Symantec

SYMANTEC INTELLIGENCE REPORT

AUGUST 2015

Welcome to the August 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

August was a big month for zero-day vulnerabilities, in which a total of 11 were reported. This is by far the largest number disclosed in a given month to-date.

Six of these zero-day vulnerabilities impact industrial control systems, devices used in industrial sectors and critical infrastructures, across five vendors. The vulnerabilities cover a wide range of possible attacks, including remote code execution and denial of service attacks.

Two further zero-day vulnerabilities were discovered in the Apple OS X operating system. When used in tandem, these two vulnerabilities can cause memory corruption in the OS X kernel and gain the attacker escalated privileges on the compromised computer. For more information see the Security Response blog republished in this report.

These vulnerabilities come on the heels of a new OS X threat called OSX.Sudoprint. This threat exploits a local privilege escalation vulnerability in the OS X operating system, which was patched by Apple at the beginning of August. This threat comprised over 77 percent of the OS X threats we saw on OS X endpoints this month.

Ransomware attacks were down in August, where over 155 thousand attacks were detected. While ransomware attacks appear to be down to their lowest levels in the last 12 months, we have reason to believe that attackers have shifted tactics and are currently pushing fake security software, such as FakeAV threats, instead. However, crypto-ransomware continues to grow, setting another monthly high for the year.

In other news, the Transportation, Communications, Electric, Gas, & Sanitary Services sector was by far the most targeted sector during August, comprising 52 percent of all targeted attacks. Small businesses with less than 250 employees also made up the majority of organization sizes, where 78.4 percent of spear-phishing attacks were reported.

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

From the Security Response Blog

New Mac Os X Vulnerability Could Provide Attackers With Root Access

Symantec confirms existence of flaw, which requires victim to voluntarily run an application for exploit.

By Symantec Security Response

Symantec has confirmed the existence of two new vulnerabilities in the Mac OS X operating system which, if exploited, could allow an attacker to escalate privileges on an affected computer in order to gain root access. While the vulnerabilities require the victim to voluntarily run an application in order for an attack to be successful, they represent a threat until a patch is published by Apple.

The vulnerabilities were discovered by Italian researcher Luca Todesco, who posted a proof-of-concept exploit to Github on August 16. Todesco said that he reported the issue to Apple a few hours before making it public. Apple has yet to publicly comment on the vulnerabilities.

Analysis by Symantec has confirmed that the proof-of-concept exploit works as described. The vulnerabilities are reported to affect OS X version 10.9.5 to 10.10.5. The beta for OS X 10.11 is understood to be not affected.

The exploit uses two different vulnerabilities to create a memory corruption in the OS X kernel. This is then used to bypass security features that block exploit code from running, providing the attacker with root access.

News of the new vulnerabilities comes days after another privilege escalation vulnerability was patched by Apple. The Apple Mac OS X Prior to 10.10.5 Multiple Security Vulnerabilities (CVE-2015-3760) enabled a malicious installer to gain root access to an affected computer, allowing it to install other unauthorized software.

There have been no reports of these latest vulnerabilities being exploited in the wild; however, the likelihood of attacks will increase as news spreads.

Mitigation

Until a patch for the vulnerability is issued, affected Mac OS X users are advised to exercise caution and only download and install new software from trusted sources.

Mac OS X users are advised to apply any security updates to the OS as soon as they become available.

Analysis of this vulnerability is ongoing and further updates may be published if new information is uncovered.

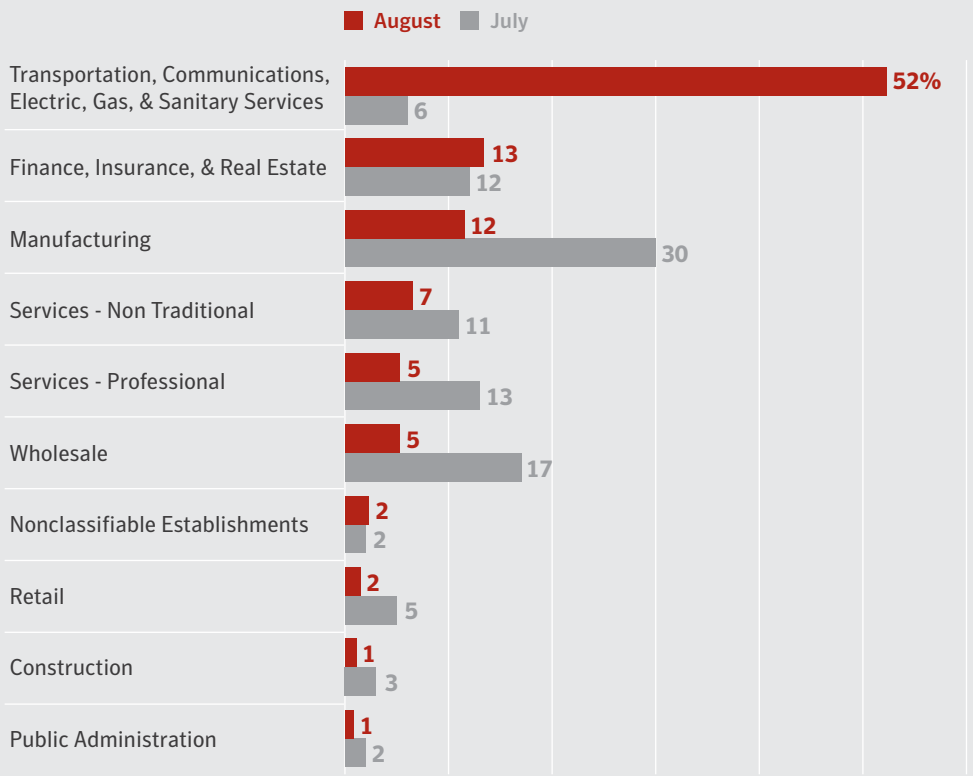
About the Security Response blog

In the Symantec Intelligence Report we republish a blog that highlights key data or an event that stood out during the month. Our security researchers around the world frequently publish new blogs during the month on topics such as malware, security risks, vulnerabilities, and spam. For the latest security news and information, visit:

http://www.symantec.com/connect/symantec-blogs/security-response

AUGUST IN NUMBERS

Targeted Attacks & Phishing



Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec

The Transportation, Communications, Electric, Gas, & Sanitary Services sector was by far the most targeted sector during August, comprising 52 percent of all targeted attacks.

Company Size	August	July
1-250	78.4%	33.2%
251-500	2.8%	12.6%
501-1000	3.3%	7.7%
1001-1500	2.3%	3.0%
1501-2500	1.4%	9.3%
2501+	11.7%	34.1%

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec

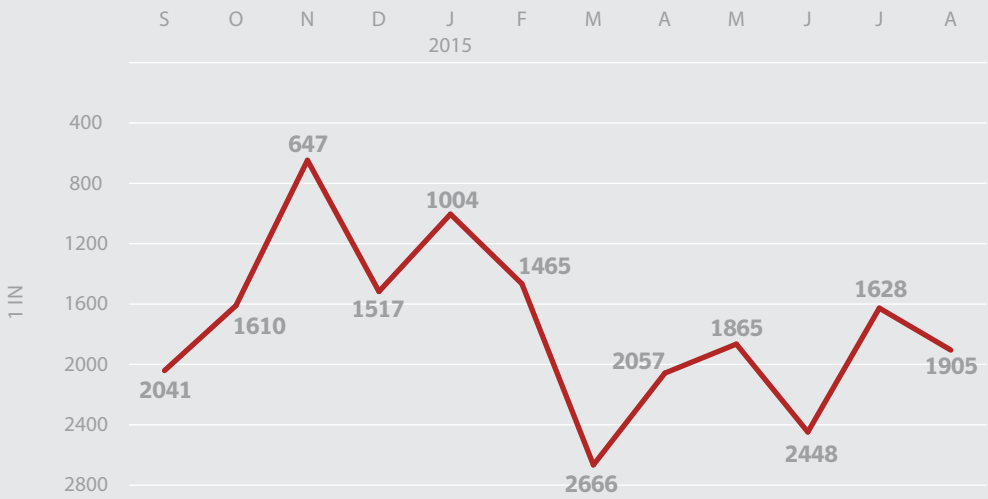
Small businesses with less than 250 employees were the target of 78.4 percent of spear-phishing attacks in August, up from 33.2 percent in July. In contrast, 11.7 percent of attacks were directed at large enterprises.

Rank	Attachment Type	August Overall Percentage
1	.txt	32.2%
2	.doc	29.7%
3	.exe	17.3%
4	.ace	10.2%
5	.pdf	5.0%
6	.xls	1.9%
7	.pps	1.2%
8	.fas	1.2%
9	.scr	0.6%
10	.class	0.3%

Attachments Used in Spear-Phishing Attacks

Source: Symantec

- *The most commonly seen attachment type used in targeted attacks were .txt files, followed by .doc files, at 32.2 percent and 29.7 percent respectively. Executable files with the .exe extension came in third with 17.3 percent.*



Phishing Rate

Inverse Graph: Smaller Number = Greater Risk

Source: Symantec

- *The overall phishing rate has decreased slightly this month, where one in 1,905 emails was a phishing attempt.*

Industry	August	July
Agriculture, Forestry, & Fishing	1 in 943.7	1 in 837.1
Public Administration	1 in 1,177.7	1 in 1,359.2
Nonclassifiable Establishments	1 in 1,414.3	1 in 1,564.4
Services - Professional	1 in 1,474.3	1 in 1,566.8
Services - Non Traditional	1 in 1,917.3	1 in 1,320.5
Wholesale	1 in 2,241.0	1 in 2,343.8
Finance, Insurance, & Real Estate	1 in 2,320.3	1 in 1,357.6
Construction	1 in 2,361.4	1 in 2,241.5
Mining	1 in 2,907.0	1 in 2,017.1
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 3,246.0	1 in 3,114.3

Proportion of Email Traffic Identified as Phishing by Industry Sector

Source: Symantec.cloud

- *The Agriculture, Forestry, & Fishing sector was again the most targeted Industry overall for phishing attempts in August, where phishing comprised one in every 943.7 emails. This rate has been higher in this sector than in any other industry since April.*

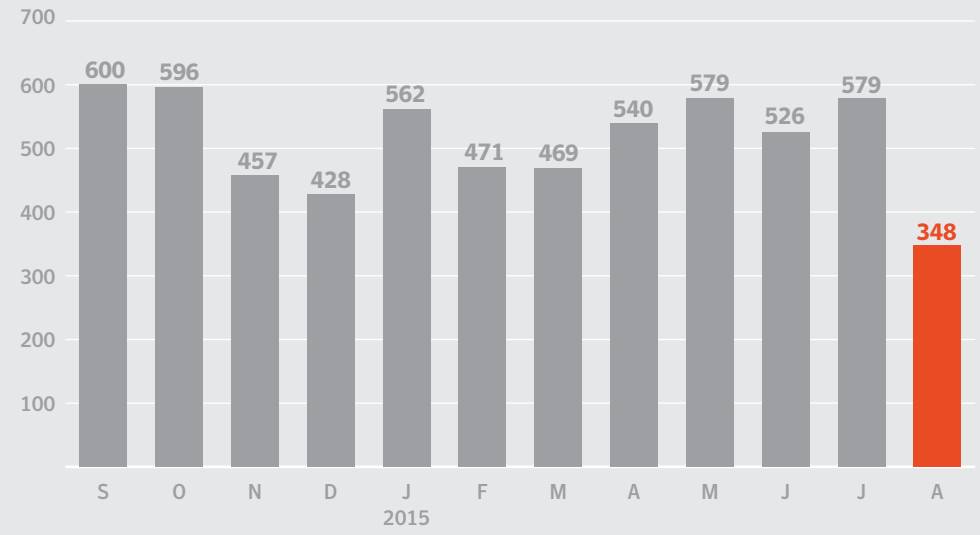
Company Size	August	July
1–250	1 in 1,573.9	1 in 1,288.9
251–500	1 in 1,367.0	1 in 1,613.7
501–1000	1 in 1,736.5	1 in 1,899.6
1001–1500	1 in 2,195.5	1 in 2,209.9
1501–2500	1 in 1,862.6	1 in 2,045.5
2501+	1 in 2,351.2	1 in 1,872.3

Proportion of Email Traffic Identified as Phishing by Organization Size

Source: Symantec.cloud

- *Companies with 251-500 employees were the most targeted organization size in August.*

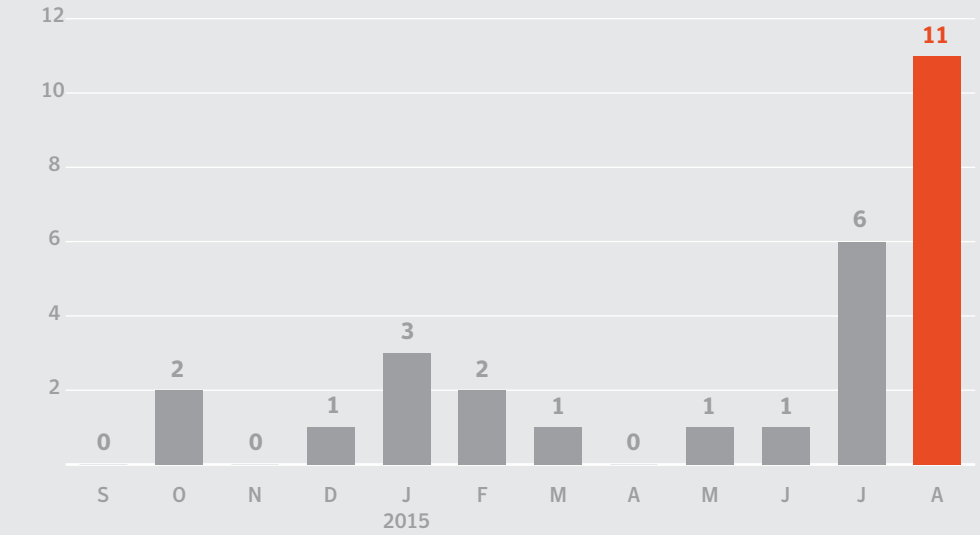
Vulnerabilities



Total Number of Vulnerabilities

Source: Symantec

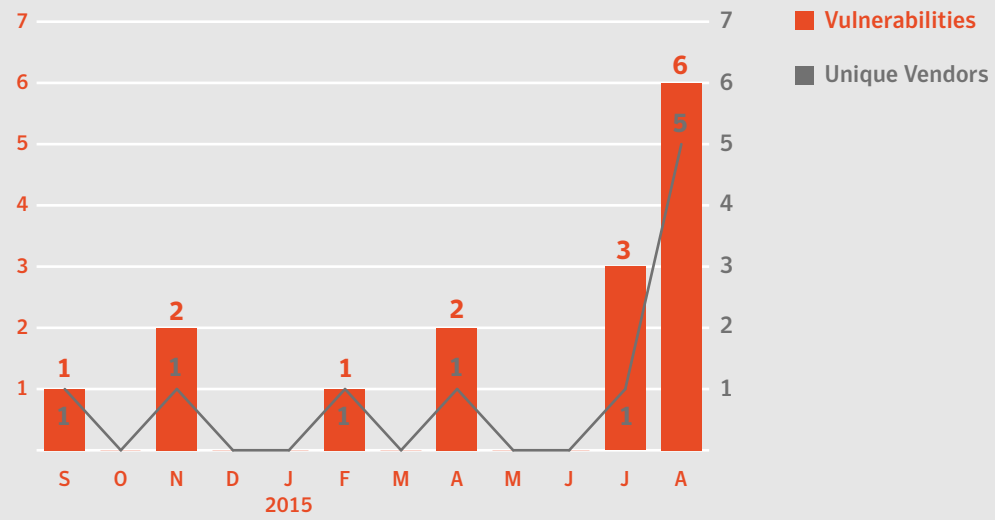
- *The number of vulnerabilities disclosed declined in August, from 579 in July to 348 reported during this month.*



Zero-Day Vulnerabilities

Source: Symantec

- *There were 11 zero-day vulnerabilities disclosed in August. This includes six targeting industrial control systems and two targeting the OS X operating system.*



Vulnerabilities Disclosed in Industrial Control Systems

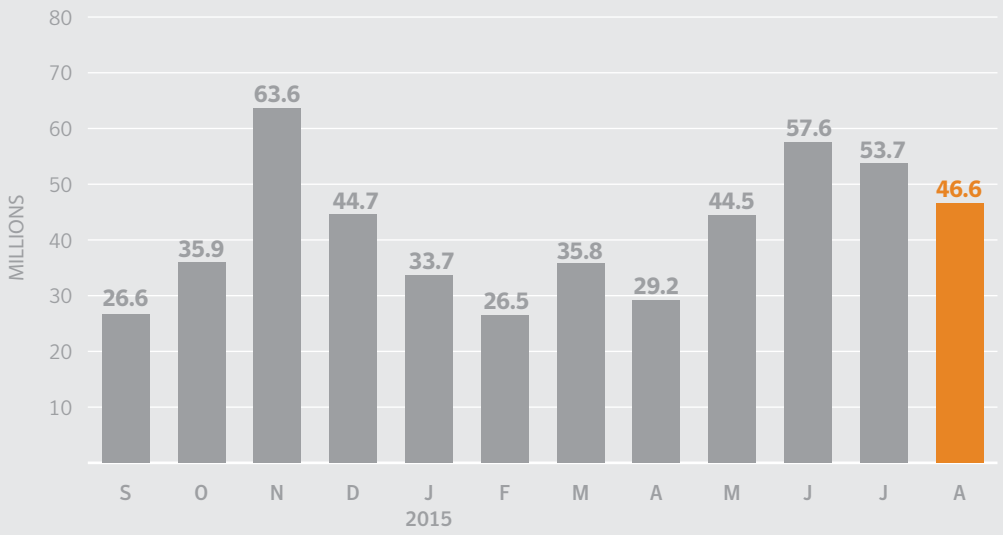
Source: Symantec

- *Six zero-day vulnerabilities in industrial control systems were reported by in August, impacting five ICS vendors.*

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 metrics 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 46.6 million new pieces of malware created in August. While down from July, this is still well above the 41.5 million monthly average seen over the last twelve months.*

Rank	Malware Name	August Percentage	Malware Name	July Percentage
1	W32.Ramnit!html	6.3%	W32.Almanahe.B!inf	6.6%
2	W32.Almanahe.B!inf	5.5%	W32.Ramnit!html	5.8%
3	W32.Sality.AE	5.2%	W32.Sality.AE	5.7%
4	W32.Downadup.B	3.7%	W32.Downadup.B	4.1%
5	W32.Ramnit.B	3.6%	W32.Ramnit.B	3.4%
6	W32.Ramnit.B!inf	2.6%	Trojan.Swifi	3.2%
7	W97M.Downloader	1.9%	W32.Ramnit.B!inf	2.5%
8	Trojan.Swifi	1.8%	W97M.Downloader	2.0%
9	W32.Virut.CF	1.6%	W32.Virut.CF	1.7%
10	W32.Chir.B@mm(html)	1.3%	W32.SillyFDC.BDP!lnk	1.7%

Top 10 Malware

Source: Symantec

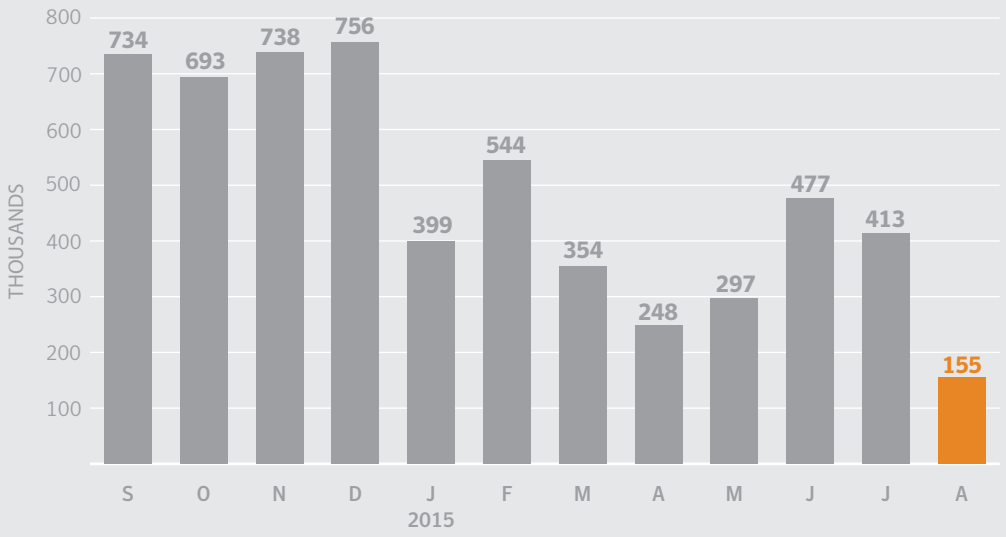
- *W32.Ramnit!html and W32.Almanahe.B!inf continue to be the most commonly seen malware detections in August.*

Rank	Malware Name	August Percentage	Malware Name	July Percentage
1	OSX.Sudoprint	77.3%	OSX.RSPlug.A	61.9%
2	OSX.RSPlug.A	7.5%	OSX.Wirelurker	10.0%
3	OSX.Klog.A	4.4%	OSX.Crisis	8.4%
4	OSX.Wirelurker	1.9%	OSX.Keylogger	4.8%
5	OSX.Crisis	1.5%	OSX.Klog.A	3.5%
6	OSX.Flashback.K	1.0%	OSX.Luaddit	1.8%
7	OSX.Keylogger	1.0%	OSX.Stealbit.B	1.3%
8	OSX.Luaddit	0.8%	OSX.Flashback.K	1.3%
9	OSX.Sabpab	0.7%	OSX.Freezer	1.1%
10	OSX.Remoteaccess	0.5%	OSX.Netweird	0.8%

Top 10 Mac OS X Malware Blocked on OS X Endpoints

Source: Symantec

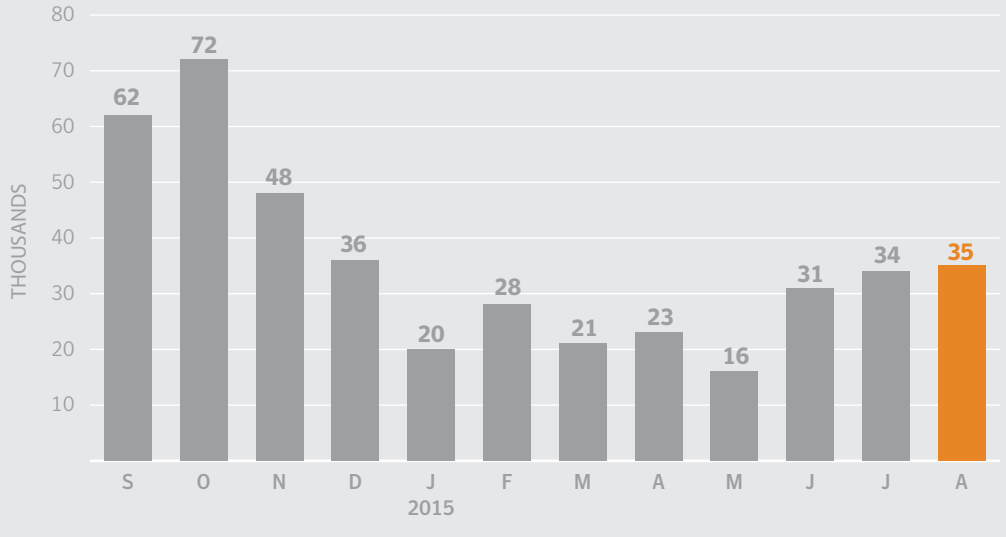
- *OSX.Sudoprint was the most commonly seen OS X threat on OS X endpoints in August. This threat takes advantage of a vulnerability targeting the OS X operating system that was discovered in July and patched earlier this month.*



Ransomware Over Time

Source: Symantec

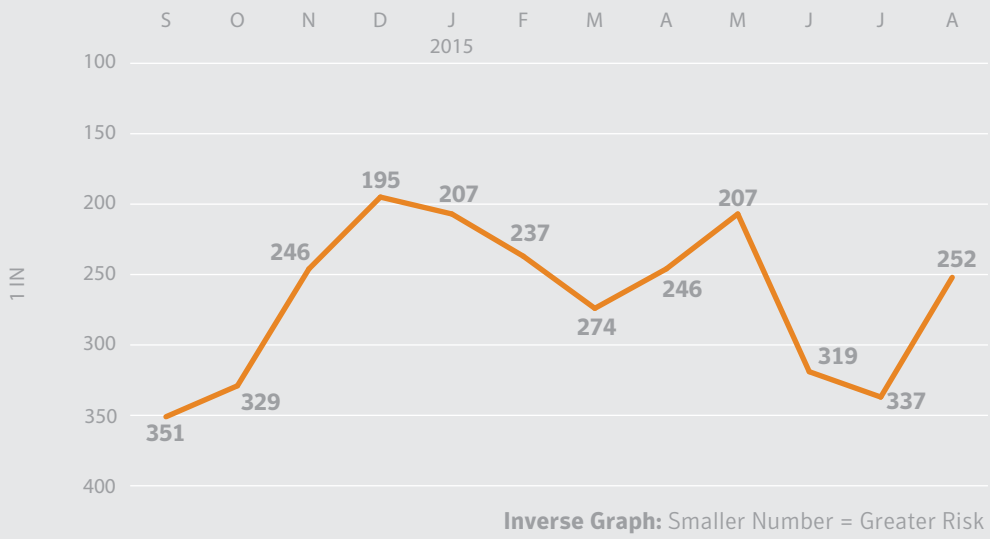
- *Ransomware attacks were down in August, where over 155 thousand attacks were detected.*
- *While ransomware attacks appear to be down to their lowest levels in the last 12 months, we have reason to believe that attackers have shifted tactics and are currently pushing FakeAV threats instead.*



Crypto-Ransomware Over Time

Source: Symantec

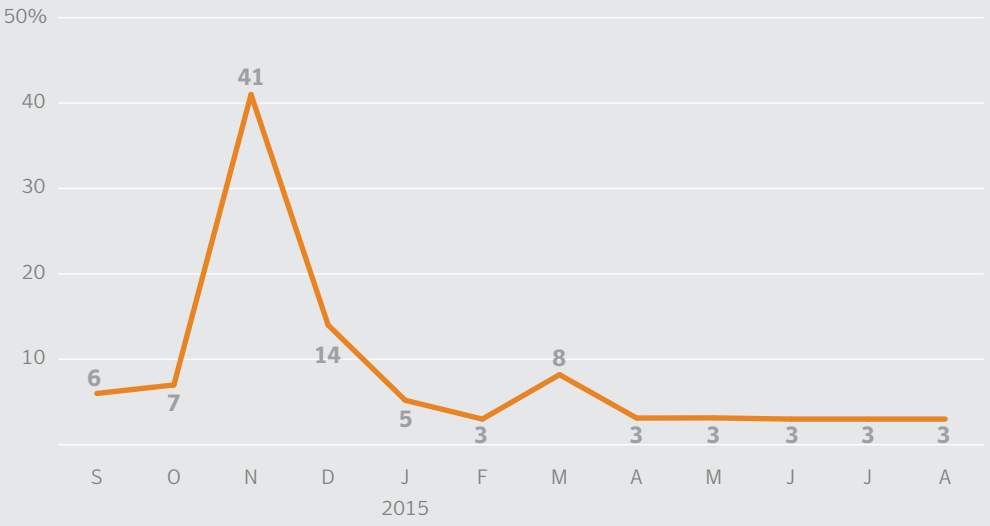
- *Crypto-ransomware was up during August, setting another high for 2015.*



Proportion of Email Traffic in Which Malware Was Detected

Source: Symantec

- *The proportion of email traffic containing malware increased this month, where one in 252 emails contained malware.*



Percent of Email Malware as URL vs. Attachment by Month

Source: Symantec

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

Industry	August	July
Public Administration	1 in 154.4	1 in 288.9
Agriculture, Forestry, & Fishing	1 in 227.6	1 in 252.7
Services - Professional	1 in 249.1	1 in 338.0
Wholesale	1 in 274.6	1 in 333.3
Construction	1 in 288.0	1 in 376.3
Services - Non Traditional	1 in 311.0	1 in 280.1
Finance, Insurance. & Real Estate	1 in 351.4	1 in 416.4
Nonclassifiable Establishments	1 in 385.9	1 in 519.5
Transportation, Communications, Electric, Gas. & Sanitary Services	1 in 392.6	1 in 392.4
Mining	1 in 484.9	1 in 438.3

Proportion of Email Traffic Identified as Malicious by Industry Sector

Source: Symantec.cloud

- *Public Administration was the most targeted sector in August, where one in every 252.7 emails contained malware.*

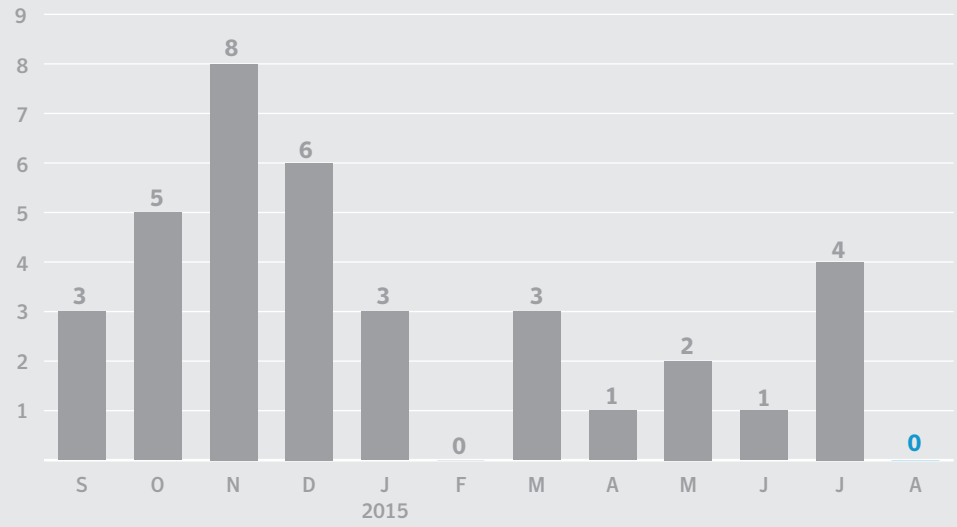
Company Size	August	July
1-250	1 in 162.1	1 in 275.8
251-500	1 in 206.0	1 in 259.5
501-1000	1 in 249.1	1 in 351.1
1001-1500	1 in 291.3	1 in 389.5
1501-2500	1 in 299.8	1 in 373.2
2501+	1 in 409.7	1 in 401.7

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 August, where one in 162.1 emails was malicious.*

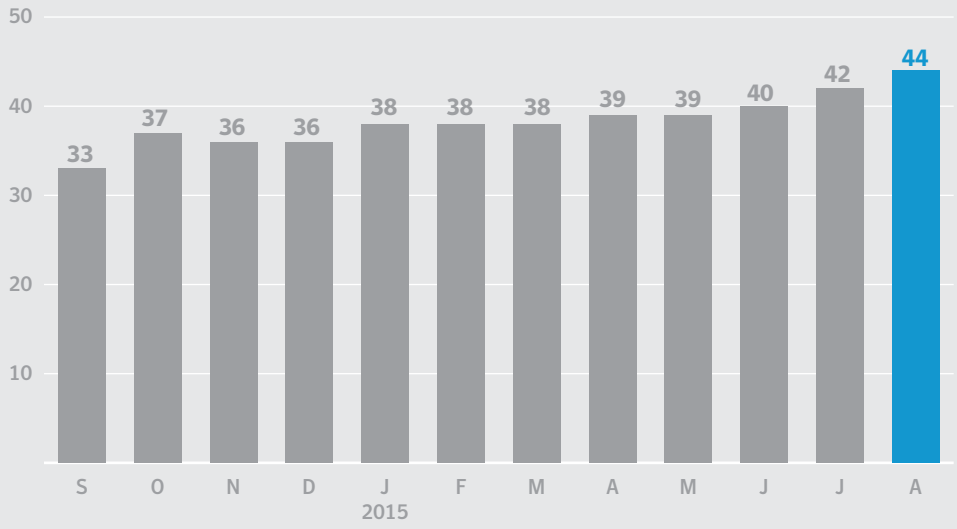
Mobile & Social Media



Android Mobile Malware Families by Month

Source: Symantec

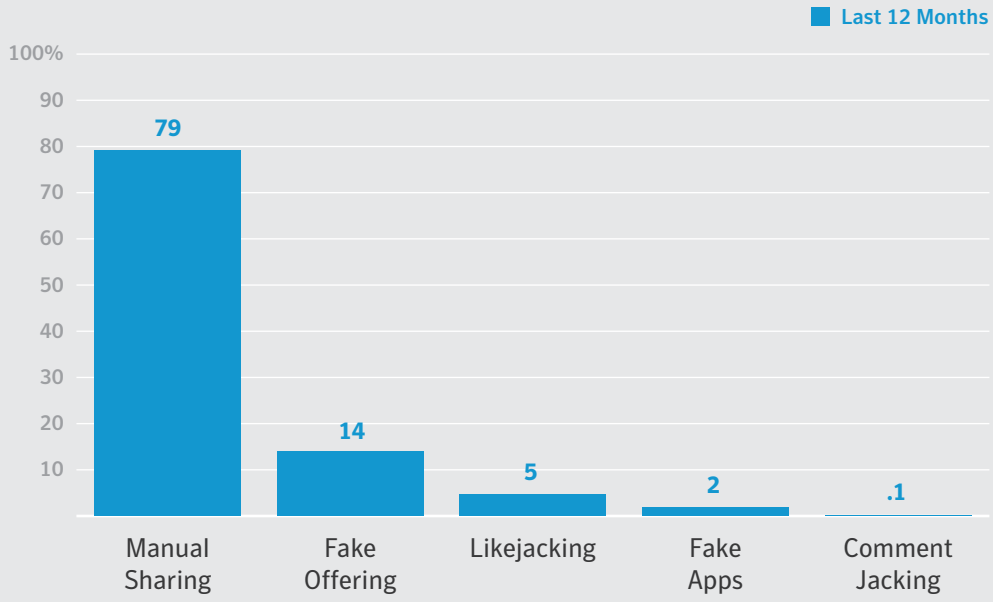
- *In August there were no new mobile malware families discovered.*



New Android Variants per Family by Month

Source: Symantec

- *There was an average of 44 Android malware variants per family in the month of in August.*



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, 79 percent of social media threats required end users to propagate them.*
- *Fake offerings comprised 14 percent of social media threats.*

Spam

52.5%
+2.4% pts
August

50.1%
+.4% pts
July

49.7%
-1.8% pts
June

Overall Email Spam Rate

Source: Symantec

- *The overall email spam rate in August was 52.5 percent, up 2.4 percentage points from July.*

Industry	August	July
Mining	54.8%	55.7%
Manufacturing	53.9%	53.8%
Construction	53.4%	53.0%
Services - Professional	53.1%	52.5%
Retail	52.7%	53.0%
Services - Non Traditional	52.6%	51.9%
Nonclassifiable Establishments	52.6%	52.0%
Public Administration	52.5%	–
Agriculture, forestry & fishing	52.4%	52.2%
Wholesale	52.4%	52.1%

Proportion of Email Traffic Identified as Spam by Industry Sector

Source: Symantec.cloud

- *At 54.8 percent, the Mining sector again had the highest spam rate during August. The Manufacturing sector came in second with 53.9 percent.*

Company Size	August	July
1–250	52.7%	52.3%
251–500	53.0%	52.6%
501–1000	52.9%	52.3%
1001–1500	52.3%	51.9%
1501–2500	52.6%	52.2%
2501+	52.6%	52.4%

Proportion of Email Traffic Identified as Spam by Organization Size

Source: Symantec.cloud

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

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