Symantec

SYMANTEC INTELLIGENCE REPORT

JANUARY 2015

CONTENTS

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.

Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 41.5 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

The average number of spear-phishing attacks rose to 42 per day in January, up from 33 in December. Finance, Insurance, & Real Estate overtook Manufacturing in the Top-Ten Industries targeted for the month of January. The overall phishing rate also rose slightly in January, to one in 1,004 emails.

There were ten data breaches reported in January that took place during the same month. This number is likely to rise as more data breaches that occurred during the month are reported. In comparison, there were 14 new data breaches reported during January that took place between February and December of 2014.

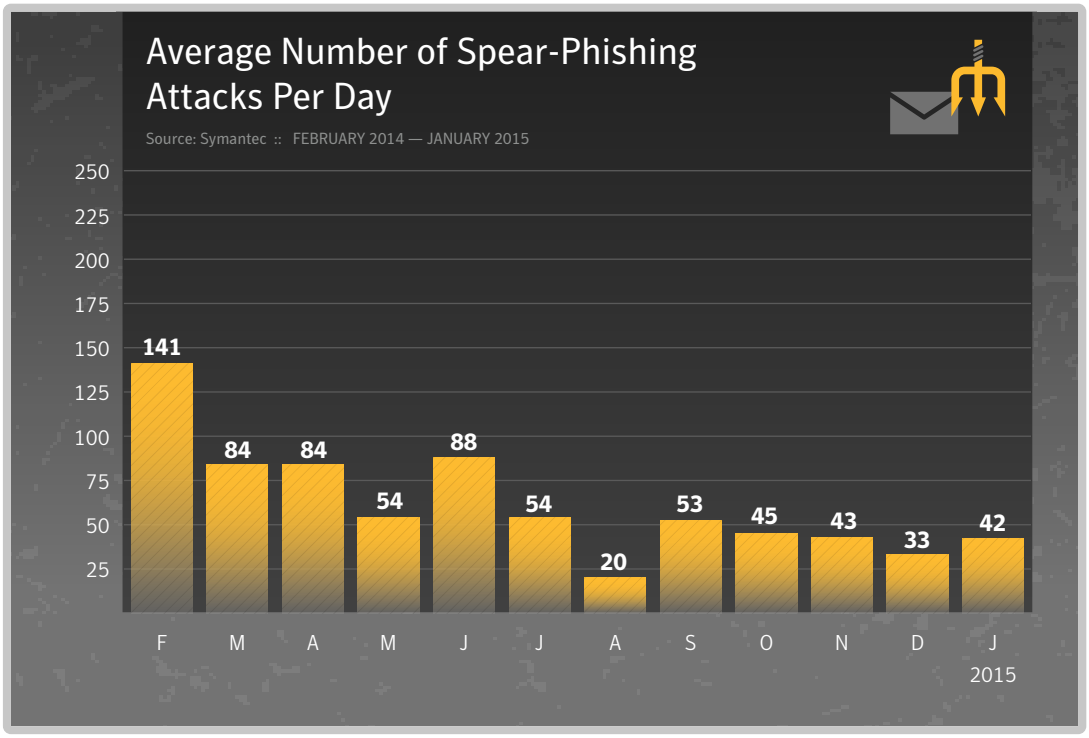
Vulnerabilities are up during the month of January, with 494 disclosed and two zero-days discovered. Google Chrome reported the most browser vulnerabilities during the month of January, after Microsoft Internet Explorer lead for a number of months. Oracle, reporting on the Java program, disclosed the most plug-in vulnerabilities over the same time period. In previous month's Adobe has held the top spot, with its Acrobat and Flash plug-ins.

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

TARGETED ATTACKS + DATA BREACHES

Targeted Attacks



At a Glance

- *The average number of spear-phishing attacks rose to 42 per day in January, up from 33 in December.*
- *The .doc file type was the most common attachment type used in spear-phishing attacks. The .class file type came in second.*
- *Organizations with 1-250 employees were the most likely to be targeted in January.*
- *Finance, Insurance, & Real Estate lead the Top-Ten Industries targeted, followed by Manufacturing.*

Attachments Used in Spear-Phishing Emails

Source: Symantec :: JANUARY 2015

Executable type	January	December
.doc	46.1%	26.7%
.class	9.9%	2.2%
.txt	8.3%	1.3%
.bin	8.0%	1.6%
.xls	7.8%	–
.ace	5.0%	–
.vbs	2.4%	–
.exe	2.0%	15.7%
.pdf	1.9%	1.6%
.rtf	1.3%	–

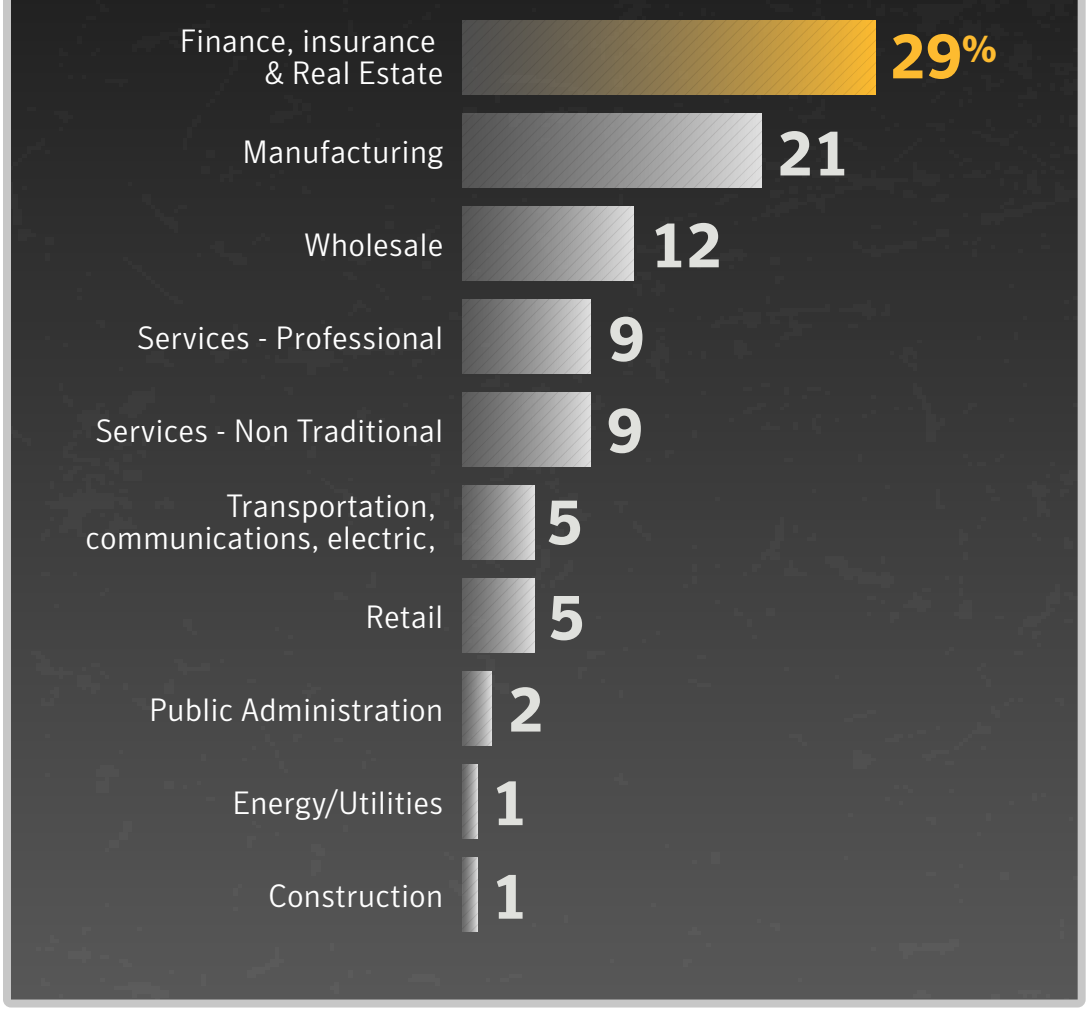
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: JANUARY 2015

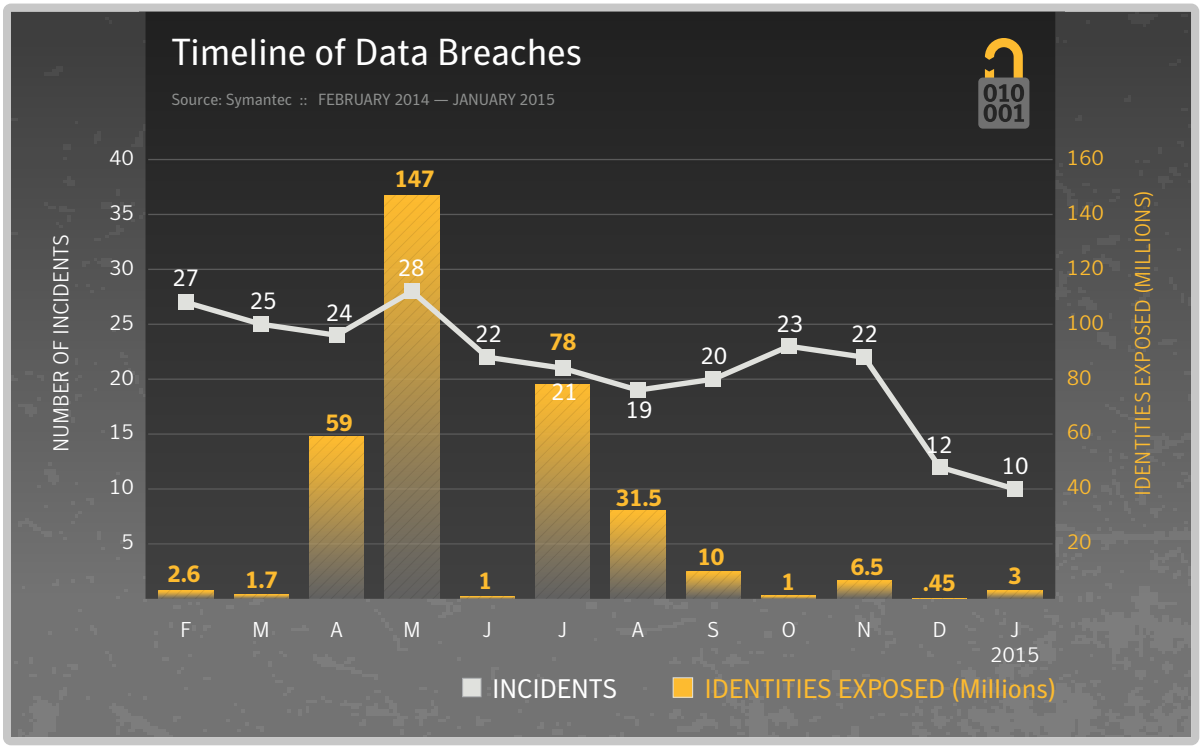
Organization Size	January	December
1-250	35.2%	31.5%
251-500	7.8%	11.5%
501-1000	14.7%	6.6%
1001-1500	4.3%	3.5%
1501-2500	5.3%	9.3%
2500+	32.7%	37.6%

Top-Ten Industries Targeted in Spear-Phishing Attacks

Source: Symantec :: JANUARY 2015

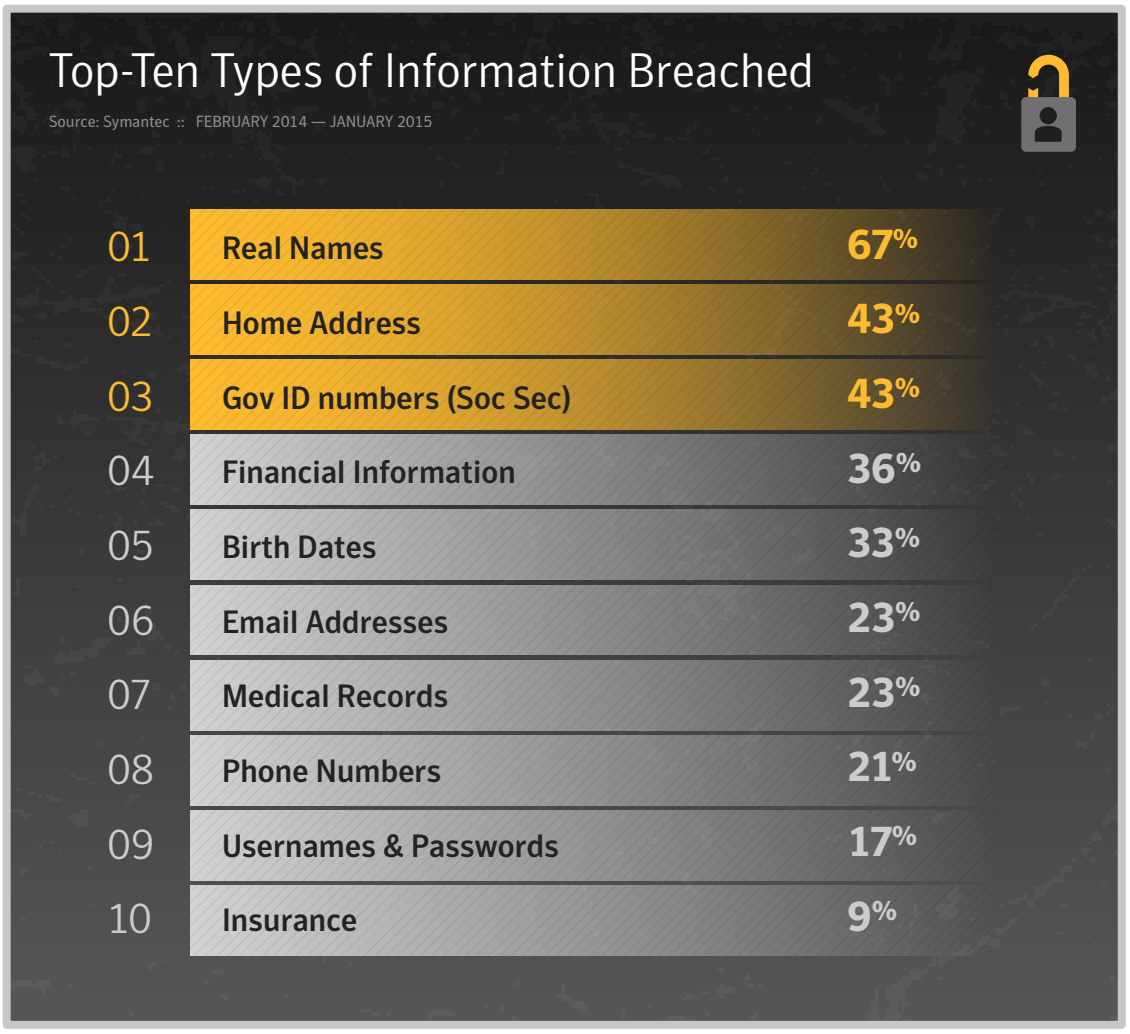


Data Breaches



At a Glance

- *There were ten data breaches reported in January that took place during the same month. This number is likely to rise as more data breaches that occurred during the month are reported.*
- *In comparison, there were 14 new data breaches reported during January that took place between February and December of 2014.*
- *Real names, home addresses, and government ID numbers, such as Social Security numbers, are currently the top three types of data exposed in data breaches.*



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.

MALWARE TACTICS

Malware Tactics

Top-Ten Malware

Source: Symantec :: JANUARY 2015

Rank	Name	January	December
1	W32.Ramnit!html	6.5%	5.1%
2	W32.Almanahe.B!inf	5.8%	5.2%
3	W32.Sality.AE	5.5%	5.0%
4	W32.Ramnit.B	4.4%	3.7%
5	W32.Downadup.B	2.7%	2.4%
6	W32.Ramnit.B!inf	2.7%	2.3%
7	W32.SillyFDC.BDP!lnk	2.1%	1.6%
8	W32.Virut.CF	1.7%	1.7%
9	W97M.Downloader	1.2%	–
10	W32.SillyFDC	1.1%	1.1%

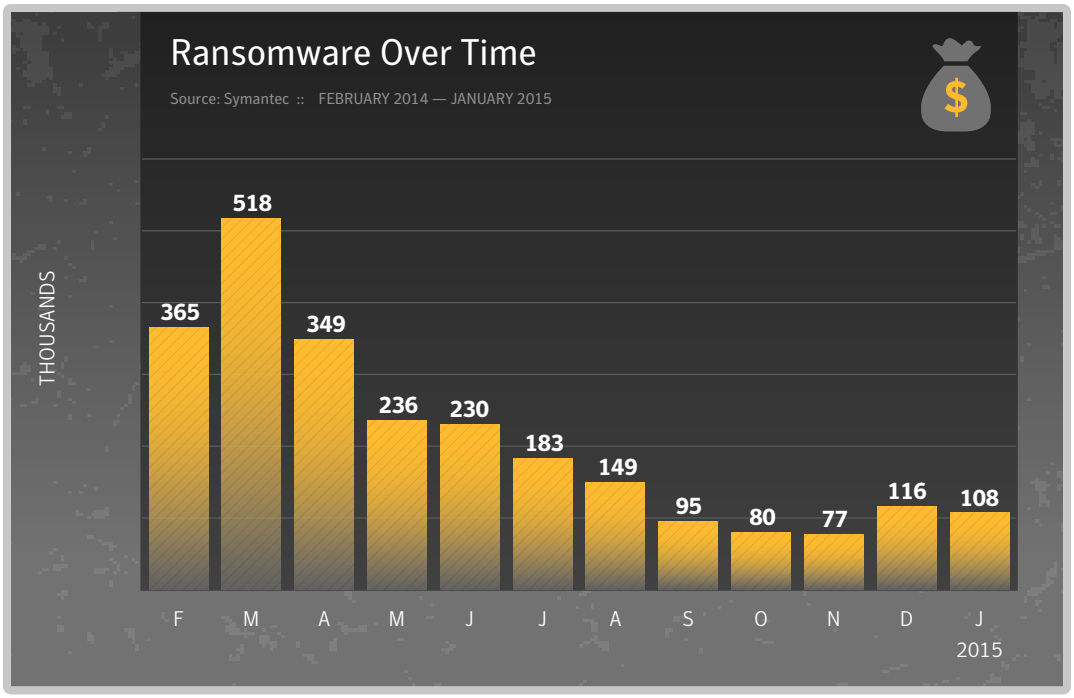
At a Glance

- W32.Ramnit!html *was the most common malware blocked in January.*
- *W32.Ramnit and W32.Sality variants continue to dominate the top-ten malware list.*
- *The most common OSX threat seen on OSX was OSX.RSPlug.A, making up 19.2 percent of all OSX malware found on OSX Endpoints.*
- *The amount of ransomware seen during January decreased slightly when compared to December.*

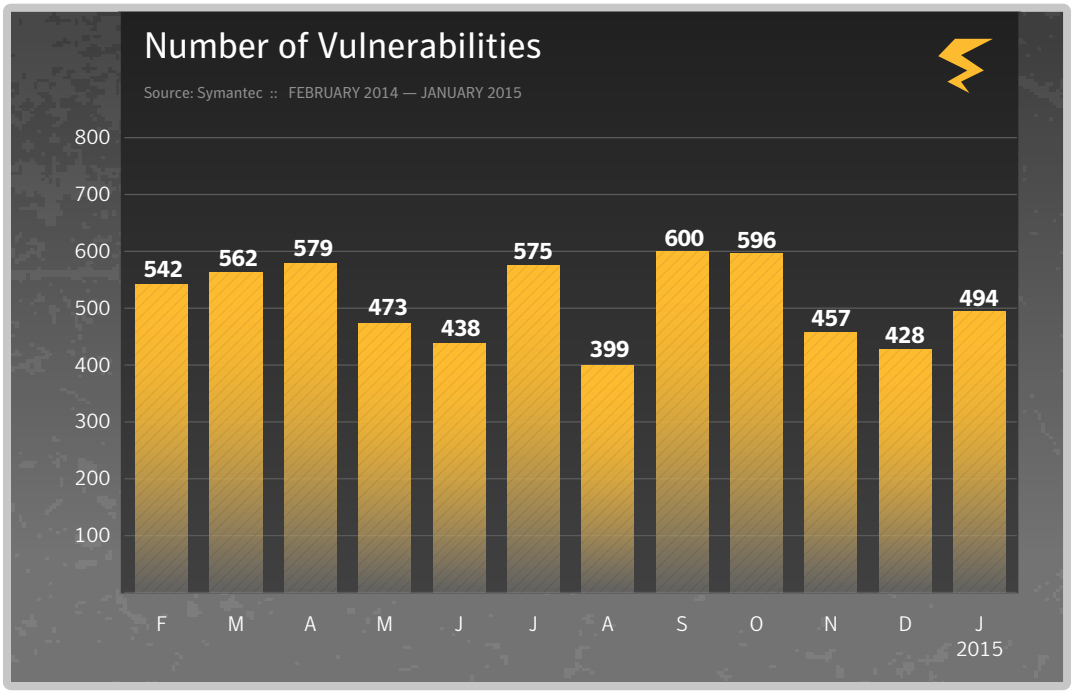
Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: JANUARY 2015

Rank	Malware Name	January	December
1	OSX.RSPlug.A	19.2%	10.1%
2	OSX.Keylogger	18.9%	16.3%
3	OSX.Wirelurker	10.5%	13.6%
4	OSX.Klog.A	9.3%	7.6%
5	OSX.Okaz	8.8%	11.2%
6	OSX.Luaddit	8.0%	9.3%
7	OSX.Stealbit.B	6.1%	4.1%
8	OSX.Flashback.K	3.2%	6.3%
9	OSX.Freezer	2.6%	2.7%
10	OSX.Weapox	2.4%	–

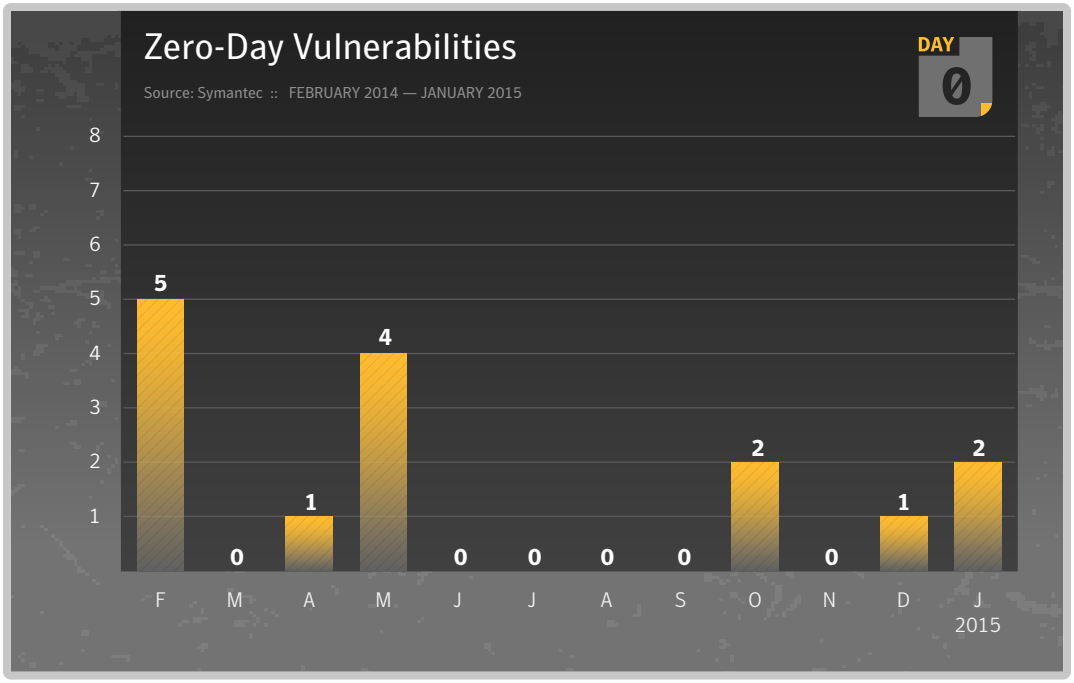

Ransomware Over Time
Source: Symantec :: FEBRUARY 2014 — JANUARY 2015
THOUSANDS
365
518
349
236
230
183
149
95
80
77
116
108
F
M
A
M
J
J
A
S
O
N
D
J
2015

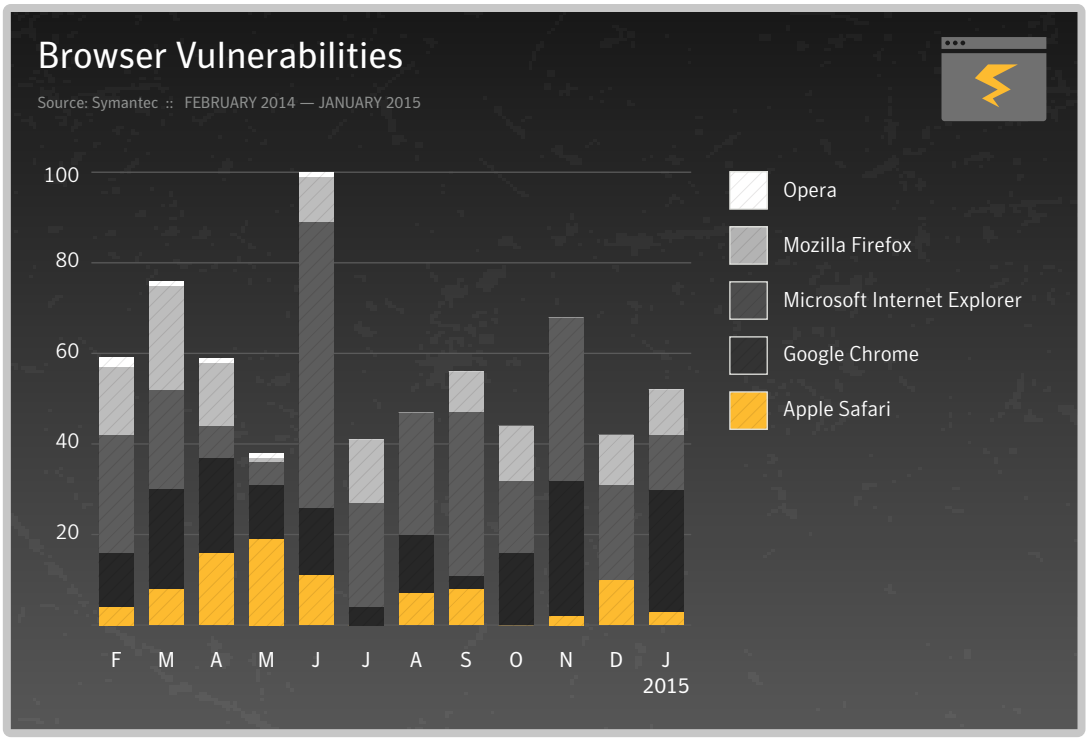
Vulnerabilities

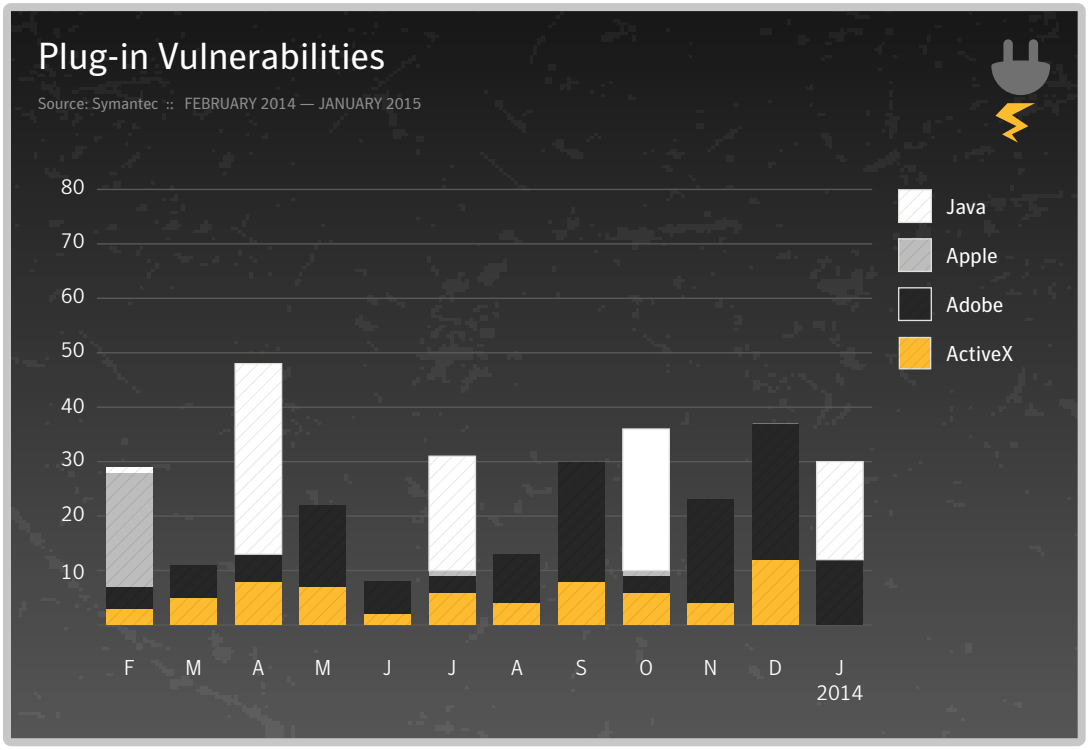


At a Glance

- *There were 494 vulnerabilities disclosed during the month of January.*
- *There were two zero-day vulnerability disclosed during January.*
- *Google Chrome reported the most browser vulnerabilities during the month of January.*
- *Oracle, reporting on the Java program, disclosed the most plug-in vulnerabilities over the same time period.*

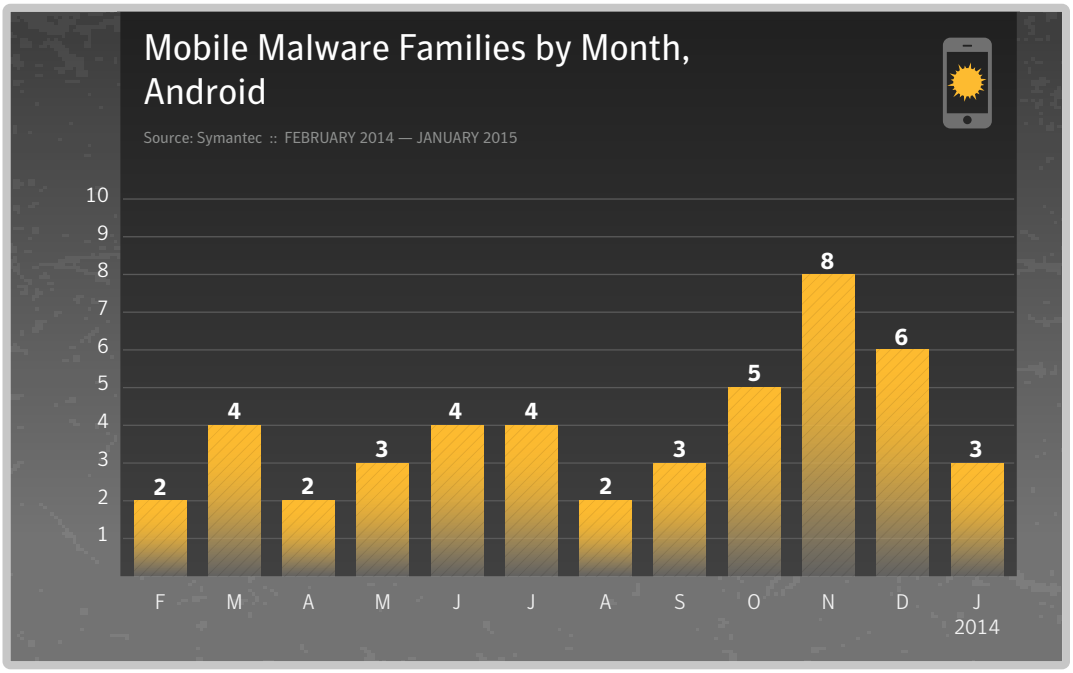



Browser Vulnerabilities
Source: Symantec :: FEBRUARY 2014 — JANUARY 2015
100
80
60
40
20
F M A M J J A S O N D J
2015
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


Plug-in Vulnerabilities
Source: Symantec :: FEBRUARY 2014 — JANUARY 2015
80
70
60
50
40
30
20
10
F M A M J J A S O N D J
2014
Java
Apple
Adobe
ActiveX

MOBILE THREATS

Mobile

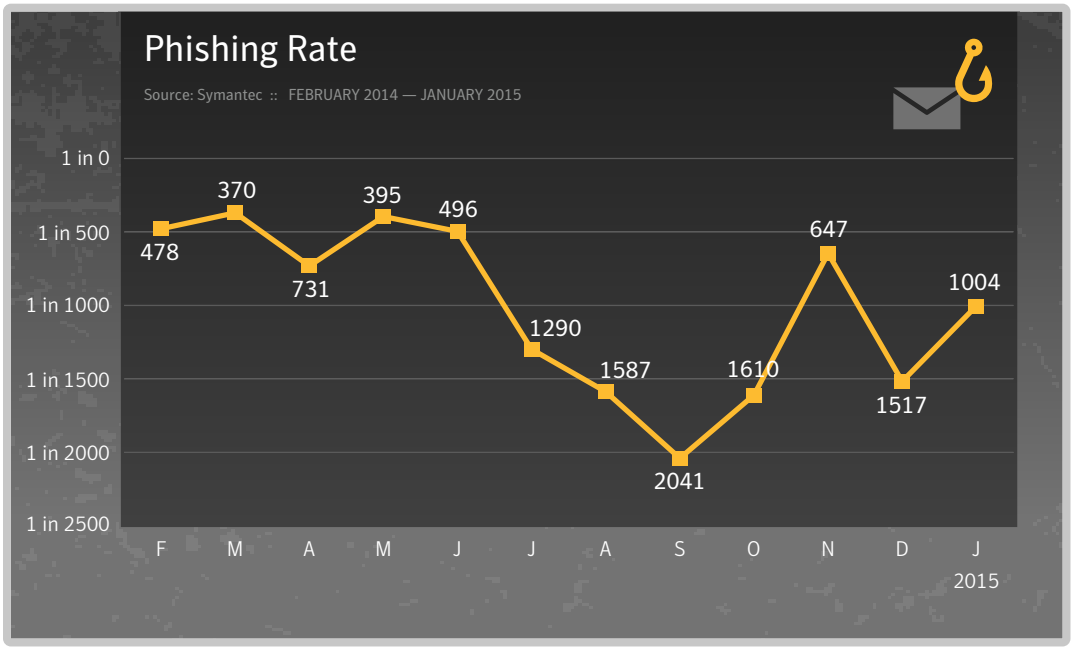


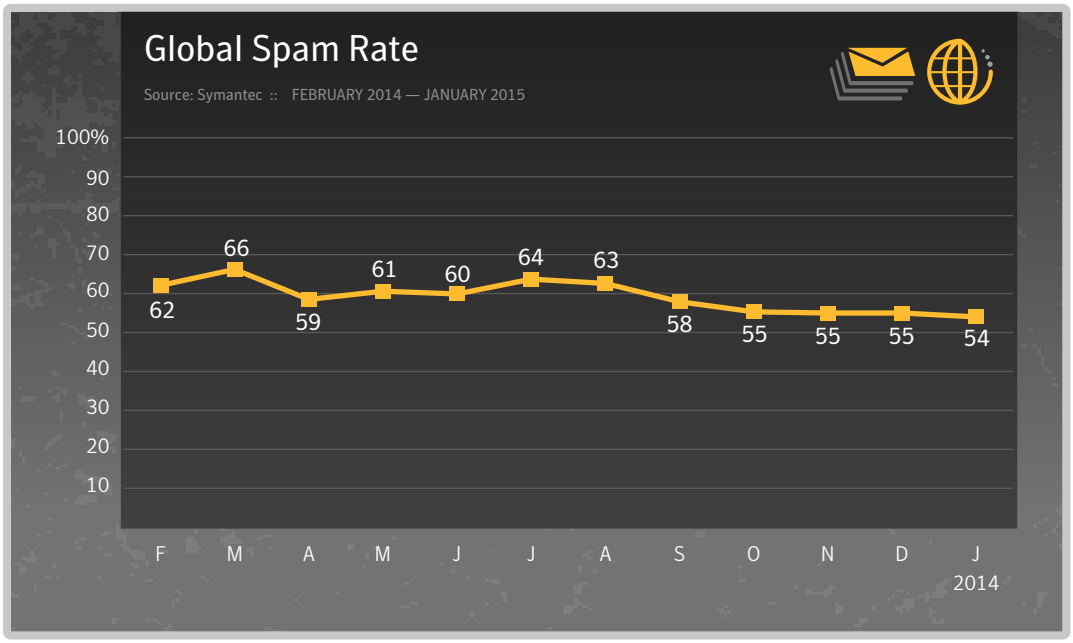
At a Glance

- *There were three Android malware families discovered in January.*

PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

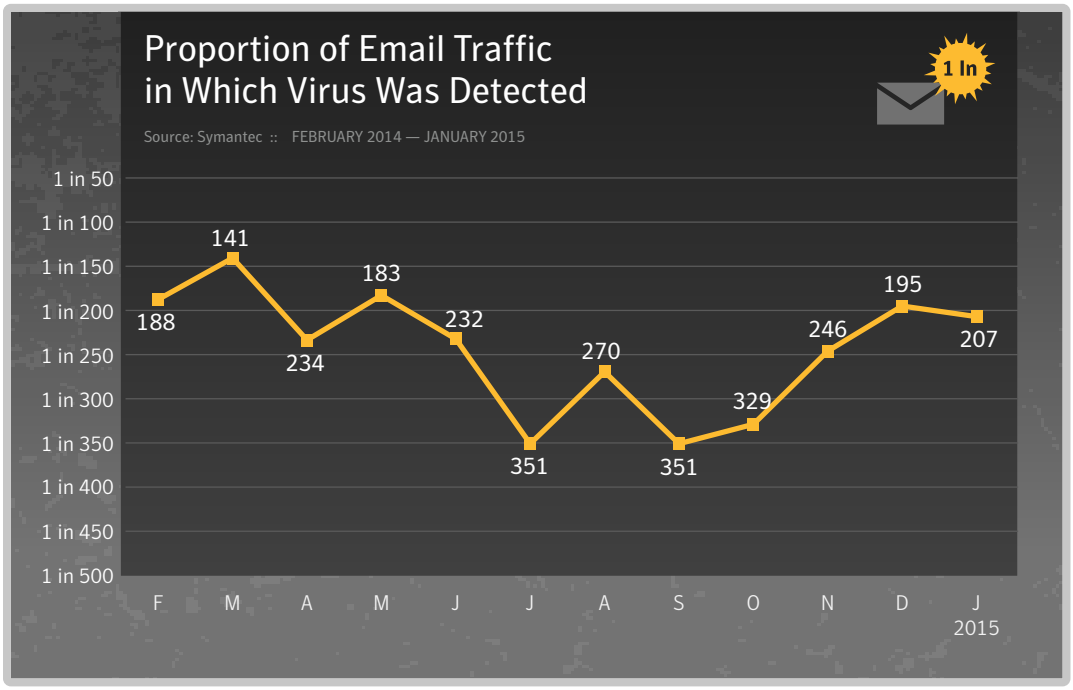


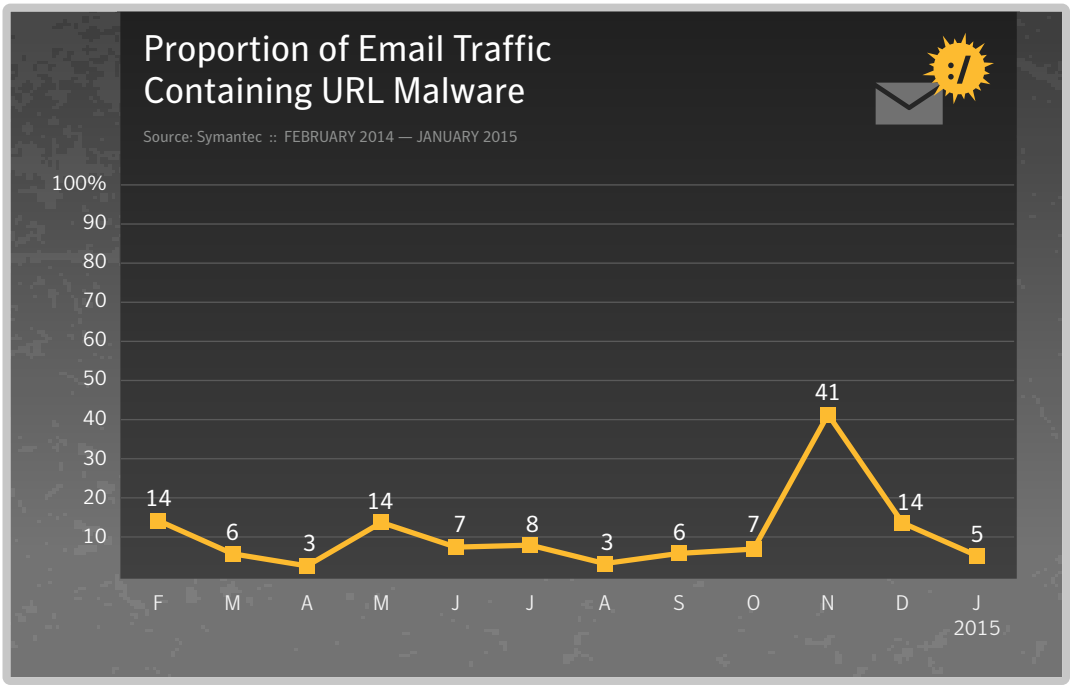


At a Glance

- *The phishing rate rose in January, at one in 1,004 emails, up from one in 1,517 emails in December.*
- *The global spam rate was 54 percent for the month of January.*
- *One out of every 207 emails contained a virus.*
- *Of the email traffic in the month of December, 5 percent contained a malicious URL.*

Email Threats





About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: 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/

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