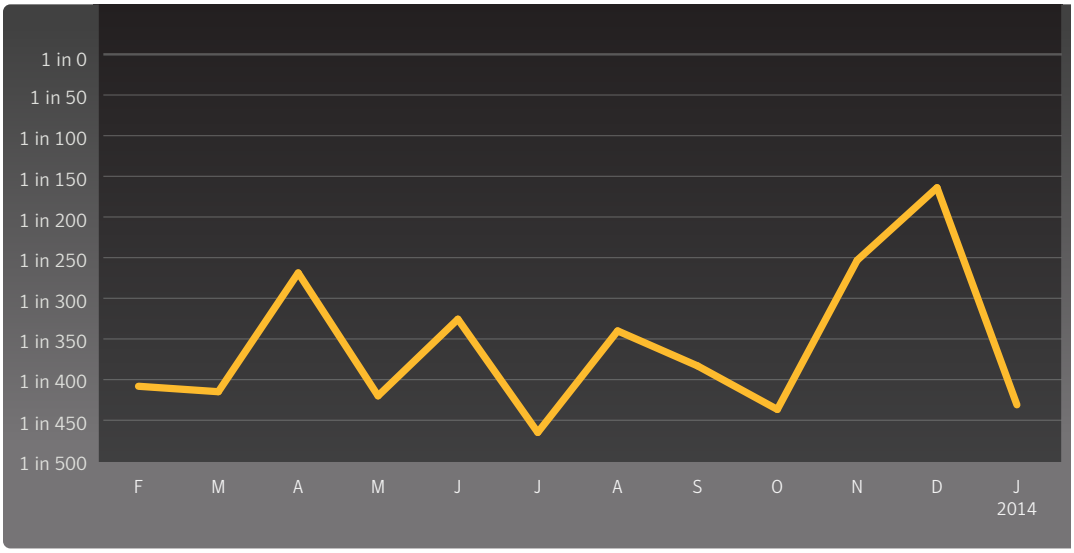
Top 10 Email Virus Sources

Source: Symantec

Geography	Percent
United States	66.5%
United Kingdom	15.0%
Australia	4.1%
Netherlands	2.1%
France	1.8%
Germany	1.2%
Japan	1.2%
South Africa	1.1%
Canada	0.9%
Hong Kong	0.7%

Proportion of Email Traffic in Which Virus Was Detected

Source: Symantec



Top 5 Activity for Malware Destination by Industry

Source: Symantec

Industry	Rate
Public Administration	1 in 309
Agriculture, forestry & fishing	1 in 332
Services - Professional	1 in 343
Wholesale	1 in 397
Services - Non Traditional	1 in 467

Top 5 Activity for Malware Destination by Geographic Location

Source: Symantec

Geography	Rate
Hungary	1 in 217
South Africa	1 in 221
United Kingdom	1 in 287
Hong Kong	1 in 306
Ireland	1 in 344

Top 5 Activity for Malware Destination by Company Size

Source: Symantec

Company Size	Rate
1-250	1 in 398
251-500	1 in 383
501-1000	1 in 459
1001-1500	1 in 396
1501-2500	1 in 475
2501+	1 in 459

Endpoint Security

At a Glance

- Variants of W32.Ramnit accounted for 9.4 percent of all malware blocked at the endpoint.
- In comparison, 6.1 percent of all malware were variants of W32.Sality.
- Approximately 49.5 percent of the most frequently blocked malware last month was identified and blocked using generic detection.

Top 10 Most Frequently Blocked Malware

Source: Symantec

Malware	Percent
W32.Sality.AE	5.4%
W32.Ramnit!html	3.8%
W32.Almanahe.B!inf	3.4%
W32.Downadup.B	3.4%
W32.Ramnit.B	3.1%
Trojan.Zbot	2.5%
W32.Ramnit.B!inf	2.2%
W32.SillyFDC	1.7%
W32.Virut.CF	1.7%
W32.SillyFDC.BDP!lnk	1.0%

Policy Based Filtering

At a Glance

- The most common trigger for policy-based filtering applied by Symantec Web Security .cloud for its business clients was for the "Social Networking" category, which accounted for 51.7 percent of blocked Web activity in January.
- "Advertisement & Popups" was the second-most common trigger, comprising 20.5 percent of blocked Web activity.

Policy Based Filtering

Source: Symantec

Category	Percent
Social Networking	51.7%
Advertisement & Popups	20.5%
Streaming Media	4.3%
Hosting Sites	3.2%
Computing & Internet	2.8%
Chat	1.9%
Search	1.5%
Gambling	1.0%
News	0.9%
Entertainment	0.8%

About Symantec

Symantec protects the world's information and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

More Information

- Security Response Publications: http://www.symantec.com/security_response/publications/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec. Confidence in a connected world.

For specific country offices and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com