Symantec

SYMANTEC INTELLIGENCE REPORT

DECEMBER ⌖ 2014

CONTENTS

Summary

Welcome to the December 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.

This month's report takes us through December with a number of rolling 12-month metrics that we've tracked over the last year. However, it's important to point out that this is a snapshot of monthly data for December, as opposed to a year-end summary of activity in 2014. We will be exploring 2014 as a whole in the upcoming Internet Security Threat Report XX, scheduled for publication in the coming months.

In December there were eight data breaches reported that took place within the month of December. This number is likely to rise as more data breaches that occurred during the month are reported in the future. For instance, there were 14 new data breaches reported during December that took place between January and November.

The most commonly encountered malware in December was Trojan.Swifi. This threat is a Trojan horse that may be downloaded from a Web site and exploits a vulnerability in Adobe Flash Player.

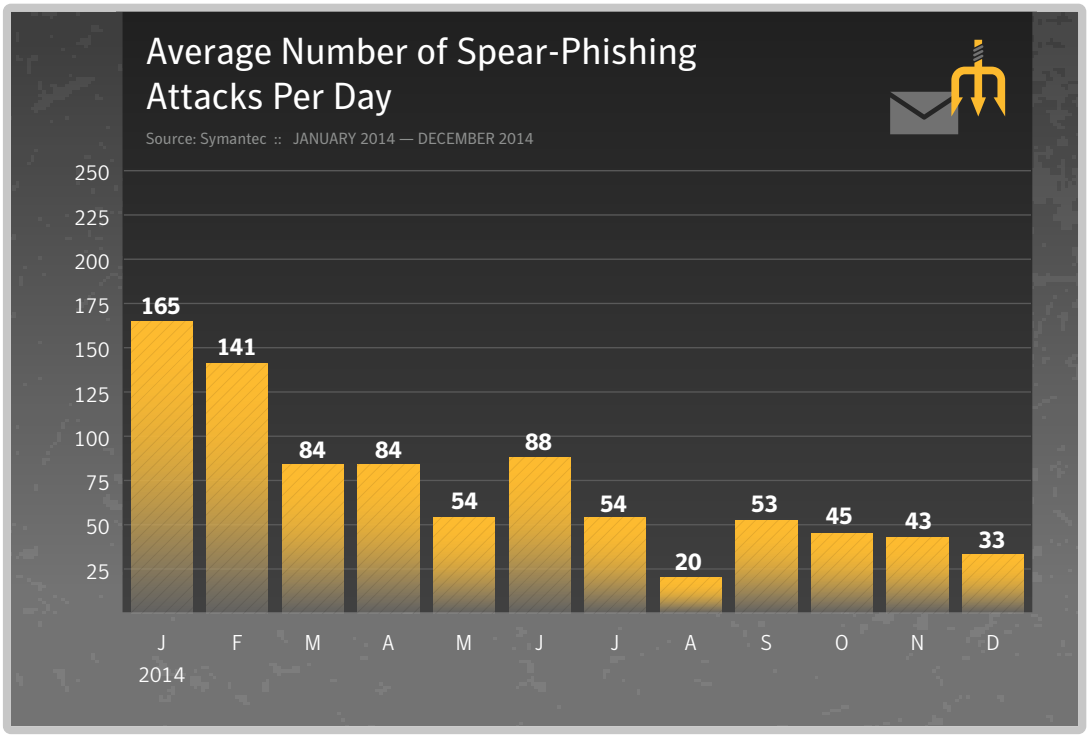
A new zero-day vulnerability was also disclosed during the month of December. The Adobe Flash Player CVE-2014-9163 Stack Based Buffer Overflow Vulnerability may allow attackers to execute arbitrary code within the context of the affected application or result in denial-of-service conditions if the exploit fails.

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 dropped to 33 per day in December, down from 43 in November.*
- *The .doc file type was the most common attachment type used in spear-phishing attacks. The .exe file type came in second.*
- *Organizations with 2500+ employees were the most likely to be targeted in December.*
- *Manufacturing lead the Top-Ten Industries targeted, followed by Finance, Insurance, & Real Estate.*

Attachments Used in Spear-Phishing Emails

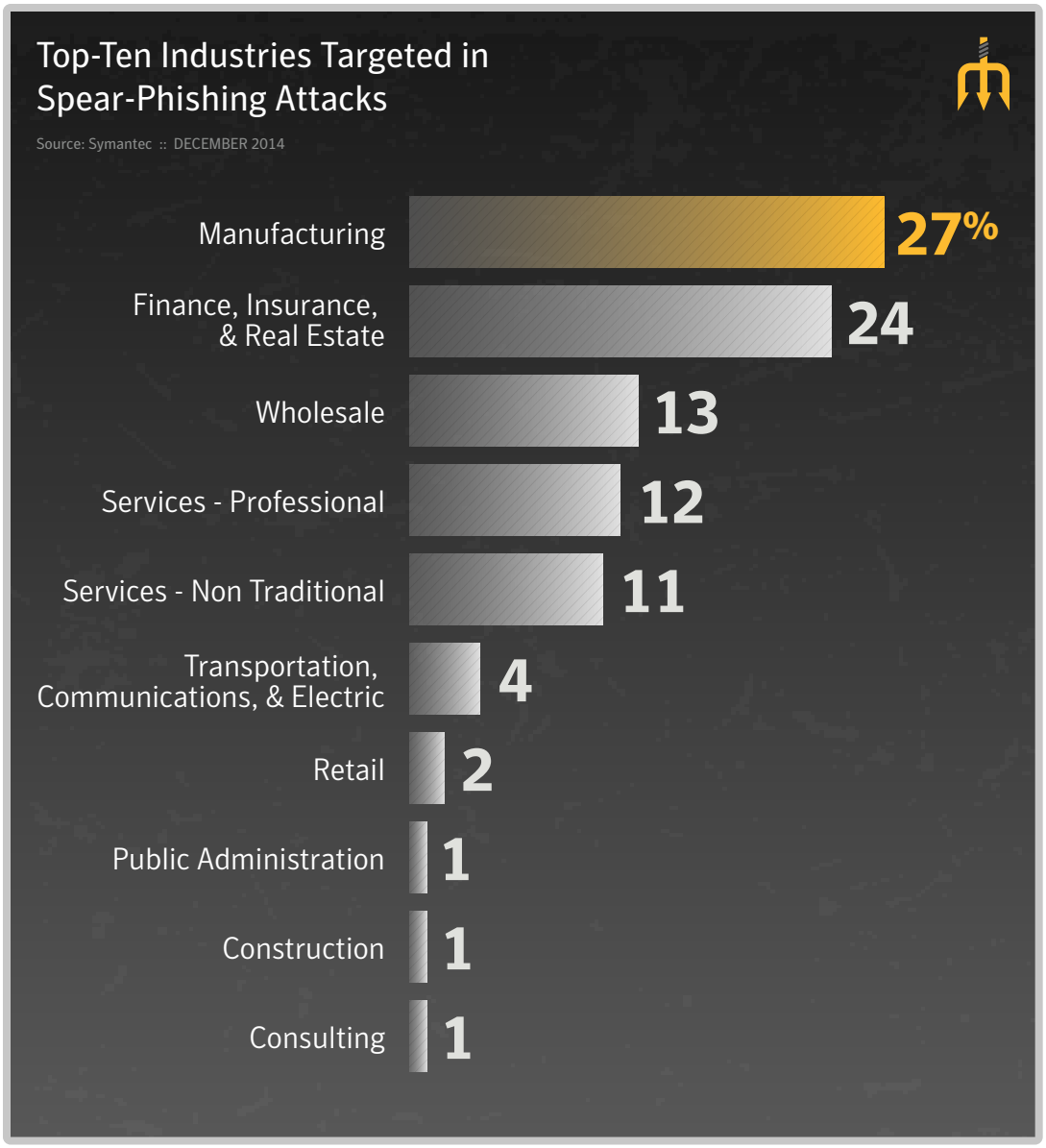
Source: Symantec :: DECEMBER 2014

Executable type	December	November
.doc	26.7%	25.9%
.exe	15.7%	16.4%
.au3	8.2%	8.6%
.scr	5.0%	5.3%
.jpg	4.6%	4.8%
.class	3.4%	2.2%
.pdf	1.6%	1.6%
.bin	1.5%	1.6%
.txt	1.4%	1.3%
.dmp	1.0%	1.0%

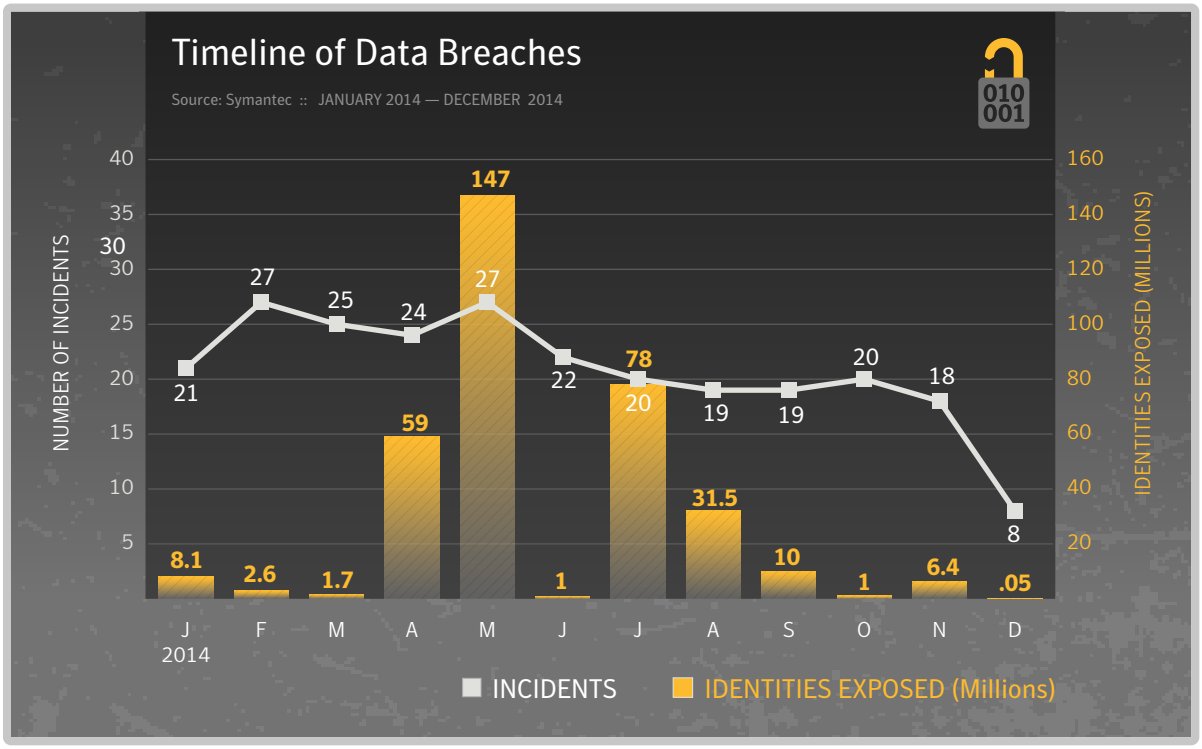
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: DECEMBER 2014

Organization Size	December	November
1-250	31.5%	34.4%
251-500	11.5%	8.4%
501-1000	6.6%	8.8%
1001-1500	3.5%	3.2%
1501-2500	9.3%	4.5%
2500+	37.6%	40.7%

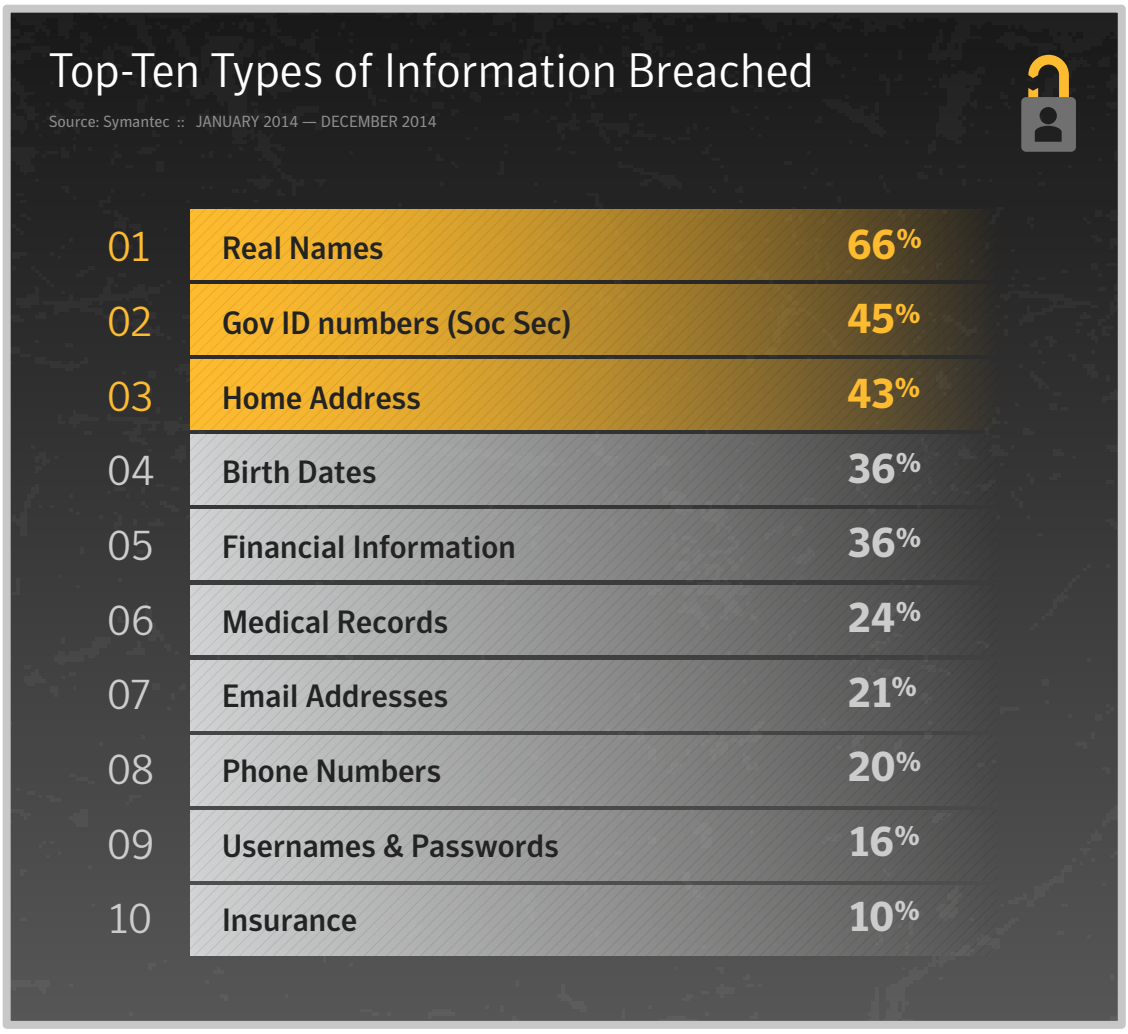

Top-Ten Industries Targeted in Spear-Phishing Attacks
Source: Symantec :: DECEMBER 2014
Manufacturing
27%
Finance, Insurance, & Real Estate
24
Wholesale
13
Services - Professional
12
Services - Non Traditional
11
Transportation, Communications, & Electric
4
Retail
2
Public Administration
1
Construction
1
Consulting
1

Data Breaches



At a Glance

- *There were eight data breaches reported this month that took place during the month of December. 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 December that took place between January and November.*
- *Real names, government ID numbers, such as Social Security numbers, and home addresses 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 :: DECEMBER 2014

Rank	Name	December	November
1	Trojan.Swifi	7.0%	1.4%
2	W32.Almanahe.B!inf	5.2%	4.5%
3	W32.Ramnit!html	5.1%	4.4%
4	W32.Sality.AE	5.0%	4.8%
5	W32.Ramnit.B	3.7%	2.7%
6	W32.Downadup.B	2.4%	3.0%
7	W32.Ramnit.B!inf	2.3%	2.3%
8	W32.Virut.CF	1.7%	1.5%
9	W32.SillyFDC.BDP!lnk	1.6%	1.6%
10	W32.SillyFDC	1.1%	1.4%

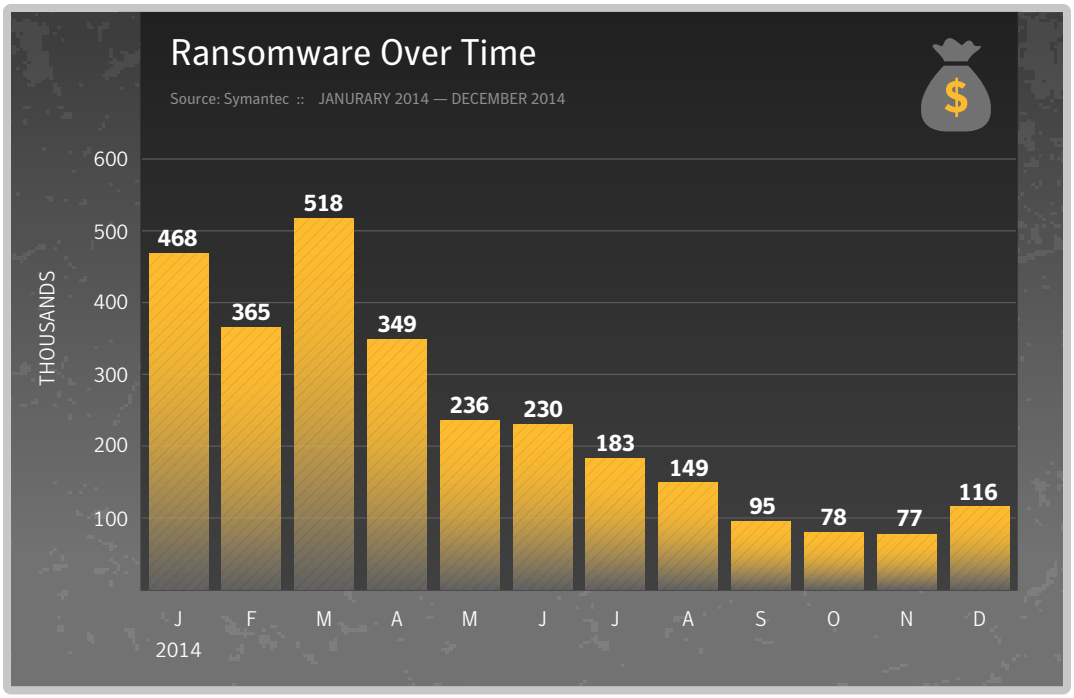
Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: DECEMBER 2014

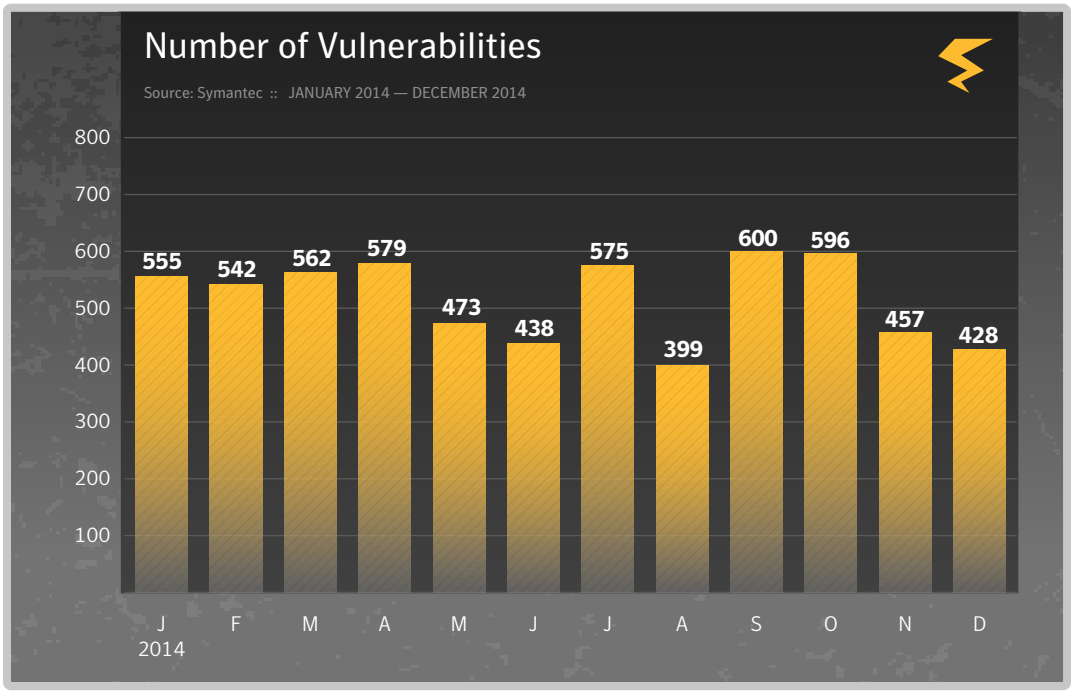
Rank	Malware Name	December	November
1	OSX.Keylogger	16.3%	11.8%
2	OSX.Wirelurker	13.6%	–
3	OSX.Okaz	11.2%	13.4%
4	OSX.RSPlug.A	10.1%	11.0%
5	OSX.Luaddit	9.3%	–
6	OSX.Klog.A	7.6%	8.4%
7	OSX.Flashback.K	6.3%	15.7%
8	OSX.Stealbit.B	4.1%	7.6%
9	OSX.Freezer	2.7%	–
10	OSX.Netweird	2.2%	3.7%

At a Glance

- *Trojan.Swifi was the most common malware blocked in December, up from tenth place in November.*
- *W32.Ramnit variants continue to dominate the top-ten malware list.*
- *The most common OSX threat seen on OSX was OSX.Keylogger, making up 16.3 percent of all OSX malware found on OSX Endpoints.*
- *The amount of ransomware seen during December increased when compared to previous months. Overall ransomware activity has remained low since March of this year.*

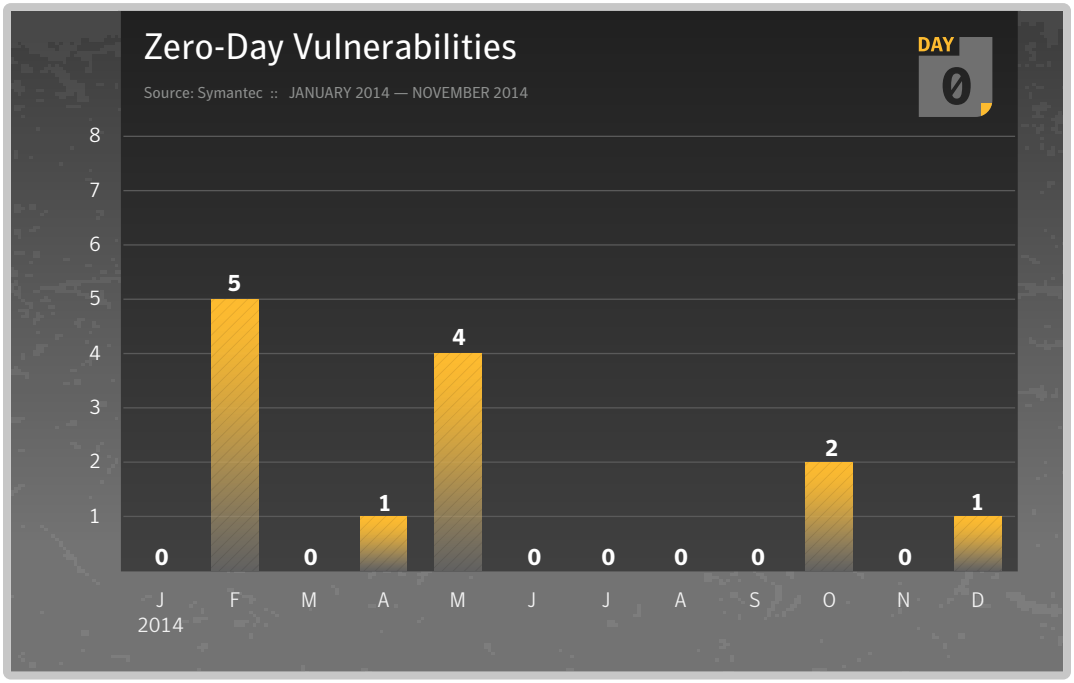

Ransomware Over Time
Source: Symantec :: JANURARY 2014 — DECEMBER 2014
THOUSANDS
600
500
400
300
200
100
468
365
518
349
236
230
183
149
95
78
77
116
J
F
M
A
M
J
J
A
S
O
N
D
2014

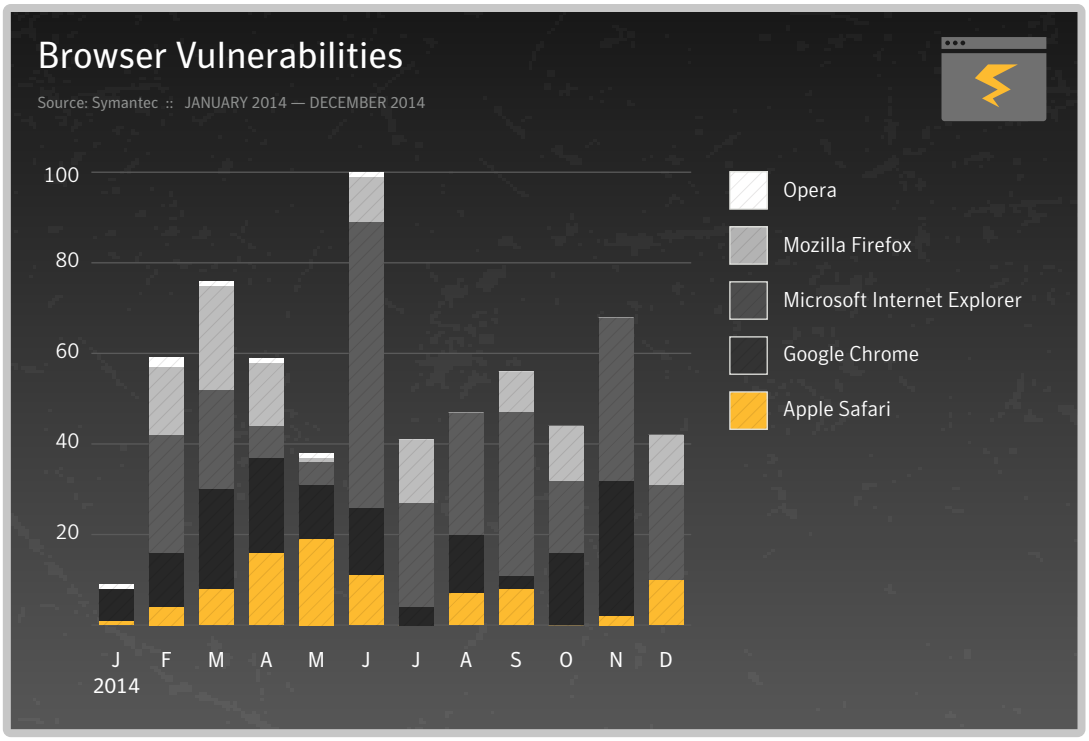
Vulnerabilities

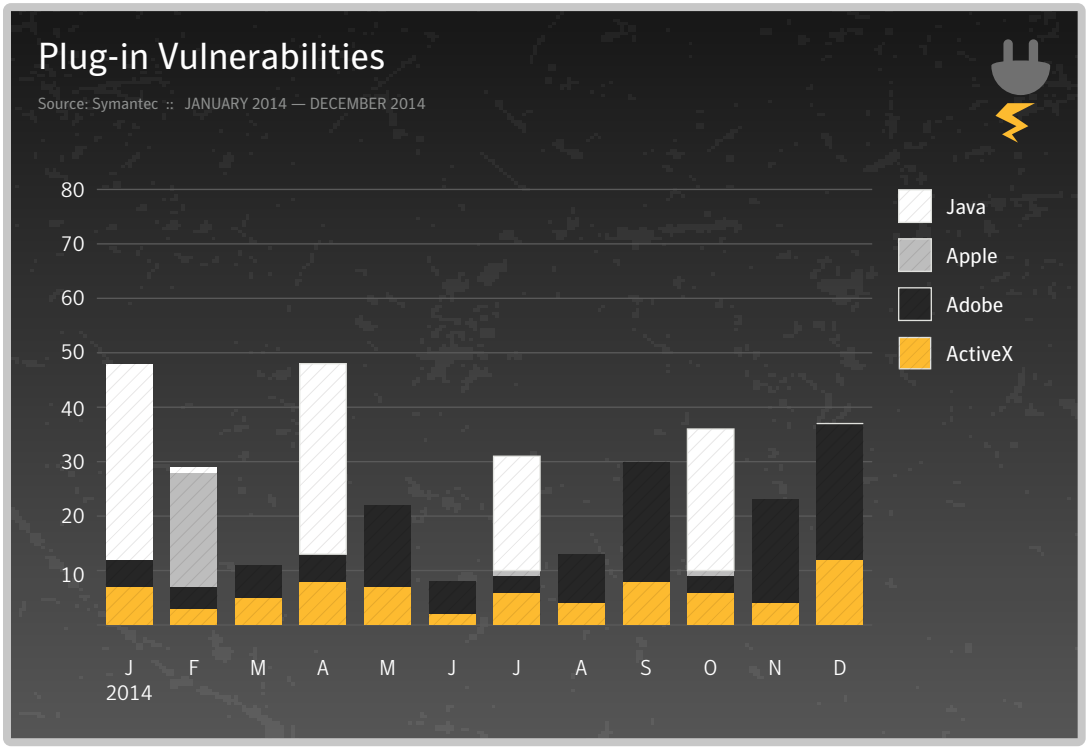


At a Glance

- *There were 428 vulnerabilities disclosed during the month of December.*
- *There was one zero-day vulnerability disclosed during December (CVE-2014-9163).*
- *Internet Explorer has reported the most browser vulnerabilities during the month of December.*
- *Adobe, reporting on Acrobat and Flash programs, disclosed the most plug-in vulnerabilities over the same time period.*

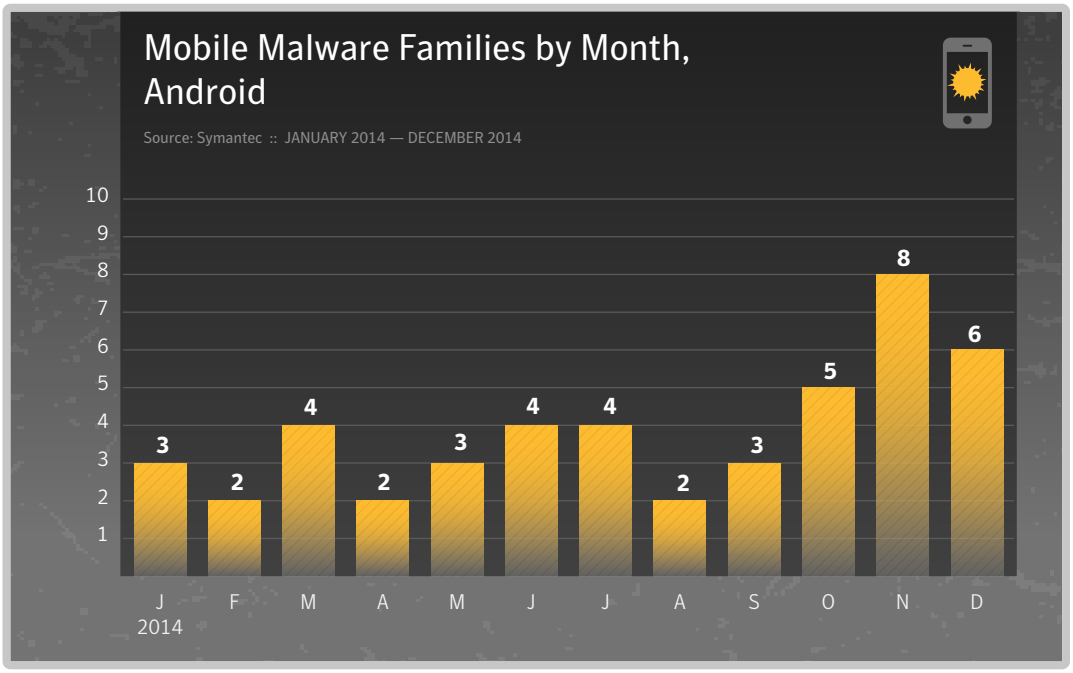



Browser Vulnerabilities
Source: Symantec :: JANUARY 2014 — DECEMBER 2014
100
80
60
40
20
J
F
M
A
M
J
J
A
S
O
N
D
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


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

MOBILE THREATS

Mobile

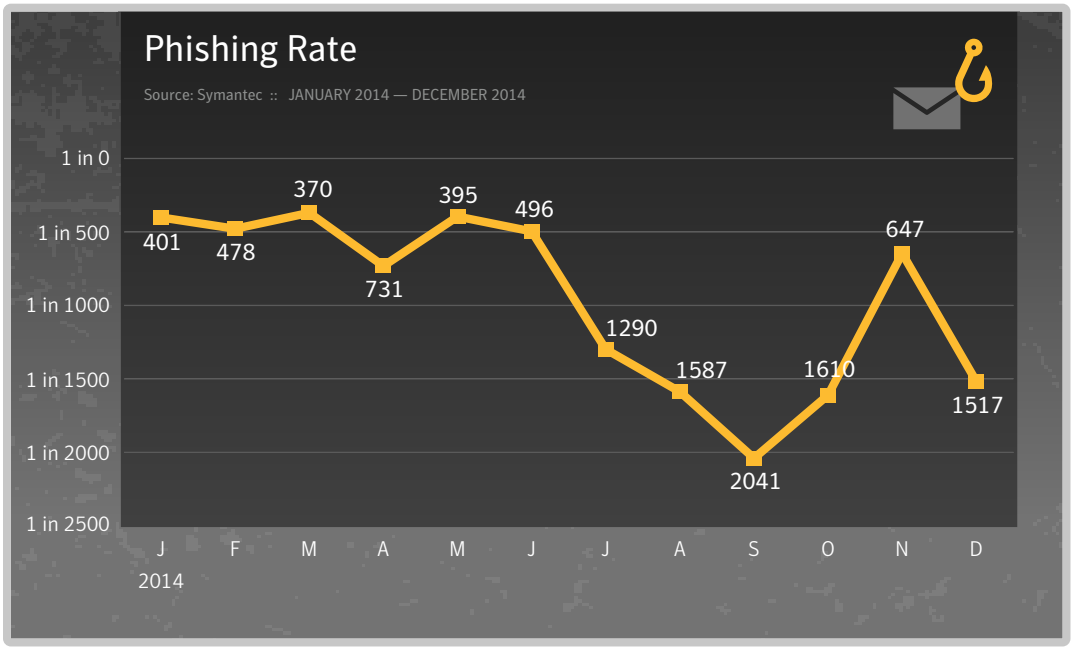


At a Glance

- *There were six Android malware families discovered in December.*

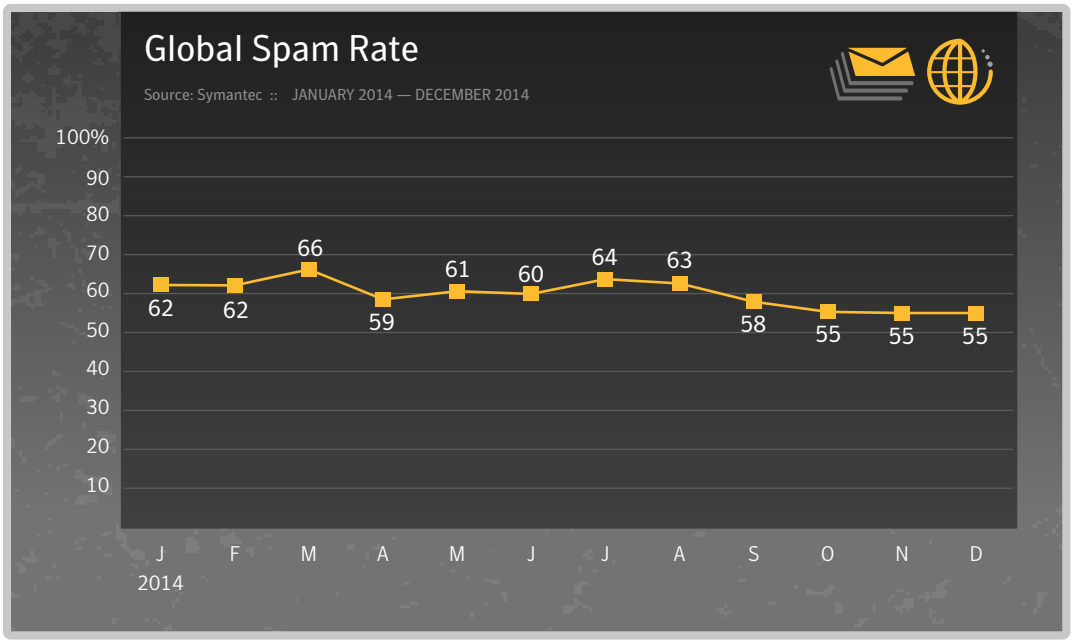
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

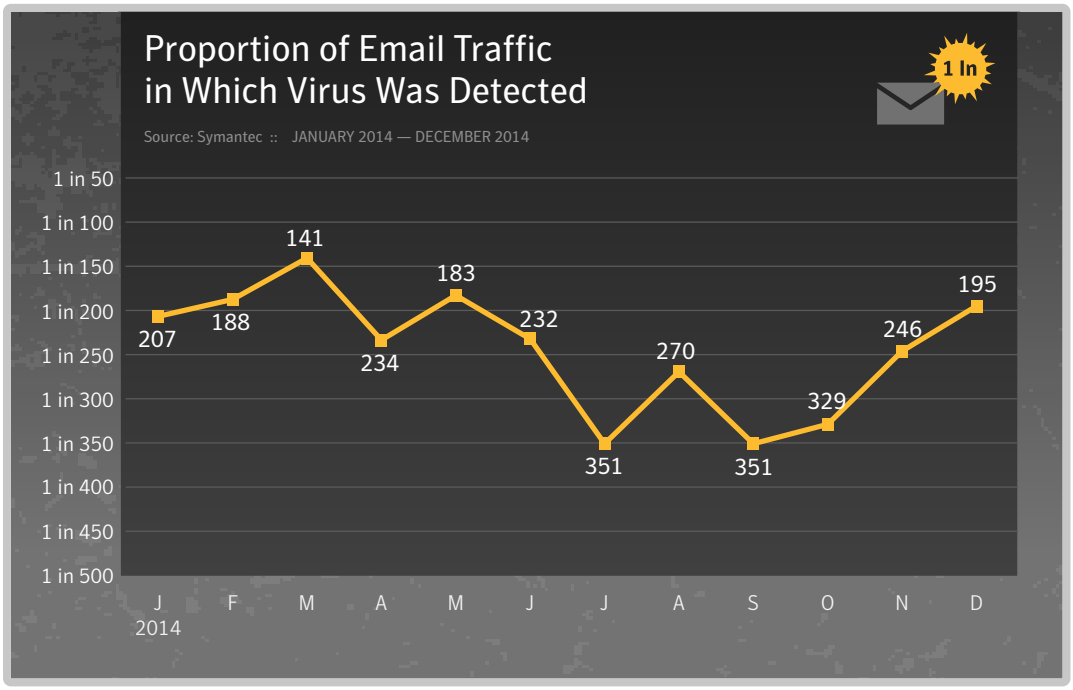


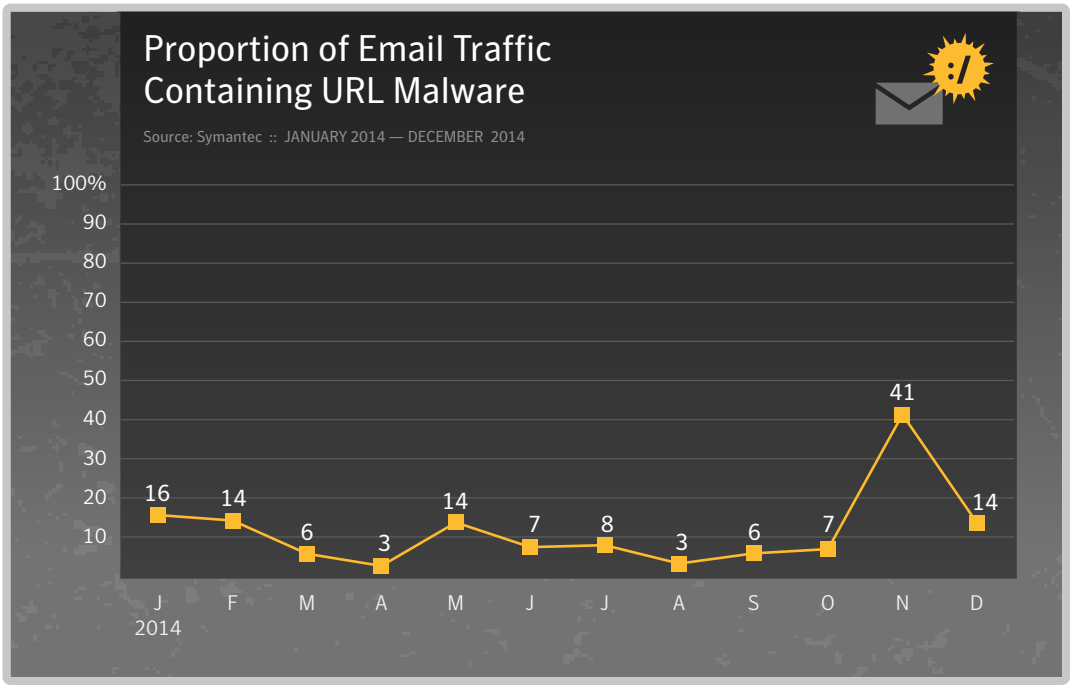
At a Glance

- *The phishing rate dropped in December, at one in 1,517 emails, down from one in 647 emails in December.*
- *The global spam rate was 55.3 percent for the month of December.*
- *One out of every 195 emails contained a virus.*
- *Of the email traffic in the month of December, 14 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