Symantec

SYMANTEC INTELLIGENCE REPORT

MAY 2014

CONTENTS

Summary

Welcome to the May 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.

Welcome to the May Symantec Intelligence Report. After publishing our annual Internet Security Threat Report, we're back to take a look at the monthly trends in the threat landscape since the report was published.

Up until May, the year has been relatively quiet on the data breach front. This follows three consecutive months at the end of last year with data breaches that resulted in the exposure of over 100 million identities each month, leading us to call 2013 the year of the "mega-breach." May sees the return of another large data breach, this time exposing over 145 million identities in one breach.

In terms of targeted attacks, spear phishing attacks per day started out fairly high, where January saw 165 attacks in an average day. However this attack rate has slowly declined as the year has progressed, currently sitting at 54 attacks per day for the month of May.

Ransomware is another area of the threat landscape where we have seen modest declines so far this year. Back in November of 2013, Ransomware activity peaked, where Symantec was blocking 861,000 potential Ransomware infections in the month. These numbers remained relatively high in the first few months of 2014, but have declined significantly in April and May, currently sitting at only 17% of the peak activity seen last November.

In other news, May saw the disclosure of four zero-day vulnerabilities, there were 66 Android malware variants for every family, and phishing, spam, and email virus rates were all up in May after drops in April.

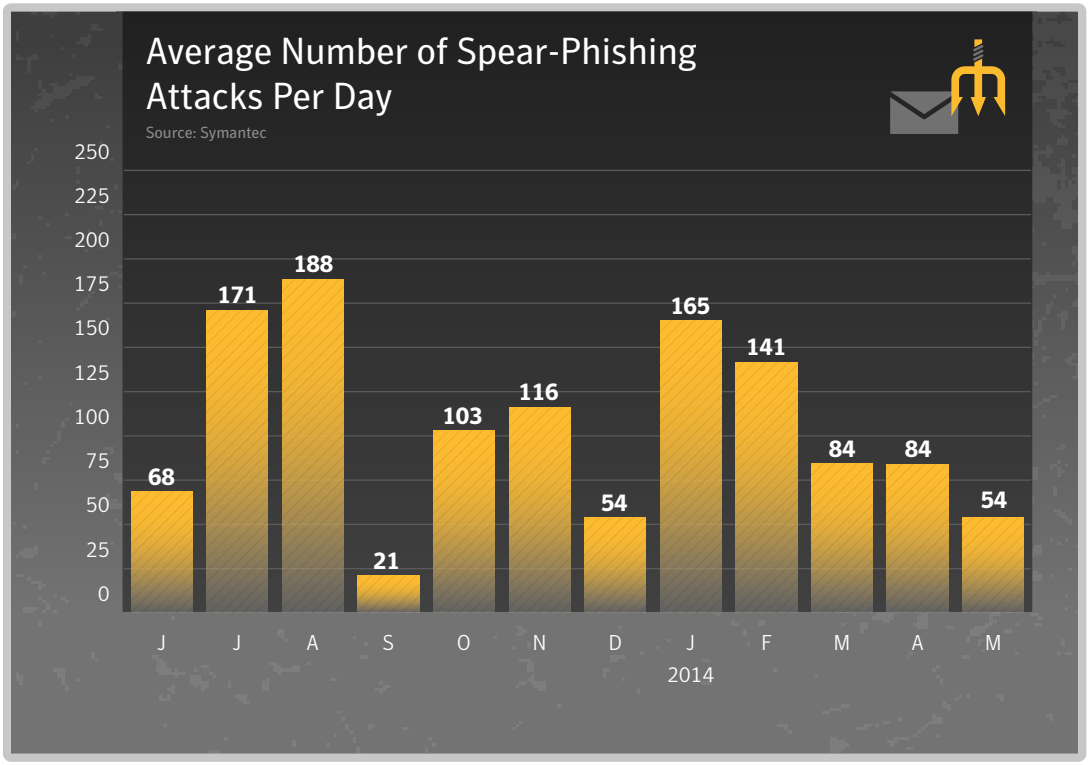
We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

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 again in May, down to 54 per day.*
- *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.*
- *Non-Traditional Services, such as Hospitality, Recreational, and Repair service, were the most commonly targeted industry, followed by Manufacturing.*

Attachments Used in Spear-Phishing Emails

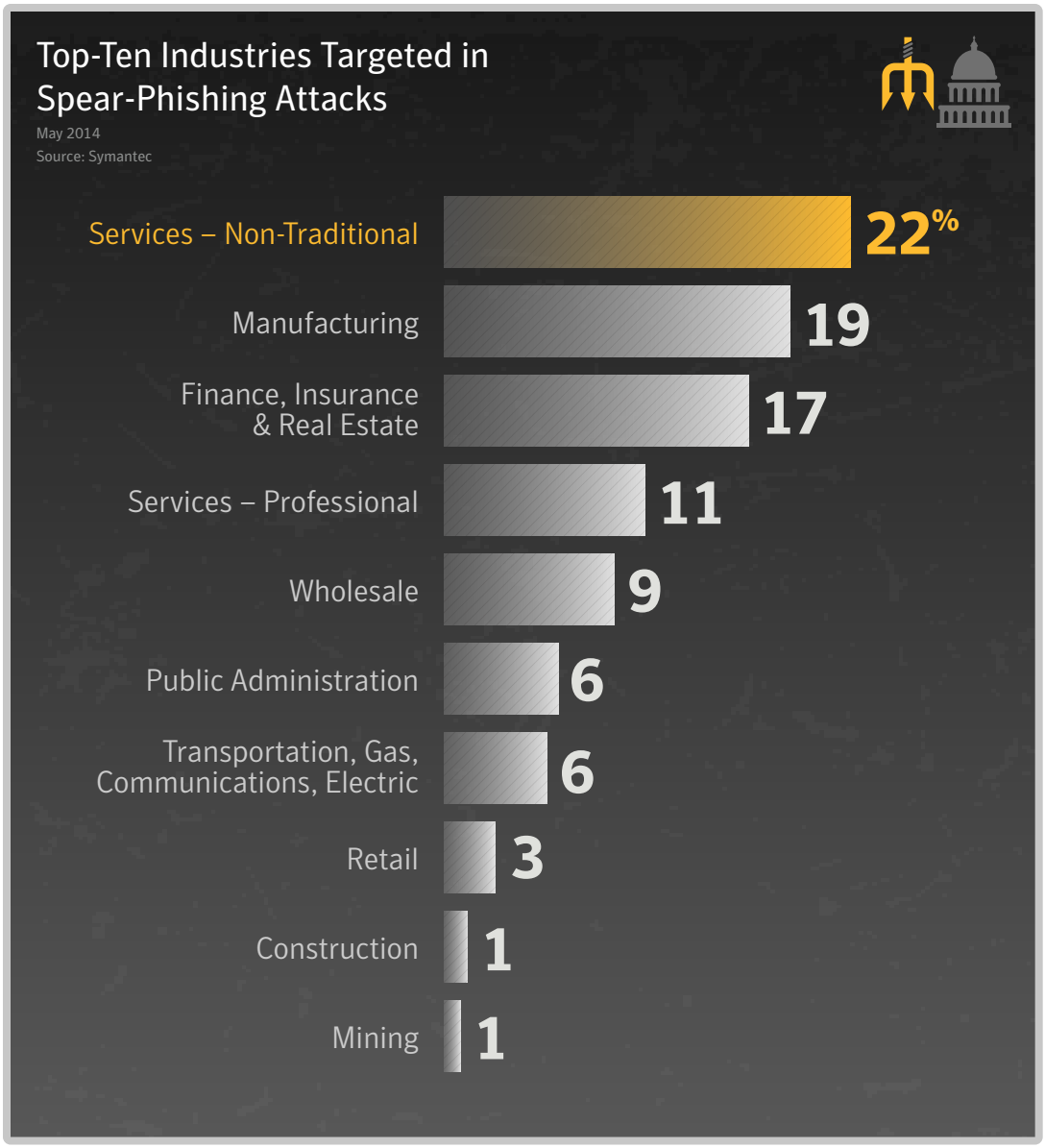
May 2014
Source: Symantec

Executable type	May	April
.doc	17.7%	17.9%
.exe	16.1%	16.5%
.au3	11.8%	11.7%
.jpg	7.0%	7.7%
.scr	6.4%	6.8%
.class	1.6%	1.8%
.pdf	1.3%	0.8%
.bin	1.2%	1.3%
.com	0.6%	0.6%
.dmp	0.6%	0.3%

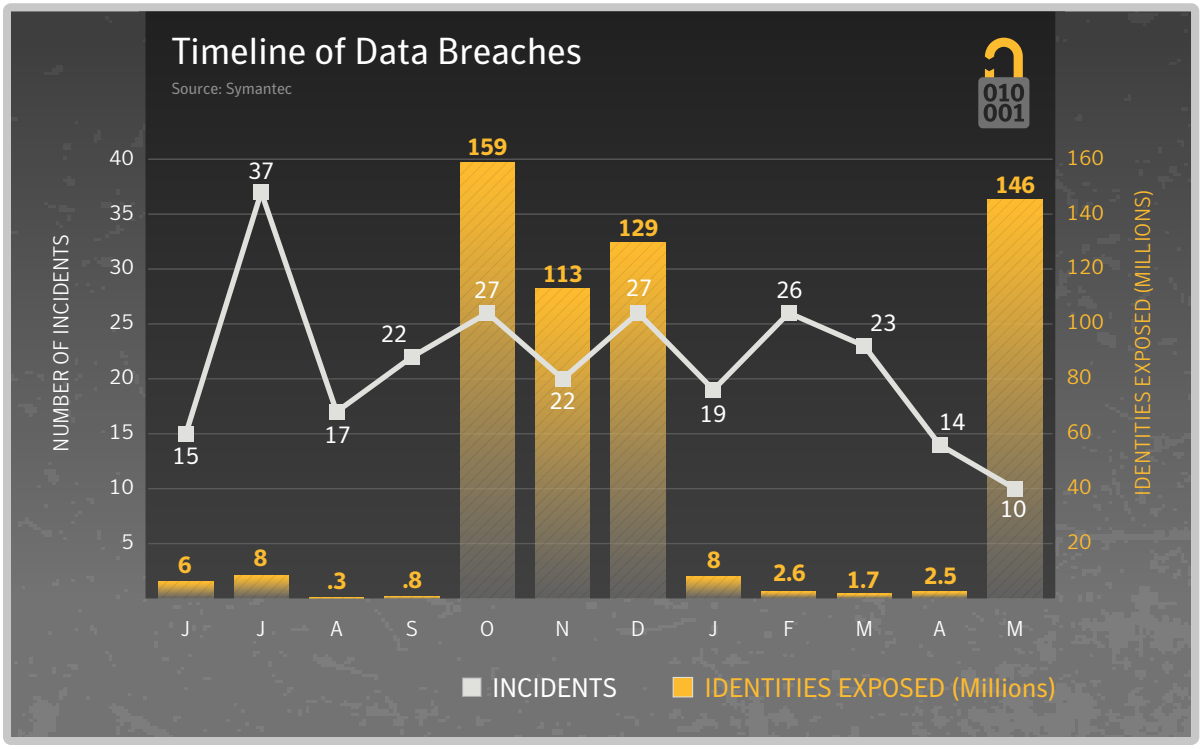
Spear-Phishing Attacks by Size of Targeted Organization

May 2014
Source: Symantec

Organization Size	May	April
1-250	37.0%	38.0%
251-500	8.6%	8.6%
501-1000	9.0%	9.0%
1001-1500	3.0%	2.8%
1501-2500	4.1%	4.1%
2500+	38.3%	37.5%


Top-Ten Industries Targeted in Spear-Phishing Attacks
May 2014
Source: Symantec
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

- *May saw the disclosure of a large data breach, resulting in as many as 145 million identities potentially exposed from the breach.*
- *The number of identities exposed each month had been relatively light for the first few months of 2014, following a series of massive data breaches in the last quarter of 2013.*
- *Hackers have been responsible for 48 percent of data breaches in the last 12 months.*
- *Real names, birth dates, and government ID numbers, such as Social Security numbers, were the top three types of data exposed in data breaches.*

Total Data Breaches

259

June 2013 – May 2014

Total Identities Exposed

577 Million

June 2013 – May 2014

Top Causes of Data Breaches

June 2013—May 2014
Source: Symantec

		Number of Incidents
Hackers	48%	124
Accidentally Made Public	24%	61
Theft or Loss of Computer or Drive	21%	54
Insider Theft	7%	17
Unknown	2%	2
Fraud	1%	1
TOTAL		259

Top-Ten Types of Information Breached

June 2013—May 2014
Source: Symantec

01	Real Names	75%
02	Home Address	46%
03	Government ID Numbers (Social Security)	45%
04	Birth Dates	43%
05	Medical Records	32%
06	Financial Information	27%
07	Phone Numbers	21%
08	Email Addresses	17%
09	User Names & Passwords	14%
10	Insurance	8%

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

May 2014

Source: Symantec

Rank	Name	Percentage
1	W32.Sality.AE	5.2%
2	W32.Ramnit!html	4.9%
3	W32.Almanahe.B!inf	3.8%
4	W32.Ramnit.B	3.6%
5	W32.Downadup.B	2.9%
6	W32.Ramnit.B!inf	2.6%
7	Trojan.Zbot	2.1%
8	W32.SillyFDC.BDP!lnk	1.9%
9	W32.Virut.CF	1.5%
10	W32.SillyFDC	1.2%

At a Glance

- *W32.Sality and W32. Ramnit variants continue to dominate the top-ten malware list.*
- *The most common threat on OSX was OSX.SMSSend, making up 28 of all malware found on OSX Endpoints.*
- *The United States continues to be the largest source of bot activity.*
- *Ransomware continues to decline in 2014, down to 17 percent of the levels seen at the malware's peak in November 2013.*

Malicious Activity by Source: Bots

May 2014

Source: Symantec

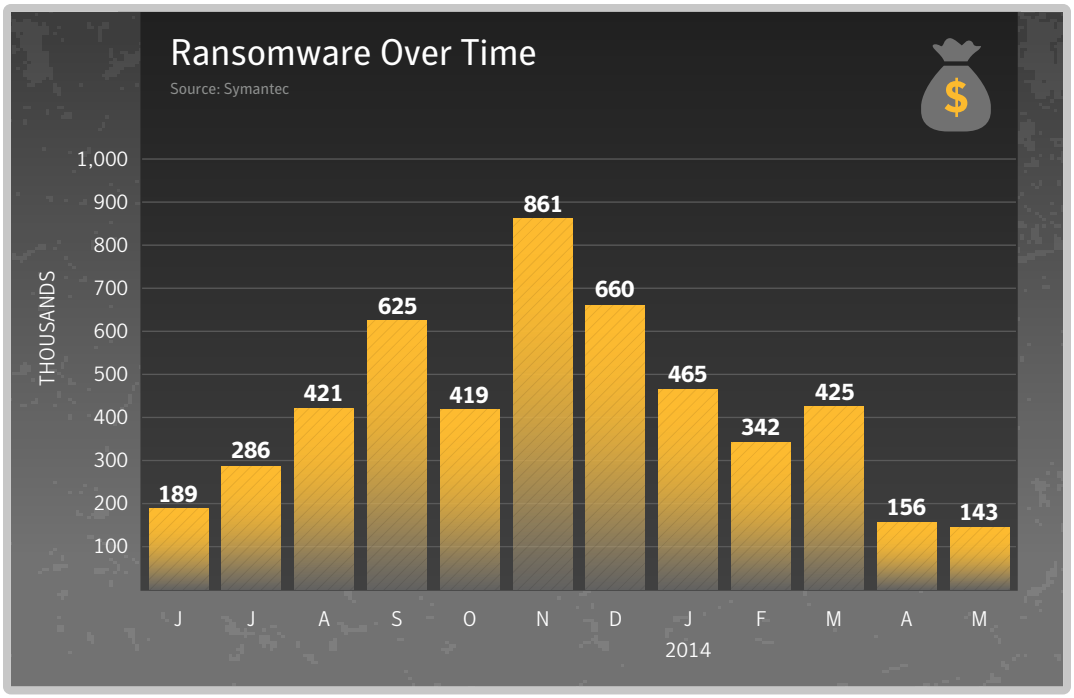
Rank	Country/Region	Percent
1	United States	22.5%
2	China	10.8%
3	Taiwan	8.1%
4	Hungary	5.8%
5	Italy	5.2%
6	Brazil	4.2%
7	Canada	3.1%
8	Japan	3.0%
9	France	2.9%
10	Germany	2.9%

Top-Ten Mac OSX Malware Blocked on OSX Endpoints

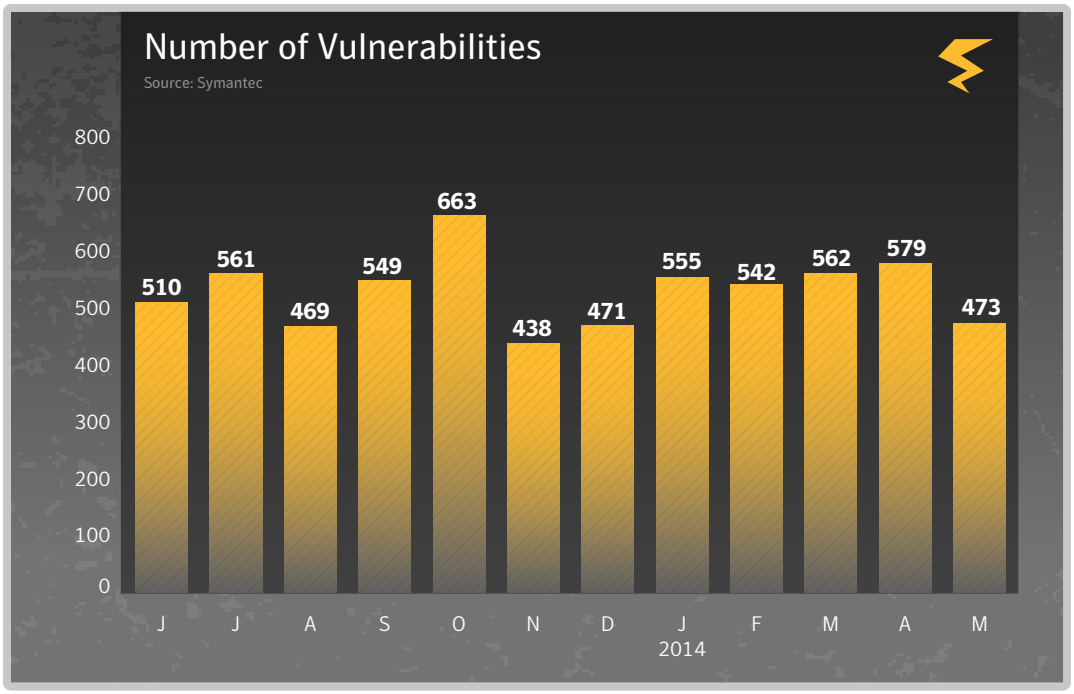
May 2014

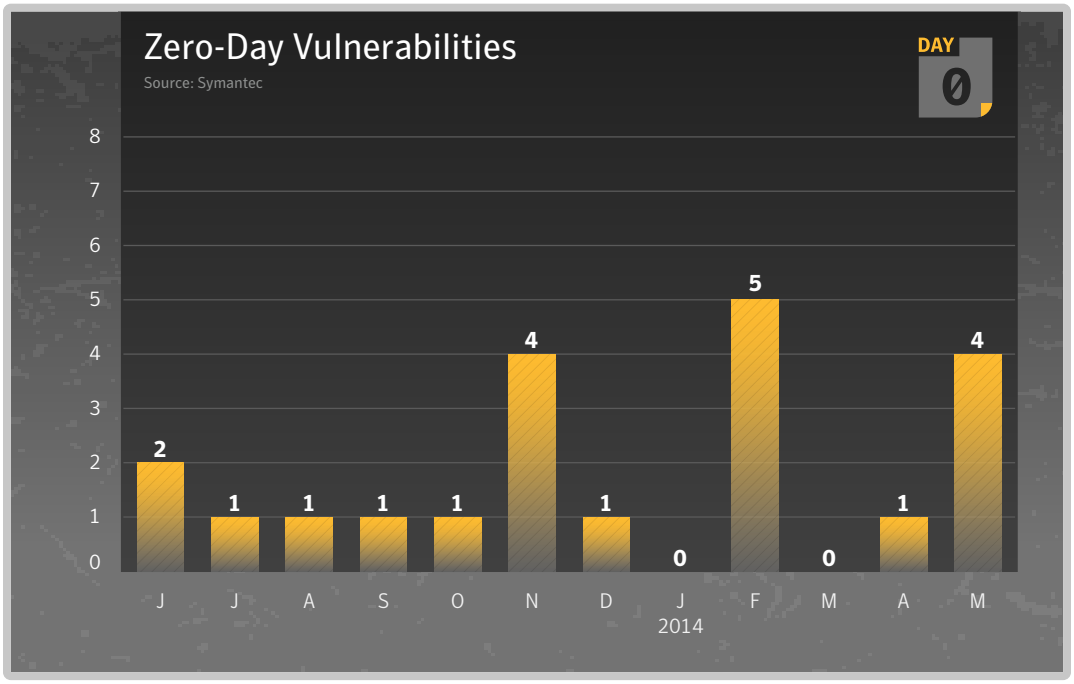
Source: Symantec

Malware Name	Percent of Mac Threats Detected on Macs
OSX.SMSSend	28.0%
OSX.RSPlug.A	23.0%
OSX.Flashback.K	13.5%
OSX.HelIRTS	7.4%
OSX.Sabpab	7.1%
OSX.Keylogger	5.2%
OSX.Klog.A	4.0%
OSX.Flashback	2.9%
OSX.Loosemaque	2.4%
OSX.Remoteaccess	2.4%


Ransomware Over Time
Source: Symantec
THOUSANDS
1,000
900
800
700
600
500
400
300
200
100
189
286
421
625
419
861
660
465
342
425
156
143
J
J
A
S
O
N
D
J
F
M
A
M
2014

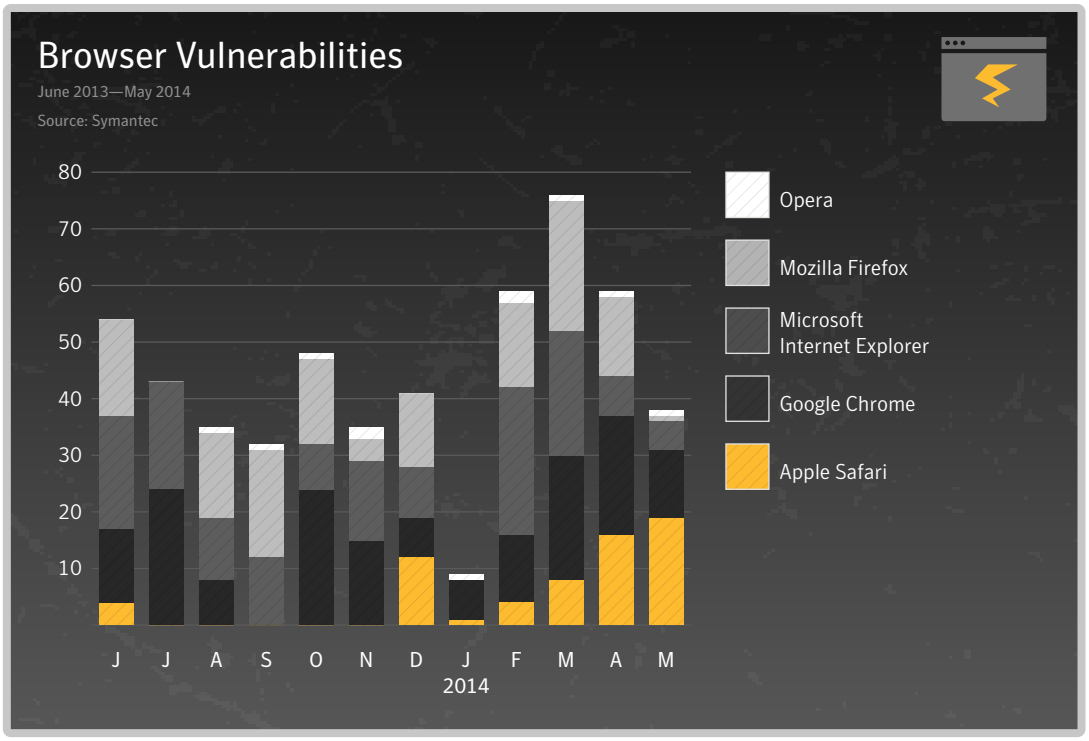
Vulnerabilities

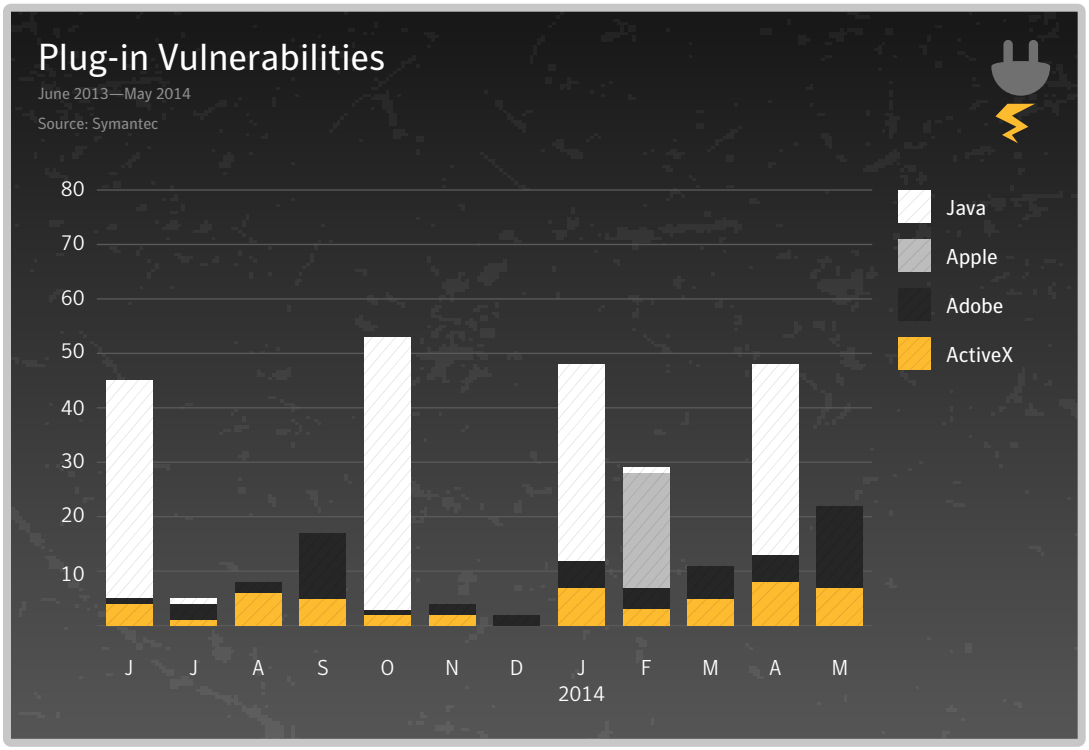




At a Glance

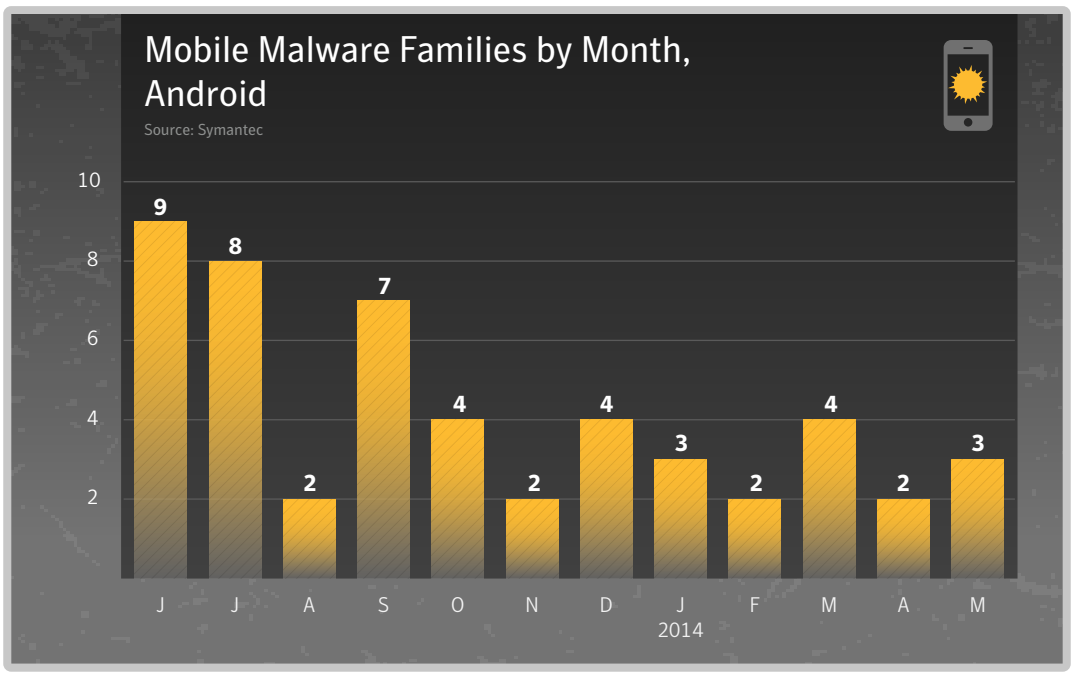
- *Vulnerabilities are at their lowest levels so far in 2014.*
- *There were four zero-day vulnerabilities discovered in May.*
- *Google Chrome has reported the most browser vulnerabilities in the last 12 months.*
- *Oracle's Java reported the most plug-in vulnerabilities over the same time period.*

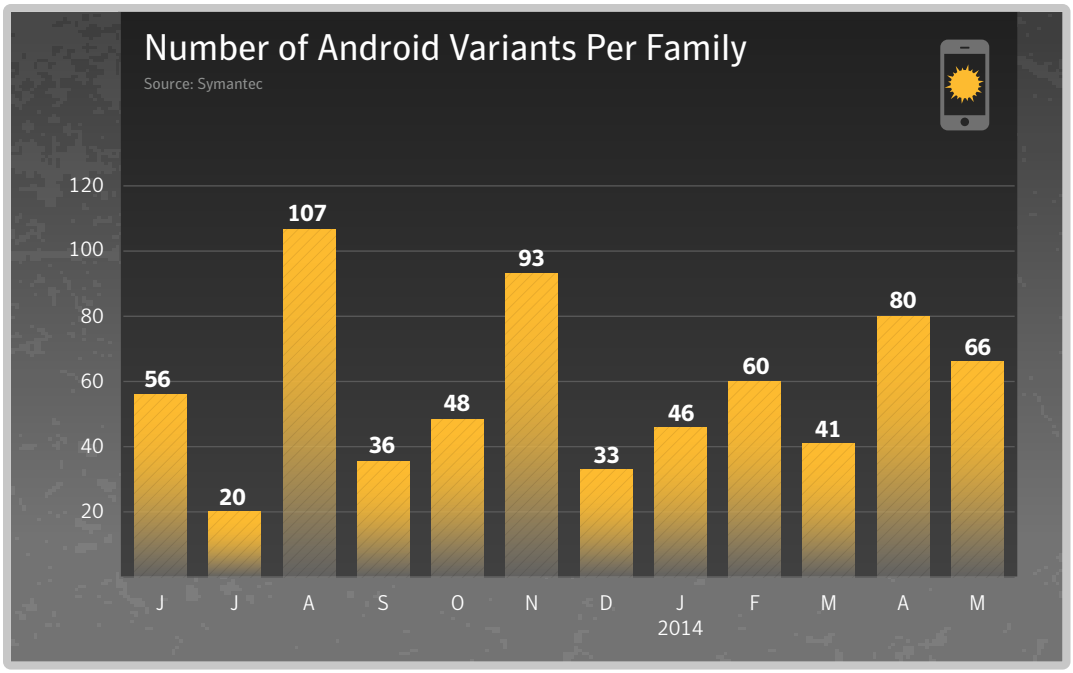

Browser Vulnerabilities
June 2013—May 2014
Source: Symantec
80
70
60
50
40
30
20
10
J J A S O N D J F M A M
2014
Opera
Mozilla Firefox
Microsoft Internet Explorer
Google Chrome
Apple Safari


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

SOCIAL MEDIA + MOBILE THREATS

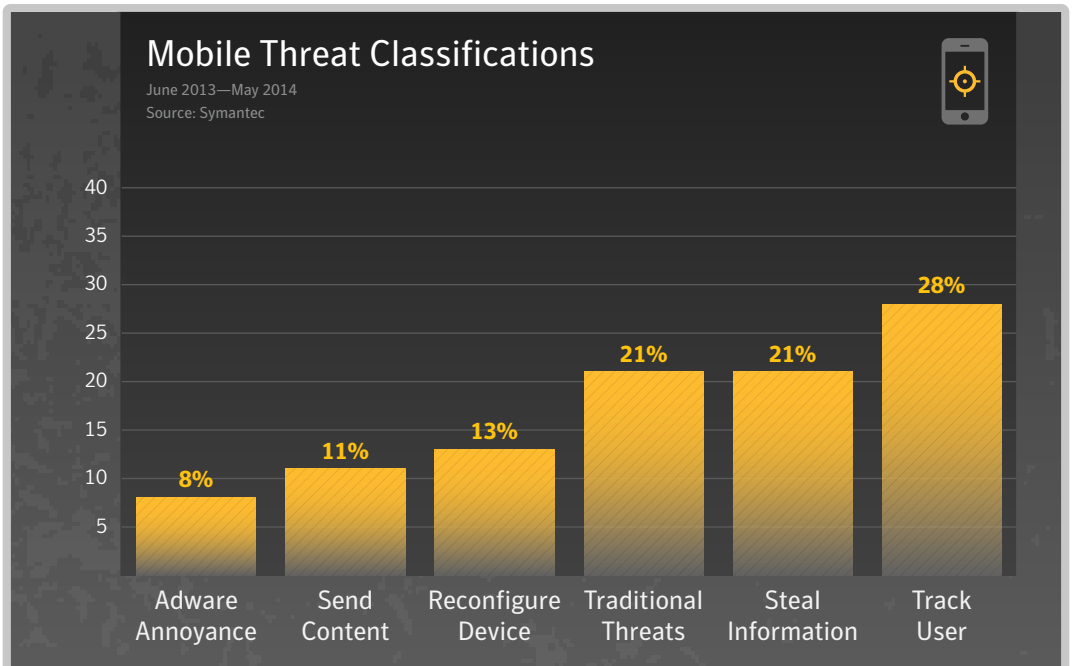
Mobile





At a Glance

- *There were three Android malware families discovered in the month of May.*
- *The number of variants per family was down slightly from it's 2014 peak in April.*
- *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.*



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.

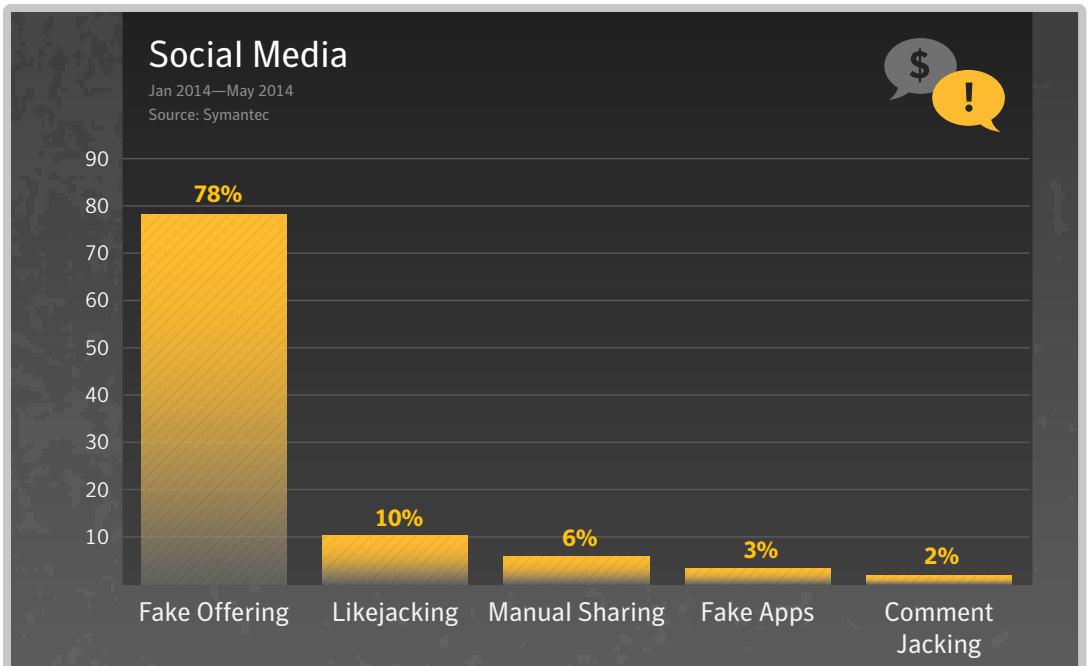
Traditional Threats Threats that carry out traditional malware functions, such as back doors and downloaders.

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.

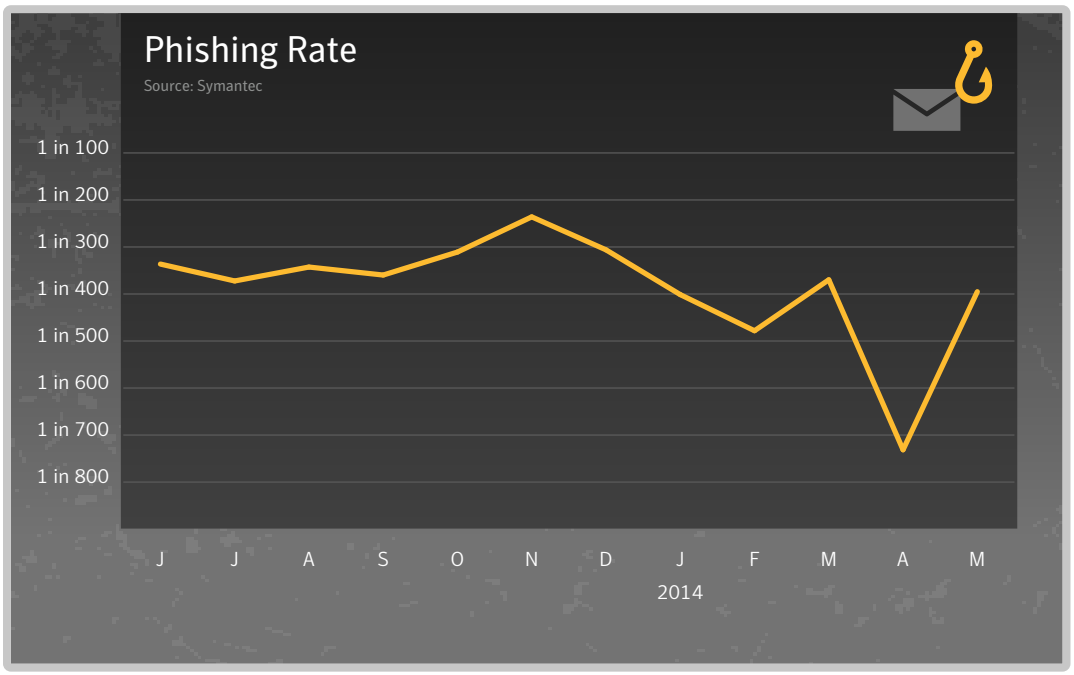
Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

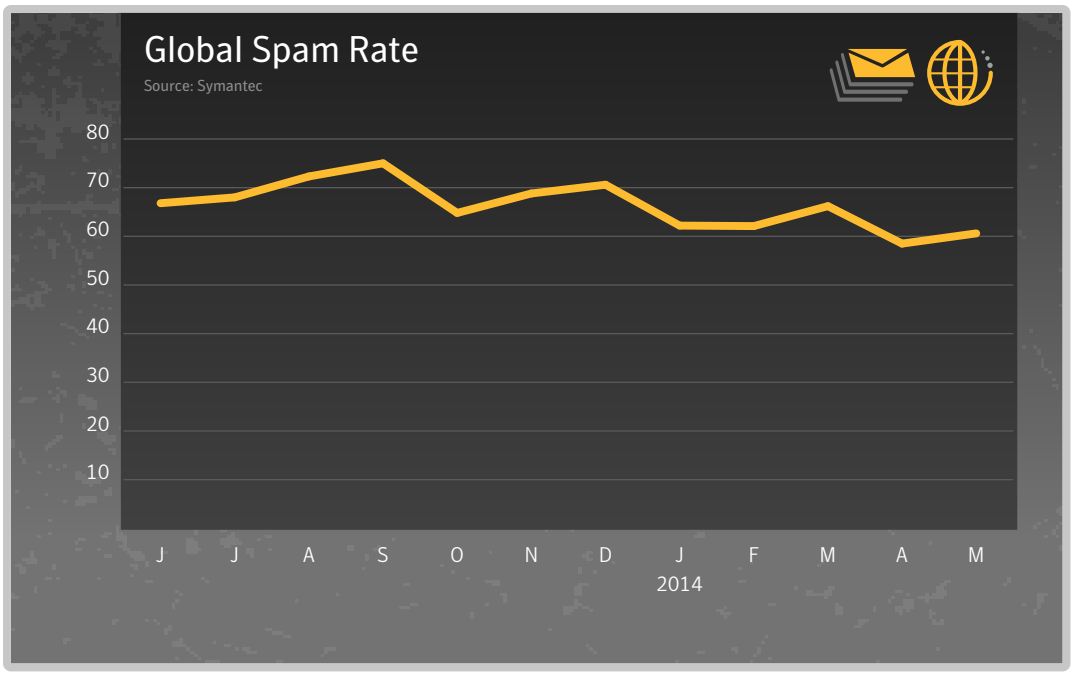
Comment Jacking Similar to likejacking, this type of scam relies on users clicking links that are added to comments by attackers. The links may lead to malware or survey scams.

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

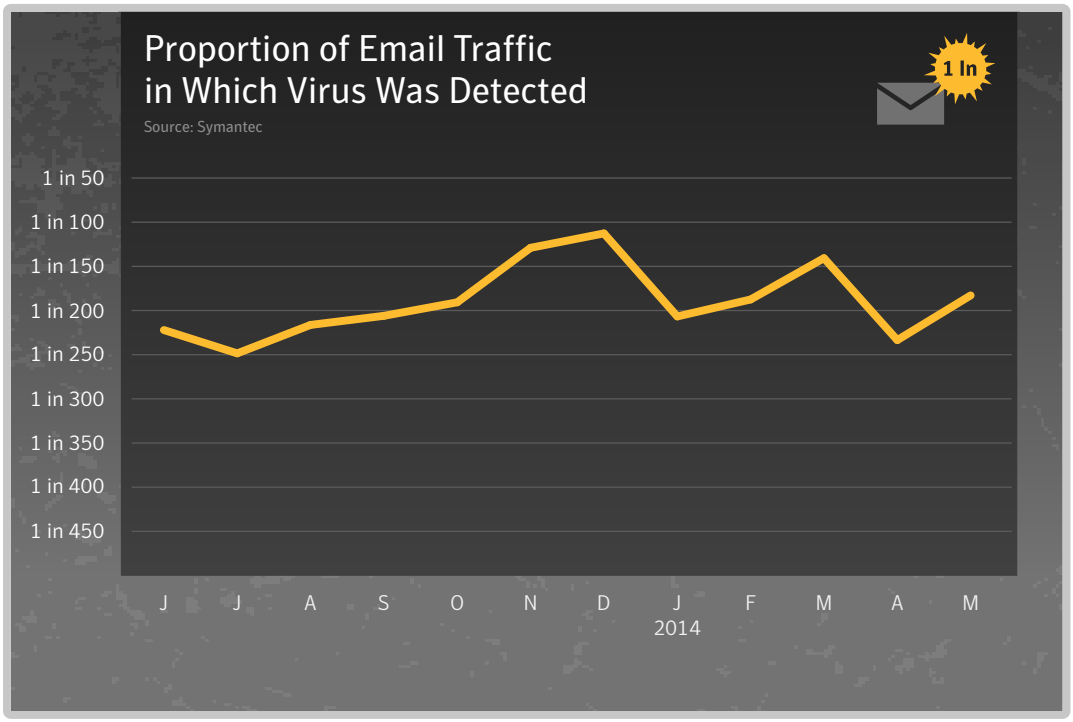


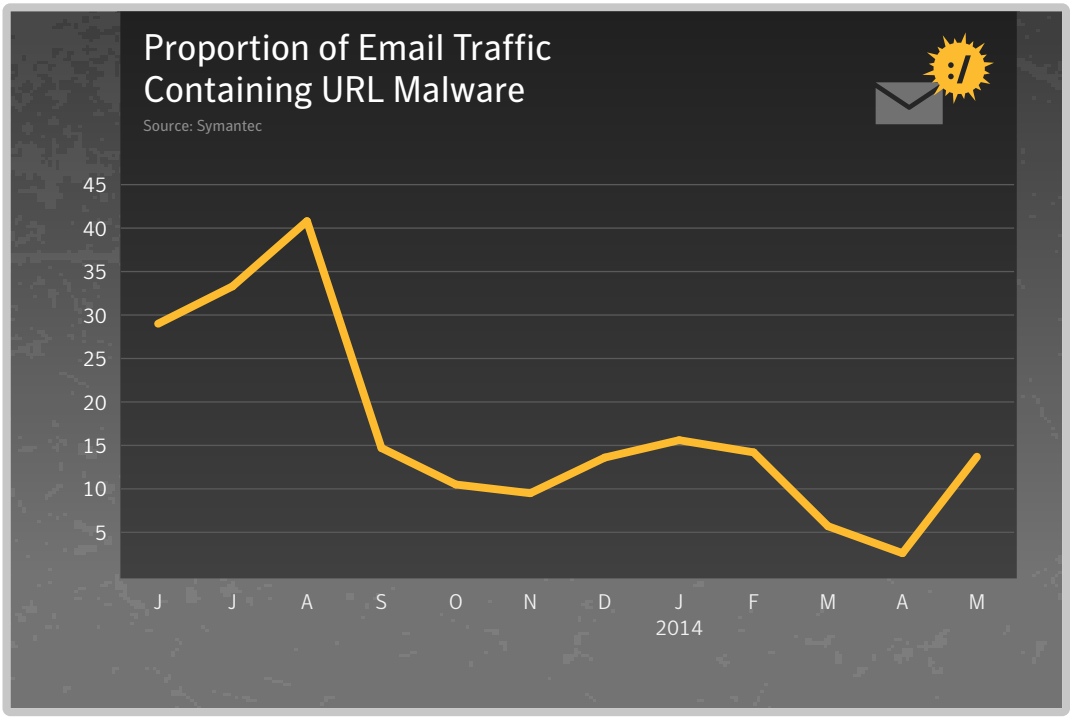


At a Glance

- *The phishing rate for May was one in 395 emails, up from one in 731 emails in April.*
- *The global spam rate was 60.6 percent for the month of May.*
- *One out of every 183 emails contained a virus.*
- *Of the email traffic in the month of May, 13.7 percent contain a malicious URL, up from a low of 2.6 percent in April.*

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