Symantec

SYMANTEC INTELLIGENCE REPORT

OCTOBER ⌖ 2014

CONTENTS

Summary

Welcome to the October 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 number of spear phishing attacks per day continues to trend downward over the last twelve months, coming in at 45 per day in October. Of the attachments used in such email-based attacks, the .doc attachment type comprised 62.5 percent and .exe attachments made up 14.4 percent. Of the industries attacked, the category of Finance, Insurance, and Real Estate received 28 percent of all spear phishing attempts in the month of October, followed by Manufacturing at 17 percent.

The largest data breach that was disclosed in October took place back in July. This breach had previously been reported; however, we learned this month that the breach resulted in the exposure of identities within 76 million households, plus information on an additional seven million small businesses.

In the Mac threat landscape, OSX.Okaz was the most frequently encountered OSX risk seen on OSX endpoints, making up 28.8 percent of OSX risks. OSX.Okaz is an adware program that may modify browser homepage and search settings.

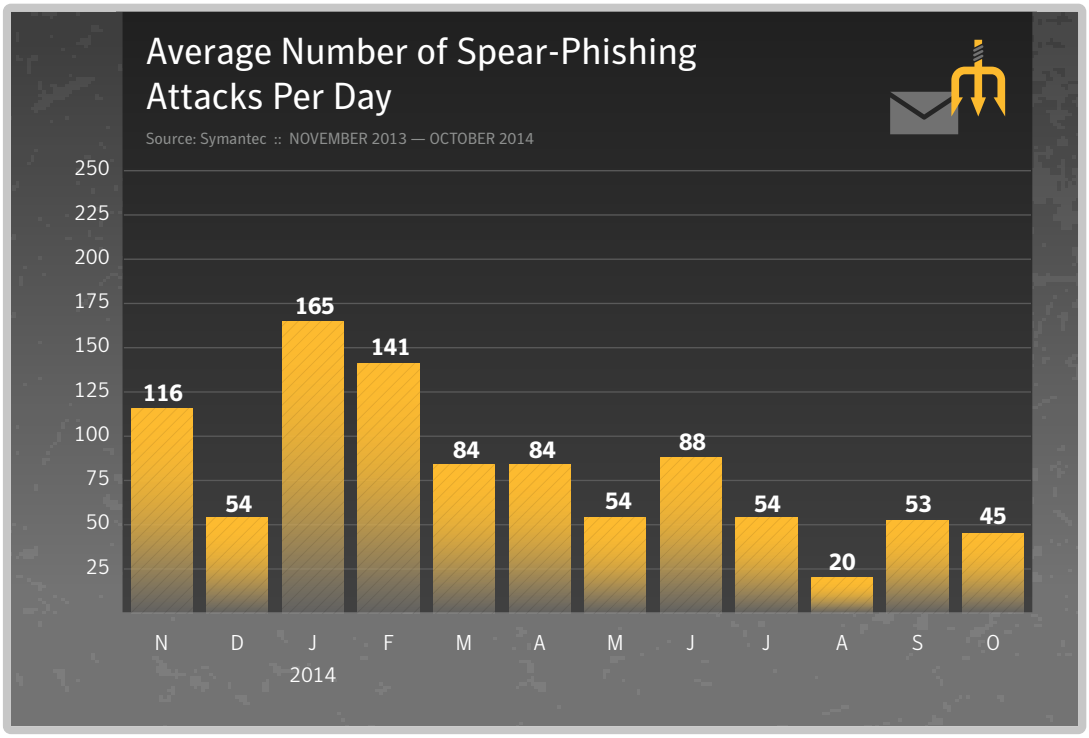
Finally, Ransomware as a whole continues to decline as the year progresses. However, the amount of crypto-style ransomware seen continues to increase. This particularly aggressive form of ransomware made up 55 percent of all ransomware in the month of October.

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 45 per day in October, down from 53 in September.*
- *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 October.*
- *Finance, Insurance, & Real Estate lead the Top-Ten Industries targeted, followed by Manufacturing.*

Attachments Used in Spear-Phishing Emails

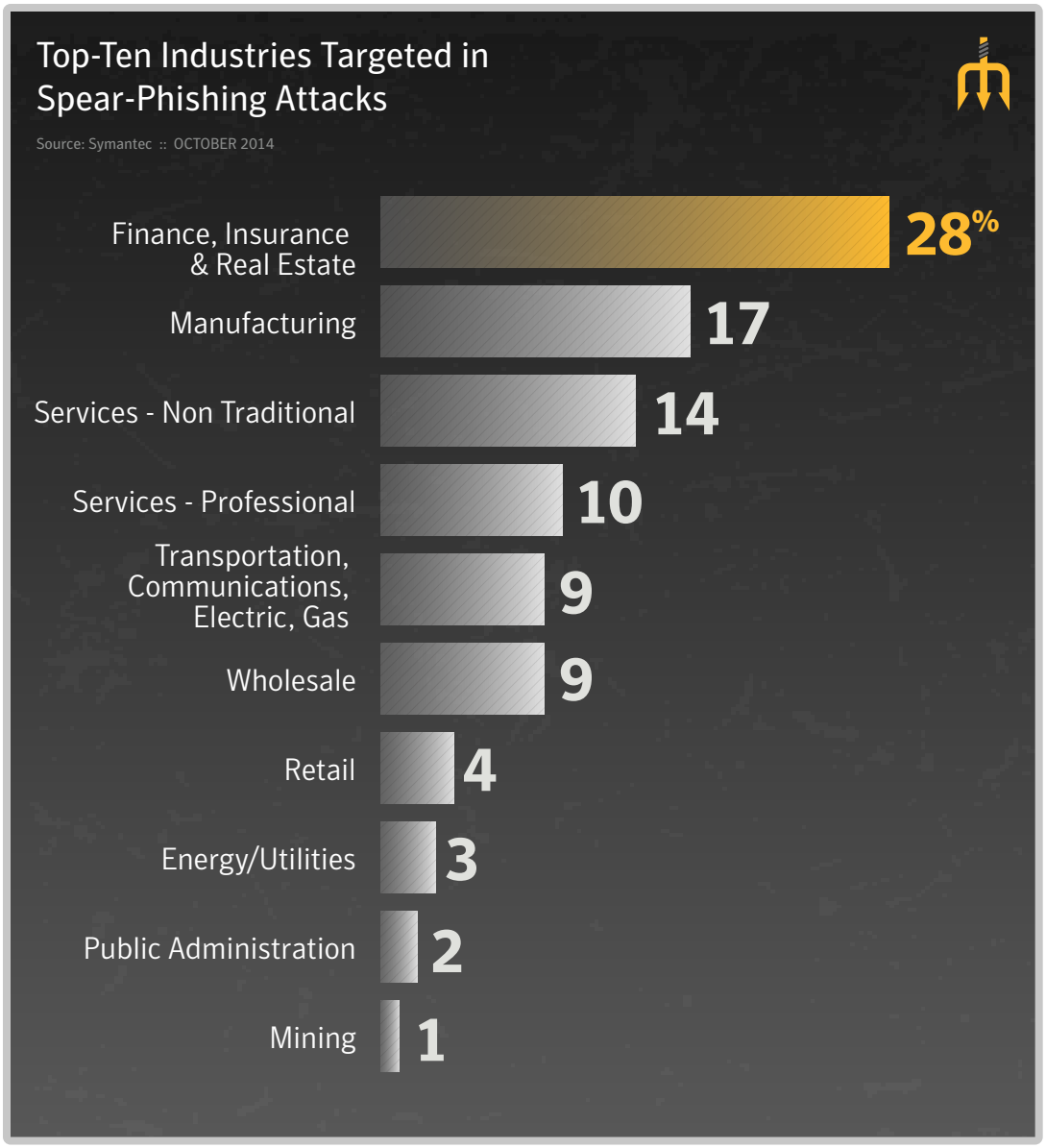
Source: Symantec :: OCTOBER 2014

Executable type	October	September
.doc	62.5%	52.9%
.exe	14.4%	4.8%
.txt	11.2%	9.1%
.pdf	4.4%	1.0%
.ace	0.7%	–
.jpeg	0.2%	–
.htm	0.1%	–
.dmp	0.1%	9.1%
.scr	0.1%	15.4%
.rtf	0.1%	–

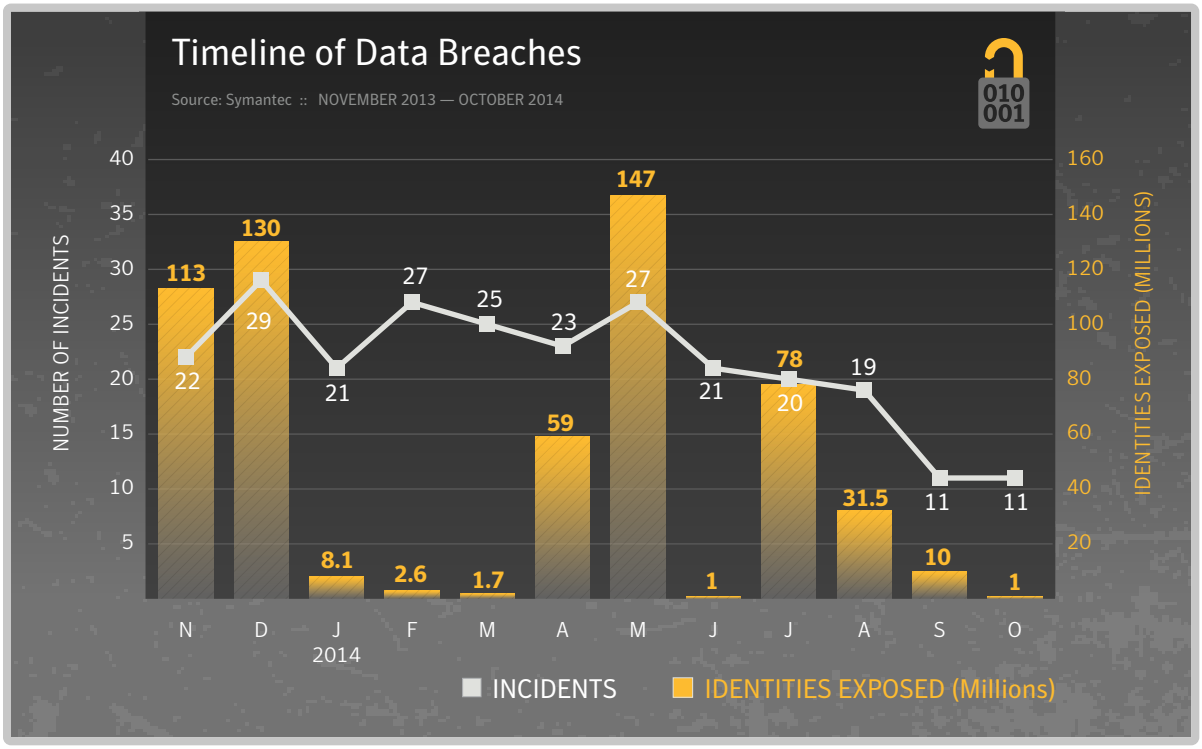
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: OCTOBER 2014

Organization Size	October	September
1-250	27.1%	32.5%
251-500	6.6%	8.7%
501-1000	8.9%	8.6%
1001-1500	2.9%	3.7%
1501-2500	11.2%	3.9%
2500+	43.3%	42.6%


Top-Ten Industries Targeted in Spear-Phishing Attacks
Source: Symantec :: OCTOBER 2014
Finance, Insurance & Real Estate
28%
Manufacturing
17
Services - Non Traditional
14
Services - Professional
10
Transportation, Communications, Electric, Gas
9
Wholesale
9
Retail
4
Energy/Utilities
3
Public Administration
2
Mining
1

Data Breaches



At a Glance

- *The largest data breach disclosed in October actually took place in July, and resulted in the exposure of at least 76 million identities.*
- *Hackers have been responsible for 57 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

NOVEMBER 2013 — OCTOBER 2014

257

Total Identities Exposed

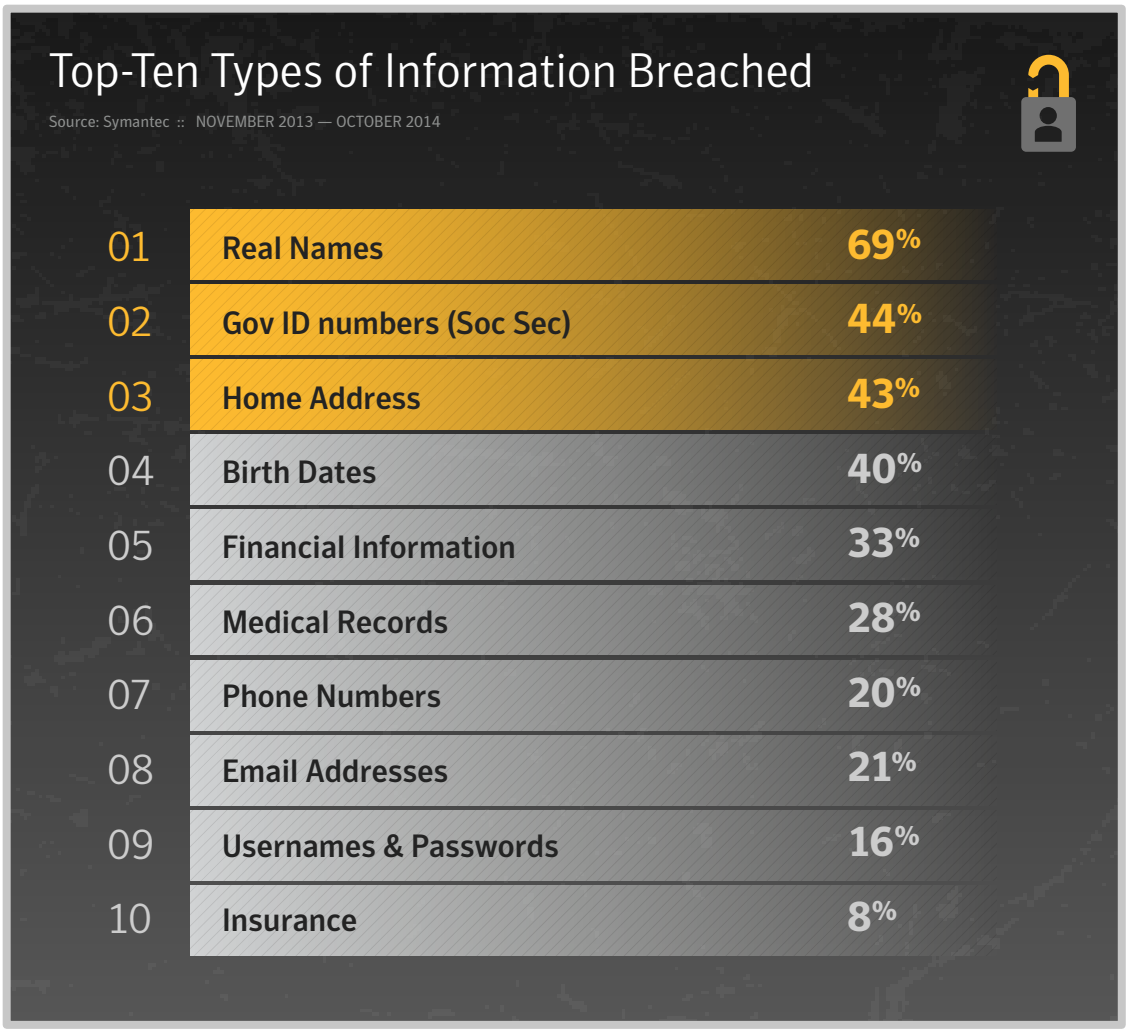
NOVEMBER 2013 — OCTOBER 2014

583 Million

Top Causes of Data Breaches

Source: Symantec :: NOVEMBER 2013 — OCTOBER 2014

		Number of Incidents
Hackers	57%	147
Accidentally Made Public	18%	46
Theft or Loss of Computer or Drive	18%	46
Insider Theft	7%	18
TOTAL		257



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 :: OCTOBER 2014

Rank	Name	October	September
1	W32.Sality.AE	4.1%	4.4%
2	W32.Ramnit!html	4.0%	4.3%
3	W32.Almanahe.B!inf	3.7%	3.7%
4	W32.Ramnit.B	2.7%	2.7%
5	W32.Downadup.B	2.5%	2.3%
6	W32.Ramnit.B!inf	2.1%	2.0%
7	W32.SillyFDC.BDP!lnk	1.4%	2.2%
8	Trojan.Zbot	1.3%	1.2%
9	W32.Virut.CF	1.3%	1.4%
10	W32.Chir.B@mm(html)	1.2%	1.4%

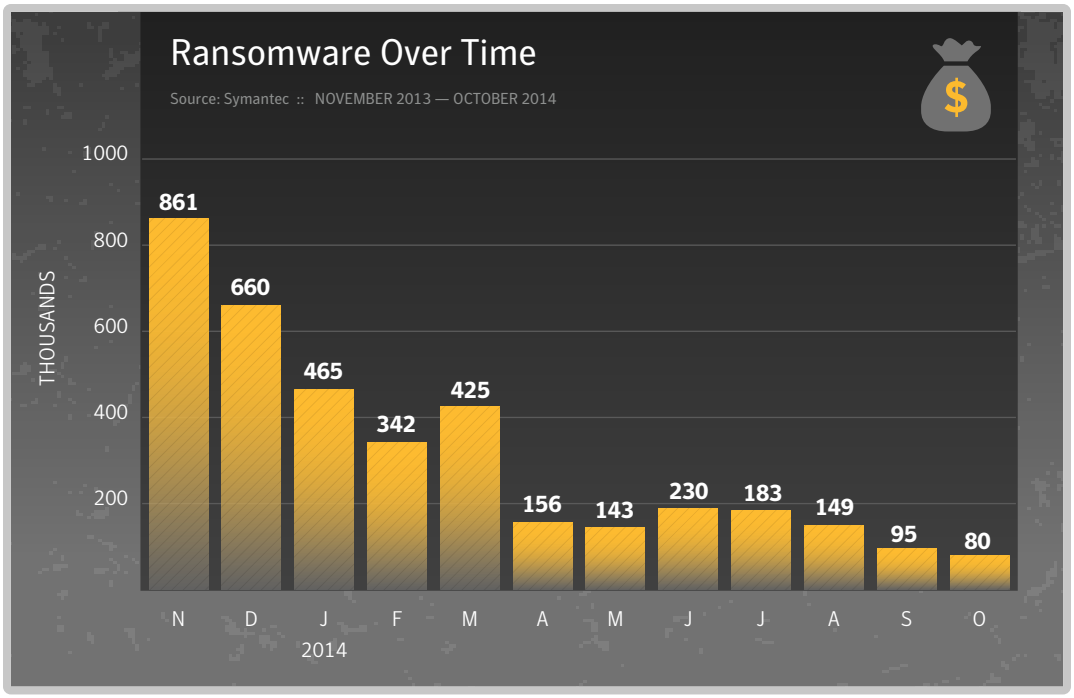
Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: OCTOBER 2014

Rank	Malware Name	October	September
1	OSX.Okaz	28.8%	7.6%
2	OSX.RSPlug.A	14.0%	26.3%
3	OSX.Keylogger	9.3%	3.6%
4	OSX.Flashback.K	5.4%	8.7%
5	OSX.Klog.A	5.2%	2.9%
6	OSX.Crisis	4.8%	8.7%
7	OSX.Stealbit.B	4.7%	5.3%
8	OSX.Flashback	3.9%	4.0%
9	OSX.Netweird	3.7%	5.2%
10	OSX.Sabpab	2.3%	2.7%

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.Okaz, making up 28.8 percent of all OSX malware found on OSX Endpoints.*
- *Overall ransomware activity has remained low since March of this year. However, crypto-style ransomware continues to increase, making up 55 percent of ransomware in October.*
- *China and the US where first and second, respectively, in October in terms of overall botnet source activity.*

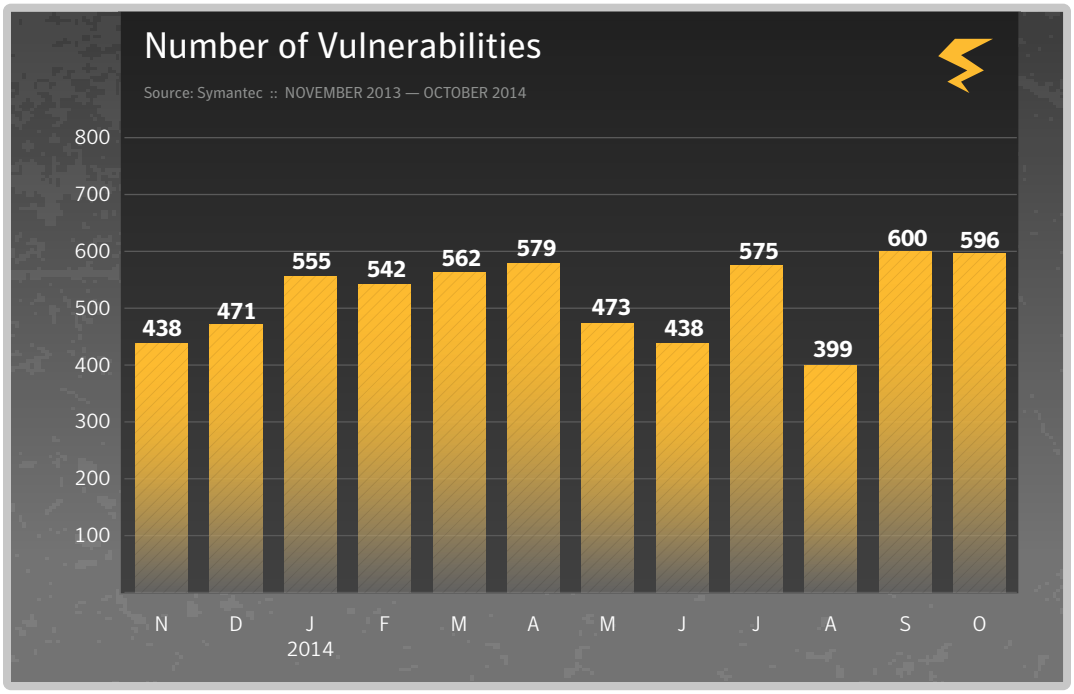


Malicious Activity by Source: Bots

Source: Symantec :: SEPTEMBER 2014

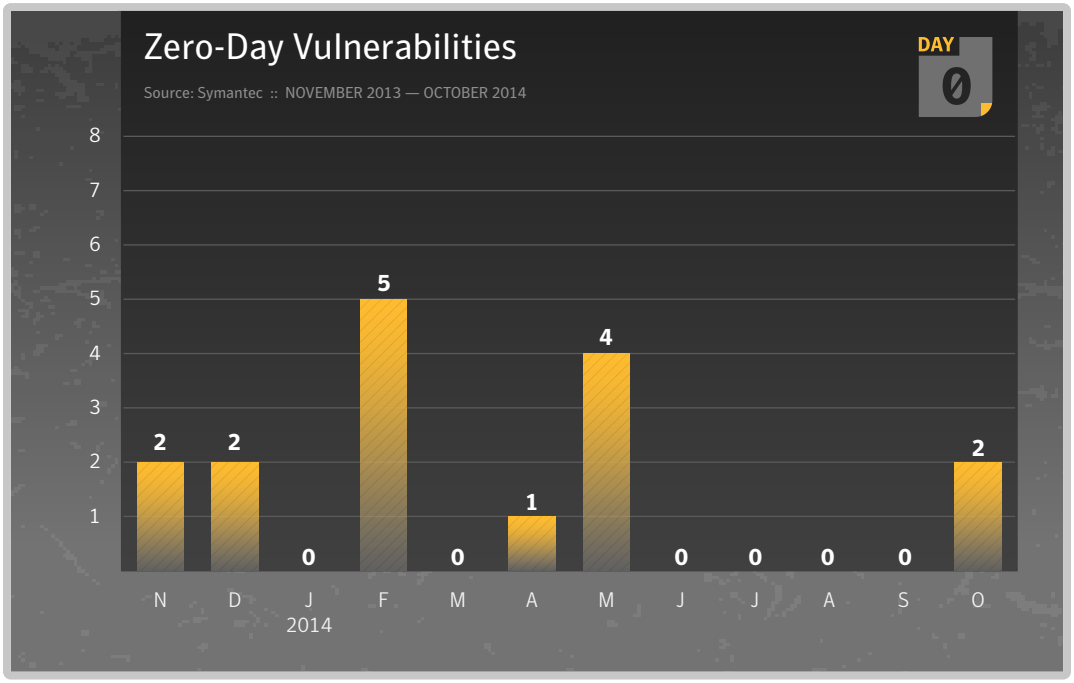
Rank	Country/Region	Percent
1	United States	26.4%
2	China	11.9%
3	Taiwan	8.2%
4	Hungary	4.8%
5	Italy	4.2%
6	Canada	3.4%
7	Japan	3.0%
8	Brazil	2.8%
9	Poland	2.3%
10	Germany	2.2%

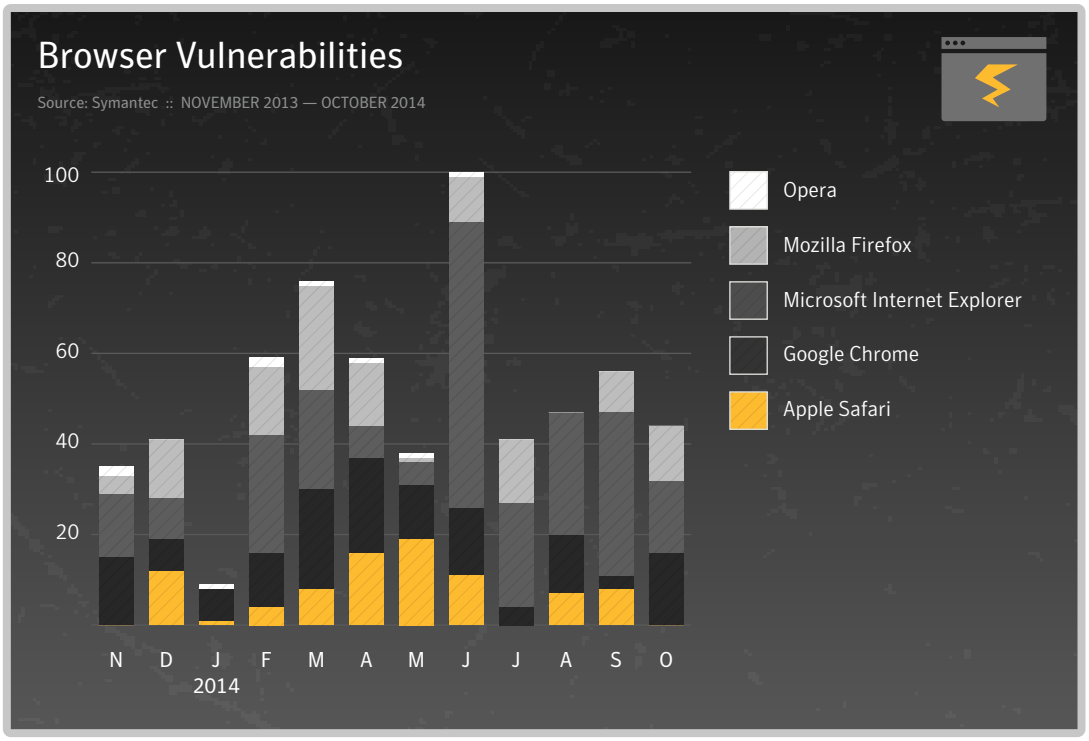
Vulnerabilities

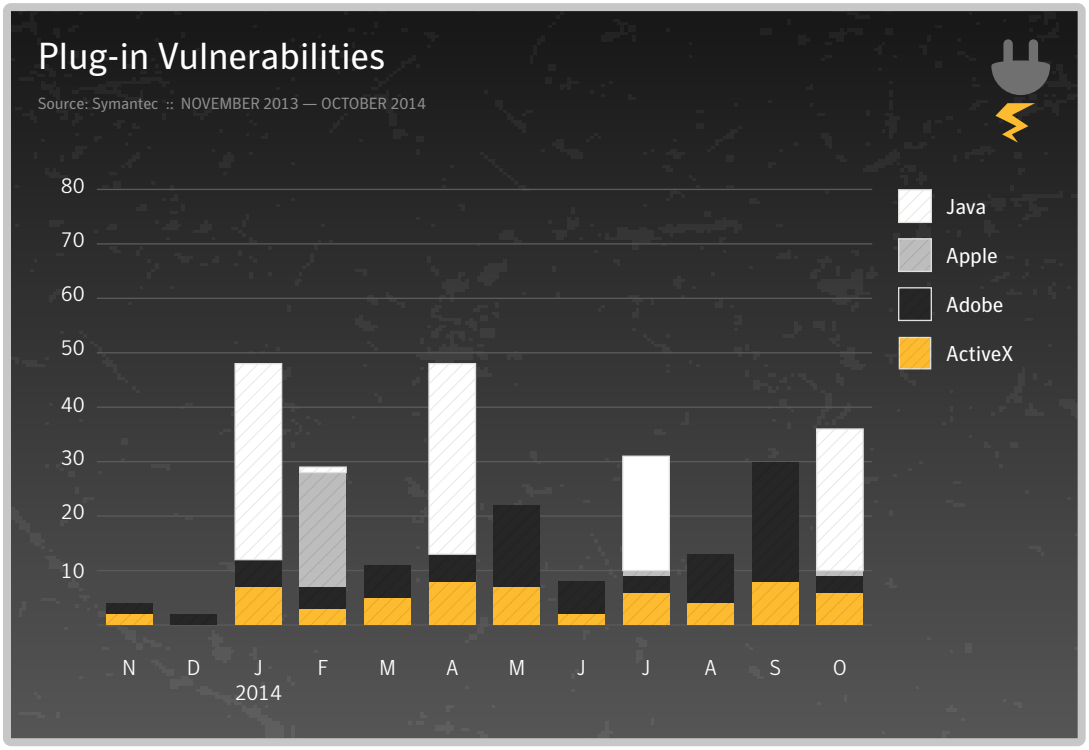


At a Glance

- *There were 596 vulnerabilities disclosed during the month of October.*
- *There were two zero-day vulnerabilities discovered in October.*
- *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.*

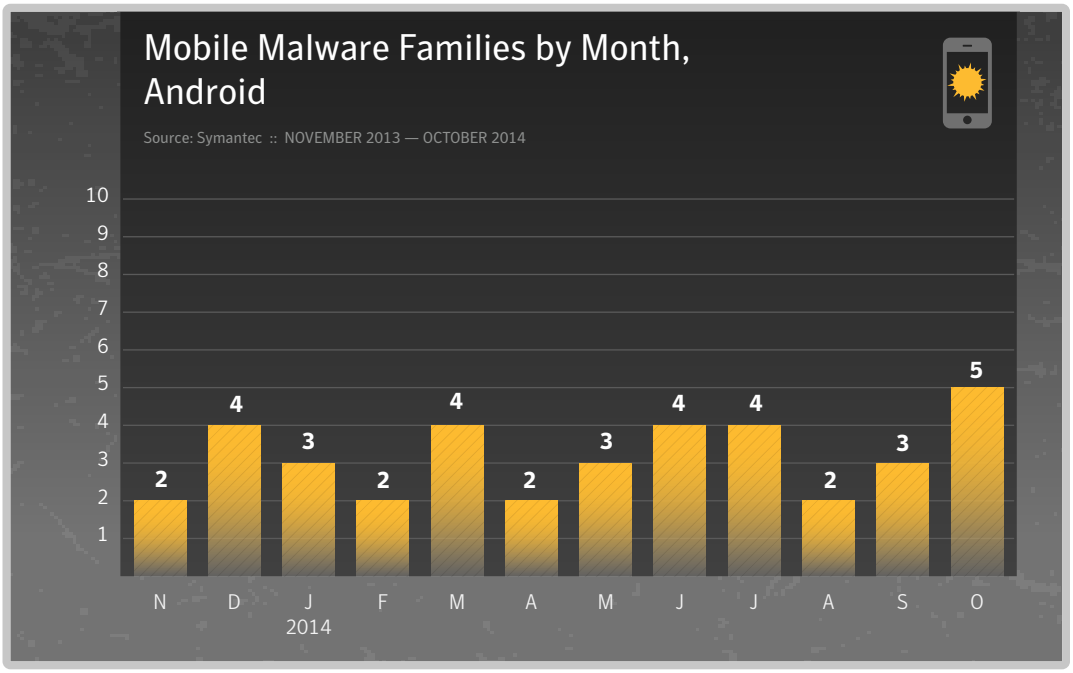



Browser Vulnerabilities
Source: Symantec :: NOVEMBER 2013 — OCTOBER 2014
100
80
60
40
20
N
D
J
F
M
A
M
J
J
A
S
O
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


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

SOCIAL MEDIA + MOBILE THREATS

Mobile

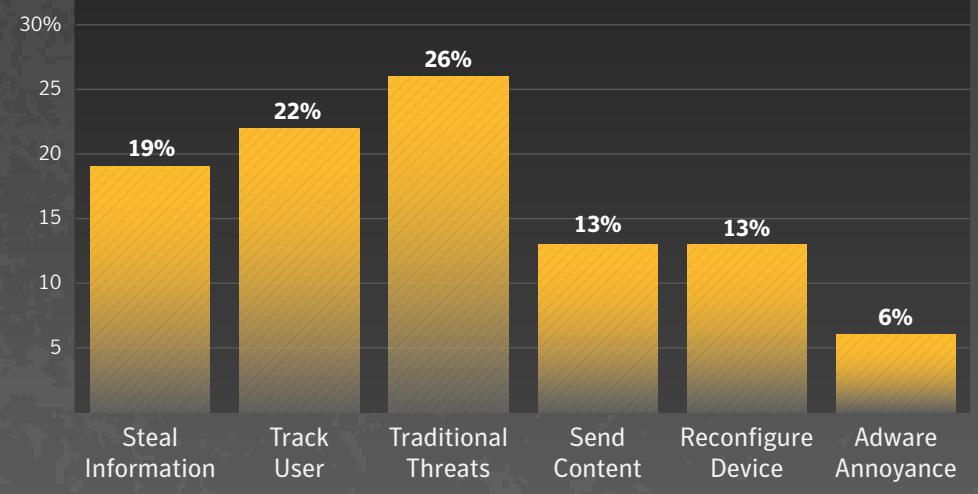


At a Glance

- *There were five Android malware families discovered in July.*
- *Of the threats discovered in the last 12 months, 26 percent are traditional threats, such as back door Trojans and downloaders.*
- *In terms of social networking scams, 38 percent were fake offerings, while 49 percent were manually shared scams.*

Mobile Threat Classifications

Source: Symantec :: NOVEMBER 2013 — OCTOBER 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.

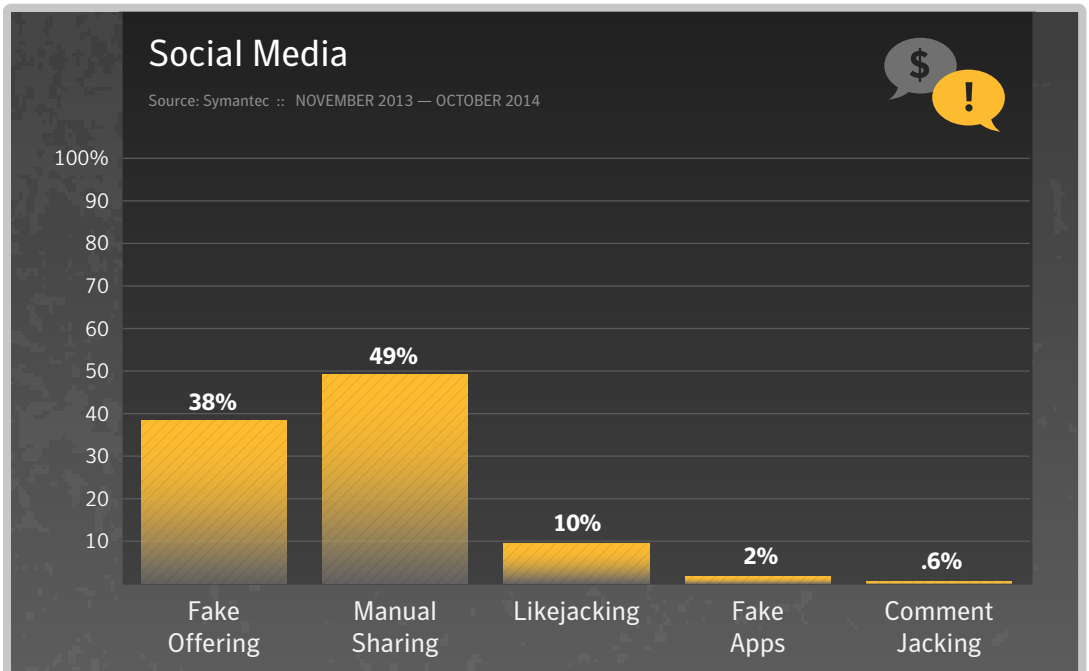
Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

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.

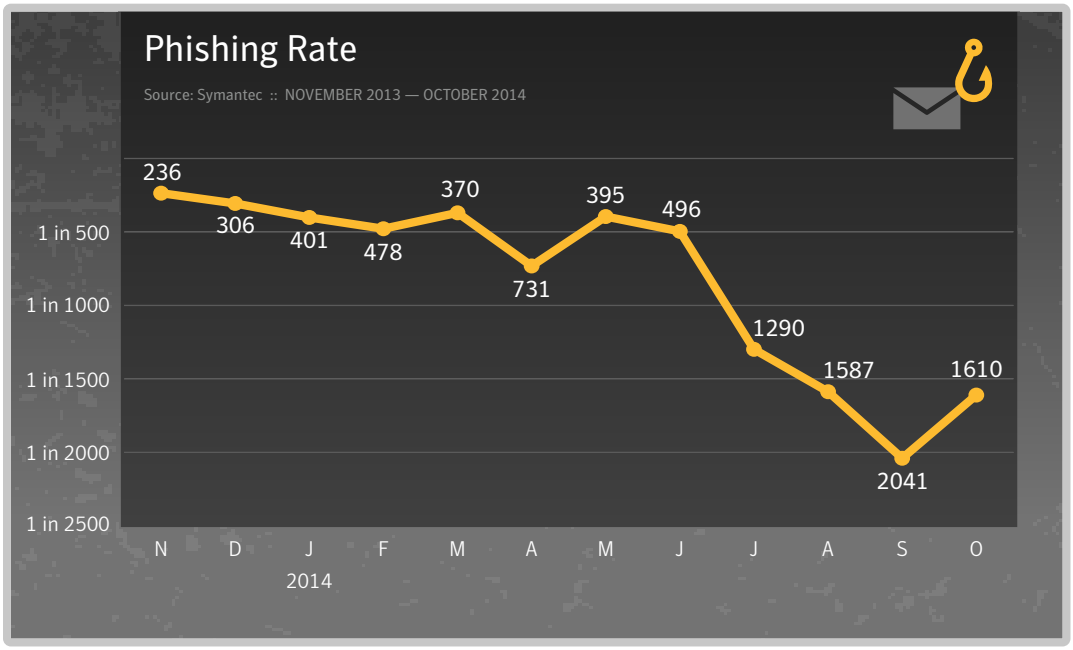
Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

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.

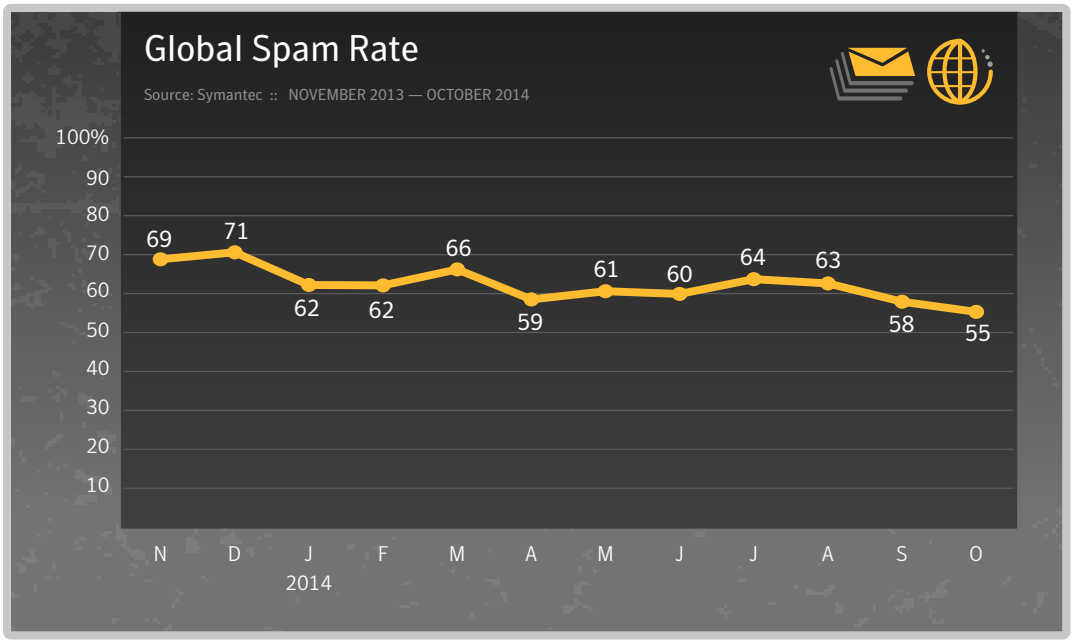
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

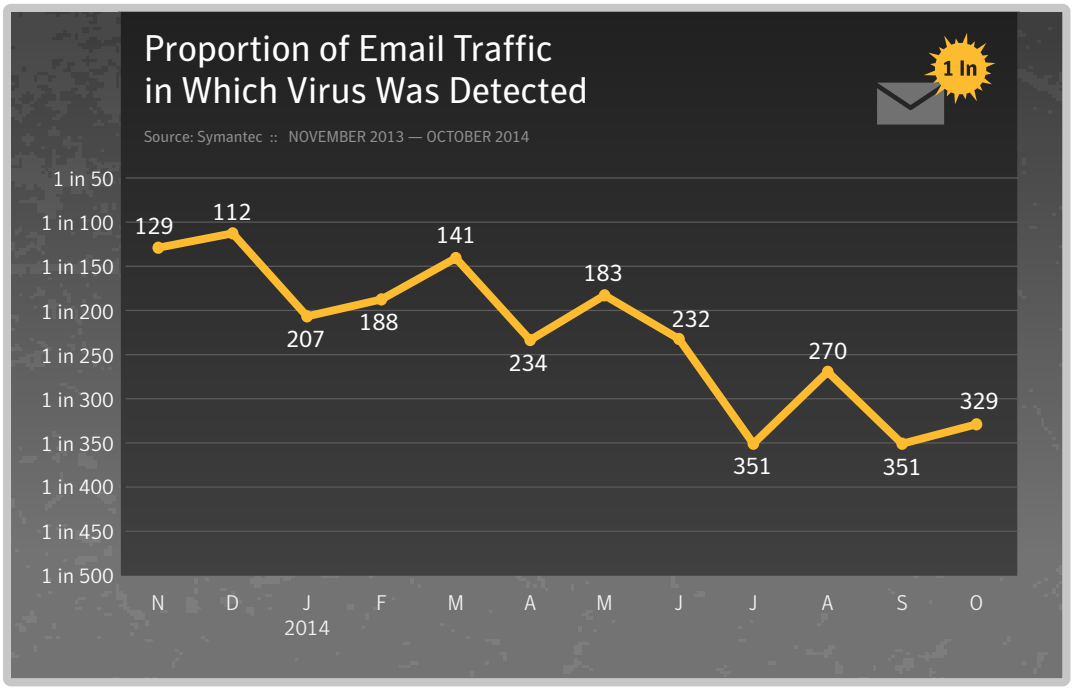


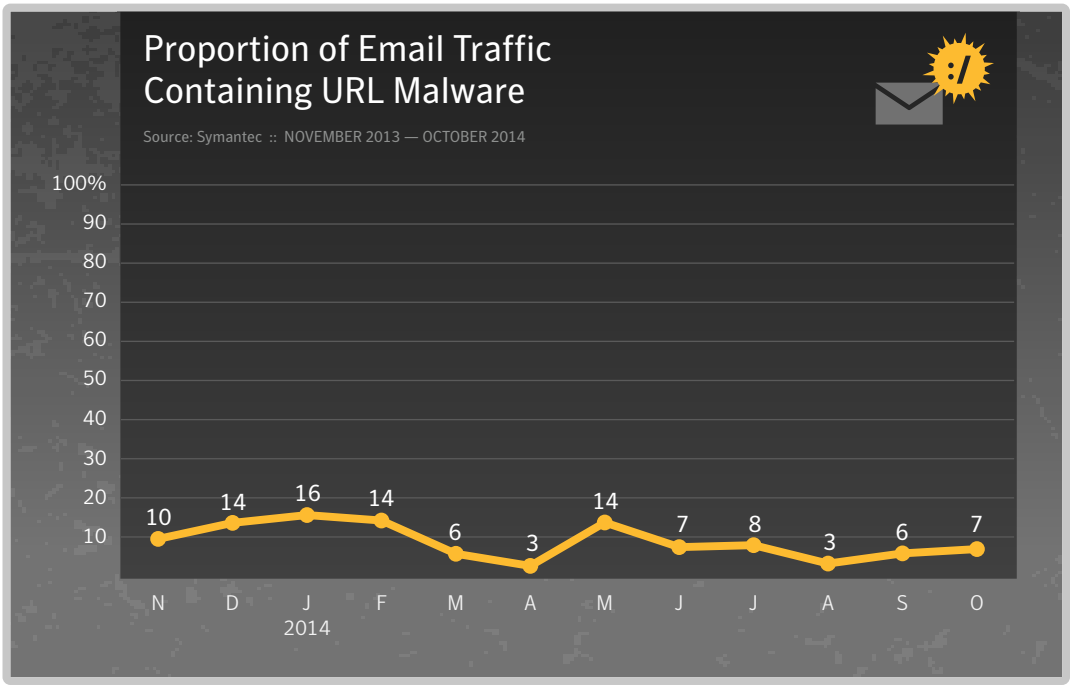
At a Glance

- *The phishing rate rose in October, at one in 1,610 emails, up from one in 2,041 emails in September.*
- *The global spam rate was 55.3 percent for the month of October.*
- *One out of every 329 emails contained a virus.*
- *Of the email traffic in the month of October, 6.9 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