Symantec

SYMANTEC INTELLIGENCE REPORT

FEBRUARY 2015

CONTENTS

Summary

Welcome to the February 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.

W32.Ramnit!html was the most common malware blocked in February. W32.Ramnit variants have dominated the top-ten malware list for quite some time. However, near the end of the month, a law enforcement operation led by Europol and assisted by Symantec, Microsoft, and a number of other industry partners, seized infrastructure owned by the cybercrime group behind Ramnit. It is likely that Ramnit's placement within the top ten list will be impacted by these actions in the coming months.

The largest data breach reported during February took place in January, and resulted in the exposure of 80 million identities. There were six data breaches reported in February that took place during the same month. This number is likely to rise as more data breaches that occurred during the month are reported.

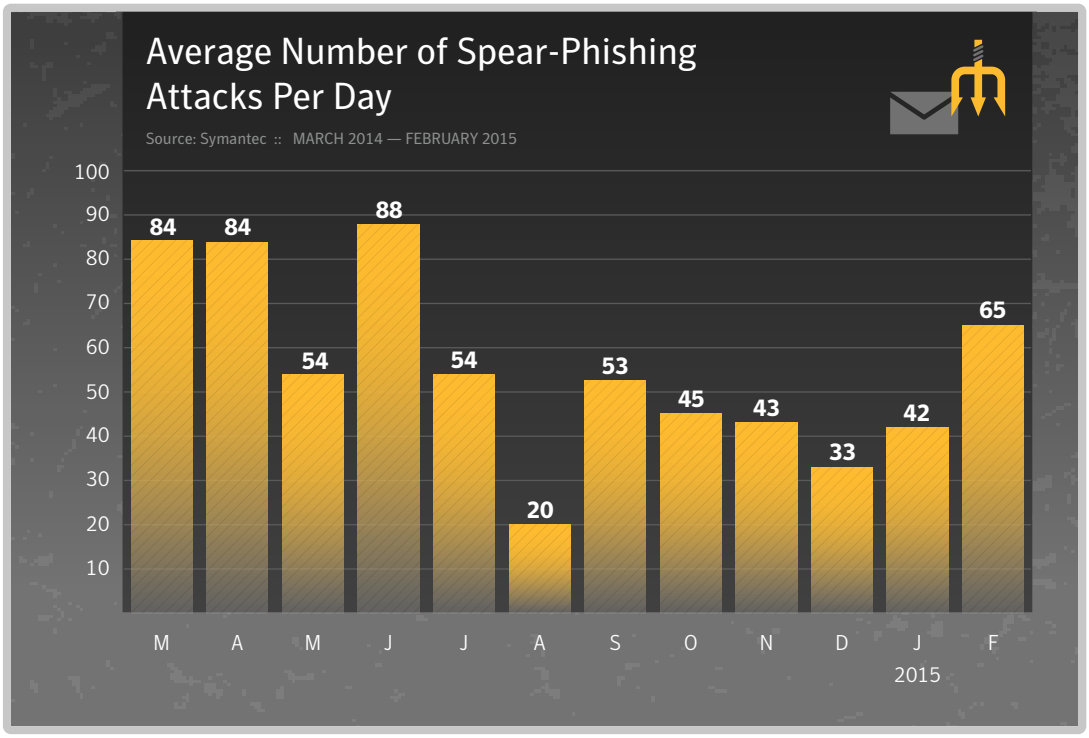
In other news, the average number of spear-phishing attacks rose to 65 per day in February, up from 42 in January. There were 400 vulnerabilities and one zero-day vulnerability disclosed during February.

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 65 per day in February, up from 42 in January.*
- *The .doc file type was the most common attachment type used in spear-phishing attacks. The .txt file type came in second.*
- *Organizations with 2500+ employees were the most likely to be targeted in February.*
- *Finance, Insurance, & Real Estate lead the Top-Ten Industries targeted, followed by Manufacturing.*

Attachments Used in Spear-Phishing Emails

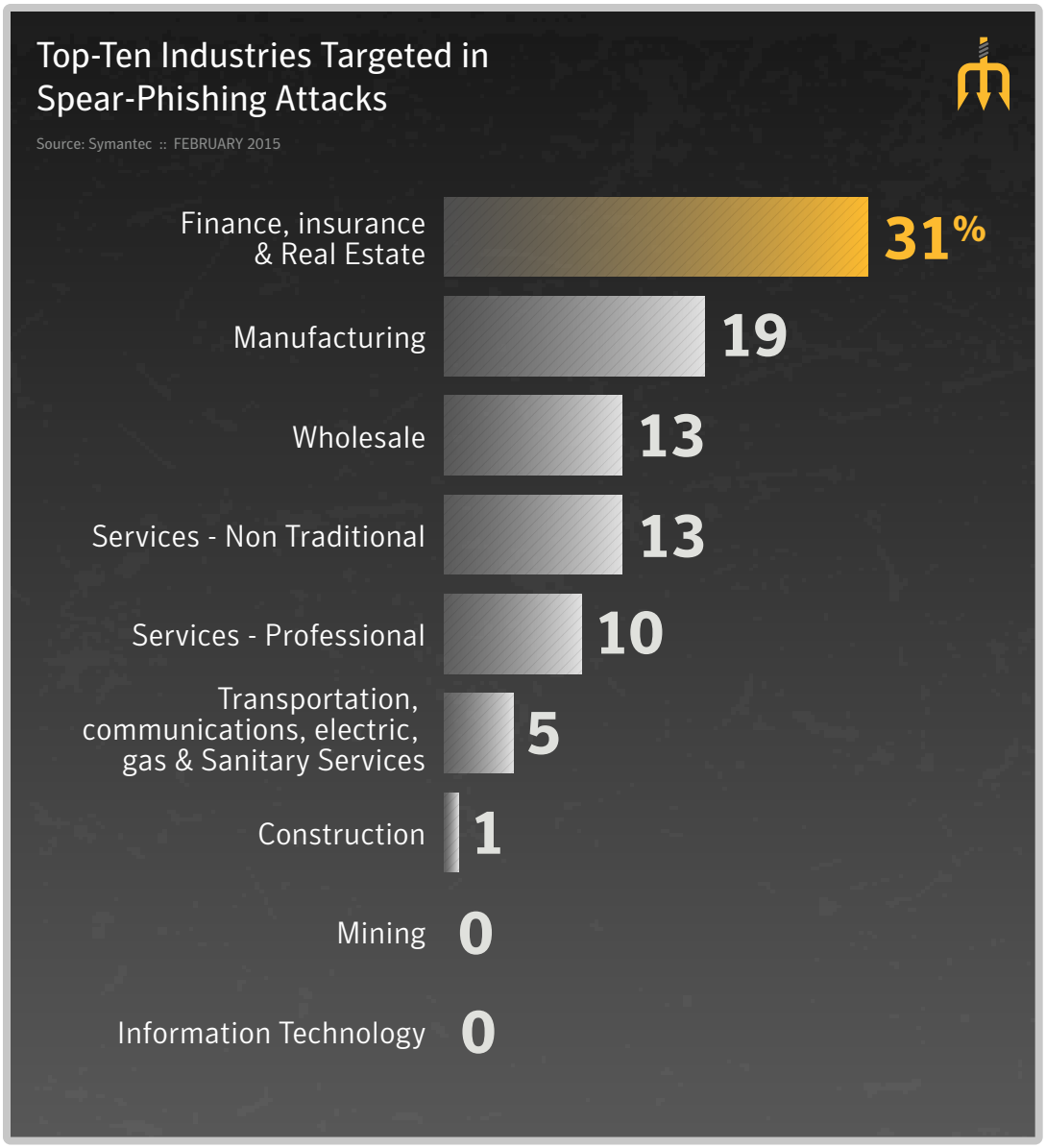
Source: Symantec :: FEBRUARY 2015

Executable type	February	January
.doc	27.6%	46.1%
.txt	21.0%	8.3%
.xls	16.2%	7.8%
.scr	12.6%	–
.rar	7.6%	–
.rtf	4.9%	1.3%
.zip	2.3%	–
.exe	2.3%	2.0%
.bin	0.9%	8.0%
.ppsx	0.4%	–

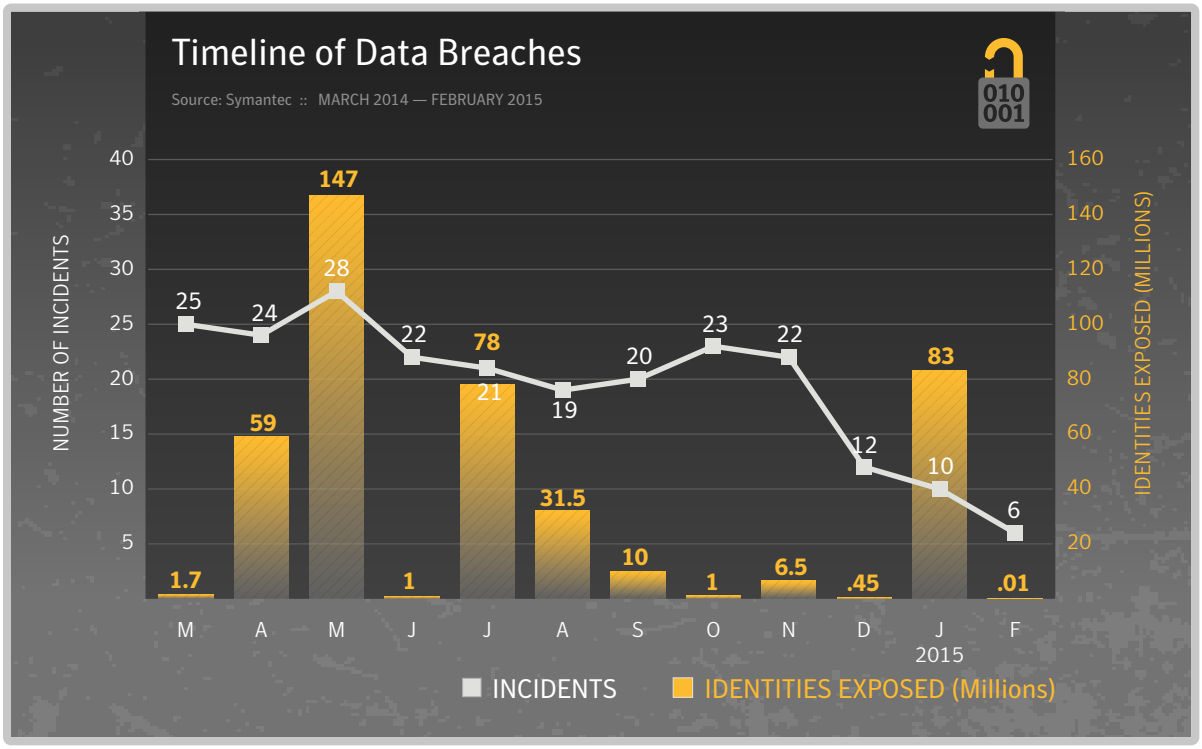
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: FEBRUARY 2015

Organization Size	February	January
1-250	29.1%	35.2%
251-500	9.0%	7.8%
501-1000	8.0%	14.7%
1001-1500	3.8%	4.3%
1501-2500	6.2%	5.3%
2500+	43.8%	32.7%

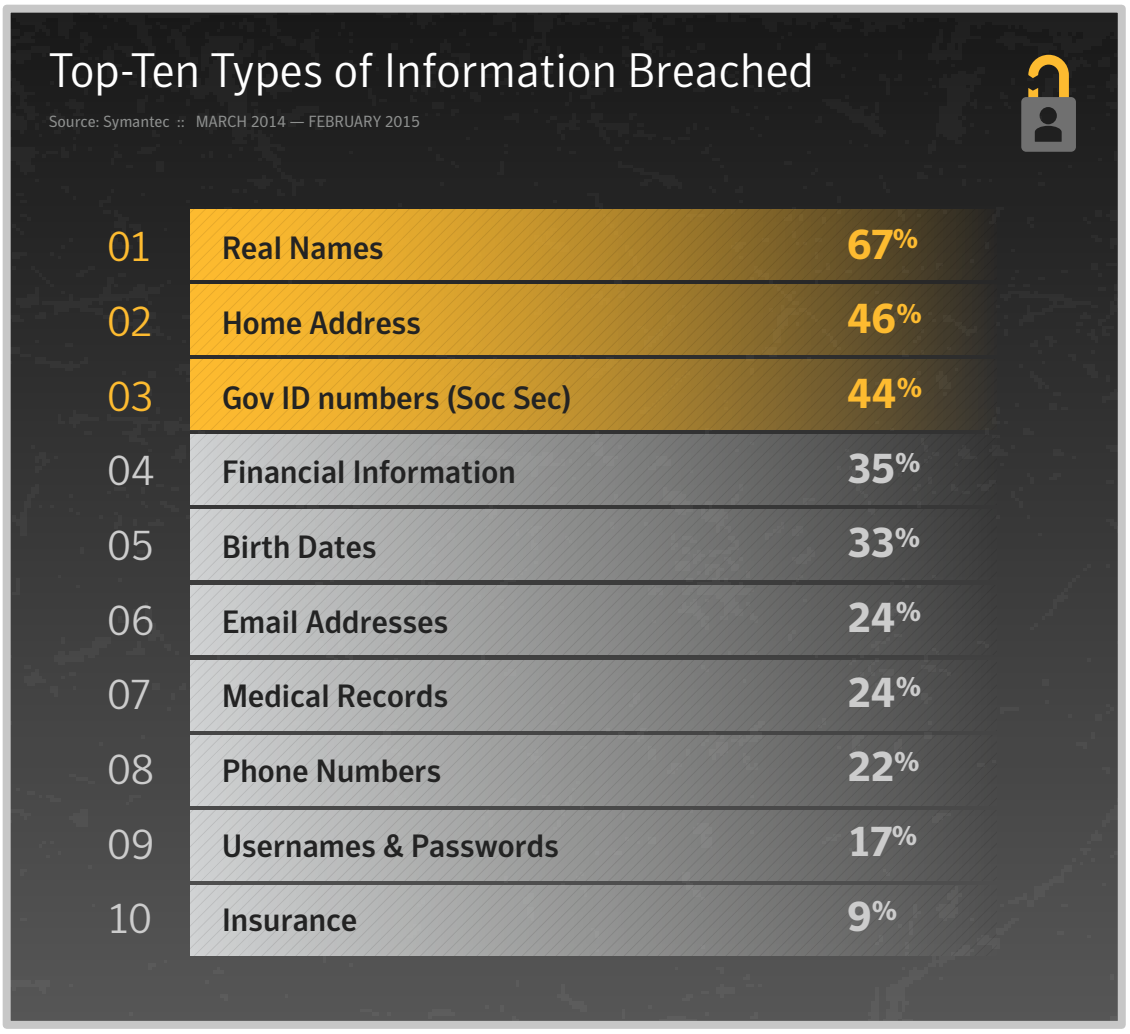

Top-Ten Industries Targeted in Spear-Phishing Attacks
Source: Symantec :: FEBRUARY 2015
Finance, insurance & Real Estate
31%
Manufacturing
19
Wholesale
13
Services - Non Traditional
13
Services - Professional
10
Transportation, communications, electric, gas & Sanitary Services
5
Construction
1
Mining
0
Information Technology
0

Data Breaches



At a Glance

- *There were six data breaches reported in February that took place during the same month. This number is likely to rise as more data breaches that occurred during the month are reported.*
- *The largest data breach reported during February took place in January, and resulted in the exposure of 80 million identities.*
- *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 :: FEBRUARY 2015

Rank	Name	February	January
1	W32.Ramnit!html	6.3%	6.5%
2	W32.Sality.AE	5.7%	5.5%
3	W32.Almanahe.B!inf	4.7%	5.8%
4	W32.Ramnit.B	4.5%	4.4%
5	W32.Downadup.B	2.9%	2.7%
6	W32.Ramnit.B!inf	2.7%	2.7%
7	W32.SillyFDC.BDP!lnk	2.0%	2.1%
8	W32.Virut.CF	1.9%	1.7%
9	Infostealer	1.7%	–
10	W32.Chir.B@mm(html)	1.3%	–

Top-Ten Mac OSX Malware Blocked on OSX Endpoints

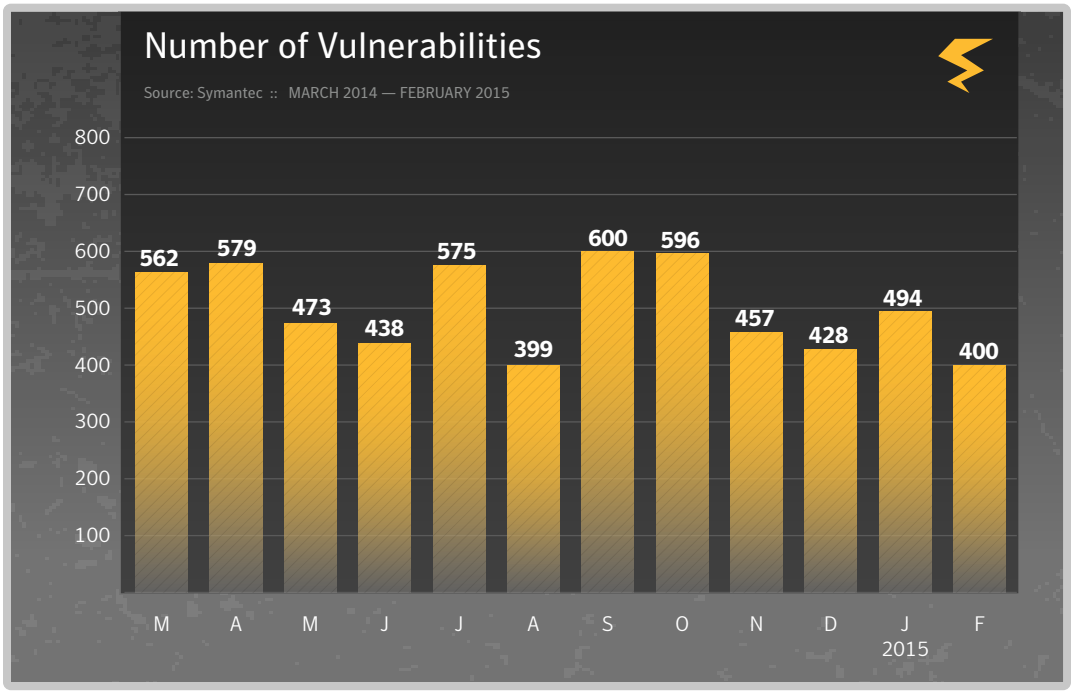
Source: Symantec :: FEBRUARY 2015

Rank	Malware Name	January	January
1	OSX.RSPlug.A	15.7%	19.2%
2	OSX.Keylogger	14.6%	18.9%
3	OSX.Klog.A	12.3%	9.3%
4	OSX.Flashback.K	9.2%	3.2%
5	OSX.Wirelurker	6.0%	10.5%
6	OSX.Flashback	5.4%	3.2%
7	OSX.Luaddit	5.1%	8.0%
8	OSX.Stealbit.B	3.6%	6.1%
9	OSX.Crisis	2.8%	–
10	OSX.Freezer	2.6%	2.6%

At a Glance

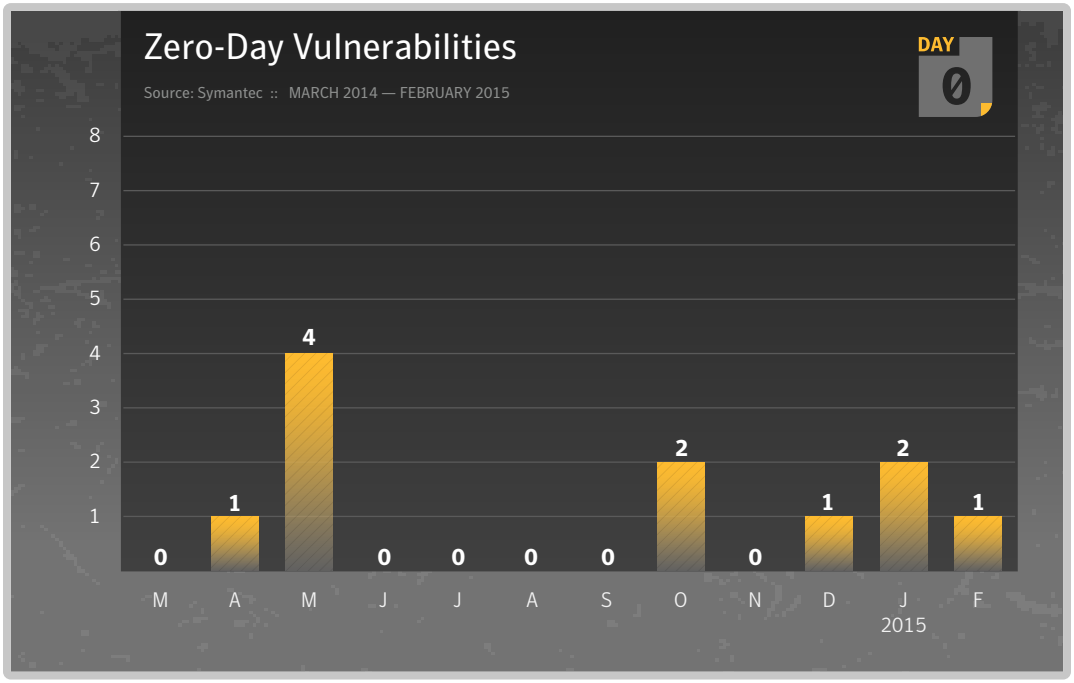
- W32.Ramnit!html *was the most common malware blocked in February.*
- *W32.Ramnit variants continue to dominate the top-ten malware list.*
- *The most common OSX threat seen on OSX was OSX.RSPlug.A, making up 15.7 percent of all OSX malware found on OSX Endpoints.*

Vulnerabilities

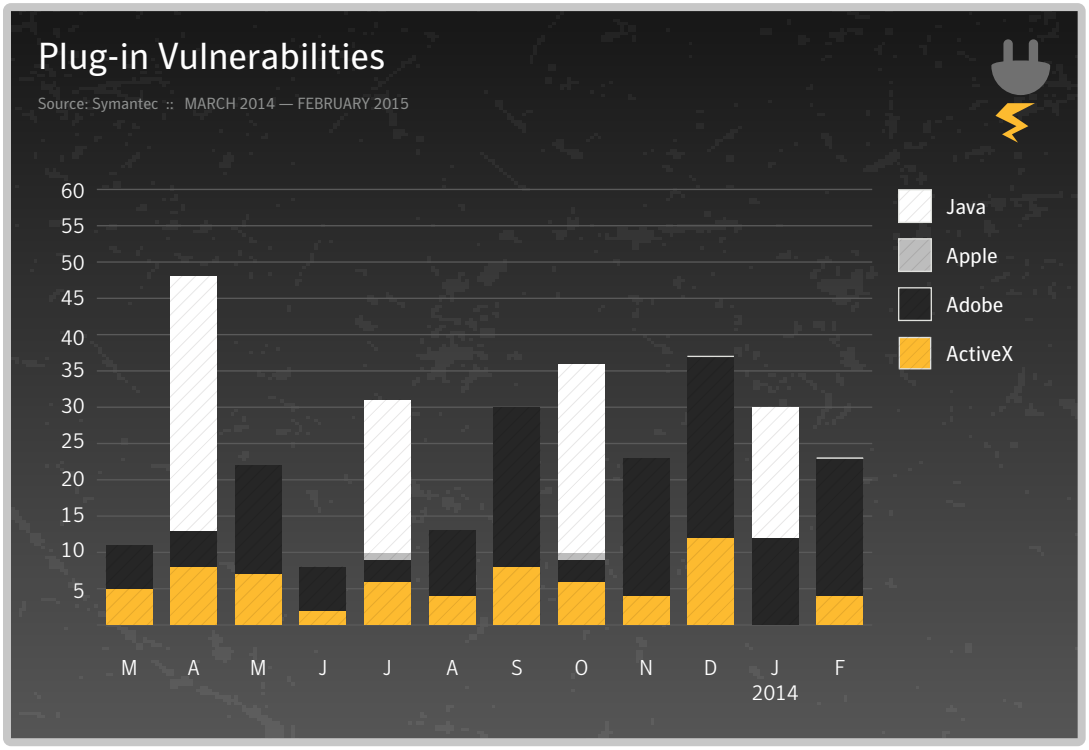


At a Glance

- *There were 400 vulnerabilities disclosed during the month of February.*
- *There was one zero-day vulnerability disclosed during February.*
- *Microsoft Internet Explorer reported the most browser vulnerabilities during the month of February.*
- *Adobe, reporting on the Acrobat and Flash programs, disclosed the most plug-in vulnerabilities over the same time period.*

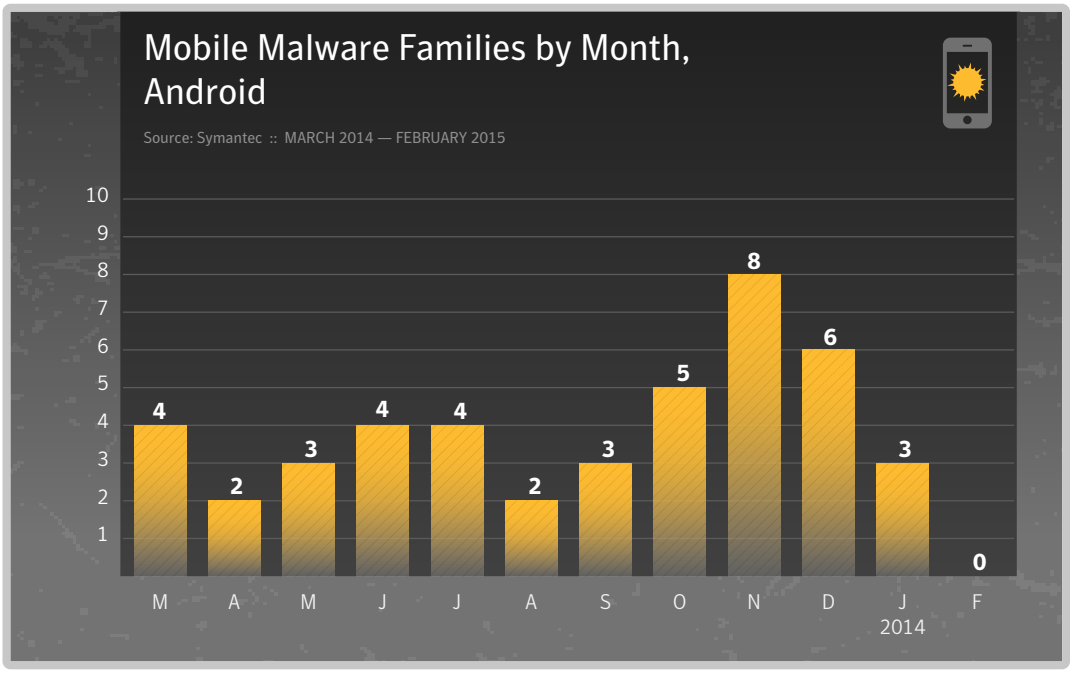



Browser Vulnerabilities
Source: Symantec :: MARCH 2014 — FEBRUARY 2015
100
90
80
70
60
50
40
30
20
10
M A M J J A S O N D J F
2015
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


Plug-in Vulnerabilities
Source: Symantec :: MARCH 2014 — FEBRUARY 2015
60
55
50
45
40
35
30
25
20
15
10
5
M A M J J A S O N D J F
2014
Java
Apple
Adobe
ActiveX

MOBILE THREATS

Mobile

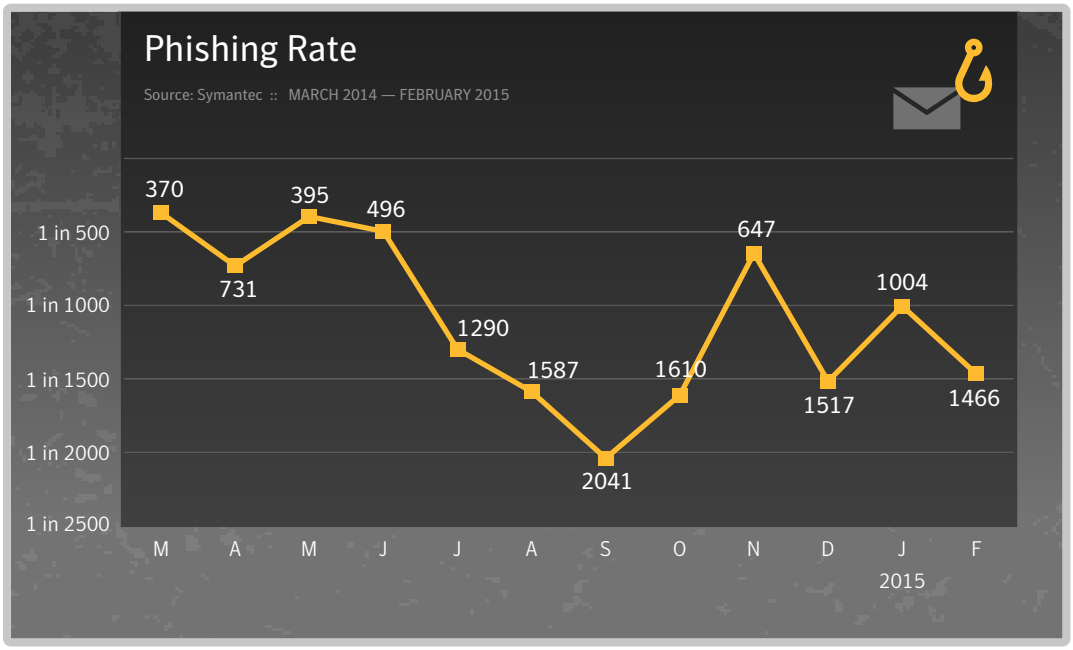


At a Glance

- *There were no new Android malware families discovered in February.*

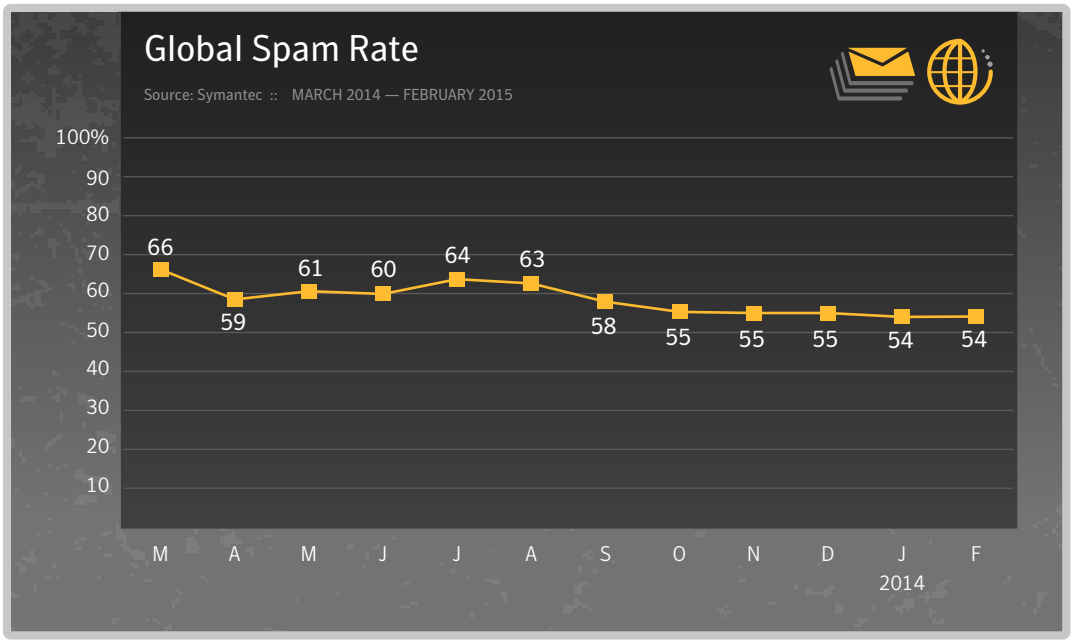
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

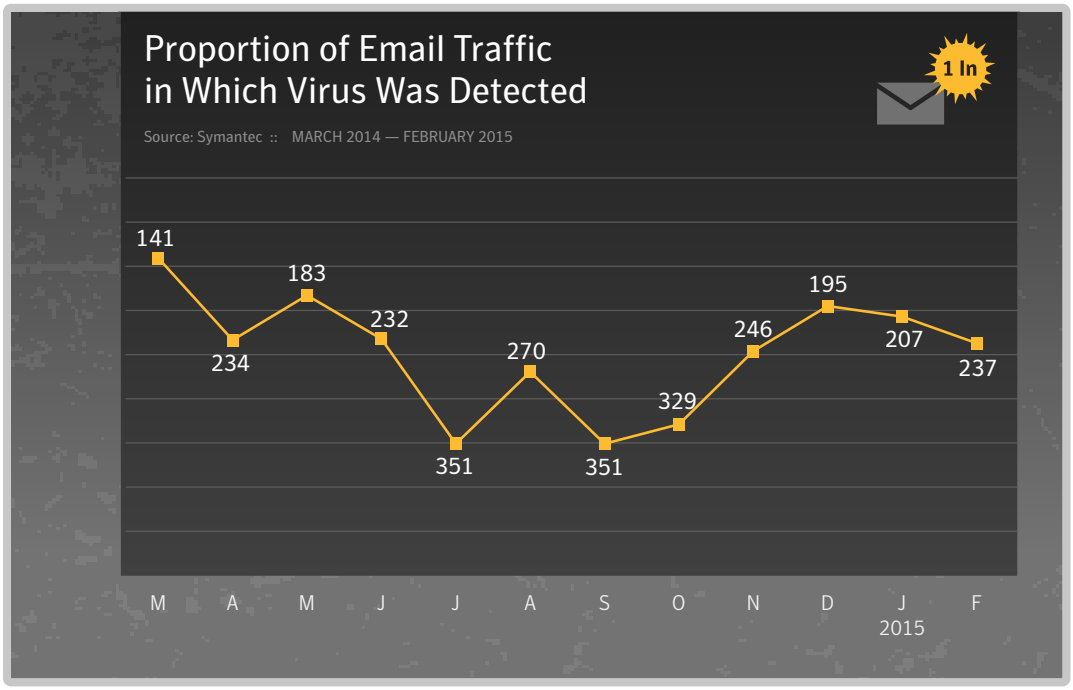


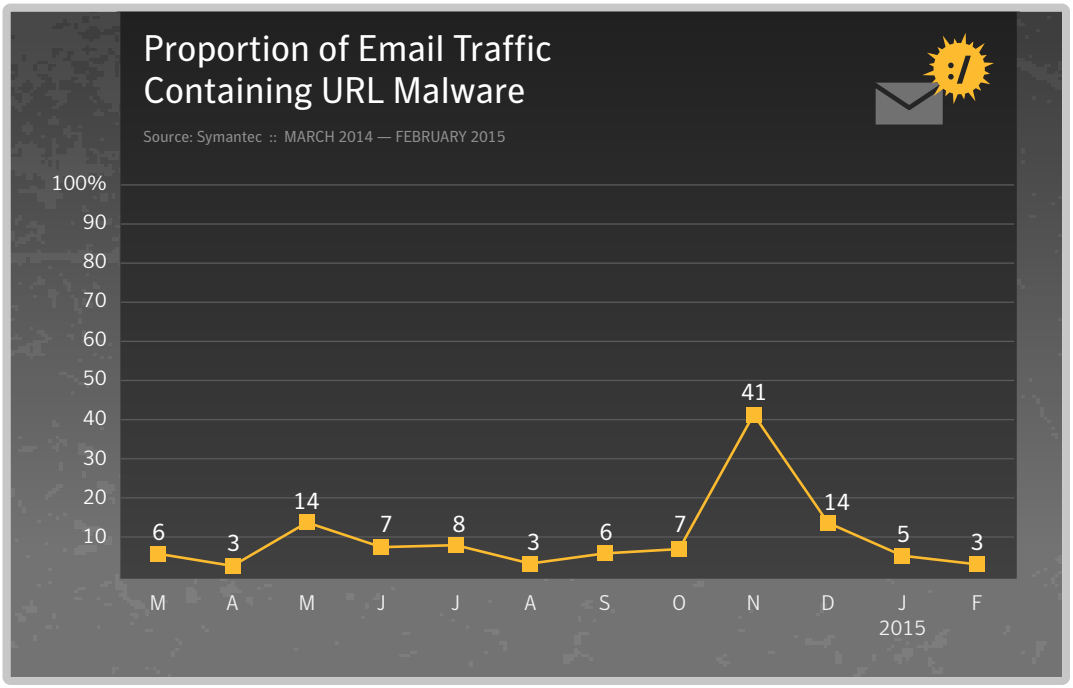
At a Glance

- *The phishing rate declined in February, at one in 1,466 emails, down from one in 1,004 emails in January.*
- *The global spam rate was 54 percent for the month of February.*
- *One out of every 237 emails contained a virus.*
- *Of the email traffic in the month of February, 3 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