Symantec

SYMANTEC INTELLIGENCE REPORT

MAY 2015

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 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

It appears as though attackers had small businesses clearly in their sights last month. All of our metrics that look at the size of organizations show businesses with less than 250 employees were subjected to the largest amount of malicious activity during the month of May. For instance, 42.5 percent of spear-phishing attacks were directed at organizations of this size during May, up from 30.6 percent in April. Small organizations were the most targeted size for overall phishing too. And while all organization sizes hovered around a 52 percent spam rate, organizations with less than 250 employees had the highest rate at 52.7 percent.

Small organizations were most likely to be targeted by malicious email in the month of May as well, where one in 141 emails contained a threat. The overall proportion of email traffic containing malware also increased this month, up from one in 246 emails in April to one in 207 emails in May. However the percentage of email malware that contained a URL remained low in May, hovering around three percent. The Public Administration sector was the most targeted industry again in May, with one in 150 emails containing malware, though this is down from one in 127 in April.

In spear-phishing attacks, Microsoft Word files—the .doc and .docx extensions—made up over 40 percent of attachments used in spear-phishing attacks during May. Microsoft Excel files also ranked highly, comprising 13.5 percent of spear-phishing attachments. While executable files, such as .bin, .exe, and .scr files, are frequently seen in spear-phishing attacks, this category of file types was down almost 25 percentage points in May. The Manufacturing sector was subjected to the largest volume of spear-phishing attacks, as 41 percent were directed at organizations in this sector.

In other news, there were more than 44.5 million new malware variants created in May, one zero-day vulnerability was reported (CVE-2015-3456), and while two vulnerabilities in industrial control systems were reported in April, none were reported this May.

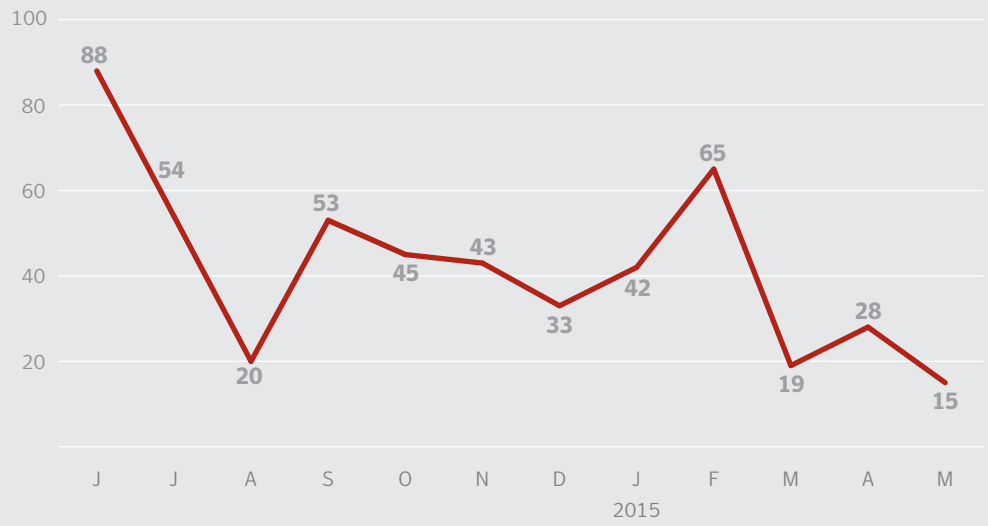
We hope that you enjoy this month's report and feel free to contact us with any comments or feedback.

Ben Nahorney, Cyber Security Threat Analyst

symantec_intelligence@symantec.com

MAY IN NUMBERS

Targeted Attacks & Phishing



Average Number of Spear-Phishing Attacks per Day

Source: Symantec

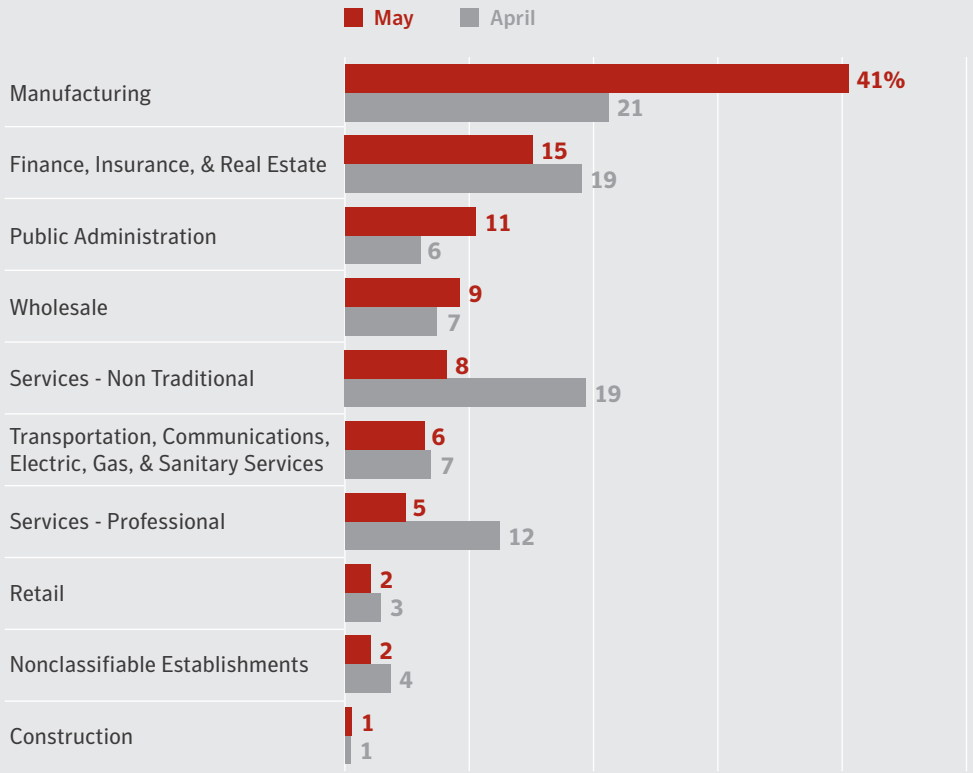
- *The average number of spear-phishing attacks per day continued to decline in May, down to 15 attacks per day.*

Rank	Attachment Type	May Overall Percentage	Attachment Type	April Overall Percentage
1	.doc	40.4%	.doc	39.3%
2	.txt	24.1%	.exe	20.5%
3	.xls	13.5%	.au3	15.0%
4	.pdf	11.6%	.scr	12.4%
5	.bin	3.9%	.jpg	3.1%
6	.exe	3.7%	.txt	1.2%
7	.ace	0.6%	.ace	0.4%
8	.scr	0.4%	.zip	0.3%
9	.rtf	0.2%	.html	0.3%
10	Other	1.5%	.cpl	0.3%

Attachments Used in Spear-Phishing Attacks

Source: Symantec

- *Microsoft Word files made up over 40 percent of attachments used in spear-phishing attacks in May, up one percentage point from April.*
- *While executable files, such as .bin, .exe, and .scr files, are frequently seen, this category of file types is down from 32.9 percent in April to eight percent in May.*



Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec

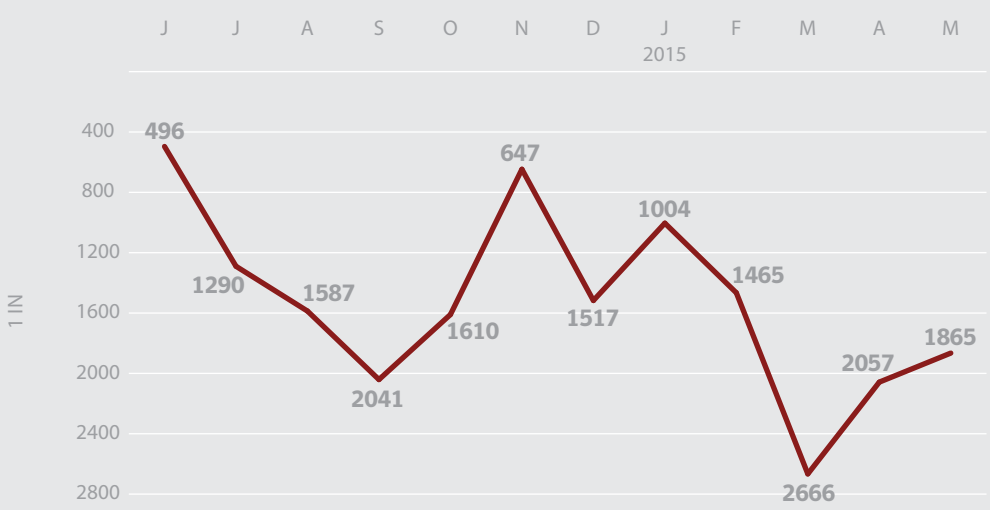
- *The Manufacturing sector was targeted with the greatest volume of spear-phishing attacks in May, as 41 percent were directed at manufacturing organizations.*

Company Size	May	April
1-250	42.5%	30.6%
251-500	5.1%	8.5%
501-1000	6.6%	12.8%
1001-1500	2.7%	2.2%
1501-2500	3.9%	3.4%
2501+	39.2%	42.5%

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec

- *Large enterprises were the target of 39.2 percent of spear-phishing attacks in May, down from 42.5 percent in April. In contrast, 42.5 percent of attacks were directed at organizations with less than 250 employees during May, up from 30.6 percent in April.*



Phishing Rate

Inverse Graph: Smaller Number = Greater Risk

Source: Symantec

- *The overall phishing rate has increased slightly for the second month in a row, where one in 1,865 emails was a phishing attempt.*

Industry	May	April
Agriculture, Forestry, & Fishing	1 in 856.0	1 in 1,111.7
Public Administration	1 in 1,289.3	1 in 1,275.5
Finance, Insurance, & Real Estate	1 in 1,349.9	1 in 3,083.8
Services - Professional	1 in 1,762.2	1 in 1,088.3
Nonclassifiable Establishments	1 in 1,834.9	1 in 2,033.4
Construction	1 in 2,124.9	1 in 2,752.2
Mining	1 in 2,230.6	1 in 3,350.4
Services - Non Traditional	1 in 2,408.2	1 in 2,471.8
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 2,840.2	1 in 3,627.8
Wholesale	1 in 2,878.2	1 in 2,668.5

Proportion of Email Traffic Identified as Phishing by Industry Sector

Source: Symantec.cloud

- *The Agriculture, Forestry, & Fishing sector was the most targeted Industry overall for phishing attempts in May, where phishing comprised one in every 856 emails. This rate was higher than any other industry in either May or April.*

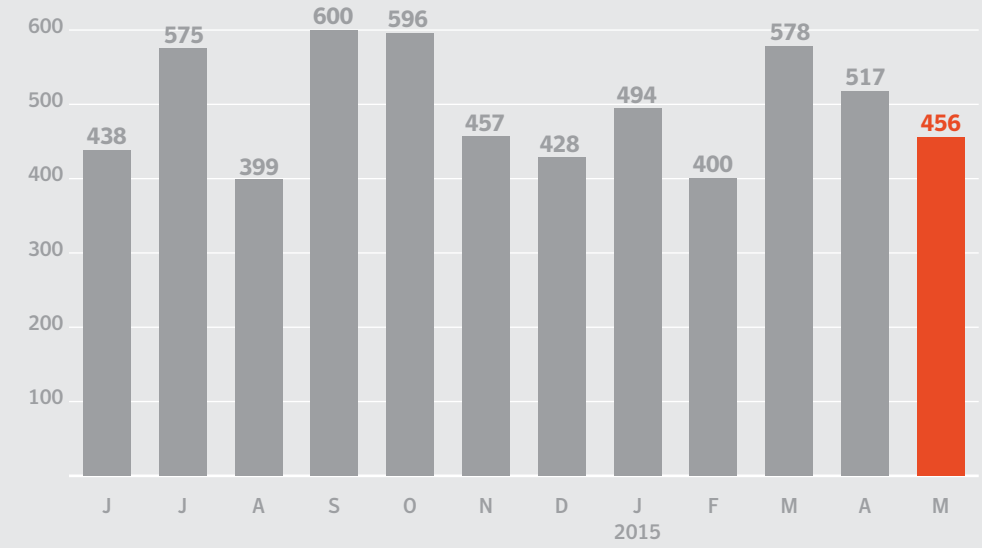
Company Size	May	April
1–250	1 in 1,473.9	1 in 1,706.8
251–500	1 in 1,629.5	1 in 1,975.1
501–1000	1 in 1,940.9	1 in 2,123.9
1001–1500	1 in 1,988.9	1 in 2,123.9
1501–2500	1 in 2,032.8	1 in 2,277.8
2501+	1 in 2,280.8	1 in 2,307.1

Proportion of Email Traffic Identified as Phishing by Organization Size

Source: Symantec.cloud

- *Small companies with less than 250 employees was the most targeted organization size in May.*

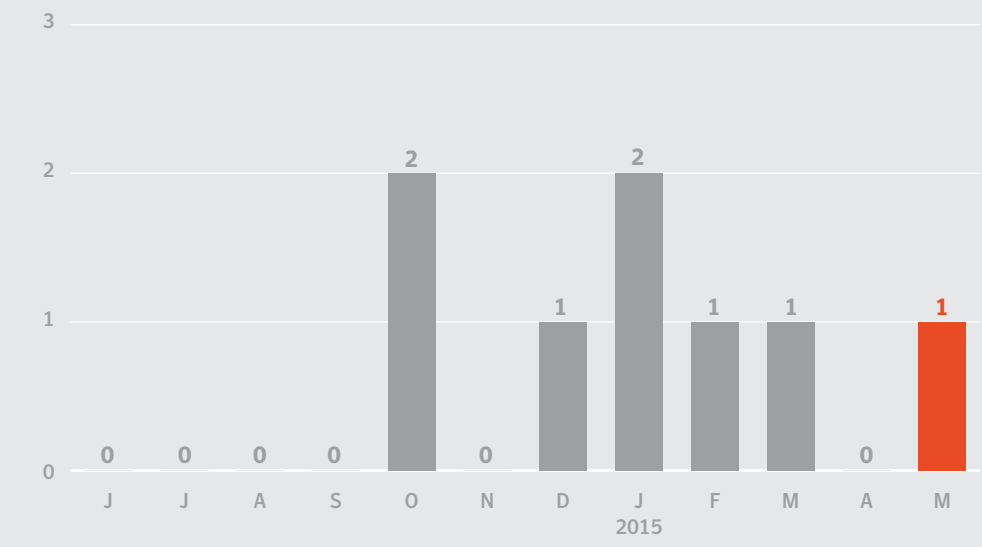
Vulnerabilities



Total Number of Vulnerabilities

Source: Symantec

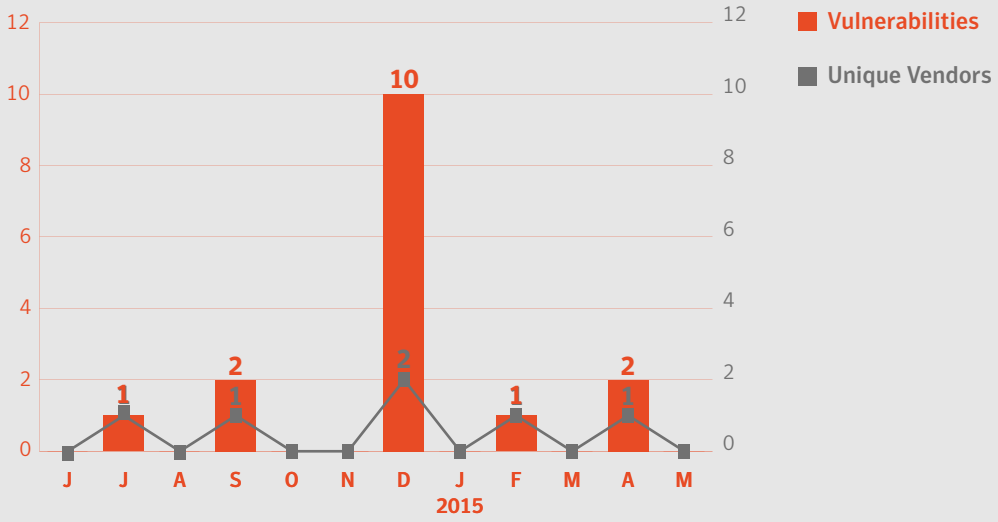
- *The number of vulnerabilities reported in May declined for the second month in a row, down to 456 vulnerabilities reported during the month.*



Zero-Day Vulnerabilities

Source: Symantec

- *There was a one zero-day vulnerability discovered in May, the Hypervisor Floppy Emulator Vulnerability (CVE-2015-3456).*

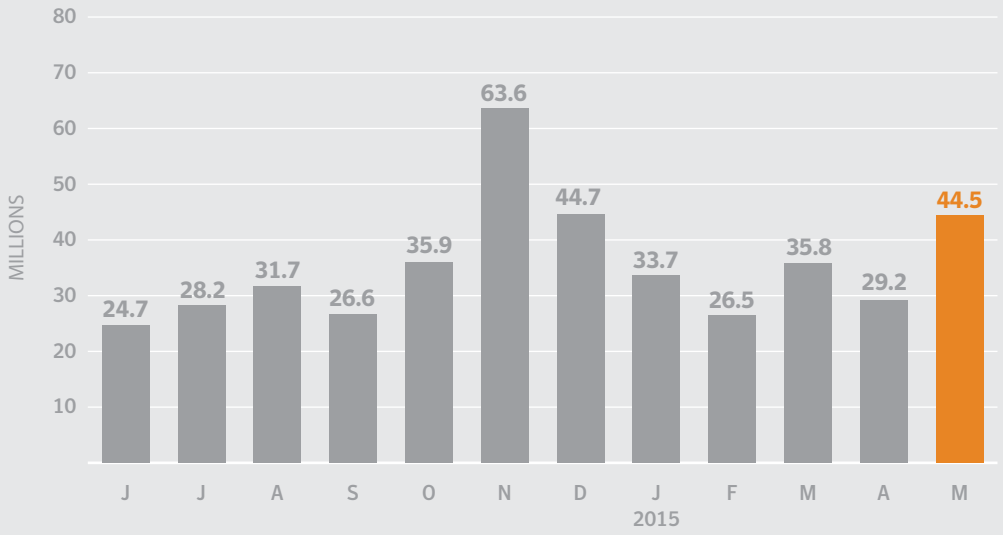


Vulnerabilities Disclosed in Industrial Control Systems

Source: Symantec

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

Malware



New Malware Variants

Source: Symantec

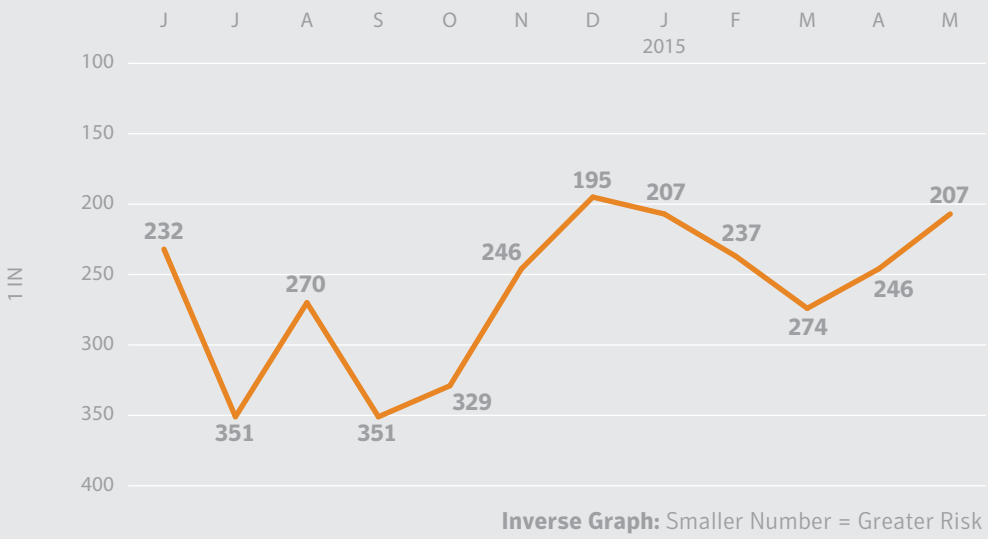
- *There were more than 44.5 million new pieces of malware created in May, up from 29.2 million created in April.*

Rank	Malware Name	May Percentage	Malware Name	April Percentage
1	OSX.RSPlug.A	23.9%	OSX.RSPlug.A	19.8%
2	OSX.Keylogger	14.0%	OSX.Wirelurker	12.2%
3	OSX.Wirelurker	9.0%	OSX.Keylogger	11.0%
4	OSX.Luaddit	8.3%	OSX.Luaddit	9.7%
5	OSX.Klog.A	8.0%	OSX.Klog.A	6.9%
6	OSX.Flashback.K	6.4%	OSX.Stealbit.B	6.3%
7	OSX.Netweird	3.9%	OSX.Flashback.K	5.7%
8	OSX.Sabpab	3.8%	OSX.Exploit.Launchd	5.2%
9	OSX.Stealbit.B	3.6%	OSX.Freezer	2.9%
10	OSX.Flashback	3.0%	OSX.Sabpab	2.8%

Top 10 Mac OS X Malware Blocked on OS X Endpoints

Source: Symantec

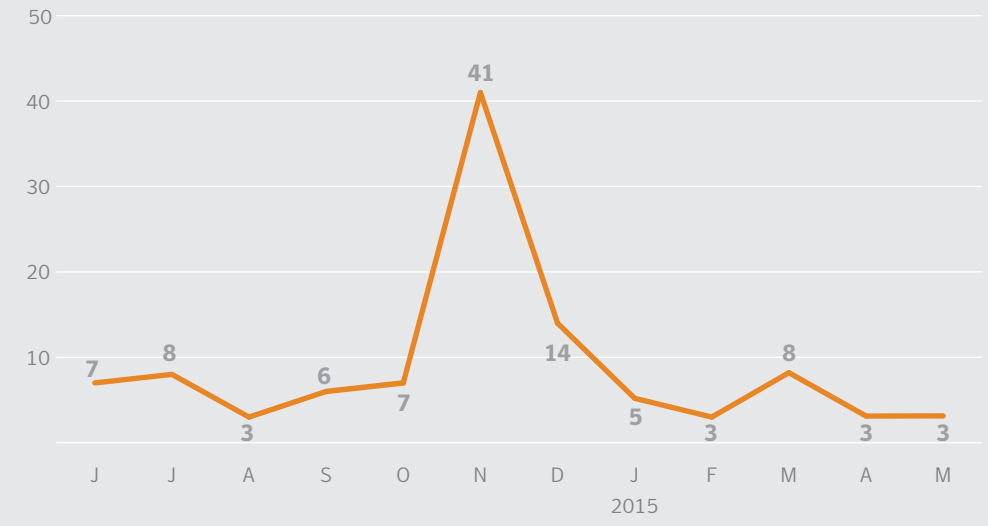
- *OSX.RSPlug.A continues to be the most commonly seen OS X threat seen on OS X endpoints in May, up four percentage points from April.*



Proportion of Email Traffic in Which Malware Was Detected

Source: Symantec

- *The proportion of email traffic containing malware increased again this month, up from one in 246 emails in April to one in 207 emails in May.*



Percent of Email Malware as URL vs. Attachment by Month

Source: Symantec

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

Industry	May	April
Public Administration	1 in 150.4	1 in 127.0
Wholesale	1 in 157.7	1 in 236.9
Services - Professional	1 in 164.5	1 in 200.9
Agriculture, Forestry, & Fishing	1 in 175.3	1 in 182.5
Services - Non Traditional	1 in 236.6	1 in 260.0
Construction	1 in 240.9	1 in 253.2
Nonclassifiable Establishments	1 in 255.9	1 in 261.6
Finance, insurance, & Real Estate	1 in 292.8	1 in 315.6
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 305.5	1 in 328.1
Mining	1 in 325.8	1 in 303.7

Proportion of Email Traffic Identified as Malicious by Industry Sector

Source: Symantec.cloud

- *The Public Administration sector was the most targeted industry again in May, with one in 150 emails containing malware. However, this is down from one in 127 in April.*

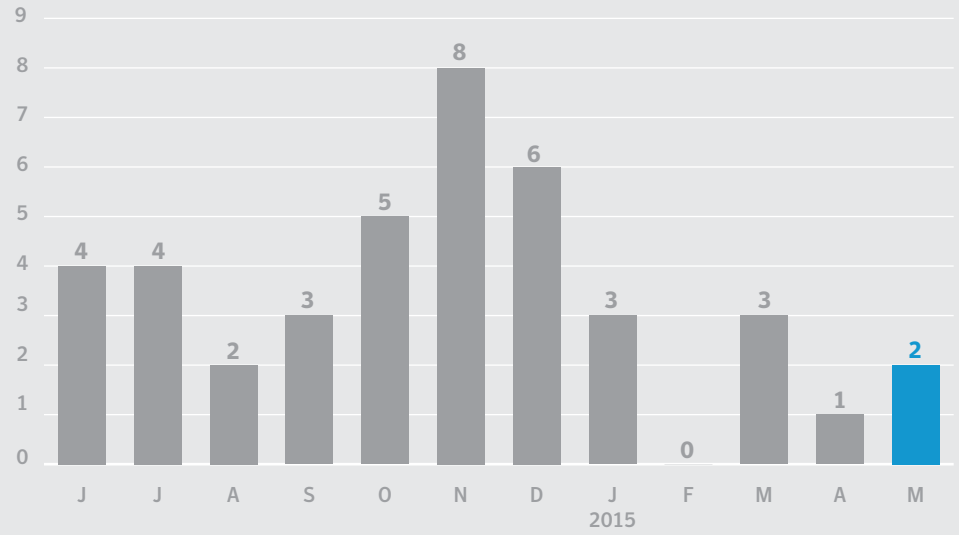
Company Size	May	April
1-250	1 in 141.3	1 in 209.7
251-500	1 in 159.5	1 in 174.2
501-1000	1 in 221.3	1 in 219.8
1001-1500	1 in 205.0	1 in 210.9
1501-2500	1 in 264.6	1 in 268.4
2501+	1 in 303.6	1 in 301.6

Proportion of Email Traffic Identified as Malicious by Organization Size

Source: Symantec.cloud

- *Organizations with less than 250 employees were most likely to be targeted by malicious email in the month of May.*

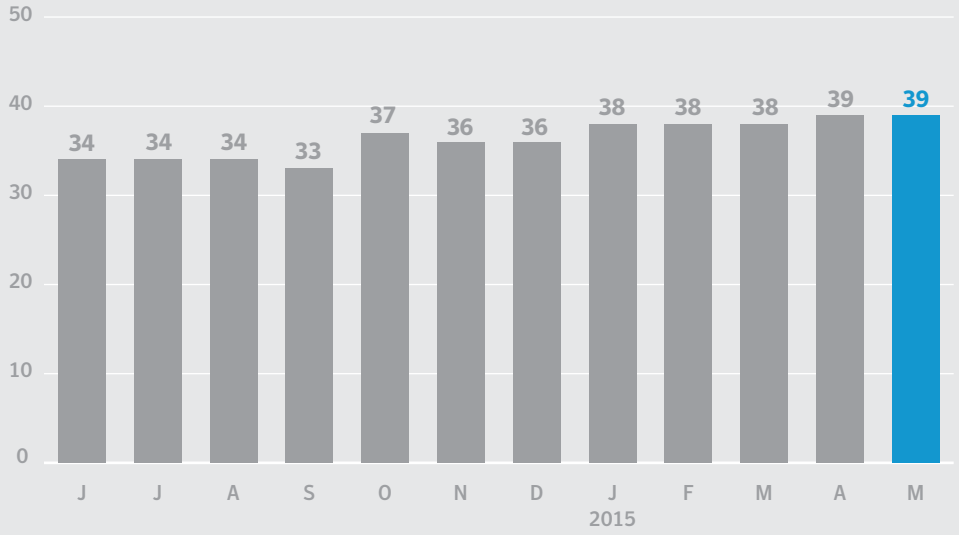
Mobile & Social Media



Android Mobile Malware Families by Month

Source: Symantec

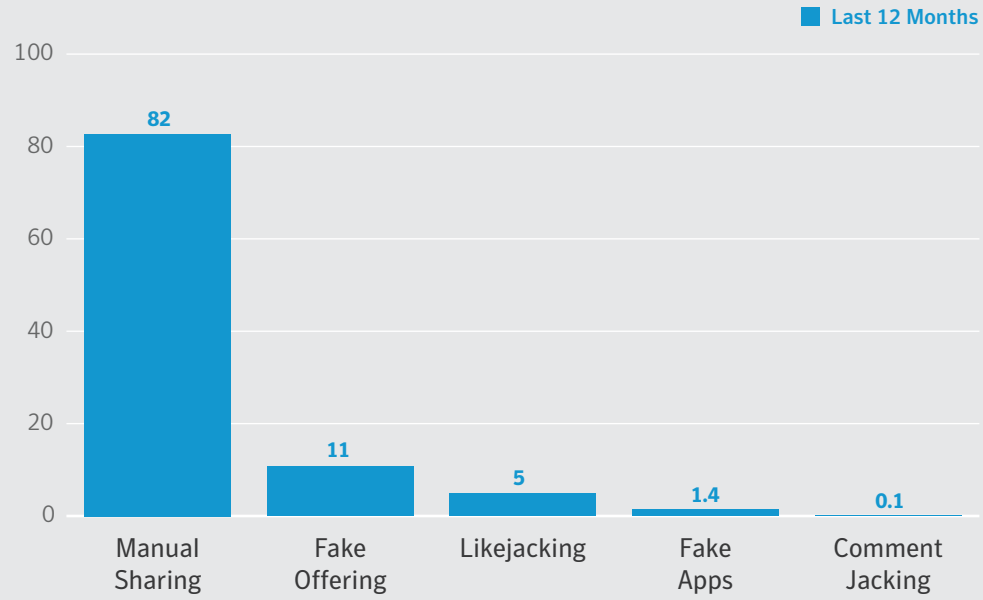
- *In May there were two new mobile malware families discovered.*



New Android Variants per Family by Month

Source: Symantec

- *There was an average of 39 Android malware variants per family in the month of in May.*



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, 82 percent of social media threats required end users to propagate them.*
- *Fake offerings comprised 11 percent of social media threats.*

Spam & Botnets

May	April	March
51.5%	**52.1%**	**55.8%**
-0.6% pts	-3.7% pts	

Overall Email Spam Rate

Source: Symantec

- *The overall email spam rate further declined in May, dropping 0.6 percentage points to 51.5 percent.*

Spam Botnet Name	Percentage of Botnet Spam
KELIHOS	19.7%
DARKMAILER	10.5%
GAMUT	7.6%
CUTWAIL	2.0%
DYRE	0.4%
SPAMSALOT	0.1%
DARKMAILER2	0.02%
DARKMAILER3	0.02%
GRUM	0.01%
ASPROX	0.01%

Top 10 Spam-Sending Botnets

Source: Symantec

- *The Kelihos botnet was the most active spamming botnet in the month of May, making of 19.7 percent of all bot-related spam traffic.*

Industry	May	April
Mining	55.38%	54.37%
Construction	54.07%	53.74%
Manufacturing	53.71%	53.40%
Services - Professional	52.54%	52.46%
Agriculture, Forestry, & Fishing	52.33%	52.33%
Retail	52.08%	52.40%
Wholesale	52.06%	52.28%
Nonclassifiable Establishments	51.75%	51.76%
Finance, Insurance, & Real Estate	51.74%	51.71%
Services - Non Traditional	51.64%	51.61%

Proportion of Email Traffic Identified as Spam by Industry Sector

Source: Symantec.cloud

- *At over 55 percent, the Mining sector had the highest spam rate during May. The Construction sector came in second with 54 percent.*

Company Size	May	April
1–250	52.66%	52.04%
251–500	52.55%	52.36%
501–1000	52.00%	52.42%
1001–1500	52.20%	52.08%
1501–2500	52.16%	52.17%
2501+	52.16%	52.11%

Proportion of Email Traffic Identified as Spam by Organization Size

Source: Symantec.cloud

- *While all organization sizes hovered around a 52 percent spam rate, organizations with less than 250 employees had the highest rate at 52.7 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