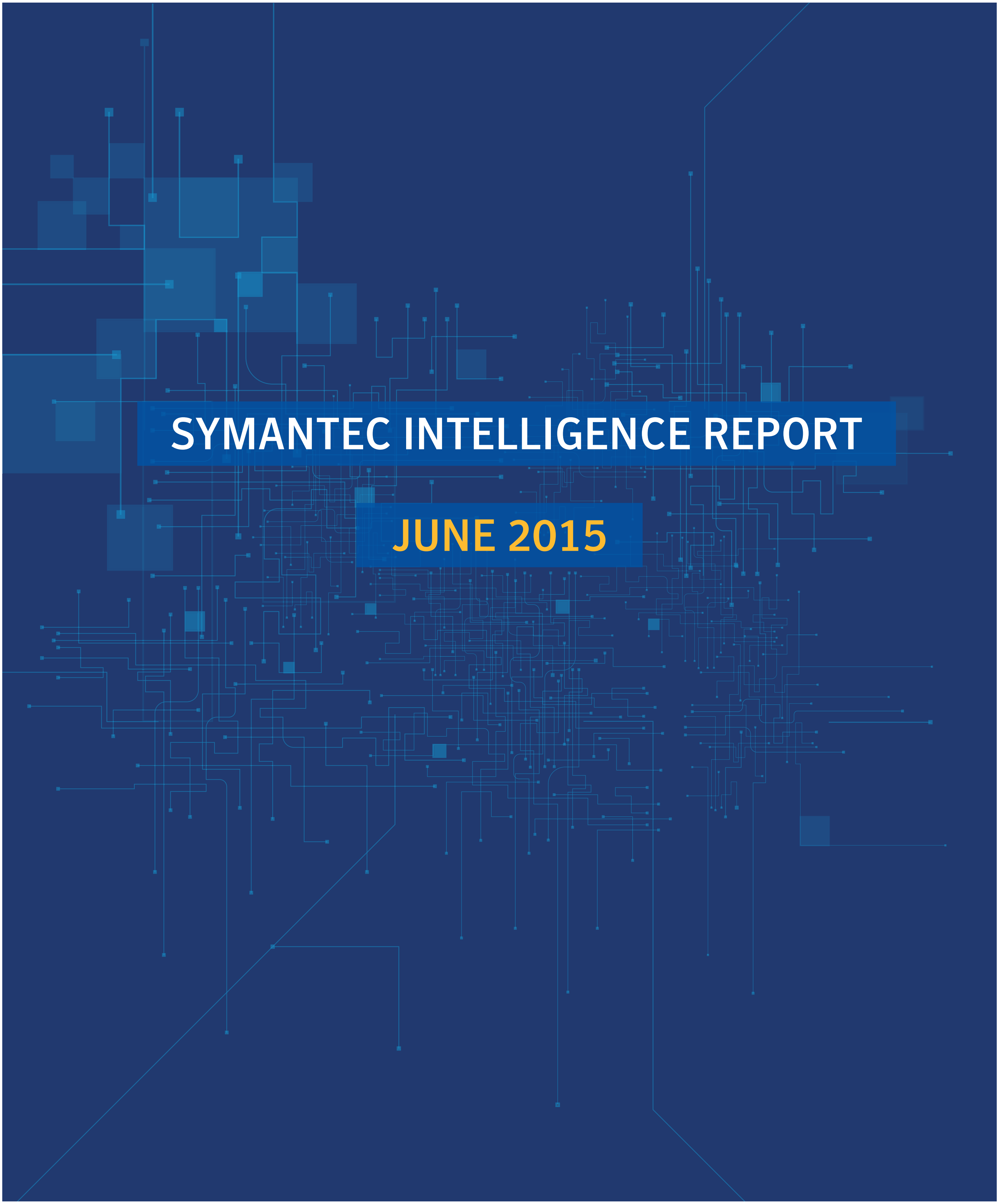
Symantec™



SYMANTEC INTELLIGENCE REPORT

JUNE 2015

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 57.6 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™ Intelligence, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

Summary

There is good news this month on the email-based front of the threat landscape. According to our metrics, the overall spam rate has dropped to 49.7 percent. This is the first time this rate has fallen below 50 percent of email for over a decade. The last time Symantec recorded a similar spam rate was clear back in September of 2003.

Phishing rates and email-based malware were also down this month. However, there were 57.6 million new malware variants created in June, up from 44.5 million pieces of malware created in May and 29.2 million in April. This increase in activity lends more evidence to the idea that, with the continued drops in email-based malicious activity, attackers are simply moving to other areas of the threat landscape.

Ransomware attacks are up in June, with over 477,000 detected during the month. While still below the levels seen at the end of 2014, this is the second month in a row ransomware attacks have increased since they reached a 12-month low in April. Crypto-ransomware is also up in June, reaching the highest levels seen since December 2014.

In other news, after a busy month in May targeted attacks against the Manufacturing industry leveled out in June, dropping from 41 percent to 22 percent. Manufacturing still comes out on top in terms of sectors subject to targeted attacks, but activity is now in line with what is being seen in the Finance, Insurance, & Real Estate sector and the Services – Professional sector, which come in at second and third place.

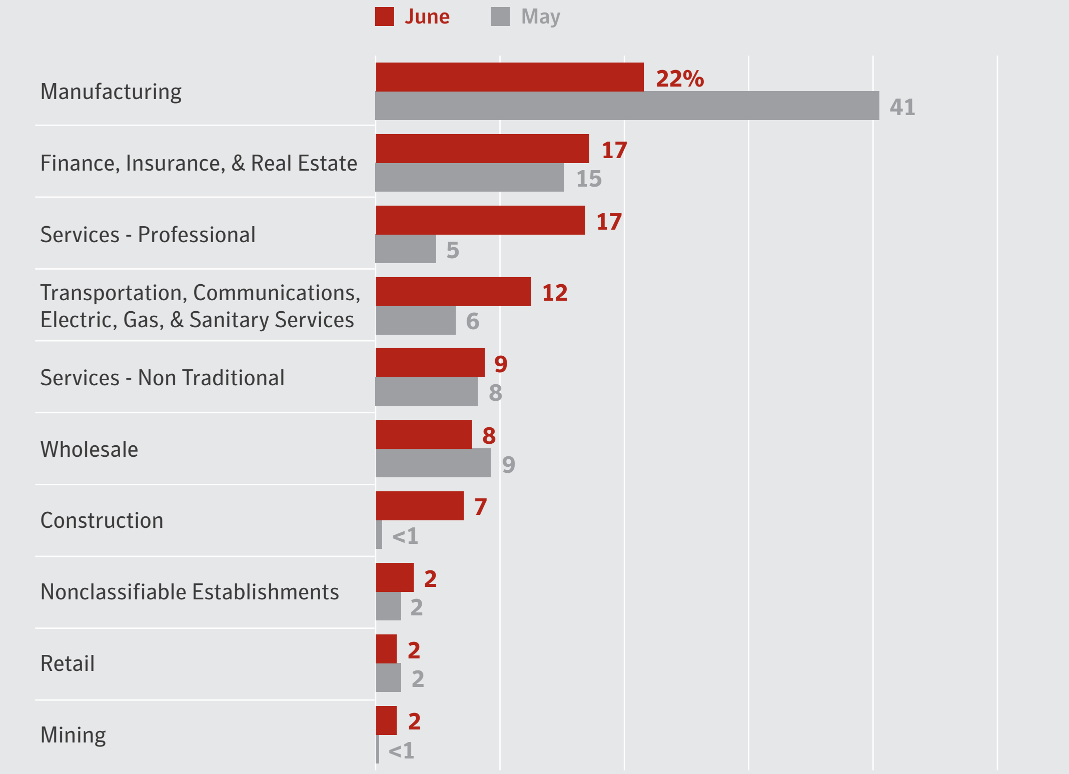
We hope that you enjoy this month’s report and feel free to contact us with any comments or feedback.

Ben Nahorney, Cyber Security Threat Analyst

symantec_intelligence@symantec.com

JUNE IN NUMBERS

Targeted Attacks & Phishing



Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec

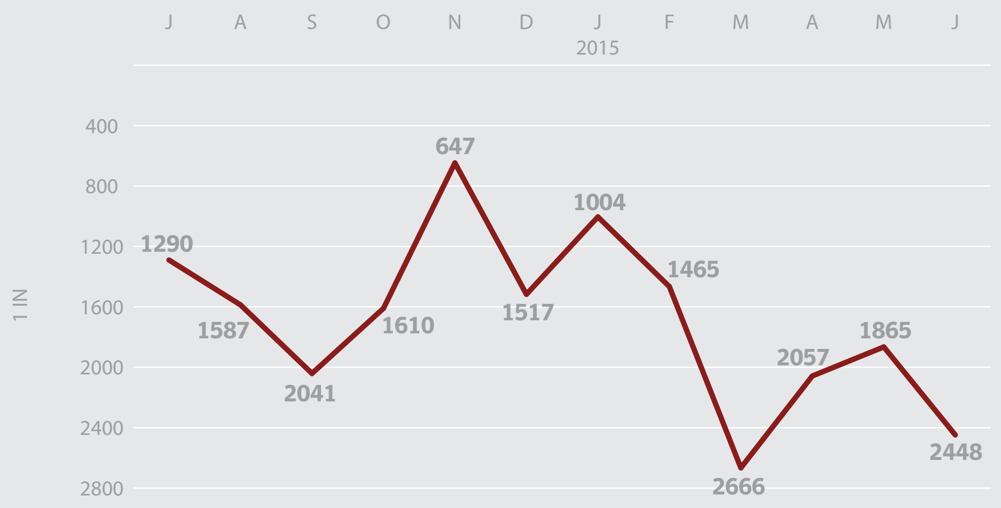
- *The Manufacturing sector was targeted with the greatest volume of spear-phishing attacks in June, as 22 percent were directed at manufacturing organizations.*

Company Size	June	May
1-250	38.1%	42.5%
251-500	15.2%	5.1%
501-1000	9.0%	6.6%
1001-1500	9.9%	2.7%
1501-2500	2.7%	3.9%
2501+	25.1%	39.2%

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec

- *Large enterprises were the target of 25.1 percent of spear-phishing attacks in June, down from 39.2 percent in May. In contrast, 38.1 percent of attacks were directed at organizations with less than 250 employees.*



Phishing Rate

Inverse Graph: Smaller Number = Greater Risk

Source: Symantec

- *The overall phishing rate has decreased slightly this month, where one in 2,448 emails was a phishing attempt.*

Industry	June	May
Agriculture, Forestry, & Fishing	1 in 1,469.9	1 in 856.0
Public Administration	1 in 2,367.3	1 in 1,289.3
Services - Professional	1 in 2,750.3	1 in 1,762.2
Nonclassifiable Establishments	1 in 2,753.1	1 in 1,834.9
Finance, Insurance & Real Estate	1 in 2,901.7	1 in 1,349.9
Construction	1 in 3,003.1	1 in 2,124.9
Mining	1 in 3,120.1	1 in 2,230.6
Services - Non Traditional	1 in 3,977.5	1 in 2,408.2
Wholesale	1 in 4,142.5	1 in 2,878.2
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 4,495.4	1 in 2,840.2

Proportion of Email Traffic Identified as Phishing by Industry Sector

Source: Symantec.cloud

- *The Agriculture, Forestry, & Fishing sector was once again the most targeted Industry overall for phishing attempts in June, where phishing comprised one in every 1,470 emails. This rate was higher than any other industry in either May or June.*

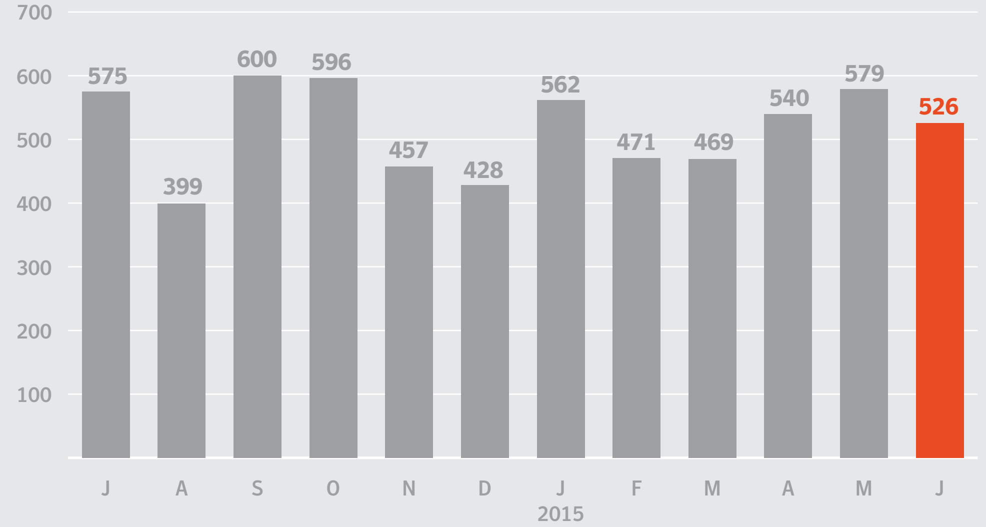
Company Size	June	May
1–250	1 in 1,552.5	1 in 1,473.9
251–500	1 in 2,553.7	1 in 1,629.5
501–1000	1 in 3,051.4	1 in 1,940.9
1001–1500	1 in 3,443.2	1 in 1,988.9
1501–2500	1 in 3,552.6	1 in 2,032.8
2501+	1 in 3,624.5	1 in 2,280.8

Proportion of Email Traffic Identified as Phishing by Organization Size

Source: Symantec.cloud

- *Small companies with less than 250 employees were again the most targeted organization size in June.*

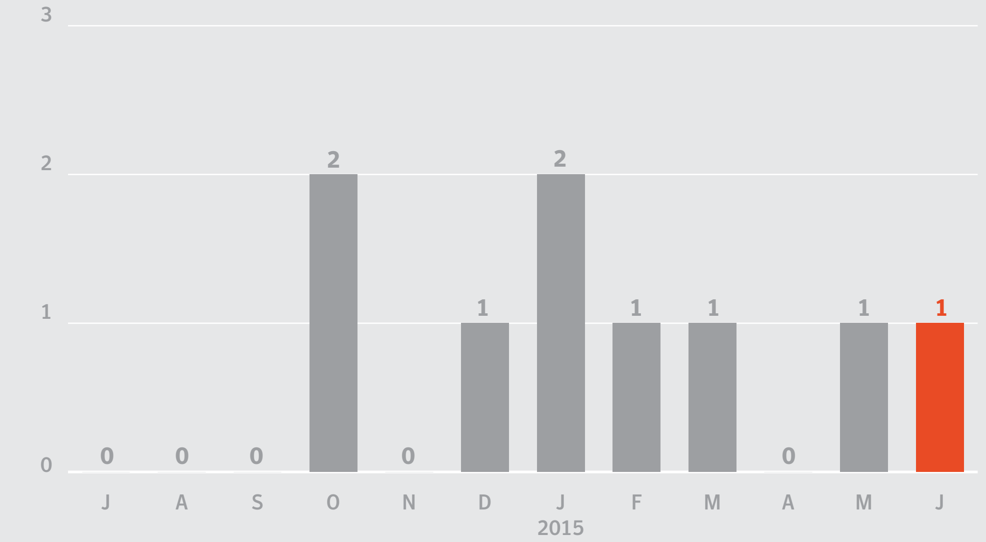
Vulnerabilities



Total Number of Vulnerabilities

Source: Symantec

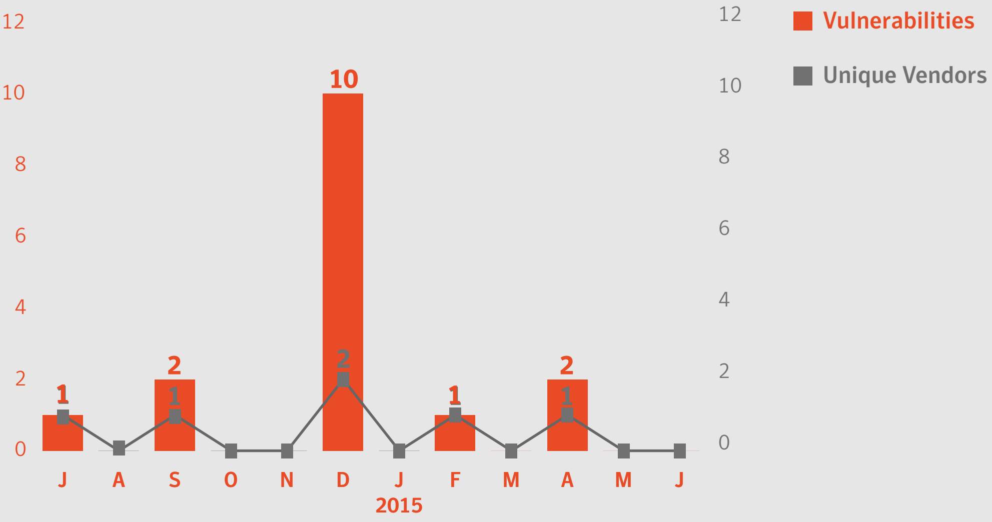
- *The number of vulnerabilities declined in June, down from 579 in May to 526 vulnerabilities reported during the month.*



Zero-Day Vulnerabilities

Source: Symantec

- *There was a one zero-day vulnerability discovered in May, the Adobe Flash Player CVE-2015-3113 Unspecified Heap Buffer Overflow Vulnerability.*



Vulnerabilities Disclosed in Industrial Control Systems

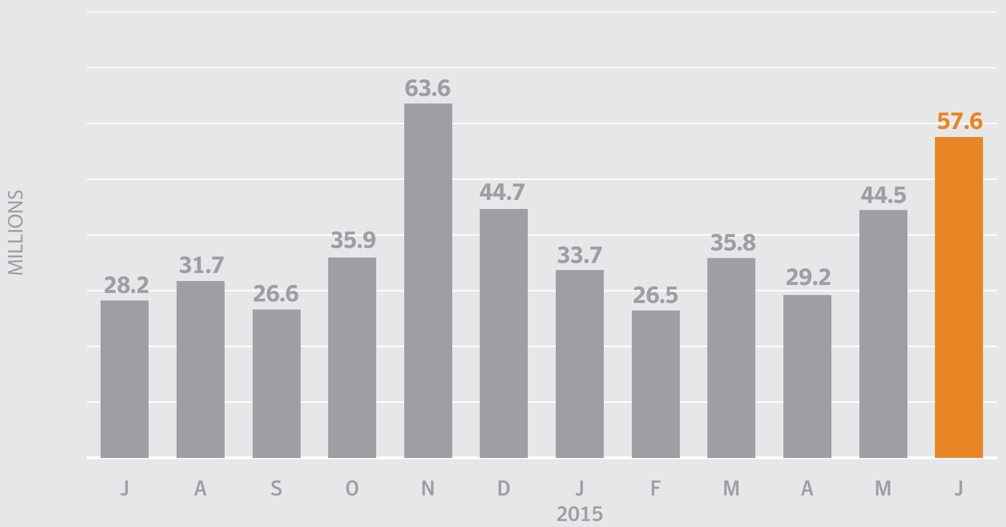
Source: Symantec

- *While two vulnerabilities in industrial control systems were reported by one vendor in April, none were reported in May or June.*

Methodology

In some cases the details of a vulnerability are not publicly disclosed during the same month that it was initially discovered. In these cases, our vulnerability metics are updated to reflect the time that the vulnerability was discovered, as opposed to the month it was disclosed. This can cause fluctuations in the numbers reported for previous months when a new report is released.

Malware



New Malware Variants

Source: Symantec

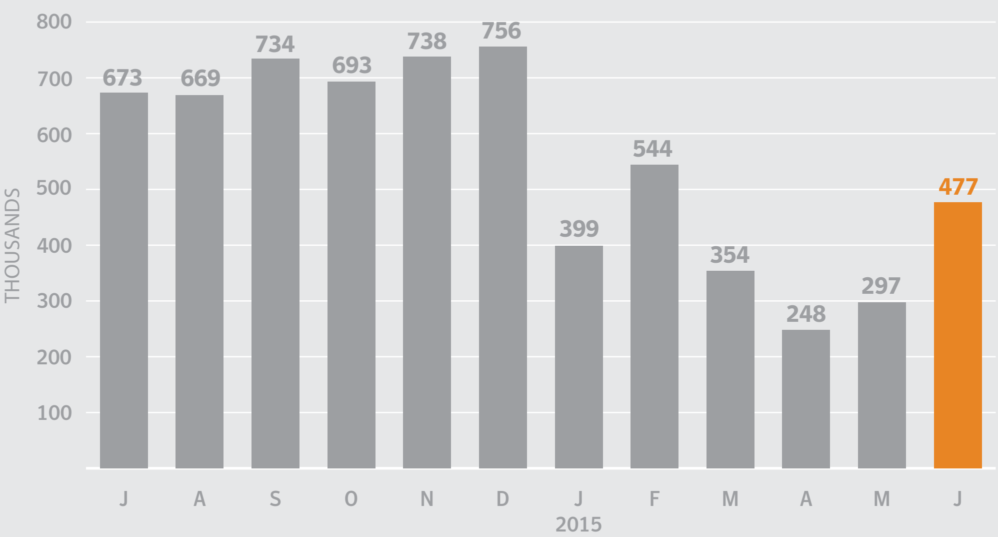
- *There were more than 57.6 million new pieces of malware created in June, up from 44.5 million created in May.*

Rank	Malware Name	June Percentage	Malware Name	May Percentage
1	OSX.RSPlug.A	29.5%	OSX.RSPlug.A	23.9%
2	OSX.Keylogger	11.6%	OSX.Keylogger	14.0%
3	OSX.Klog.A	8.9%	OSX.Wirelurker	9.0%
4	OSX.Luaddit	7.8%	OSX.Luaddit	8.3%
5	OSX.Wirelurker	7.1%	OSX.Klog.A	8.0%
6	OSX.Flashback.K	5.4%	OSX.Flashback.K	6.4%
7	OSX.Stealbit.B	4.3%	OSX.Netweird	3.9%
8	OSX.Freezer	3.2%	OSX.Sabpab	3.8%
9	OSX.Netweird	2.9%	OSX.Stealbit.B	3.6%
10	OSX.Okaz	2.5%	OSX.Flashback	3.0%

Top 10 Mac OS X Malware Blocked on OS X Endpoints

Source: Symantec

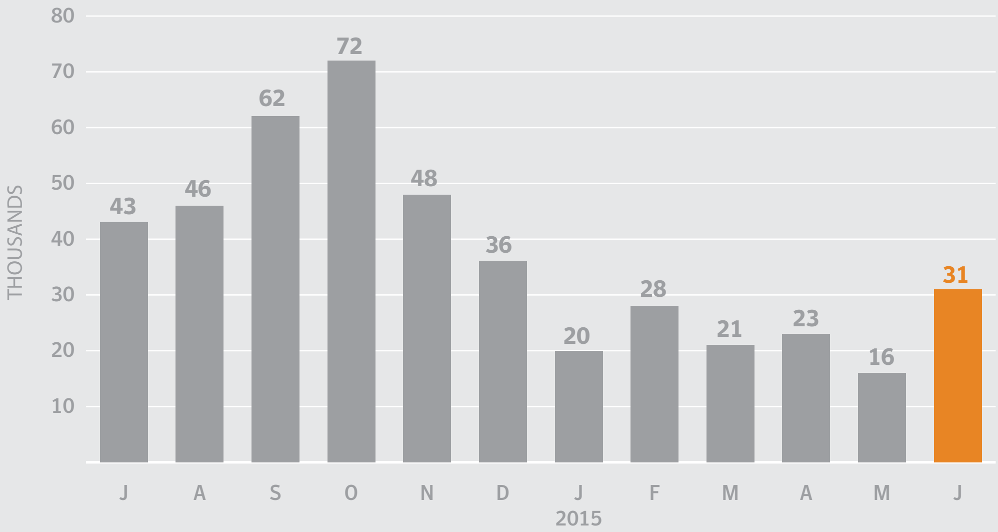
- *OSX.RSPlug.A continues to be the most commonly seen OS X threat seen on OS X endpoints in June, up 5.6 percentage points from May.*



Ransomware Over Time

Source: Symantec

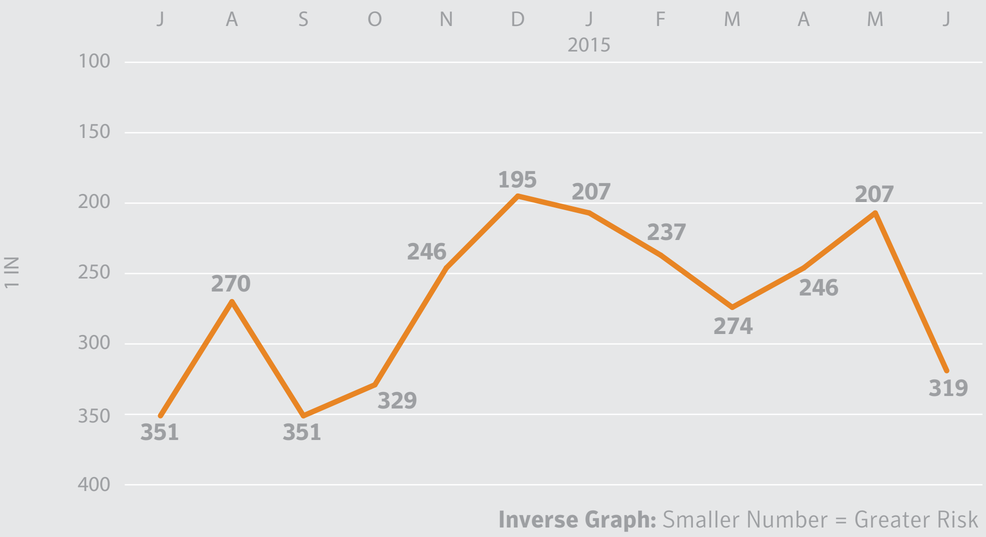
- *Ransomware attacks were up in June for the second month in a row, where over 477 thousand attacks were detected.*



Crypto-Ransomware Over Time

Source: Symantec

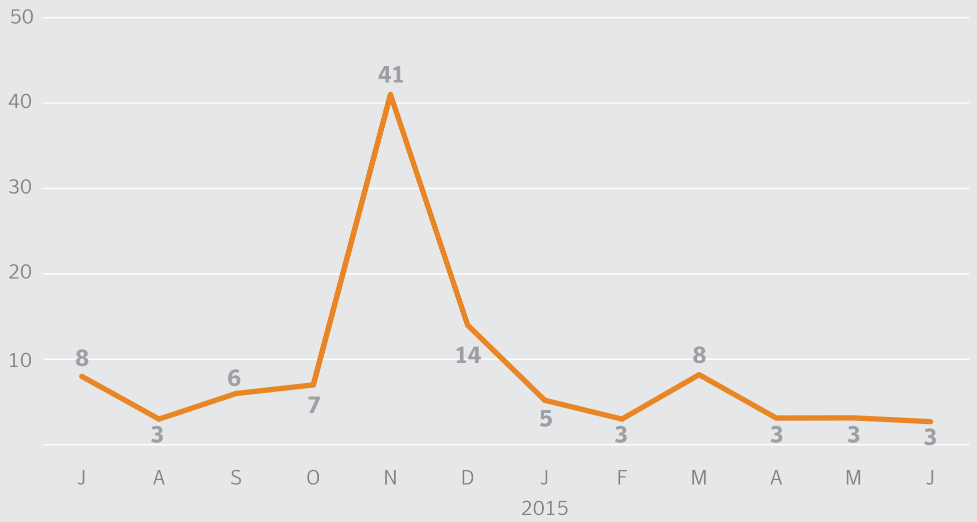
- *Crypto-ransomware was also up duing June, reaching its highest levels since December of 2014.*



Proportion of Email Traffic in Which Malware Was Detected

Source: Symantec

- *The proportion of email traffic containing malware decreased again this month, down from one in 207 emails in May to one in 319 emails in June.*



Percent of Email Malware as URL vs. Attachment by Month

Source: Symantec

- *The percentage of email malware that contains a URL remained low in June, hovering around three percent.*

Industry	June	May
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 230.2	1 in 305.5
Agriculture, Forestry, & Fishing	1 in 231.6	1 in 175.3
Public Administration	1 in 245.9	1 in 150.4
Services - Professional	1 in 296.7	1 in 164.5
Wholesale	1 in 301.6	1 in 157.7
Construction	1 in 305.8	1 in 240.9
Services - Non Traditional	1 in 365.3	1 in 236.6
Mining	1 in 371.5	1 in 325.8
Finance, Insurance, & Real Estate	1 in 481.5	1 in 292.8
Nonclassifiable Establishments	1 in 497.7	1 in 255.9

Proportion of Email Traffic Identified as Malicious by Industry Sector

Source: Symantec.cloud

- *The Transportation, Communications, Electric, Gas, & Sanitary Services sector was the most targeted industry in June, with one in 230 emails containing malware.*

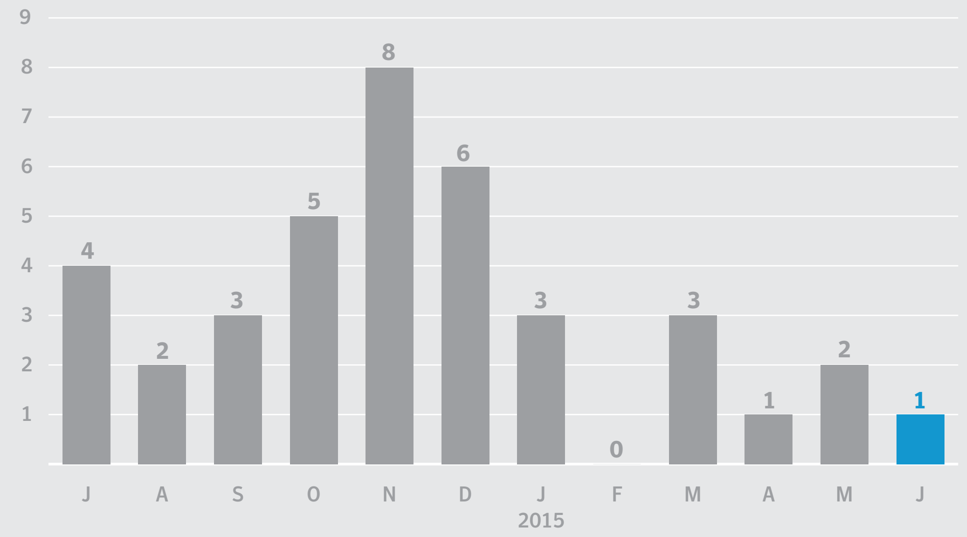
Company Size	June	May
1-250	1 in 255.6	1 in 141.3
251-500	1 in 232.9	1 in 159.5
501-1000	1 in 318.1	1 in 221.3
1001-1500	1 in 292.2	1 in 205.0
1501-2500	1 in 164.0	1 in 264.6
2501+	1 in 472.4	1 in 303.6

Proportion of Email Traffic Identified as Malicious by Organization Size

Source: Symantec.cloud

- *Organizations with 1501-2500 employees were most likely to be targeted by malicious email in the month of June, where one in 164 emails contained malware.*

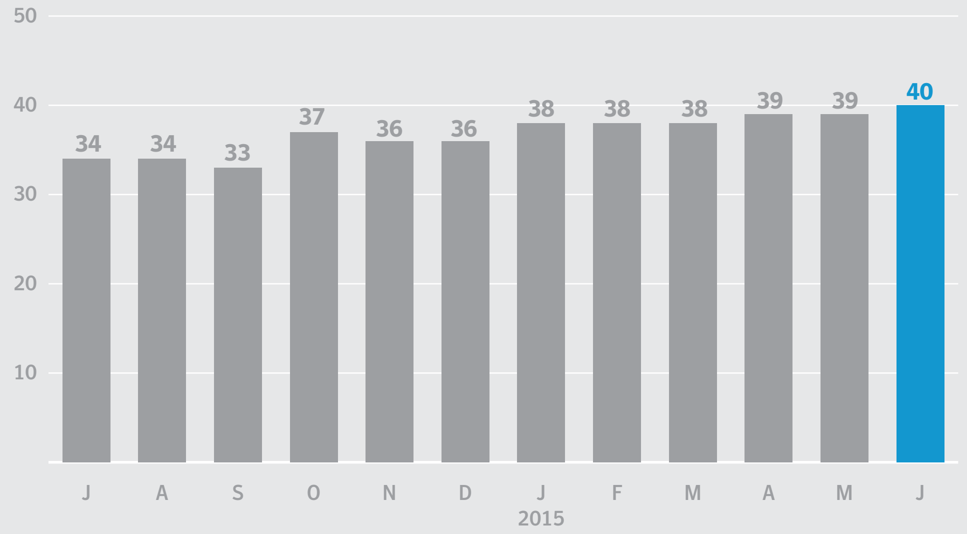
Mobile & Social Media



Android Mobile Malware Families by Month

Source: Symantec

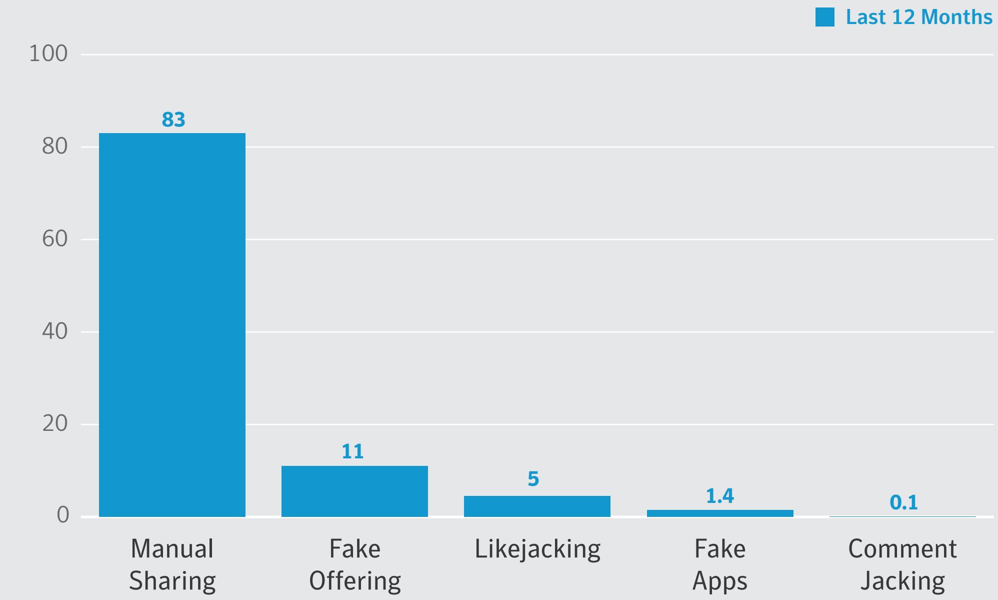
- *In June there was one new mobile malware familiy discovered.*



New Android Variants per Family by Month

Source: Symantec

- *There was an average of 40 Android malware variants per family in the month of in June.*



Manual Sharing – 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.

Fake Offering – 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.

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.

Fake Apps – 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.

Comment Jacking – This attack is similar to the "Like" jacking where the attacker tricks the user into submitting a comment about a link or site, which will then be posted to his/her wall.

Social Media

Source: Symantec

- *In the last twelve months, 83 percent of social media threats required end users to propagate them.*
- *Fake offerings comprised 11 percent of social media threats.*

Spam

49.7%	51.5%	52.1%
-1.8% pts	-0.6% pts	
June	May	April

Overall Email Spam Rate

Source: Symantec

- *The overall email spam rate further declined in June, dropping below 50 percent, to 49.7 percent.*

Industry	May	April
Mining	56.1%	55.4%
Manufacturing	53.7%	53.7%
Construction	53.3%	54.1%
Retail	53.1%	52.1%
Services - Non Traditional	53.0%	51.6%
Services - Professional	52.6%	52.5%
Agriculture, Forestry, & Fishing	52.3%	52.3%
Public Administration	52.3%	51.4%
Wholesale	52.2%	52.1%
Finance, Insurance, & Real Estate	51.9%	51.7%

Proportion of Email Traffic Identified as Spam by Industry Sector

Source: Symantec.cloud

- *At over 56 percent, the Mining sector had the highest spam rate again during June. The Manufacturing sector came in second with 54 percent.*

Company Size	May	April
1–250	52.8%	52.7%
251–500	53.2%	52.6%
501–1000	52.4%	52.0%
1001–1500	51.9%	52.2%
1501–2500	52.1%	52.2%
2501+	52.3%	52.2%

Proportion of Email Traffic Identified as Spam by Organization Size

Source: Symantec.cloud

- *While all organization sizes had around a 52-53 percent spam rate, organizations with 251-500 employees had the highest rate at 53.2 percent.*

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 2014, it recorded revenues of $6.7 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/

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

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.

04/15 21,500-21347932