Symantec

SYMANTEC INTELLIGENCE REPORT

SEPTEMBER 2014

CONTENTS

3 Summary

4 **TARGETED ATTACKS + DATA BREACHES**

5 Targeted Attacks

5 Attachments Used in Spear-Phishing Emails

5 Spear-Phishing Attacks by Size of Targeted Organization

5 Average Number of Spear-Phishing Attacks Per Day

6 Top-Ten Industries Targeted in Spear-Phishing Attacks

7 Data Breaches

7 Timeline of Data Breaches

8 Total Identities Exposed

8 Top Causes of Data Breaches

8 Total Data Breaches

9 Top-Ten Types of Information Breached

10 **MALWARE TACTICS**

11 Malware Tactics

11 Top-Ten Malware

11 Top-Ten Mac OSX Malware Blocked on OSX Endpoints

12 Ransomware Over Time

12 Malicious Activity by Source: Bots

13 Vulnerabilities

13 Number of Vulnerabilities

13 Zero-Day Vulnerabilities

14 Browser Vulnerabilities

14 Plug-in Vulnerabilities

15 **SOCIAL MEDIA + MOBILE THREATS**

16 Mobile

16 Mobile Malware Families by Month, Android

17 Mobile Threat Classifications

18 Social Media

18 Social Media

19 **PHISHING, SPAM + EMAIL THREATS**

20 Phishing and Spam

20 Phishing Rate

20 Global Spam Rate

21 Email Threats

21 Proportion of Email Traffic Containing URL Malware

21 Proportion of Email Traffic in Which Virus Was Detected

22 About Symantec

22 More Information

Summary

Welcome to the September 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 53 per day in September, after a 12-month low in August. Spear phishing activity has returned to levels seen earlier in the summer, but is still down from the 12-month average of 85 attacks per day.

The .doc file type was the most common attachment type used in spear-phishing attacks, making up more than 52.9 percent of all attachments in September. At 4.8 percent, last month's top attachment, .exe file types, dropped to fourth.

There were only four publically disclosed data breaches that took place within the month September, resulting in the exposure of 2.5 million identities. However, there were 14 additional data breaches reported in September that took place earlier in the year. The largest data breach reported in September actually took place in April, and resulted in the exposure of 56 million identities.

Ransomware continues to decline as 2014 progresses. However, crypto-style ransomware remains high, making up 38 percent of all ransomware detected in September.

There were 600 vulnerabilities disclosed in the month of September, the highest number so far in 2014 and second-highest in the last 12 months.

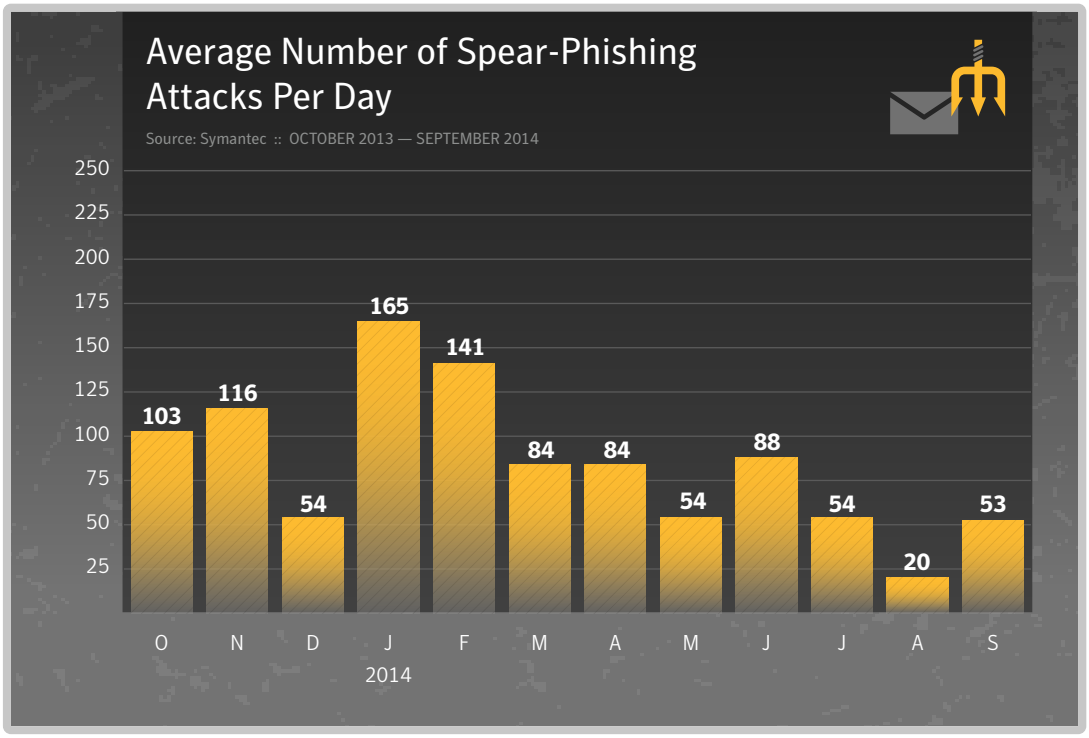
One in 2,041 emails was identified as a phishing attempt, compared with one in 1,587 for August. While at first glance this looks like a big drop, it results in only a 0.01 percentage point decrease in the overall phishing rate.

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 53 per day in September, after a 12-month low in August.*
- *The .doc file type was the most common attachment type used in spear-phishing attacks. The .exe file type dropped to fourth.*
- *Organizations with 2500+ employees were the most likely to be targeted in September.*
- *Manufacturing lead the Top-Ten Industries targeted, followed by Non-Traditional Services.*

Attachments Used in Spear-Phishing Emails

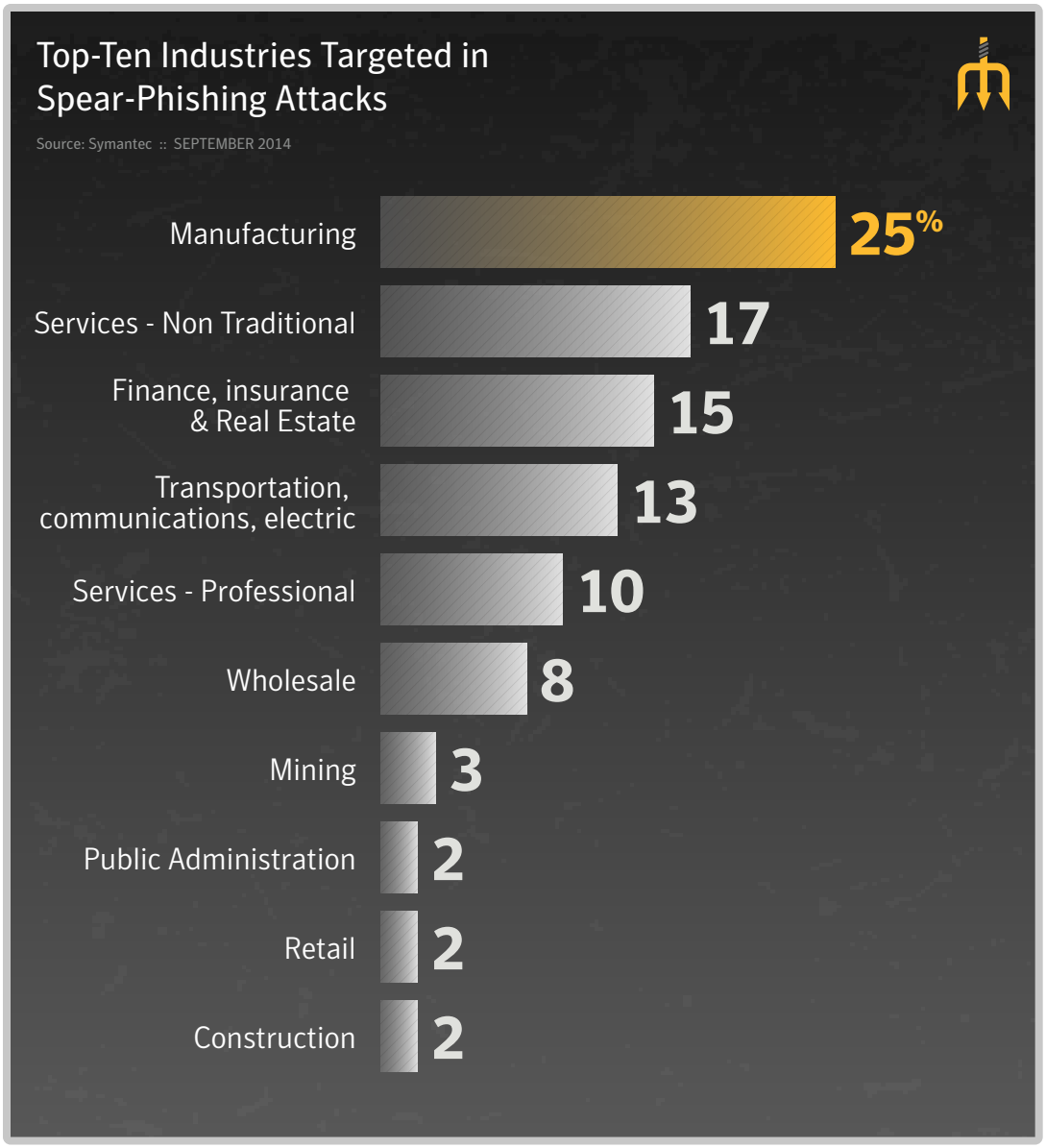
Source: Symantec :: SEPTEMBER 2014

Executable type	September	August
.doc	52.9%	22.8%
.scr	15.4%	4.4%
.dmp	9.1%	–
.exe	4.8%	31.8%
.bin	2.6%	–
.class	2.5%	4.2%
.au3	1.3%	–
.7z	1.0%	–
.pdf	1.0%	2.8%
.xls	0.3%	–

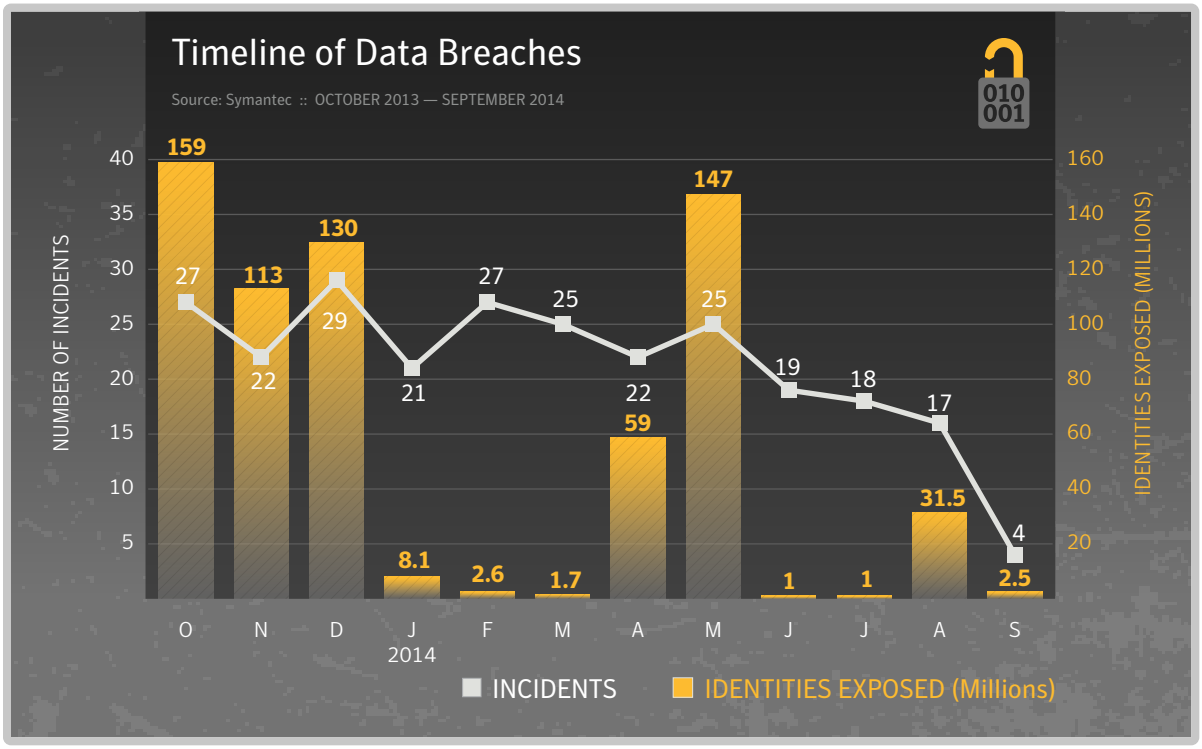
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: SEPTEMBER 2014

Organization Size	September	August
1-250	32.5%	28.8%
251-500	8.7%	7.8%
501-1000	8.6%	4.6%
1001-1500	3.7%	6.3%
1501-2500	3.9%	4.6%
2500+	42.6%	47.8%


Top-Ten Industries Targeted in Spear-Phishing Attacks
Source: Symantec :: SEPTEMBER 2014
Manufacturing
25%
Services - Non Traditional
17
Finance, insurance & Real Estate
15
Transportation, communications, electric
13
Services - Professional
10
Wholesale
8
Mining
3
Public Administration
2
Retail
2
Construction
2

Data Breaches



At a Glance

- *The largest data breach reported in September actually took place in April, and resulted in the exposure of 56 million identities.*
- *Hackers have been responsible for 56 percent of data breaches in the last 12 months.*
- *Real names, government ID numbers, such as Social Security numbers, and home addresses were the top three types of data exposed in data breaches.*

Total Data Breaches

OCTOBER 2013 — SEPTEMBER 2014

255

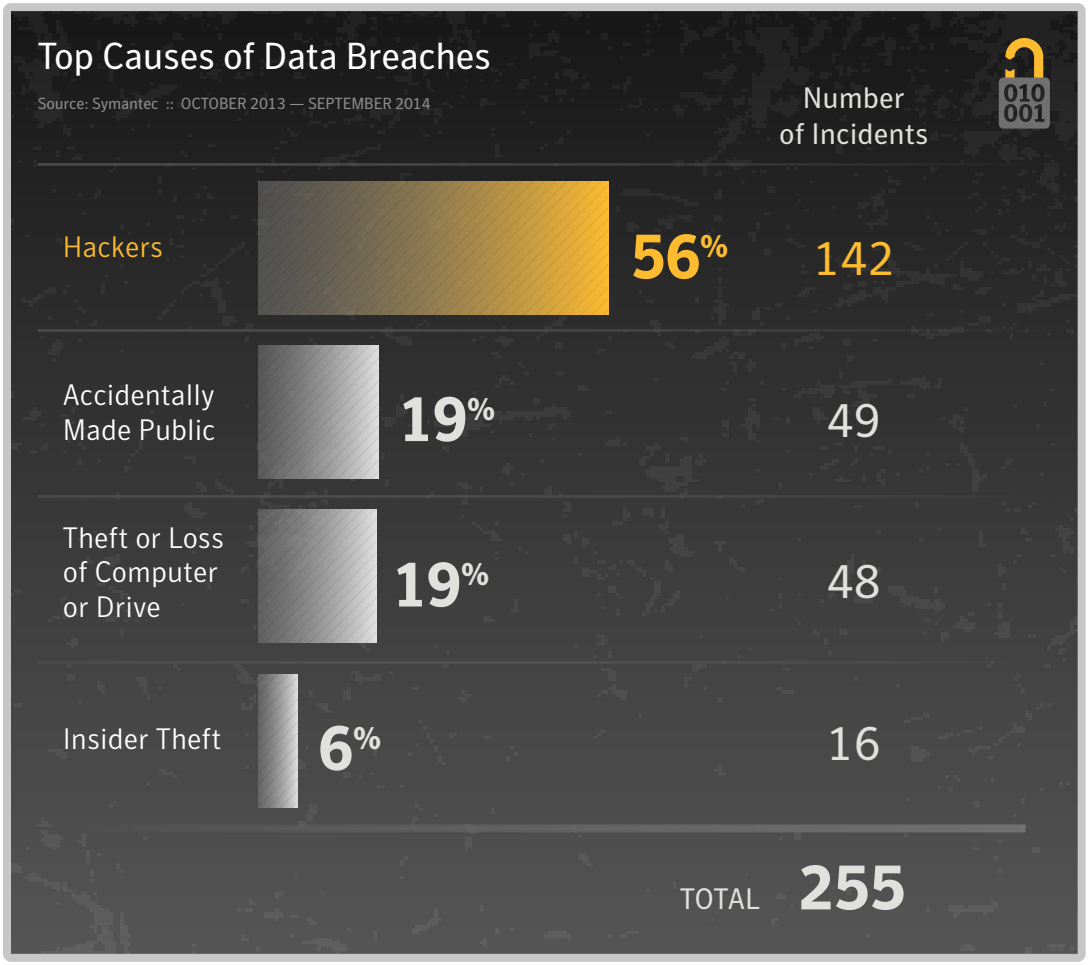
Total Identities Exposed

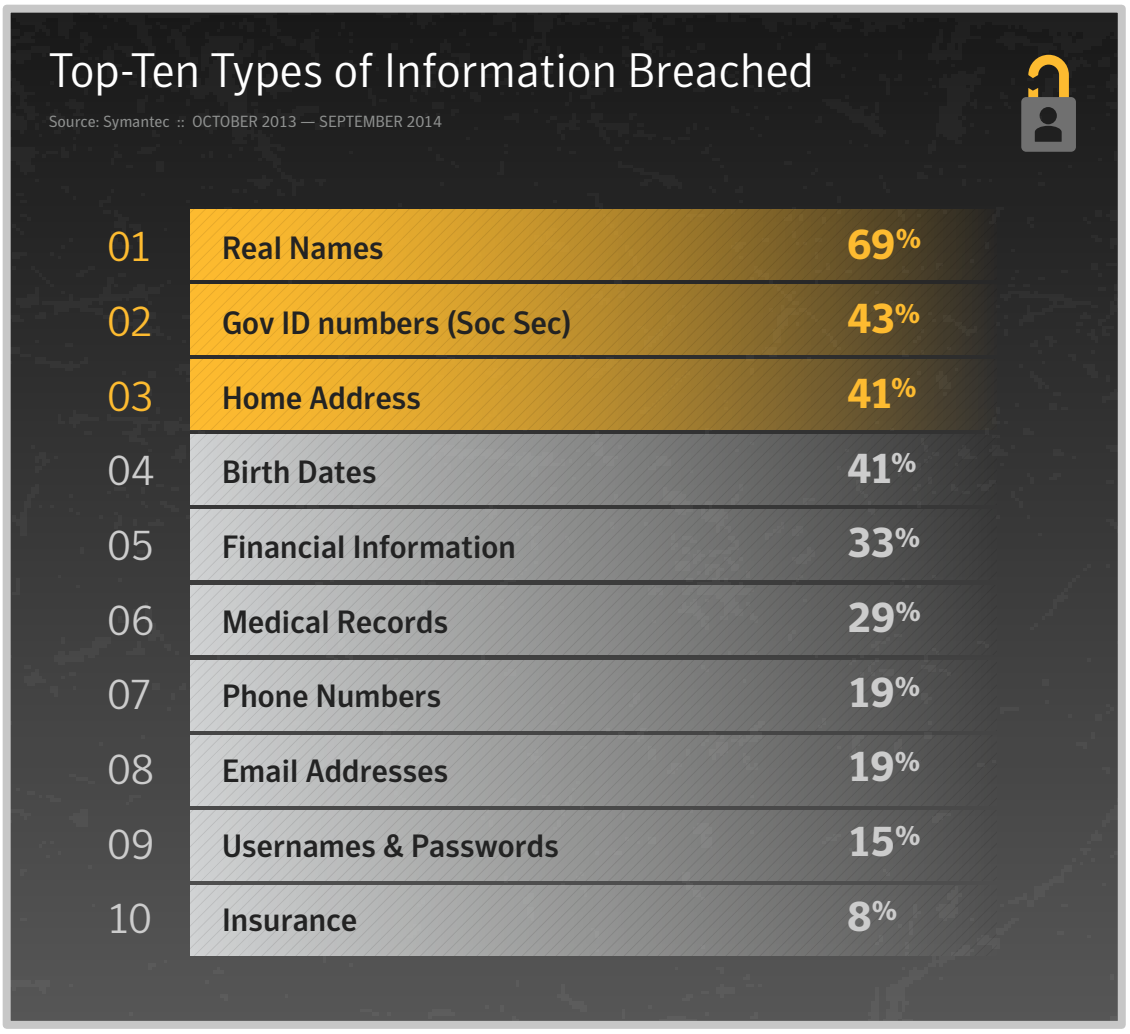
OCTOBER 2013 — SEPTEMBER 2014

656 Million

Top Causes of Data Breaches

Source: Symantec :: OCTOBER 2013 — SEPTEMBER 2014





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

MALWARE TACTICS

Malware Tactics

Top-Ten Malware

Source: Symantec :: SEPTEMBER 2014

Rank	Name	September	August
1	W32.Sality.AE	4.4%	4.3%
2	W32.Ramnit!html	4.3%	4.3%
3	W32.Almanahe.B!inf	3.7%	3.6%
4	W32.Ramnit.B	2.7%	3.0%
5	W32.Downadup.B	2.3%	2.7%
6	W32.SillyFDC.BDP!lnk	2.2%	2.3%
7	W32.Ramnit.B!inf	2.0%	1.9%
8	W32.Virut.CF	1.4%	1.2%
9	W32.Chir.B@mm(html)	1.4%	1.1%
10	Trojan.Zbot	1.2%	0.9%

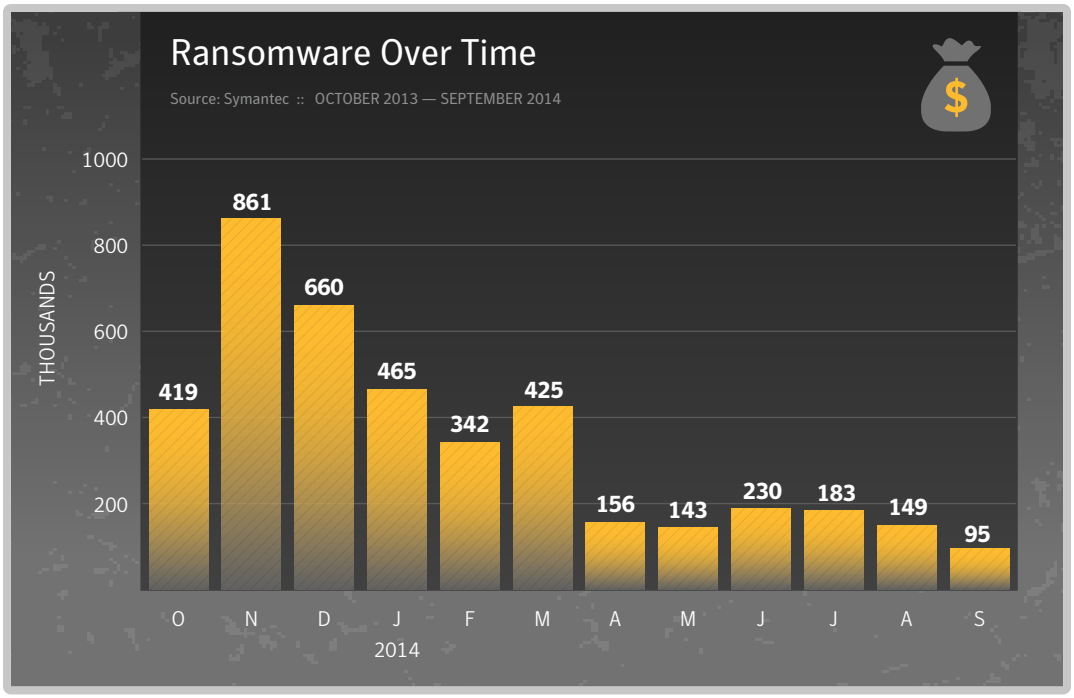
Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: SEPTEMBER 2014

Rank	Malware Name	September	August
1	OSX.RSPlug.A	26.3%	51.2%
2	OSX.Crisis	8.7%	2.2%
3	OSX.Flashback.K	8.7%	8.5%
4	OSX.Okaz	7.6%	–
5	OSX.Stealbit.B	5.3%	8.1%
6	OSX.Netweird	5.2%	2.7%
7	OSX.Flashback	4.0%	2.6%
8	OSX.Keylogger	3.6%	1.6%
9	OSX.Klog.A	2.9%	7.2%
10	OSX.Sabpab	2.7%	4.2%

At a Glance

- *W32.Sality and 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 26 percent of all OSX malware found on OSX Endpoints.*
- *Overall ransomware activity has remained low since March of this year. However, crypto-style ransomware has been on the rise this year, making up 38 percent of ransomware in September.*
- *China and the US where first and second, respectively, in September in terms of overall botnet source activity.*

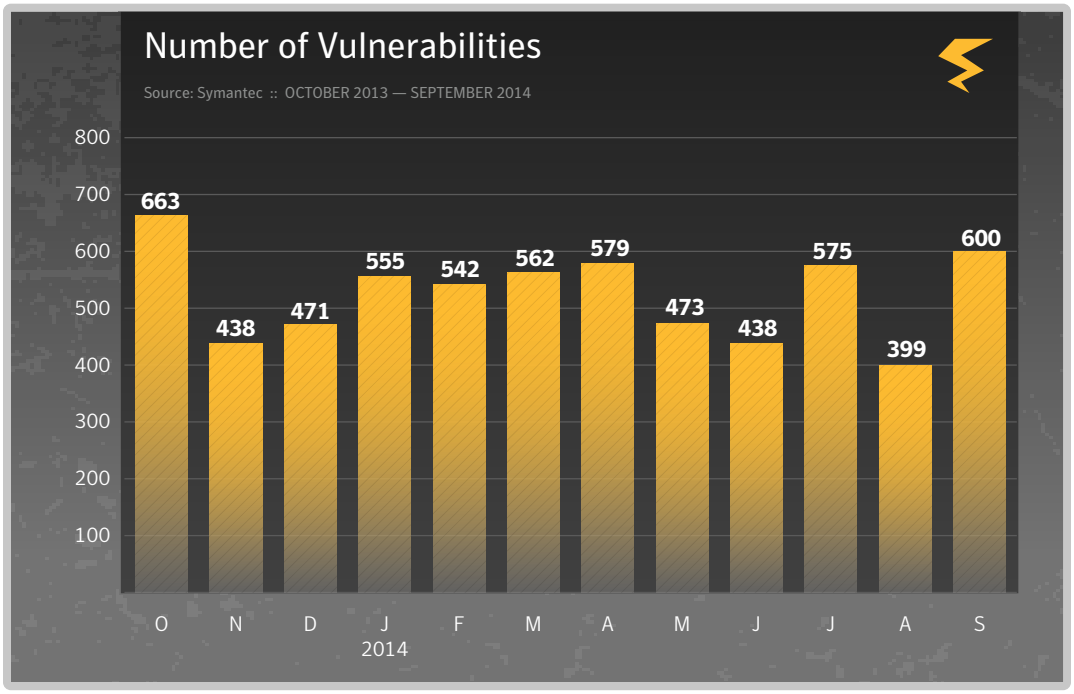


Malicious Activity by Source: Bots

Source: Symantec :: AUGUST 2014

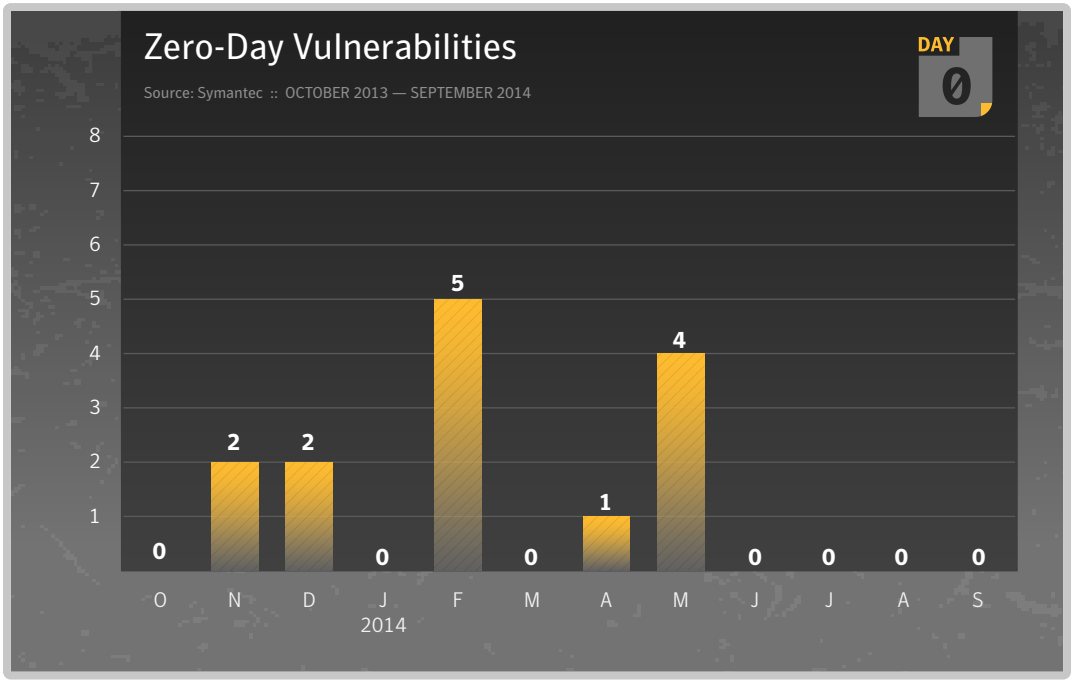
Rank	Country/Region	Percent
1	China	28.5%
2	United States	18.2%
3	Taiwan	5.4%
4	Hungary	3.7%
5	Italy	2.8%
6	Canada	2.6%
7	Brazil	2.6%
8	Germany	2.1%
9	United Kingdom	2.1%
10	Turkey	2.1%

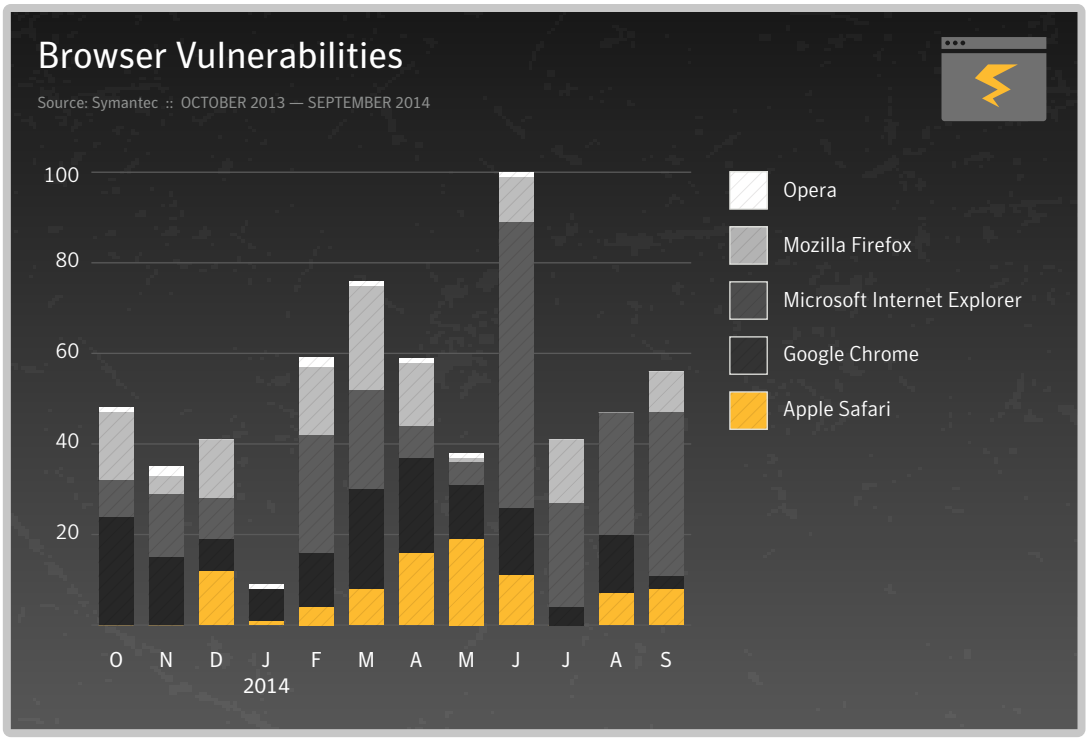
Vulnerabilities

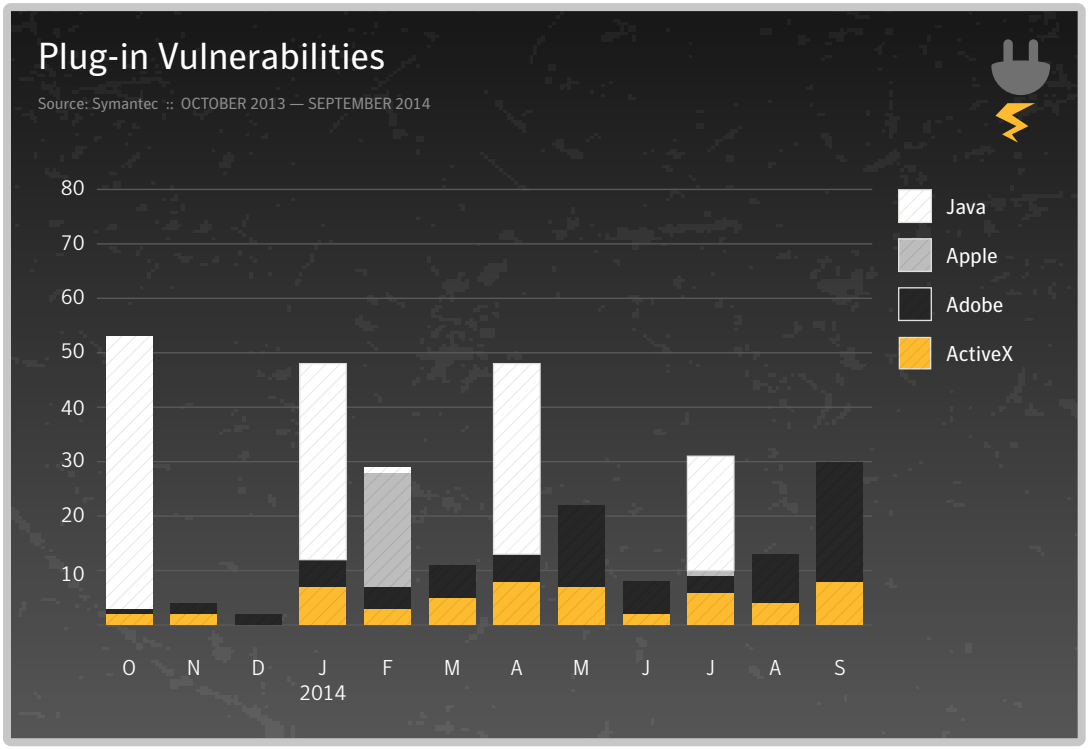


At a Glance

- *There were 600 vulnerabilities disclosed during the month of August.*
- *There were no zero-day vulnerabilities discovered in September.*
- *Internet Explorer has reported the most browser vulnerabilities in the last 12 months.*
- *Oracle's Java reported the most plug-in vulnerabilities over the same time period.*

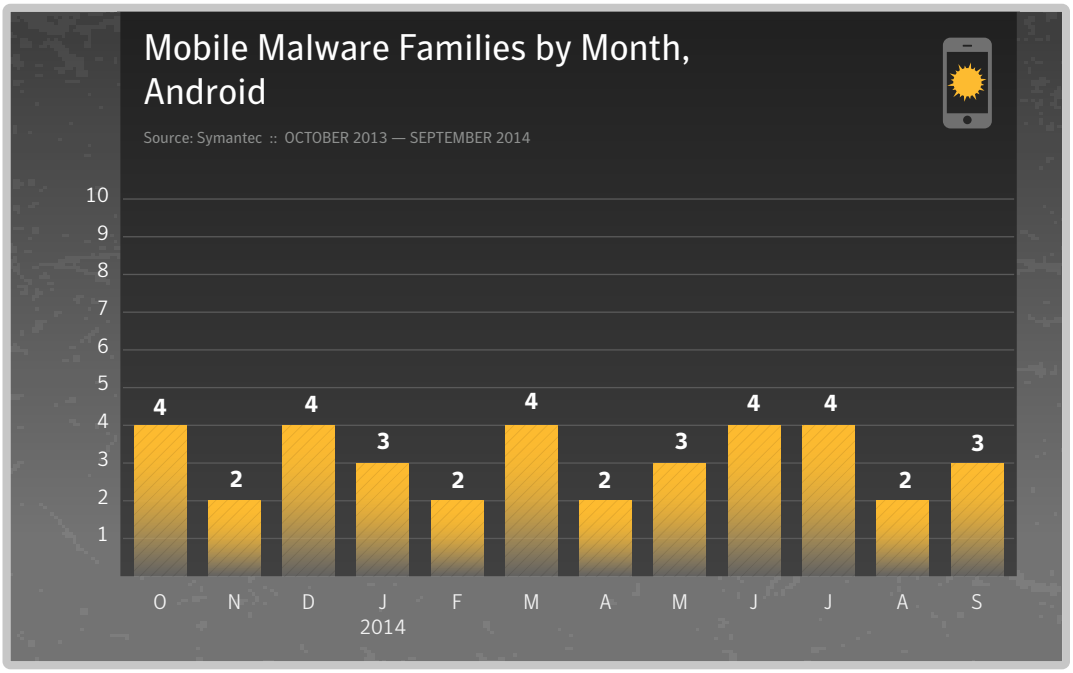



Browser Vulnerabilities
Source: Symantec :: OCTOBER 2013 — SEPTEMBER 2014
100
80
60
40
20
O N D J F M A M J J A S
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


Plug-in Vulnerabilities
Source: Symantec :: OCTOBER 2013 — SEPTEMBER 2014
80
70
60
50
40
30
20
10
O N D J F M A M J J A S
2014
Java
Apple
Adobe
ActiveX

SOCIAL MEDIA + MOBILE THREATS

Mobile

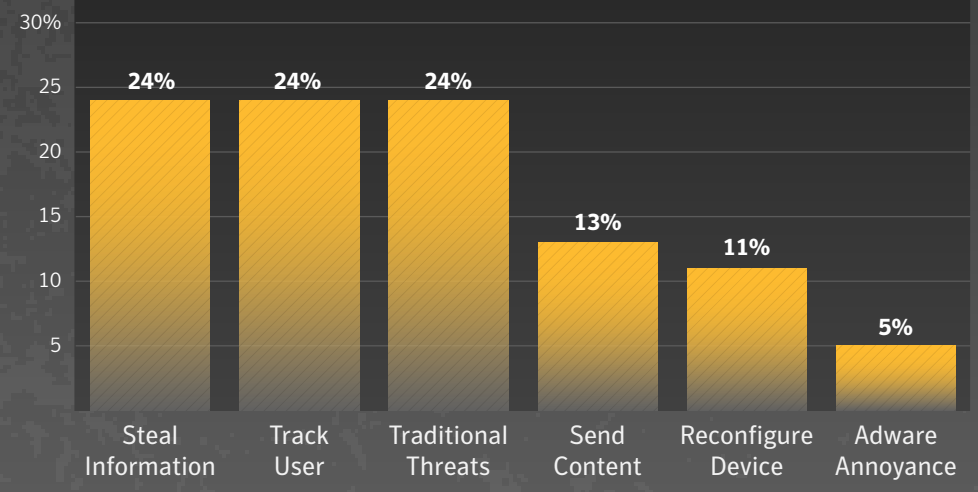


At a Glance

- *There were three Android malware families discovered in July.*
- *Of the threats discovered in the last 12 months, 24 percent steal information from the device.*
- *In terms of social networking scams, 41 percent were fake offerings, while 46 percent were manually shared scams.*

Mobile Threat Classifications

Source: Symantec :: OCTOBER 2013 — SEPTEMBER 2014



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.

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

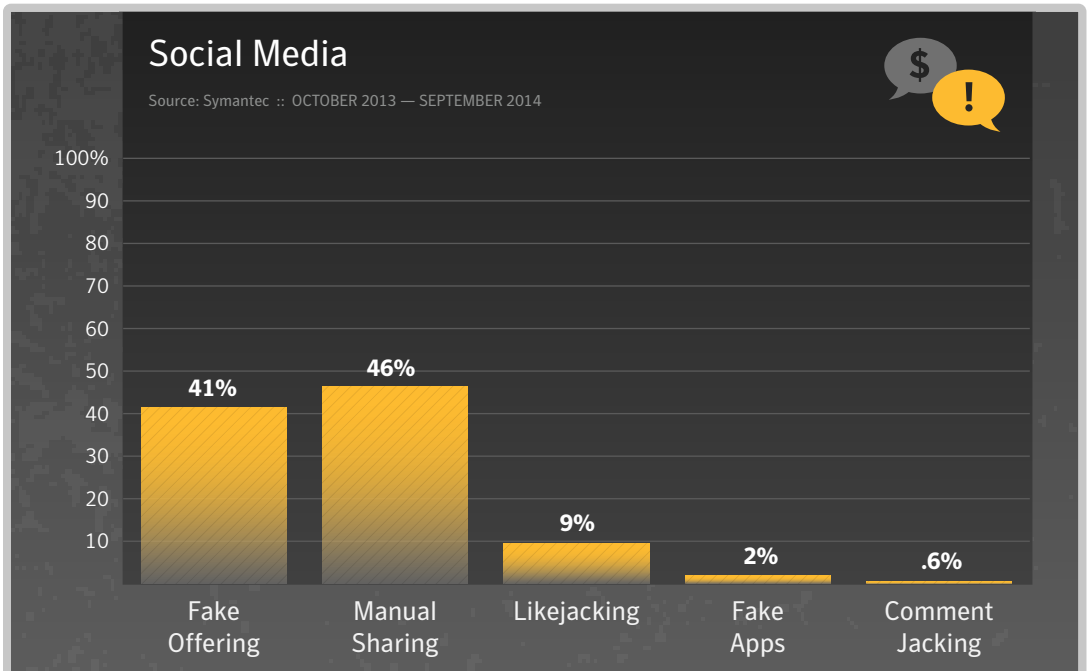
Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

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

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

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.

Social Media



Fake Offers 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.

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

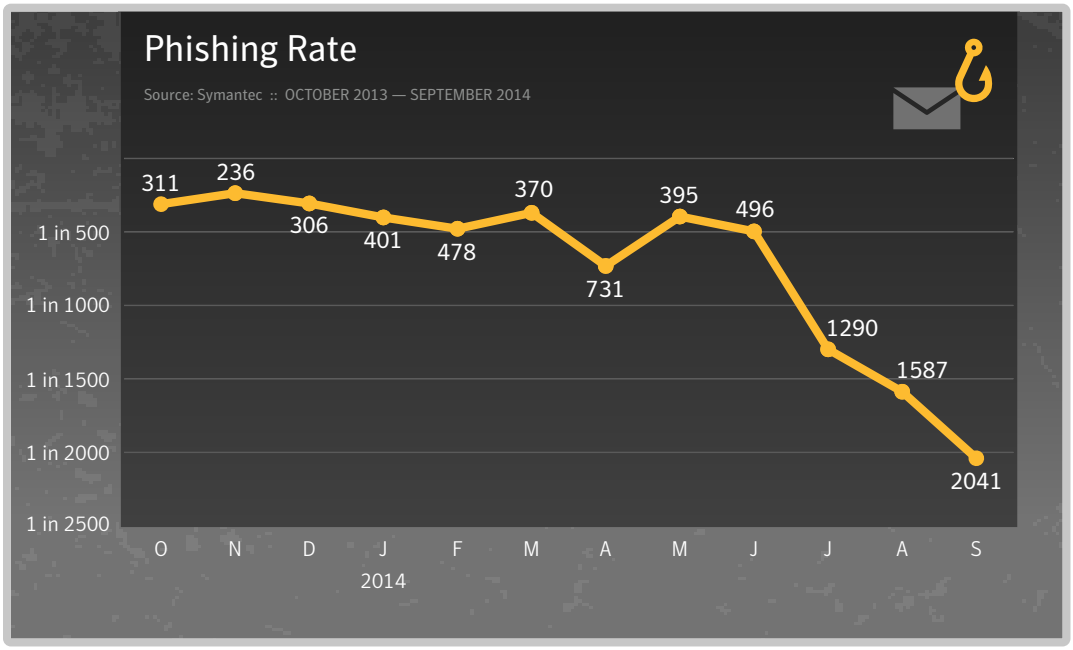
Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

Comment Jacking Similar to likejacking, this type of scam relies on users clicking links that are added to comments by attackers. The links may lead to malware or survey scams.

Fake App Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

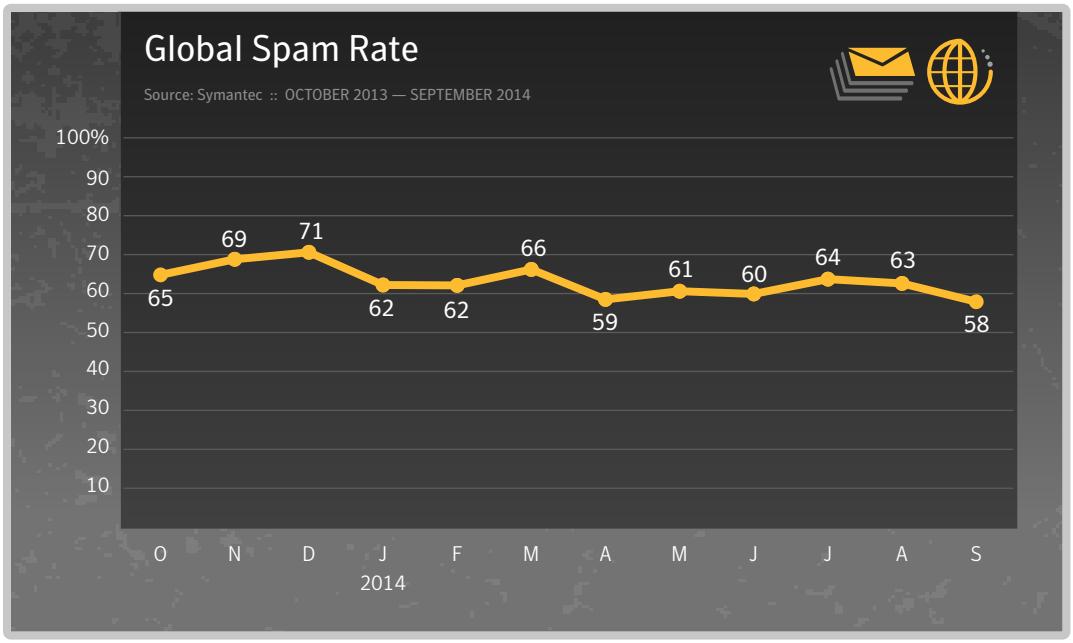
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

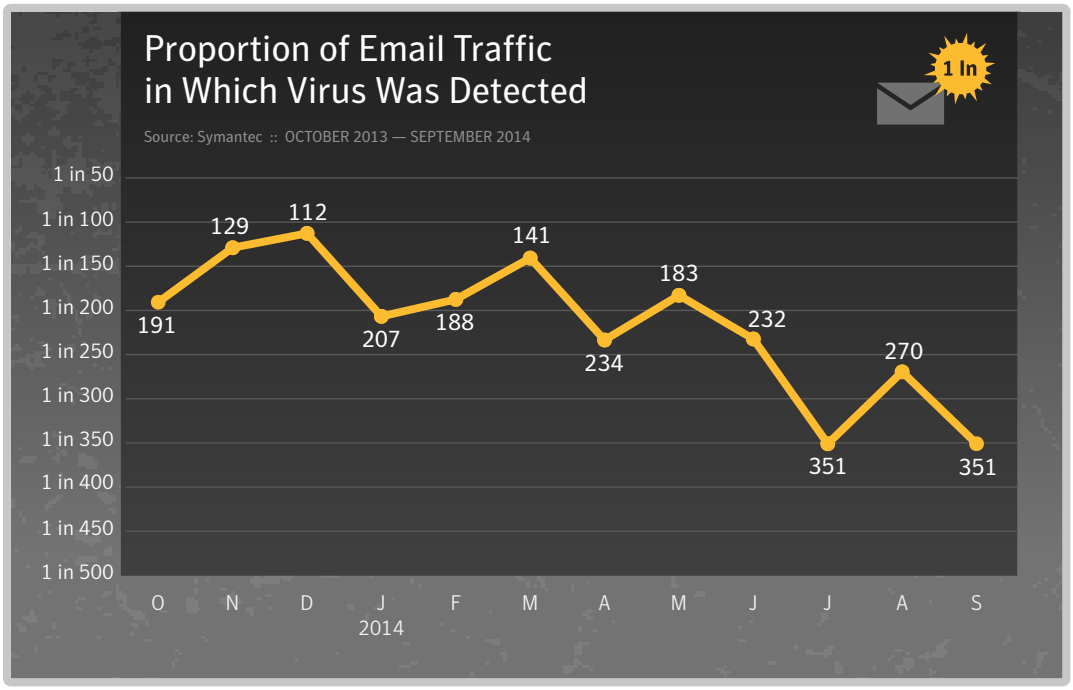


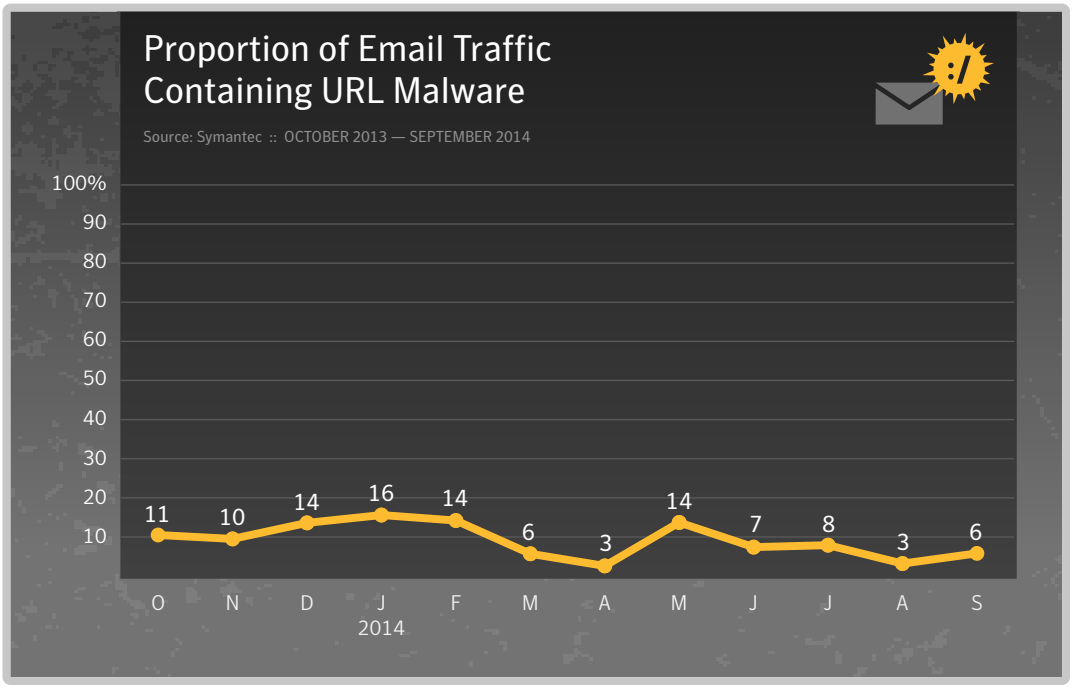
At a Glance

- *The phishing rate was down again in September, at one in 2,041 emails, down from one in 1,587 emails in August.*
- *The global spam rate was 57.9 percent for the month of September.*
- *One out of every 351 emails contained a virus.*
- *Of the email traffic in the month of August, 5.8 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

Copyright © 2014 Symantec Corporation.
All rights reserved. Symantec, the Symantec Logo,
and the Checkmark Logo are trademarks or registered
trademarks of Symantec Corporation or its affiliates in
the U.S. and other countries. Other names may
be trademarks of their respective owners