Symantec

SYMANTEC INTELLIGENCE REPORT

JUNE 2014

CONTENTS

Summary

Welcome to the June 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 largest data breach reported in June resulted in the exposure up 1.3 million identities. This seems like a small number when compared to the 145 million exposed in the largest breach of May. However, while reported in June, this breach also took place during the month of May. This brings the total number of identities exposed in May to over 147 million, which is the second-worst month for data breaches in the last 12 months.

There was an average of 88 spear-phishing attacks per day in June. This appears to be a return of spear-phishing levels seen in the months of March and April, after the average per day dropped in May.

A relatively new OSX threat by the name of OSX.Stealbit.B topped our list of OSX malware, responsible for 25.7 percent of OSX threat found on OSX systems. This threat looks for specific bitcoin-related software on OSX computers and will attempt to modify the programs in order to steal bitcoins.

The number of Android variants per family reached the lowest levels seen in the last twelve months. While there was not a significant change in the number of families discovered in June, this may indicate that attackers have had more success with their current set of threats, reducing their need to create multiple variants.

June was a quiet month for vulnerabilities, where (only) 438 were reported—tying the lowest number reported in the last 12 months. There were no zero day vulnerabilities disclosed during the month.

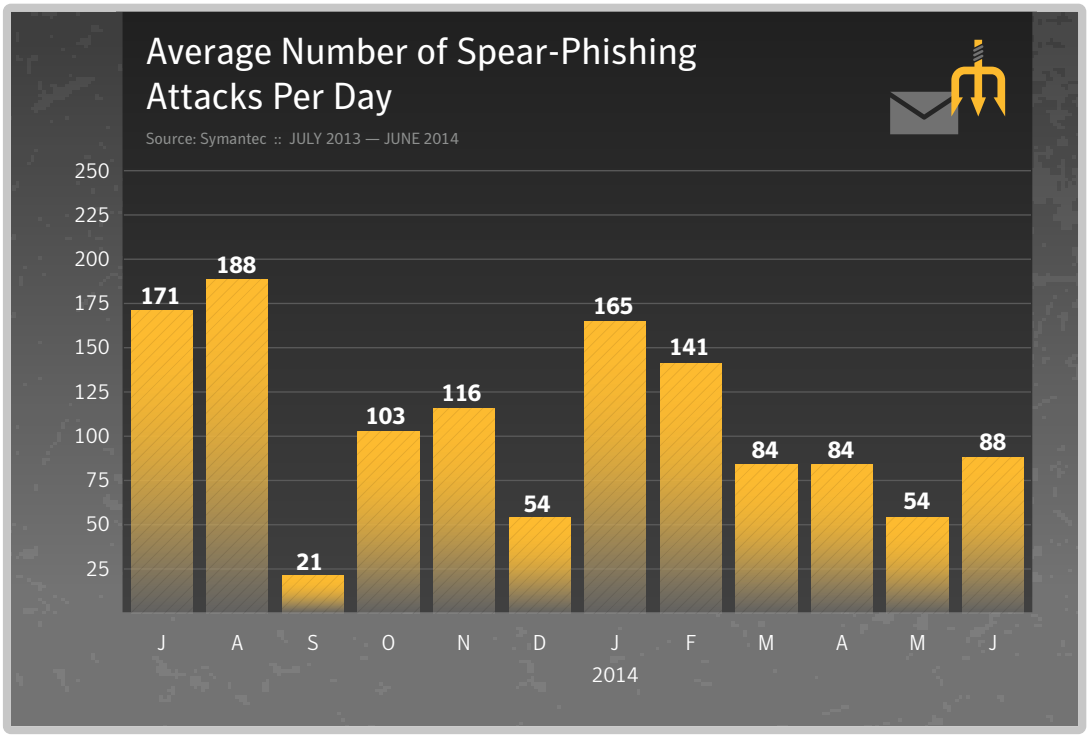
We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

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 per day returned to similar levels seen in March and April, after dropping in May.*
- *The .doc file type continues to be the most common attachment type used in spear-phishing attacks, followed by .exe files.*
- *Organizations with 2500+ employees were the most likely to be targeted in May.*
- *The Top-Ten Industries targeted remains largely unchanged from May, with minor shifts of less than one percent for various industries.*

Attachments Used in Spear-Phishing Emails

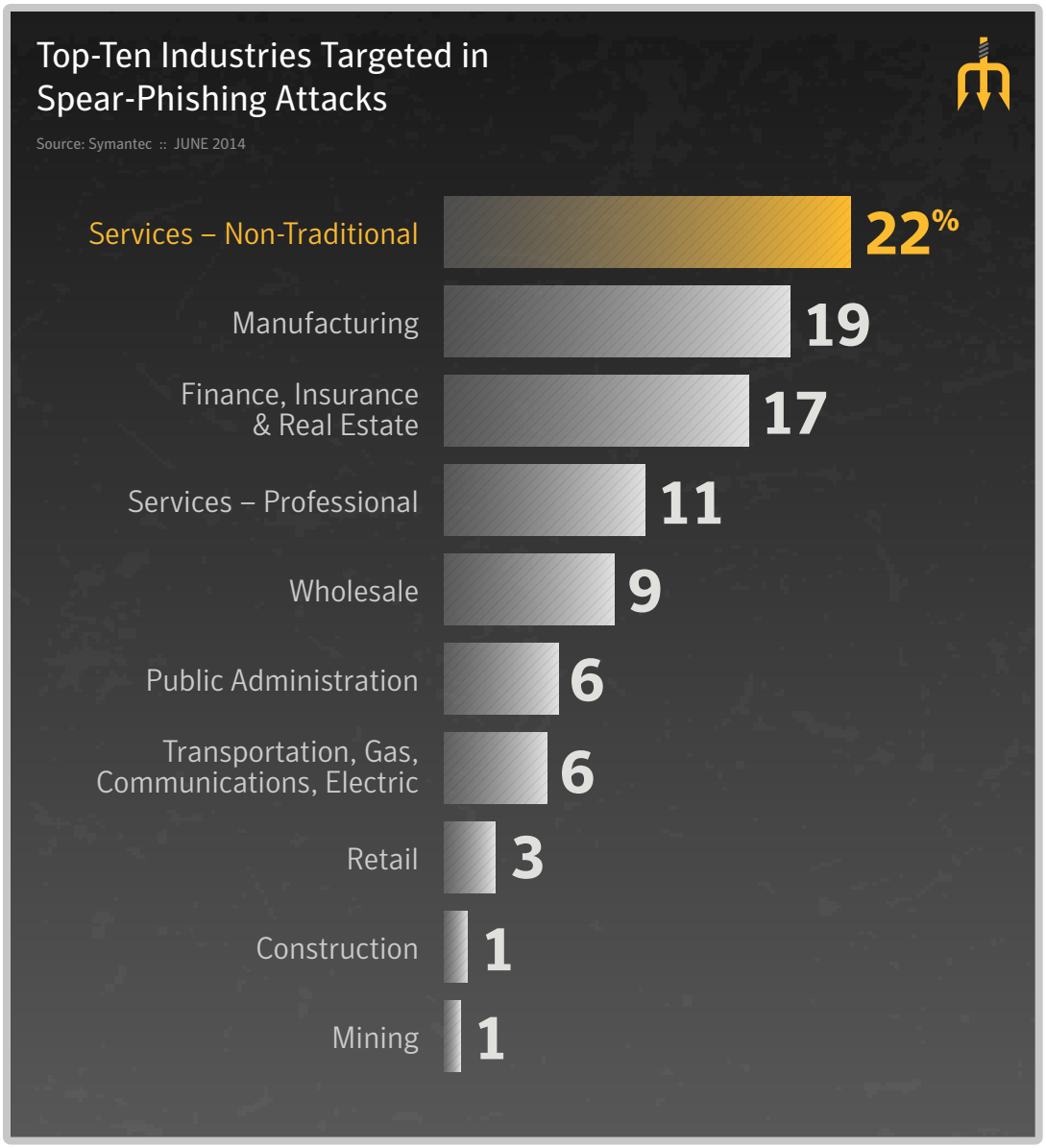
Source: Symantec :: JUNE 2014

Executable type	June	May
.doc	19.5%	17.7%
.exe	15.4%	16.1%
.au3	11.5%	11.8%
.jpg	6.2%	7.0%
.scr	5.8%	6.4%
.class	2.1%	1.6%
.pdf	1.7%	1.3%
.bin	1.1%	1.2%
.mso	0.6%	—
.dmp	0.6%	—

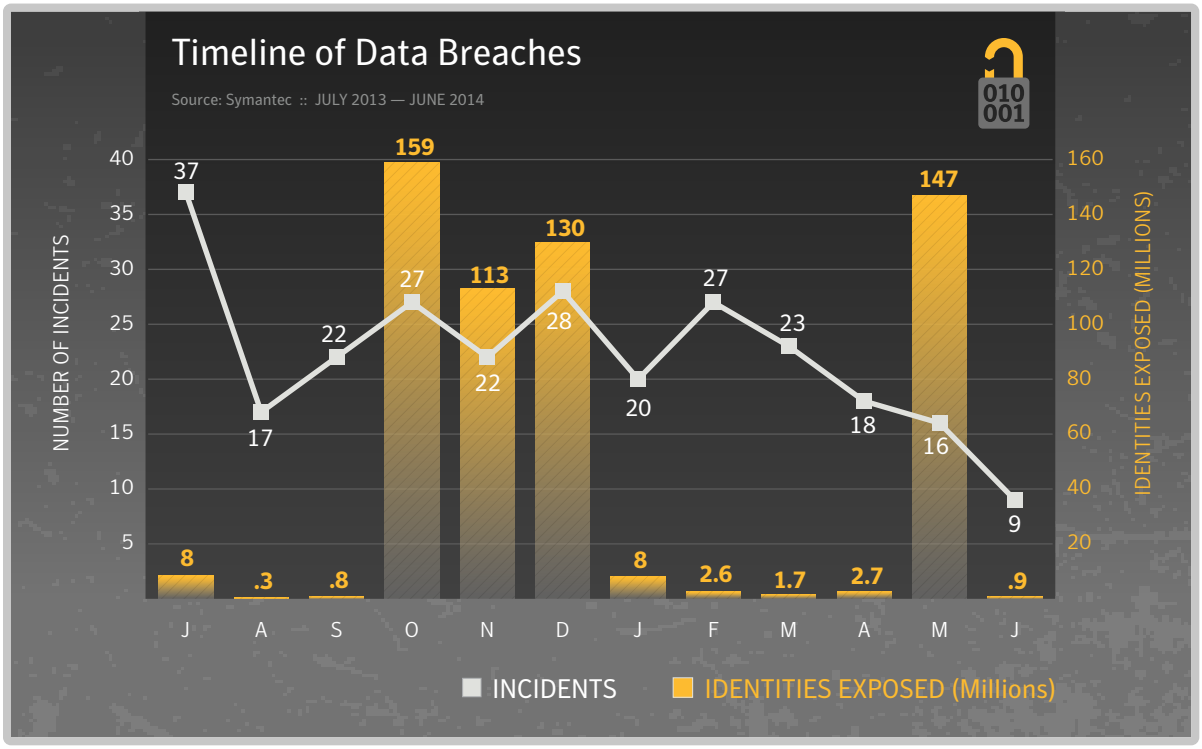
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: JUNE 2014

Organization Size	June	May
1-250	36.3%	37.0%
251-500	8.4%	8.6%
501-1000	9.3%	9.0%
1001-1500	3.0%	3.0%
1501-2500	4.1%	4.1%
2500+	38.9%	38.3%


Top-Ten Industries Targeted in Spear-Phishing Attacks
Source: Symantec :: JUNE 2014
Services – Non-Traditional
22%
Manufacturing
19
Finance, Insurance & Real Estate
17
Services – Professional
11
Wholesale
9
Public Administration
6
Transportation, Gas, Communications, Electric
6
Retail
3
Construction
1
Mining
1

Data Breaches



At a Glance

- *The largest data breach reported in June took place during the month of May.*
- *With 1.3 million identities exposed in this breach, this brings the total identities exposed in May to 147 million.*
- *Hackers have been responsible for 49 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

JULY 2013 — JUNE 2014

266

Total Identities Exposed

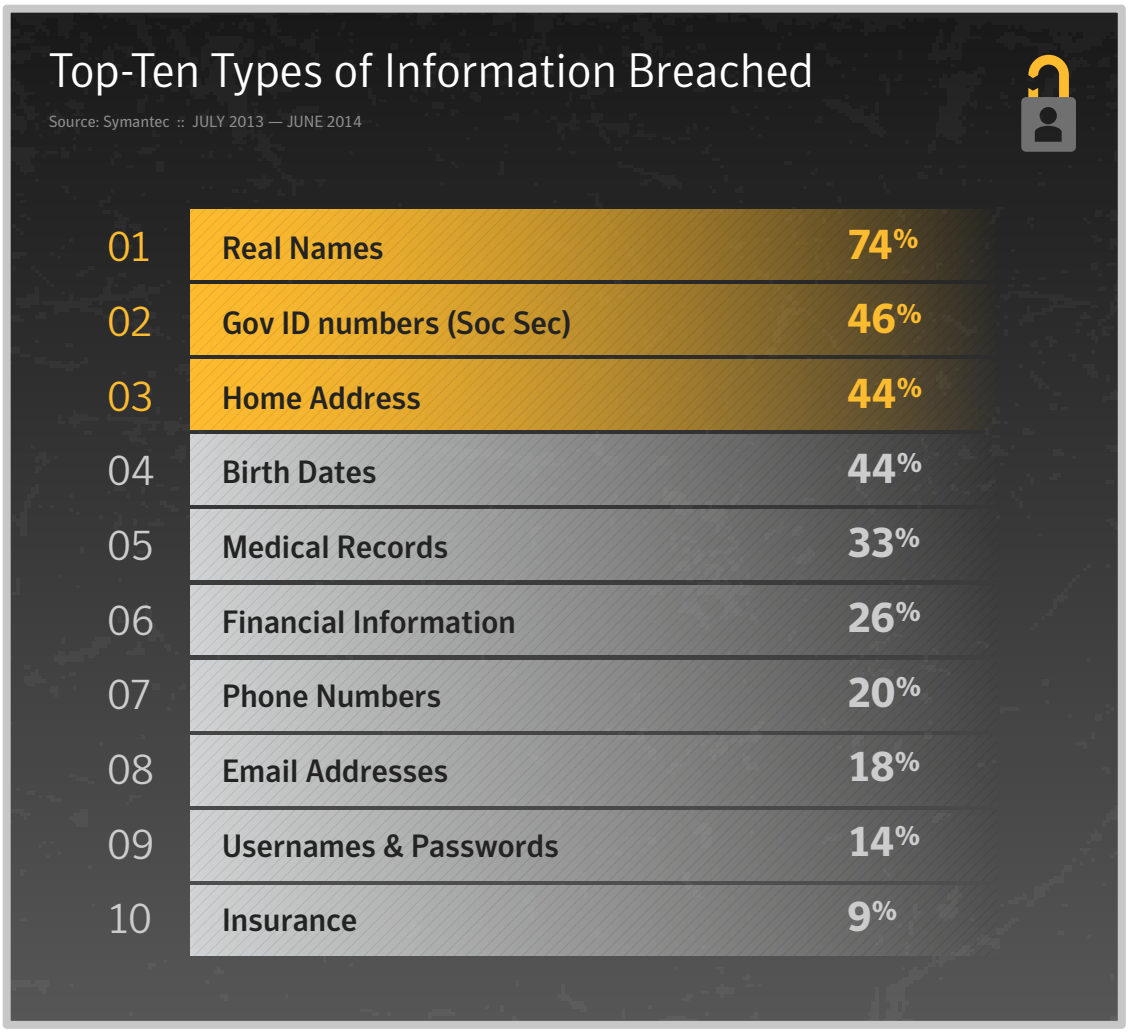
JULY 2013 — JUNE 2014

574 Million

Top Causes of Data Breaches

Source: Symantec :: JULY 2013 — JUNE 2014

		Number of Incidents
Hackers	49%	131
Accidentally Made Public	23%	62
Theft or Loss of Computer or Drive	20%	52
Insider Theft	7%	19
Fraud	.4%	1
Unknown	.4%	1
TOTAL		266



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 :: JUNE 2014

Rank	Name	Percentage
1	W32.Sality.AE	5.3%
2	W32.Ramnit!html	5.1%
3	W32.Ramnit.B	3.8%
4	W32.Almanahe.B!inf	3.7%
5	W32.Downadup.B	2.9%
6	W32.Ramnit.B!inf	2.6%
7	W32.SillyFDC.BDP!lnk	2.1%
8	W32.Virut.CF	1.6%
9	Trojan.Malscript	1.4%
10	Trojan.Zbot	1.4%

Malicious Activity by Source: Bots

Source: Symantec :: JUNE 2014

Rank	Country/Region	Percent
1	United States	21.9%
2	China	10.6%
3	Taiwan	7.1%
4	Hungary	5.0%
5	Italy	4.4%
6	Brazil	3.0%
7	Japan	2.9%
8	Canada	2.7%
9	France	2.6%
10	Germany	2.2%

At a Glance

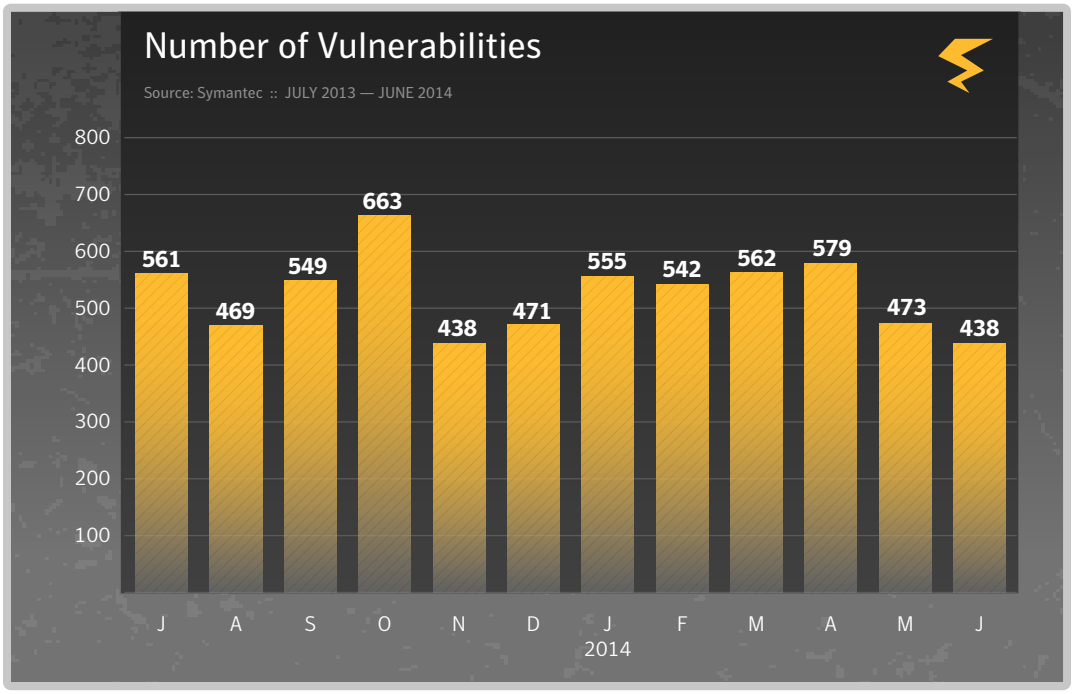
- *W32.Sality and W32.Ramnit variants continue to dominate the top-ten malware list.*
- *The United States continues to be the largest source of bot activity.*
- *The most common threat on OSX was OSX.Stealbit.B, making up 26 percent of all OSX malware found on OSX Endpoints.*

Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: JUNE 2014

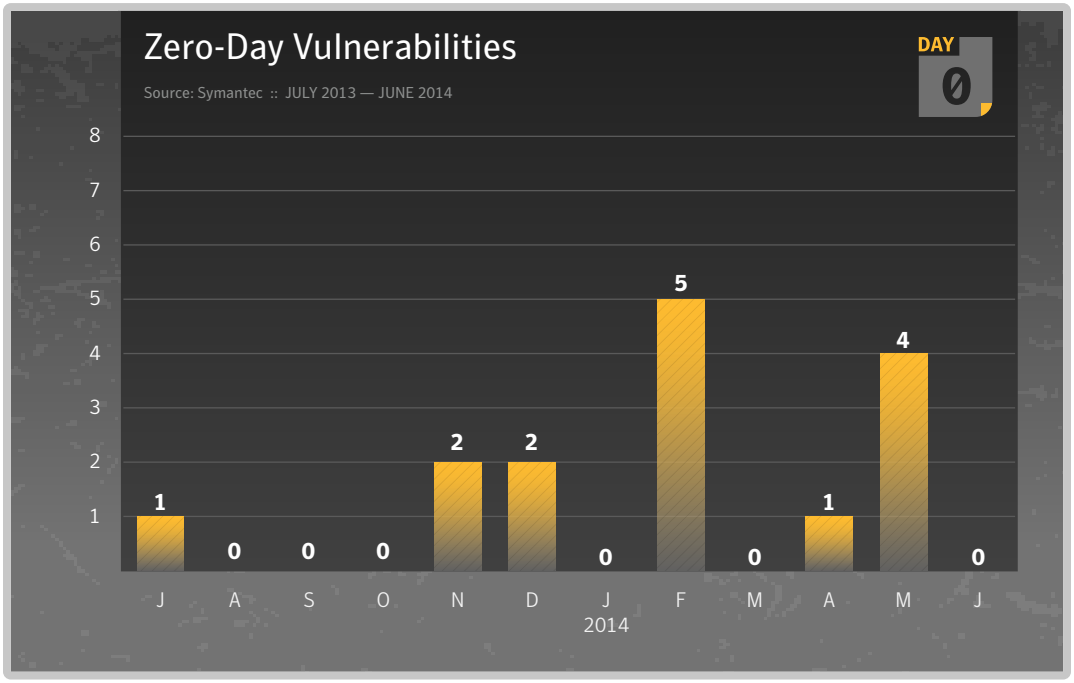
Malware Name	Percent of Mac Threats Detected on Macs
OSX.Stealbit.B	25.7%
OSX.RSPlug.A	24.1%
OSX.Flashback.K	14.7%
OSX.HelIRTS	6.0%
OSX.Sabpab	4.9%
OSX.SMSSend	4.5%
OSX.Keylogger	2.5%
OSX.Loosemaque	2.2%
OSX.Remoteaccess	2.0%
OSX.Flashback	1.6%

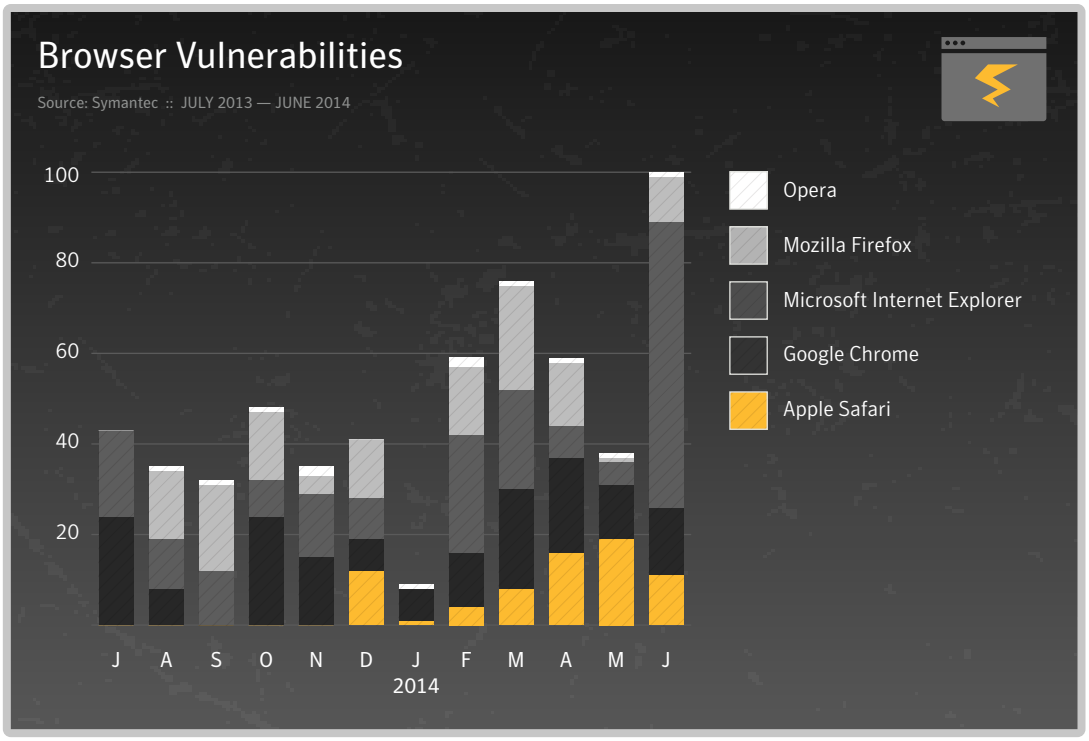
Vulnerabilities



At a Glance

- *Vulnerabilities are at their lowest levels seen in the last 12 months.*
- *There were no zero-day vulnerabilities discovered in June.*
- *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.*

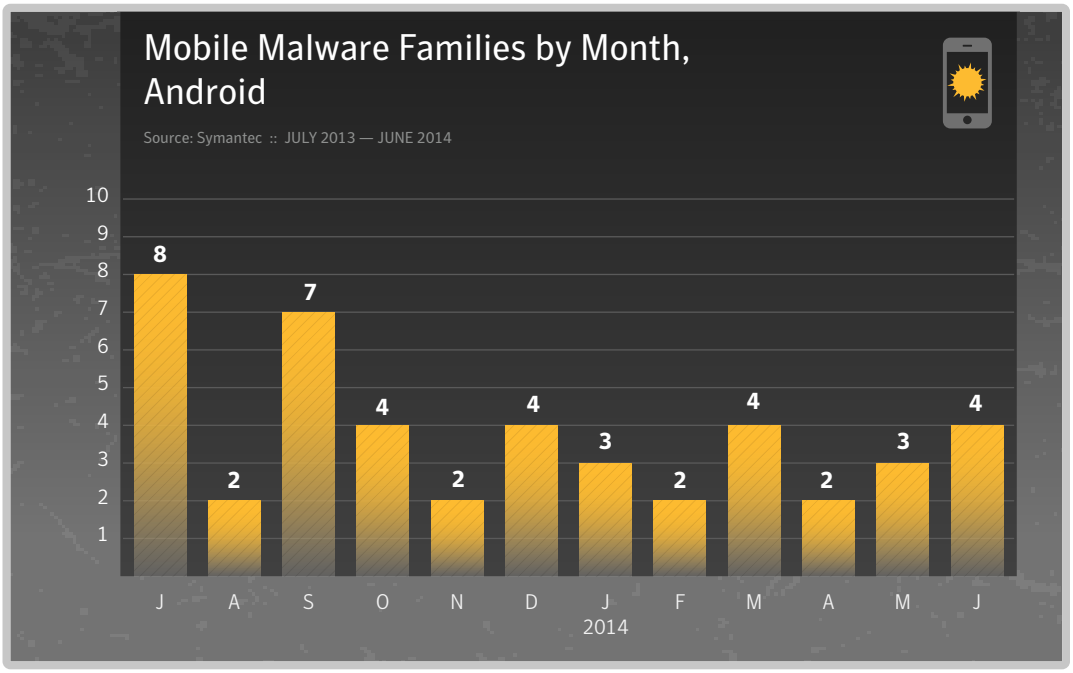



Browser Vulnerabilities
Source: Symantec :: JULY 2013 — JUNE 2014
100
80
60
40
20
J A S O N D J F M A M J
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


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

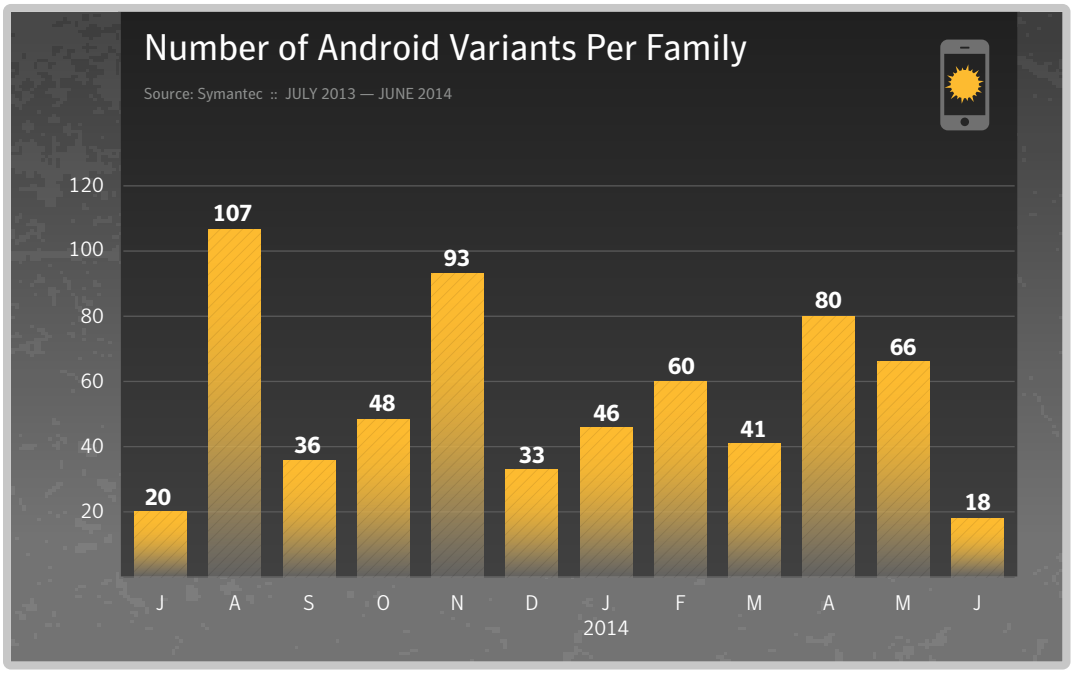
SOCIAL MEDIA + MOBILE THREATS

Mobile



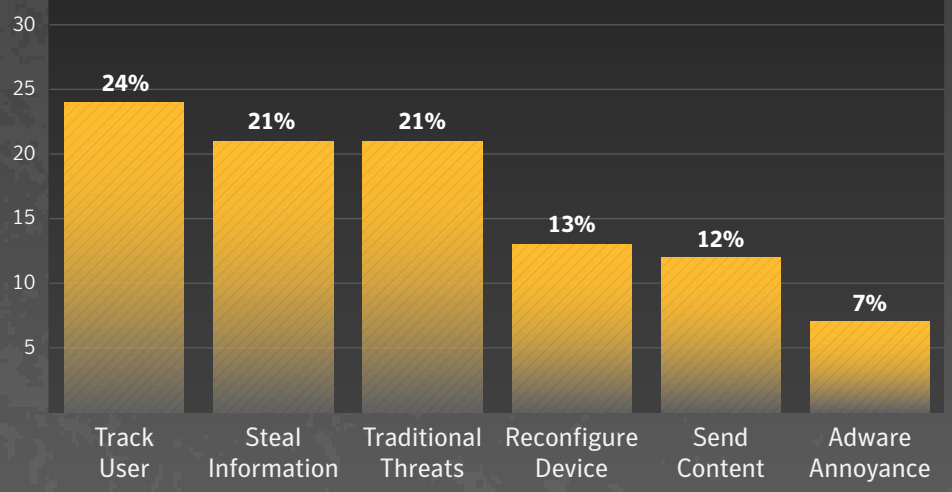
At a Glance

- *There were four Android malware families discovered in June.*
- *The number of variants per family reached its lowest levels seen in the last 12 months.*
- *Of the threats discovered in the last 12 months, 28 percent track the device's user and 21 percent steal information from the device.*
- *In terms of social networking scams, 78 percent were fake offerings.*



Mobile Threat Classifications

Source: Symantec :: JULY 2013 — JUNE 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.

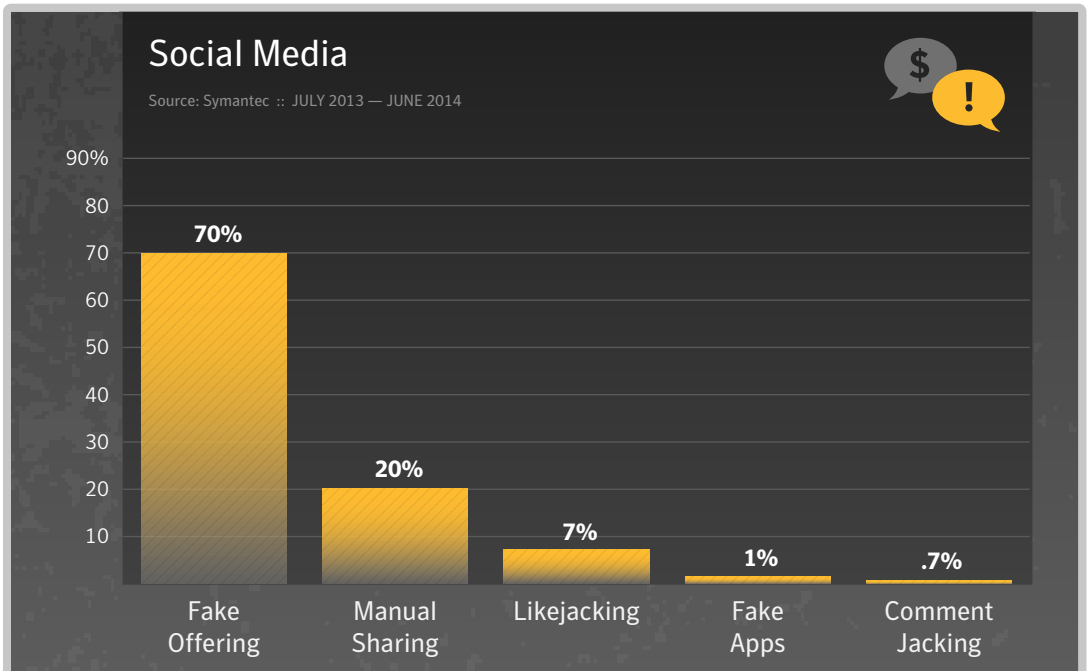
Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

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.

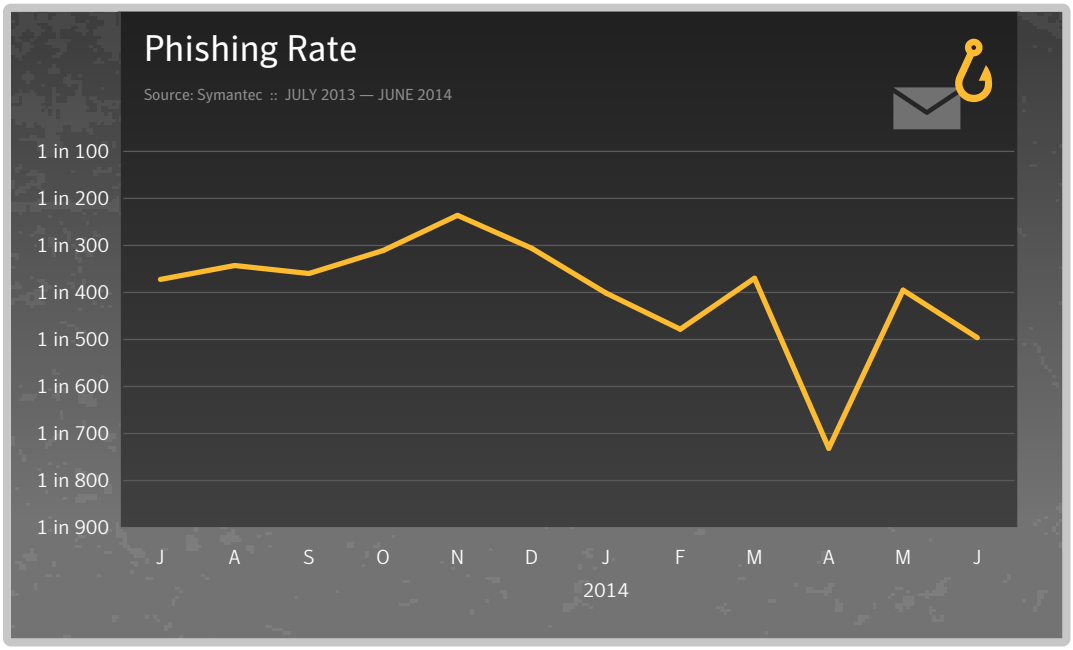
Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

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.

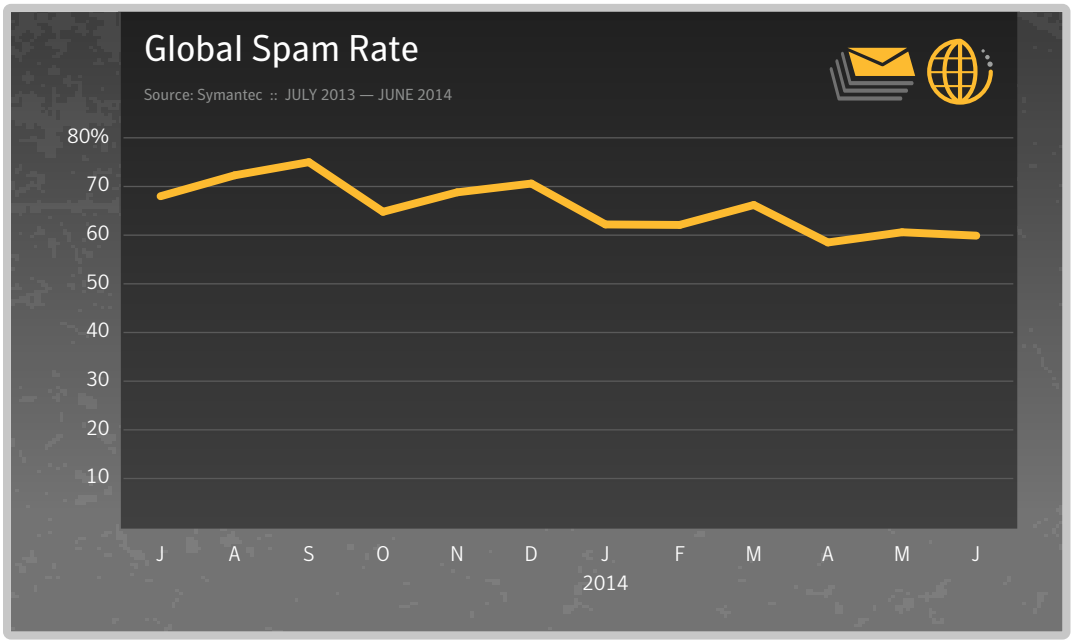
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

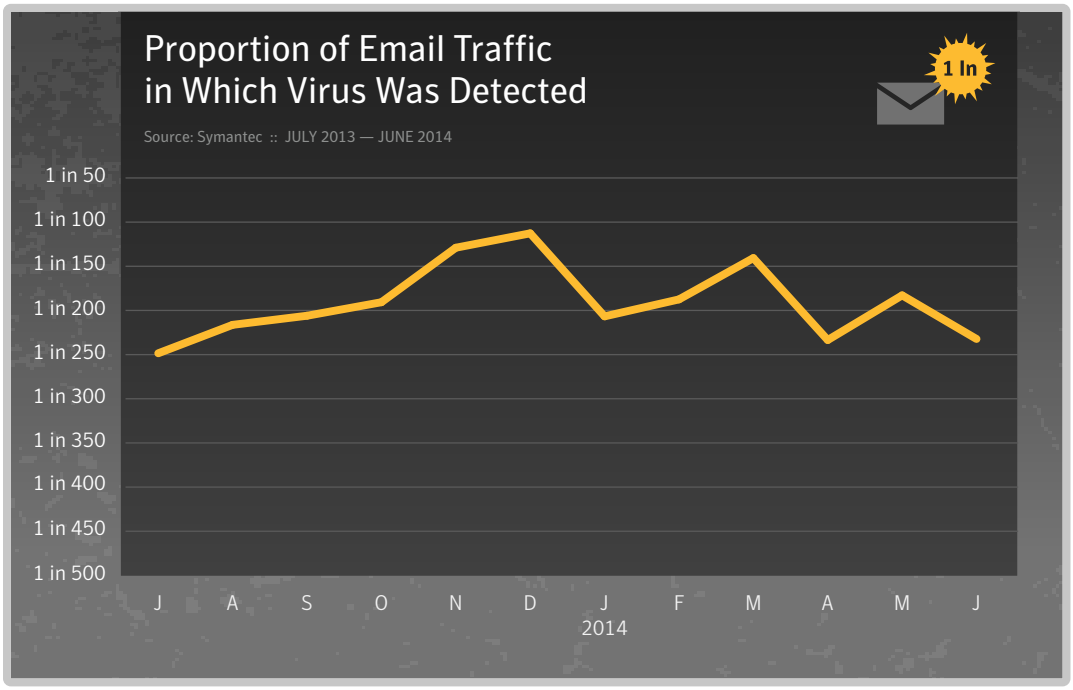


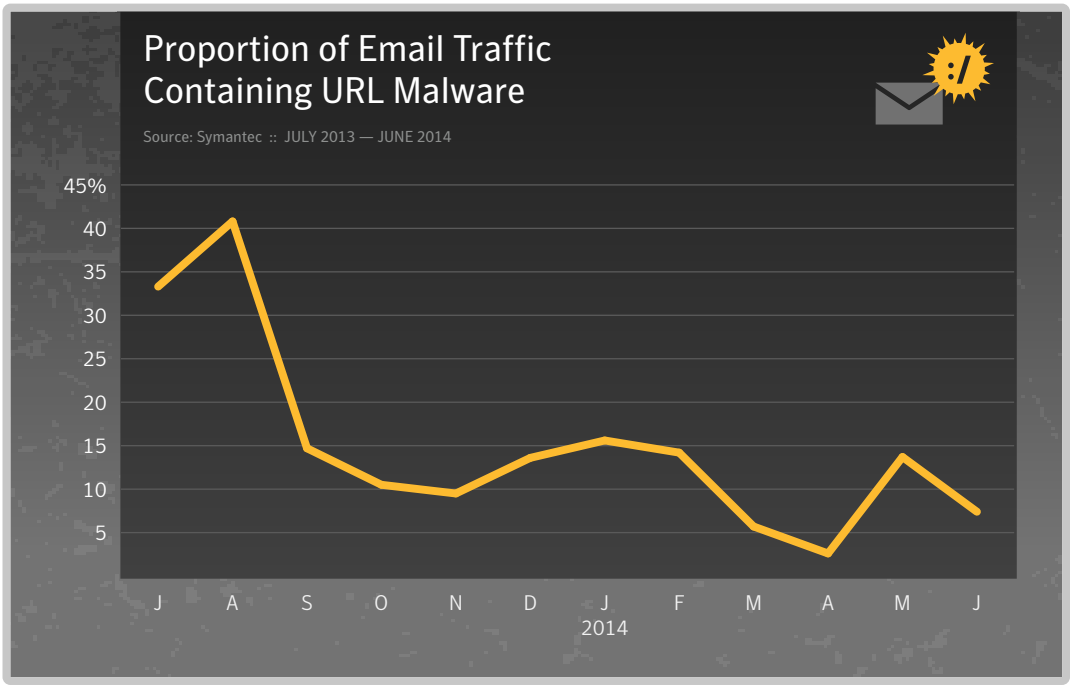
At a Glance

- *The phishing rate for June was one in 496 emails, down from one in 395 emails in May.*
- *The global spam rate was 59.9 percent for the month of June.*
- *One out of every 232 emails contained a virus.*
- *Of the email traffic in the month of June, 7.4 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