Symantec

SYMANTEC INTELLIGENCE REPORT

JULY ⌖ 2014

CONTENTS

Summary

Welcome to the July 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 per day has dropped back to a similar level seen 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, which non-traditional services, such as Business, Amusement, and Repair-related services, lead the Top-Ten Industries targeted, followed by Manufacturing.

The largest data breach reported in July resulted in the exposure of 900,000 identities. Hackers continue to be responsible for 49 percent of data breaches over the last 12 months, most often exposing real names, government ID numbers, such as Social Security numbers, and home addresses in the data breaches.

W32.Sality and W32.Ramnit variants continue to dominate the top-ten malware list. The most common OSX threat seen was OSX.RSPlug.A, making up 38 percent of all OSX malware found on OSX Endpoints.

There were 575 vulnerabilities disclosed during the month of July, though no zero-day vulnerabilities discovered. Internet Explorer has reported the most browser vulnerabilities in the last 12 months, while Oracle's Java reported the most plug-in vulnerabilities over the same time period.

There were four Android malware families discovered in July. Of the mobile threats discovered in the last 12 months, 24 percent steal information from the device and 22 percent track the device's user. In terms of social networking scams, 63 percent were fake offerings and 27 percent were manually shared scams.

Finally, the phishing rate was down in July, at one in 1,299 emails, down from one in 496 emails in June. The global spam rate was 63.7 percent for the month of July, one out of every 351 emails contained a virus, and of the email traffic in the month of July, 7.9 percent contained a malicious URL.

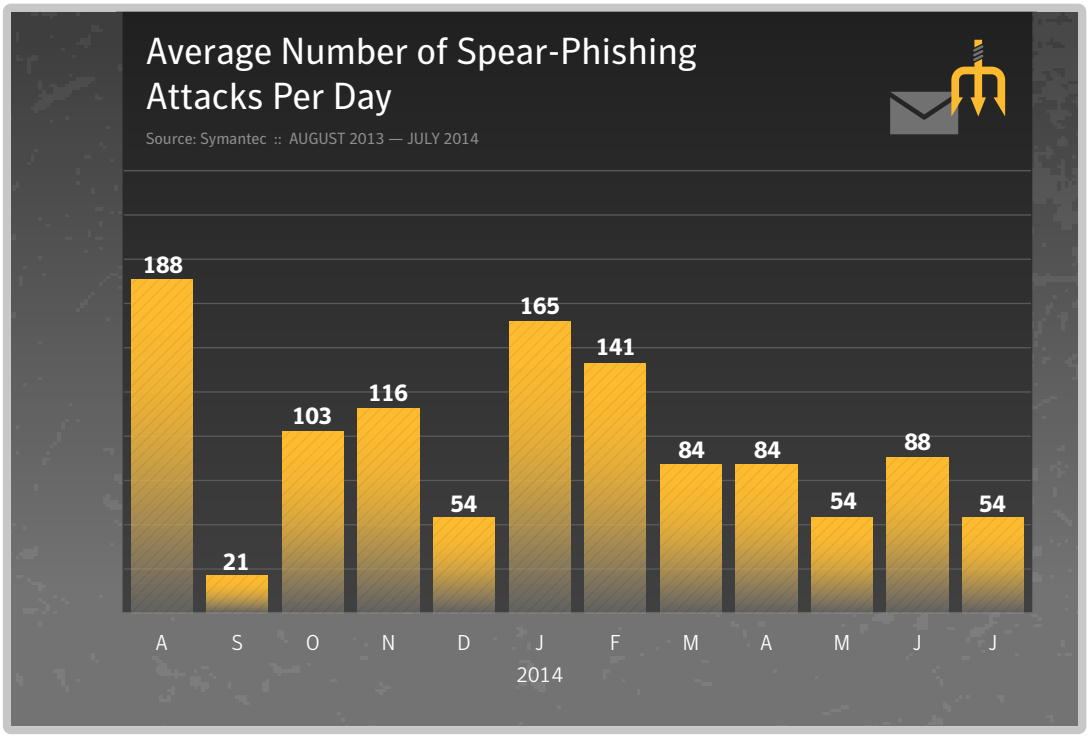
We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

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 has dropped back to a similar level seen 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 July.*
- *Non-traditional services, such as Business, Amusement, and Repair-related services, lead the Top-Ten Industries targeted, followed by Manufacturing.*

Attachments Used in Spear-Phishing Emails

Source: Symantec :: JULY 2014

Executable type	July	June
.doc	19.9%	19.5%
.exe	15.1%	15.4%
.au3	10.5%	11.5%
.jpg	5.9%	6.2%
.scr	5.6%	5.8%
.class	2.4%	2.1%
.pdf	2.0%	1.7%
.bin	1.0%	1.1%
.xls	0.7%	—
.dmp	0.6%	0.6%

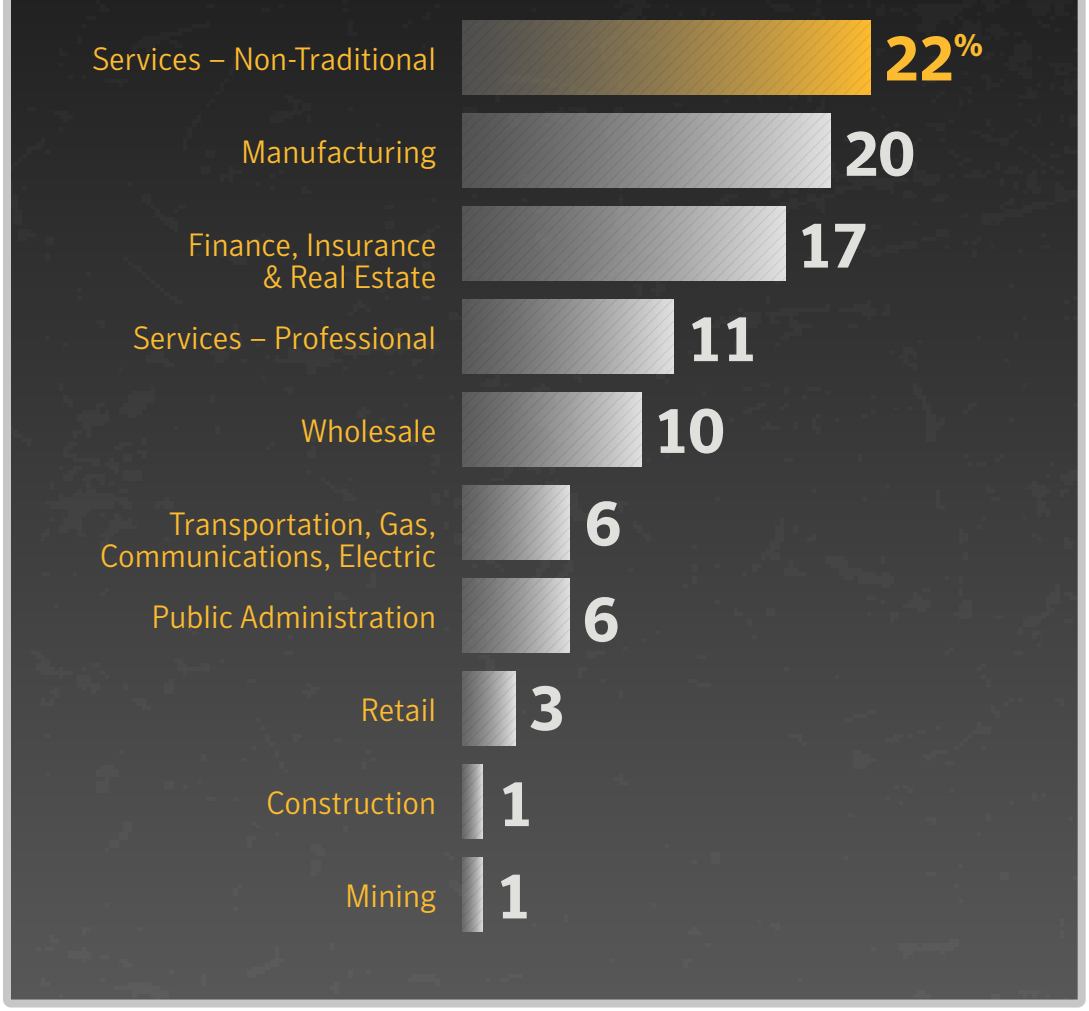
Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: JULY 2014

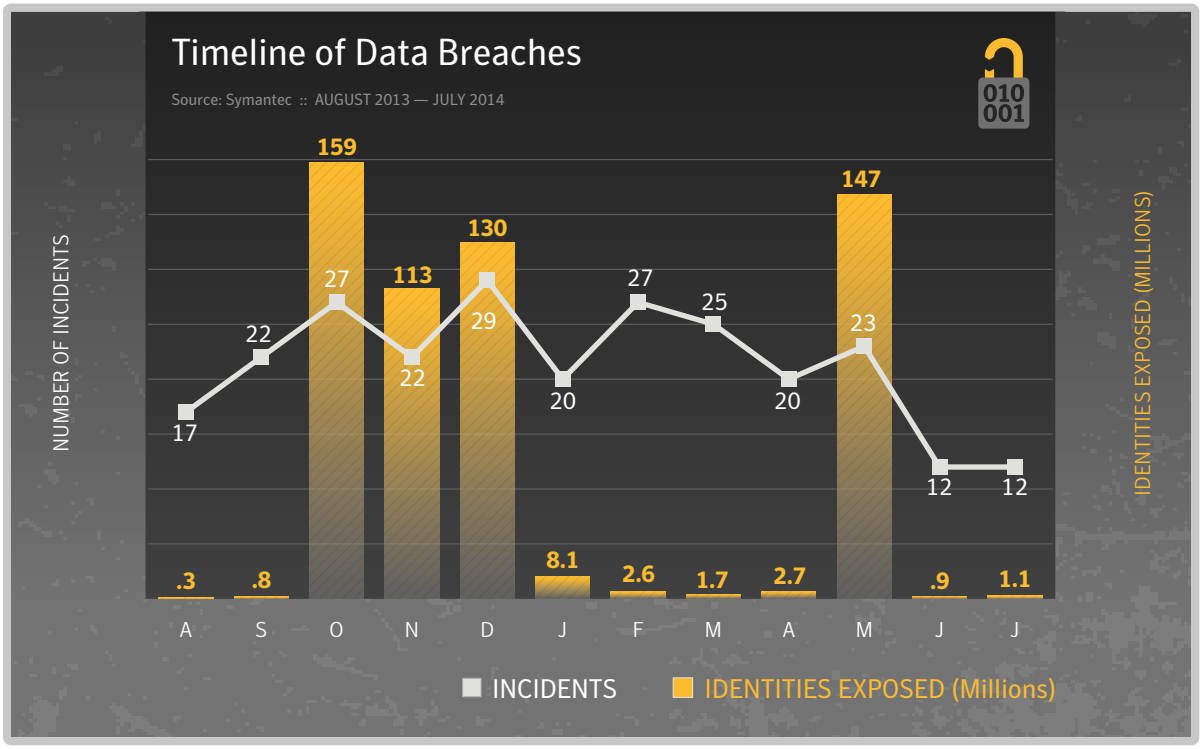
Organization Size	July	June
1-250	35.7%	36.3%
251-500	8.5%	8.4%
501-1000	9.0%	9.3%
1001-1500	3.1%	3.0%
1501-2500	4.1%	4.1%
2500+	39.6%	38.9%

Top-Ten Industries Targeted in Spear-Phishing Attacks

Source: Symantec :: JULY 2014



Data Breaches



At a Glance

- *The largest data breach reported in July resulted in the exposure of 900,000 identities.*
- *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

AUGUST 2013 — JULY 2014

256

Total Identities Exposed

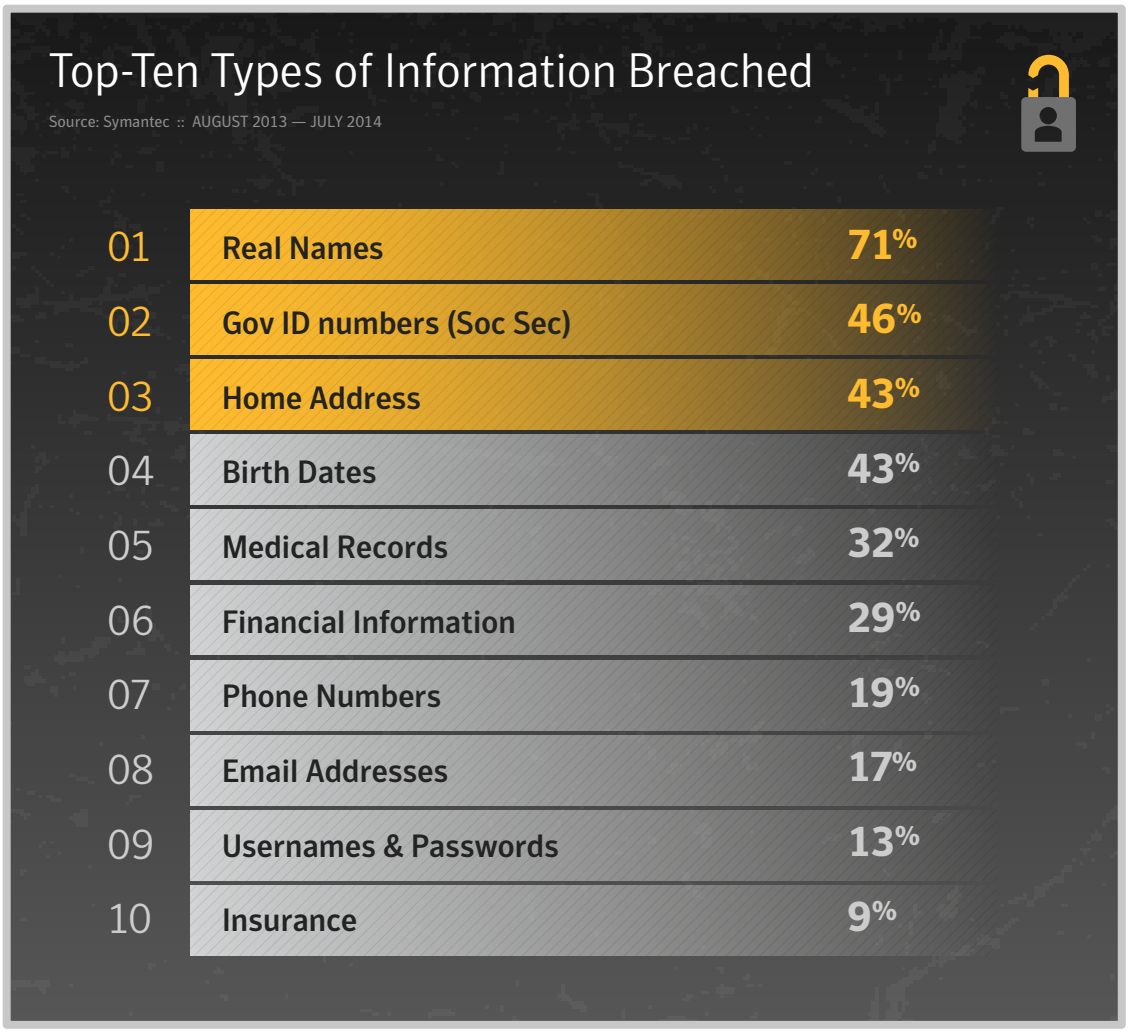
AUGUST 2013 — JULY 2014

567 Million

Top Causes of Data Breaches

Source: Symantec :: AUGUST 2013 — JULY 2014

		Number of Incidents
Hackers	49%	126
Accidentally Made Public	23%	58
Theft or Loss of Computer or Drive	20%	53
Insider Theft	7%	18
Fraud	.4%	1
TOTAL		256



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 :: JULY 2014

Rank	Name	July	June
1	W32.Sality.AE	4.8%	5.3%
2	W32.Ramnit!html	4.3%	5.1%
3	W32.Almanahe.B!inf	3.9%	3.7%
4	W32.Ramnit.B	2.9%	3.8%
5	W32.Downadup.B	2.8%	2.9%
6	W32.SillyFDC.BDP!lnk	2.1%	2.1%
7	Trojan.Webkit!html	2.0%	—
8	W32.Ramnit.B!inf	2.0%	2.6%
9	Trojan.Zbot	1.4%	1.4%
10	W32.Virut.CF	1.4%	1.6%

At a Glance

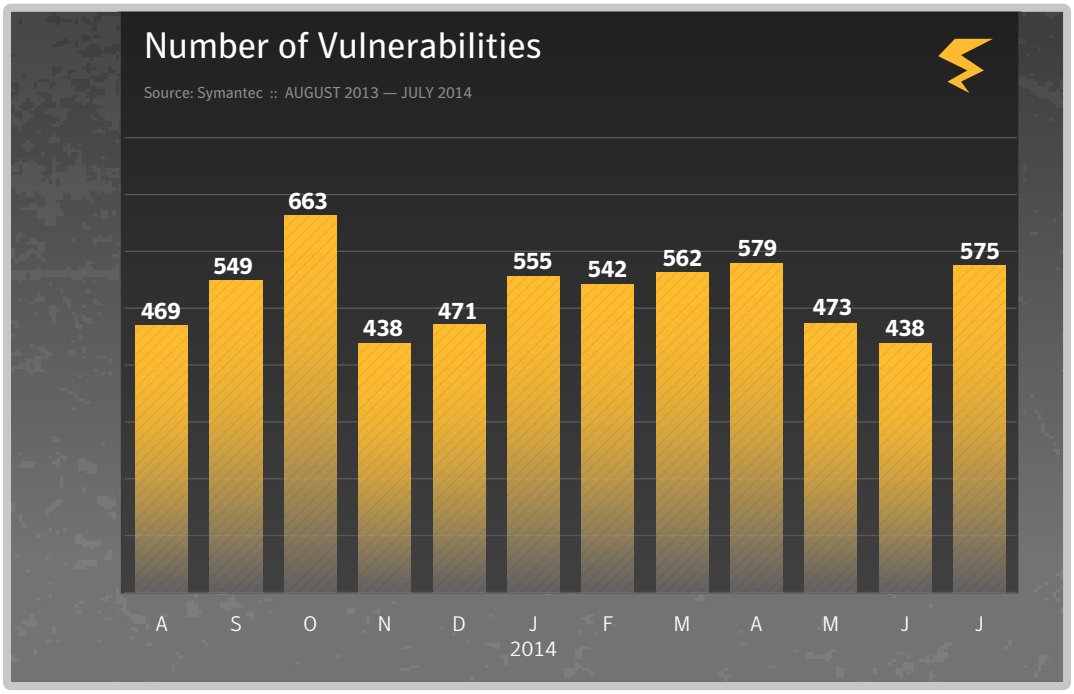
- *W32.Sality and W32.Ramnit variants continue to dominate the top-ten malware list.*
- *The most common OSX threat seen on OSX was OSX.RSPlug.A, making up 38 percent of all OSX malware found on OSX Endpoints.*

Top-Ten Mac OSX Malware Blocked on OSX Endpoints

Source: Symantec :: JULY 2014

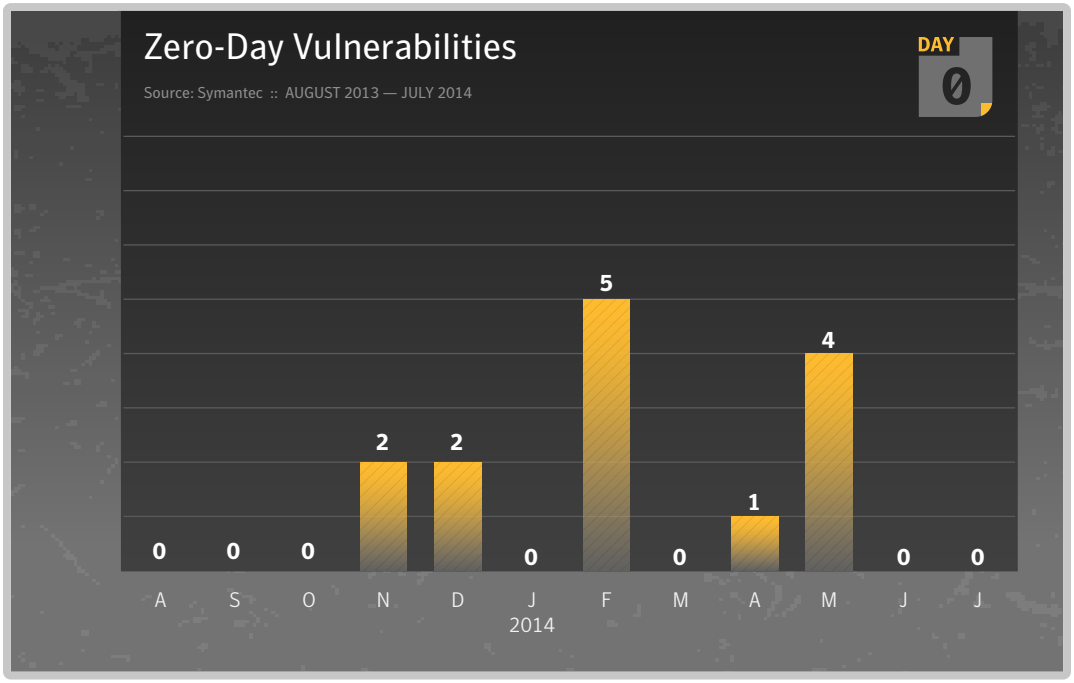
Rank	Malware Name	July	June
1	OSX.RSPlug.A	38.2%	24.1%
2	OSX.Stealbit.B	12.5%	25.7%
3	OSX.Flashback.K	8.8%	14.7%
4	OSX.Sabpab	5.8%	4.9%
5	OSX.Crisis	5.7%	—
6	OSX.Stealbit.A	2.7%	—
7	OSX.Keylogger	2.6%	2.5%
8	OSX.Flashback	2.5%	1.6%
9	OSX.Netweird	2.0%	—
10	OSX.FakeCodec	1.7%	—

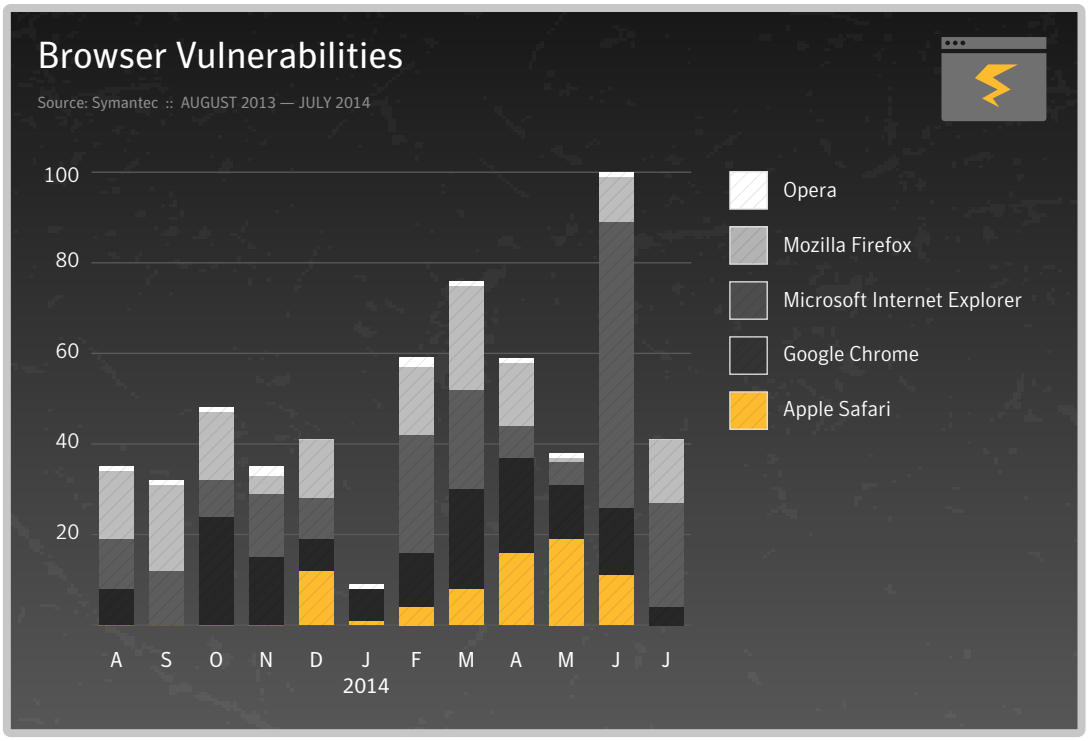
Vulnerabilities

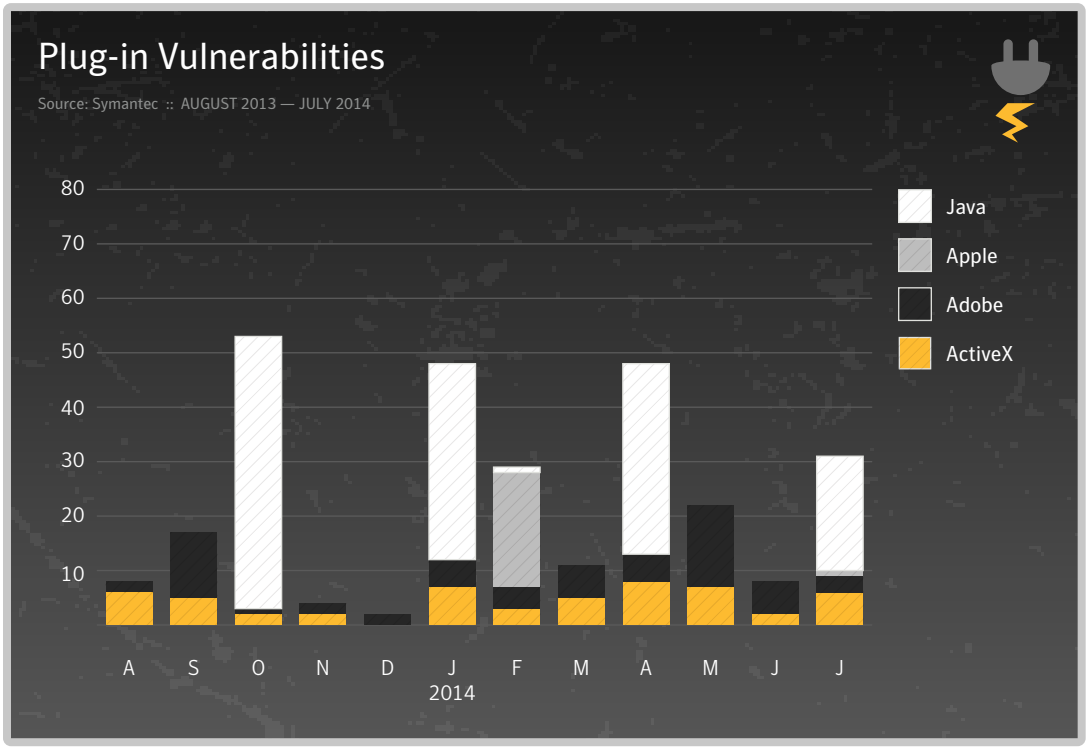


At a Glance

- *There were 575 vulnerabilities disclosed during the month of July.*
- *There were no zero-day vulnerabilities discovered in July.*
- *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.*

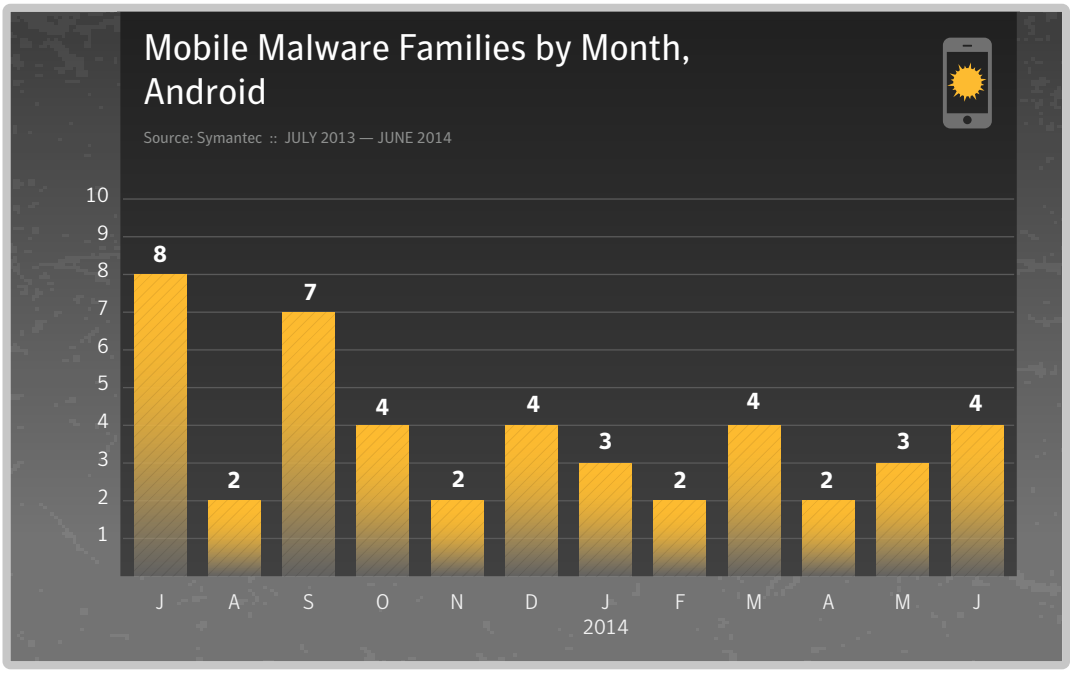



Browser Vulnerabilities
Source: Symantec :: AUGUST 2013 — JULY 2014
100
80
60
40
20
A S O N D J F M A M J J
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


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

SOCIAL MEDIA + MOBILE THREATS

Mobile

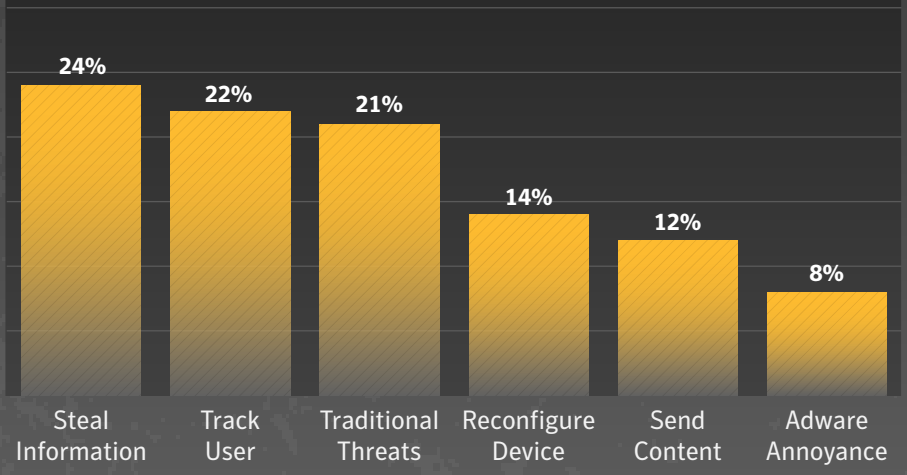


At a Glance

- *There were four Android malware families discovered in July.*
- *Of the threats discovered in the last 12 months, 24 percent steal information from the device and 22 percent track the device's user.*
- *In terms of social networking scams, 63 percent were fake offerings and 27 percent were manually shared scams.*

Mobile Threat Classifications

Source: Symantec :: AUGUST 2013 — JULY 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.

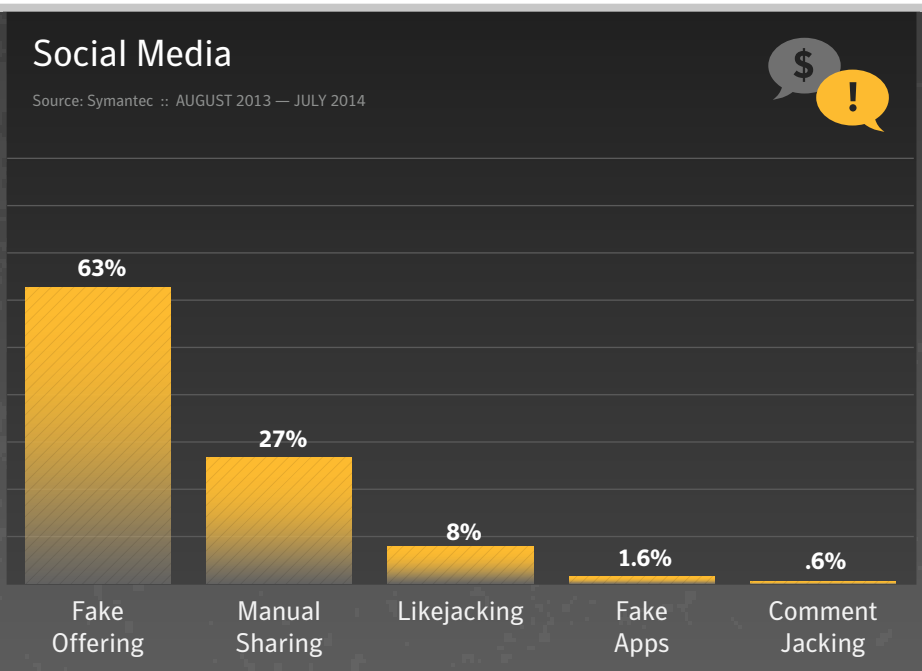
Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

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.

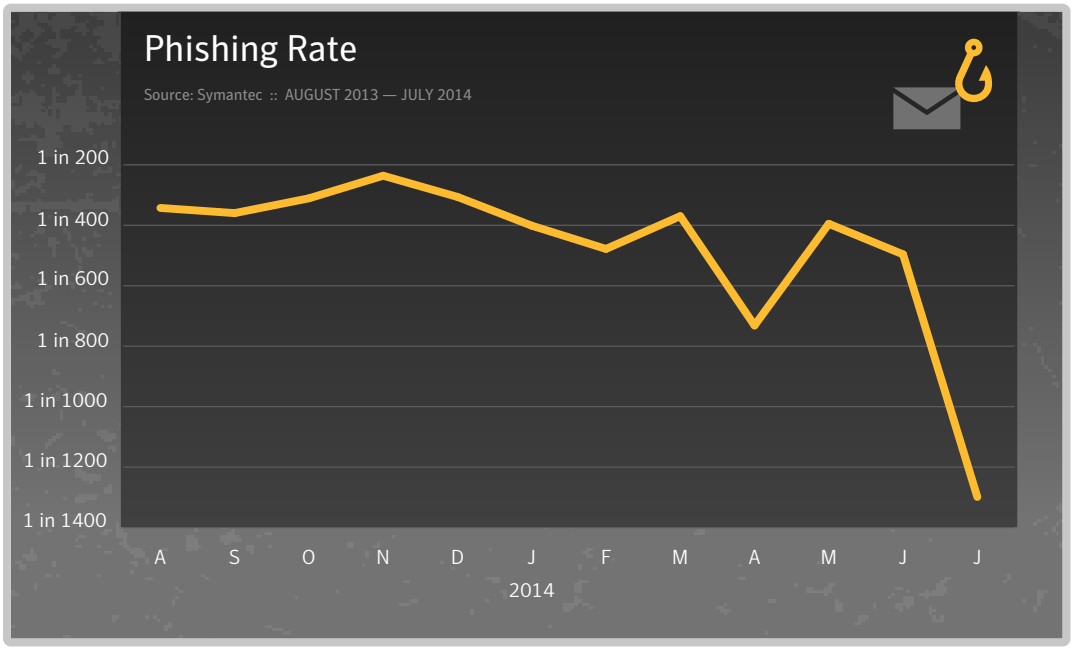
Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

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.

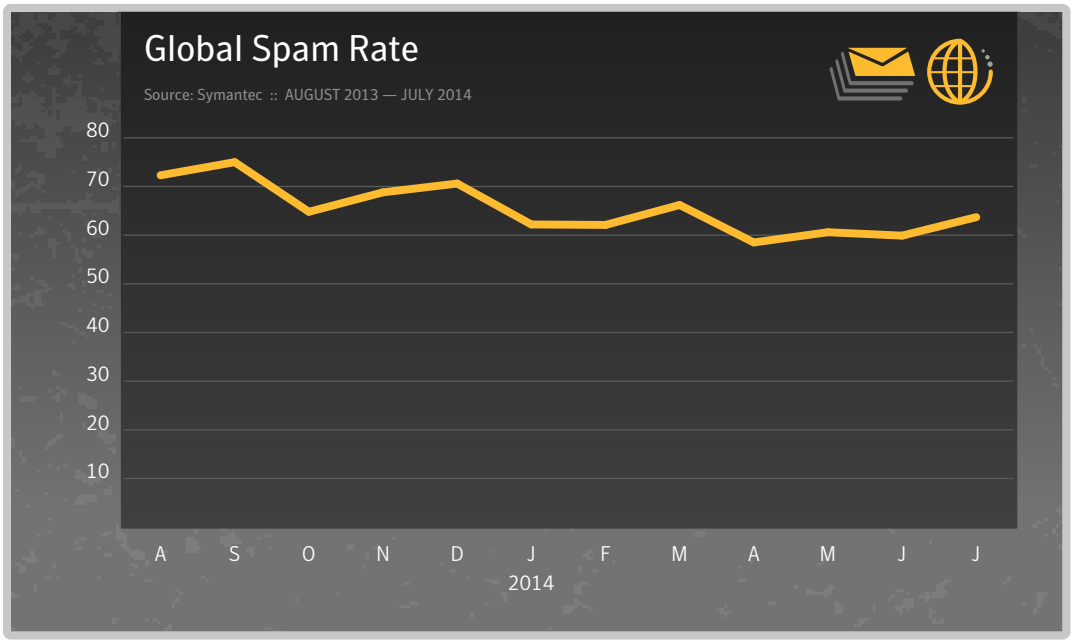
PHISHING, SPAM + EMAIL THREATS

Phishing and Spam

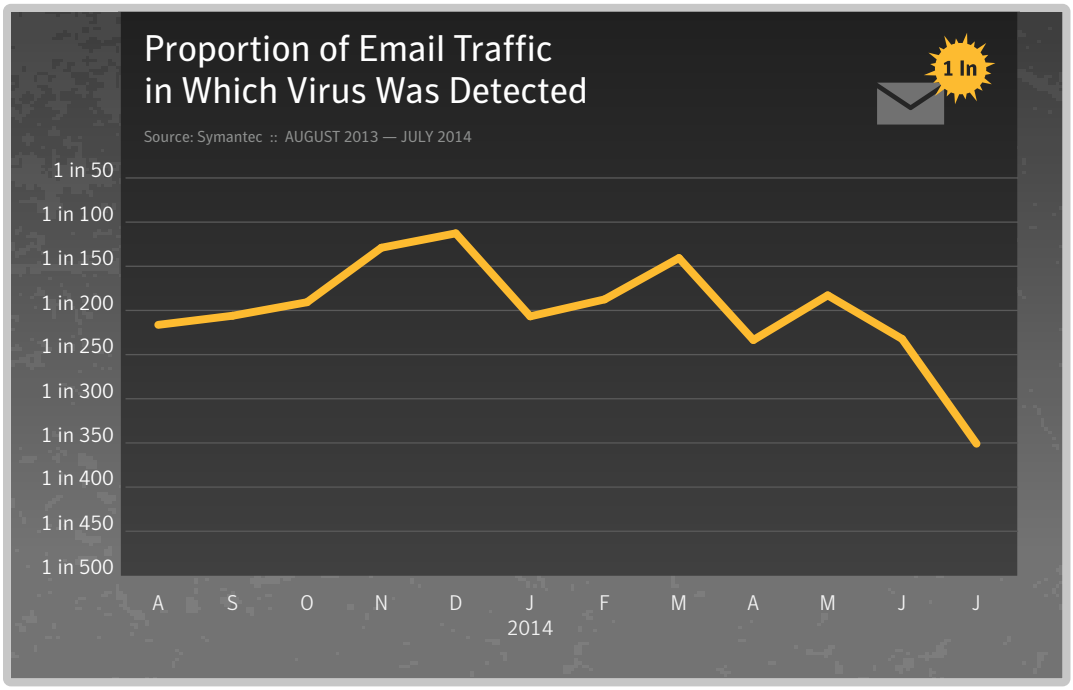


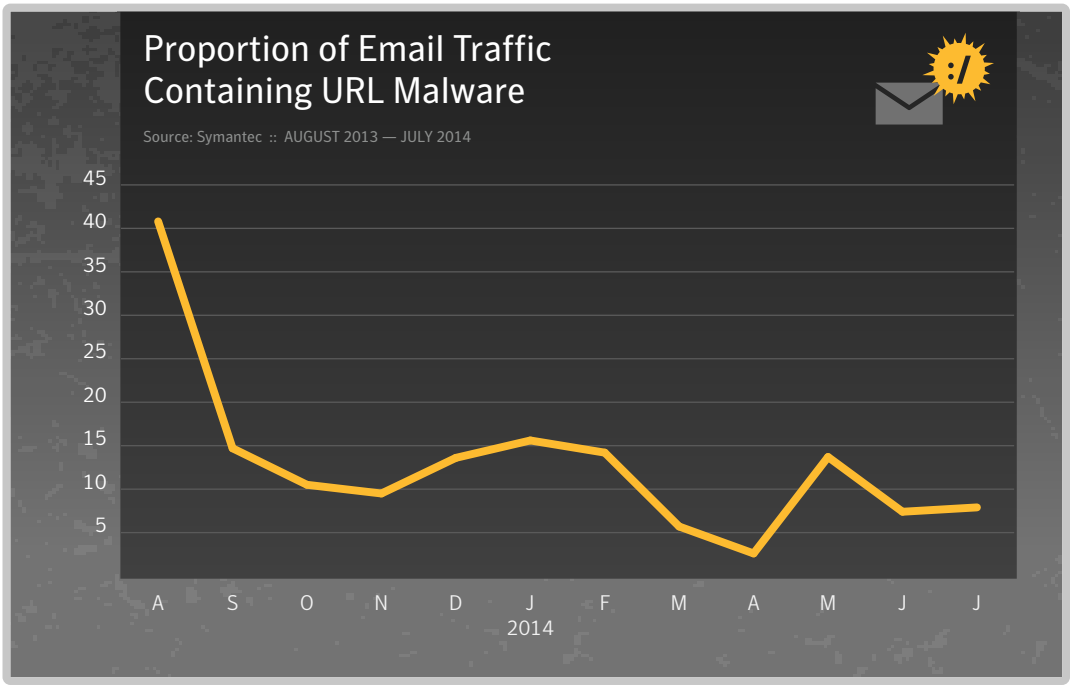
At a Glance

- *The phishing rate was down in July, at one in 1,299 emails, down from one in 496 emails in June.*
- *The global spam rate was 63.7 percent for the month of July.*
- *One out of every 351 emails contained a virus.*
- *Of the email traffic in the month of July, 7.9 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