Symantec

SYMANTEC INTELLIGENCE REPORT

NOVEMBER 2015

Welcome to the November 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

The proportion of email traffic containing malware was up in November, where one in 140 emails contained malware. Public Administration was the most targeted sector in November, with one in every 85.6 emails containing malware. Organizations with 251-500 employees were most likely to be targeted by malicious email in the month of November, where one in 93.7 emails was malicious.

In one email campaign in particular, attackers attempted to prey upon user's fears of terror attacks in light of recent international news. While the attachments were presented as security tips to help the recipients protect themselves, one of the files contained a malicious payload that included a remote access Trojan. (See this month's Security Response blog for more details.)

Interestingly, there were 19.4 million new pieces of malware created in November. This rate has steadily declined in the second half of 2015, from a high of 57.6 million seen in June. While such a decline could point to a reduction in malicious activity, it could also mean that attackers are having a higher success rate in compromising computers, thus not needing to produce as much malware to achieve their goals.

The overall email spam rate in November was also up at 54.1 percent, an increase of 0.6 percentage points from October. At 57 percent, the Mining sector again had the highest spam rate during November.

In terms of targeted attacks in general, the Finance, Insurance, & Real Estate sector was the most targeted sector during November, comprising 41 percent of all targeted attacks. Large enterprises were the target of 49.9 percent of these spear-phishing attacks.

Ben Nahorney, Cyber Security Threat Analyst

symantec_intelligence@symantec.com

Methodology

The Symantec Intelligence Report comprises monthly analysis based on the latest data available from the Symantec Global Intelligence Network. As new information is continually being discovered, some metrics published in the report may be subject to change. Subsequent reports will be updated to reflect the latest information in order to ensure the most accurate reporting and analysis of the threat landscape.

From the Security Response Blog

Terror-Alert Spam Targets the Middle East, Canada to Spread Malware

Cybercriminals spoof law enforcement officials in Dubai, Bahrain, Turkey, and Canada to send terror-alert spear-phishing emails containing Backdoor.Sockrat.

By Symantec Security Response

Last month, Symantec observed malicious emails spoofing the email address of one United Arab Emirates (UAE) law enforcement agency, particularly the Dubai Police Force. These spear-phishing emails, which read like a warning from the Dubai Police, bank on users' fear of terror attacks to trick them into executing the malicious attachments. The attachments are disguised as valuable security tips that could help recipients to protect themselves, as well as their companies and their families, from potential terror attacks that may occur in their business location.

To add more credibility to the emails, the crooks impersonate the incumbent Dubai Police lieutenant general, who is also the head of general security for the emirate of Dubai, by signing the email with his name.

The emails come with two attachments, one of which is a PDF file that is not actually malicious but acts as a decoy file. The malware resides in the other attachment, an archive, as a .jar file. Further analysis of the malware confirms that the cybercriminals behind this campaign are using a multiplatform remote access Trojan (RAT) called Jsocket (detected as Backdoor.Sockrat). This RAT is a new product from the creators of the AlienSpy RAT, which has been discontinued earlier this year.

Targets beyond the UAE

While the group behind this campaign mainly targeted UAE-based companies and employees, we have also seen similar spear-phishing runs targeting three other countries: Bahrain, Turkey and, more recently, Canada.

Like in the Dubai campaign, the cybercriminals are also using incumbent law enforcement officials' names in these countries to lend credibility to their fake terror alerts, which also purport to provide protective measures supposedly outlined in attached files. The group is expanding their reach and we may see new email models targeting additional countries.

Interestingly enough, despite not being entirely written in the countries' respective official languages, the emails are pretty crafty. All officials used in the cybercriminals' scheme are currently in office. The subject in most cases reflects the name of an employee who works for the targeted company. All these details show that the crooks did some research before sending these phishing emails. If they do not have any employee information, then they would email other targets in the company that could provide them an entry point, such as customer service representatives or IT department personnel.

At the time of writing, we can confirm that this campaign is aimed at various big companies in the Middle East and Canada. While the campaign does not target a specific type of industry, we have observed such emails sent to the following sectors: energy, defense contractor, finance, government, marketing, and IT.

With recent events such as those witnessed in Paris and Beirut, terrorist attacks have become a threat across the world, and terror groups have been known to make their presence felt online too. We may yet see more of these kinds of social engineering tactics preying on real-world fears.

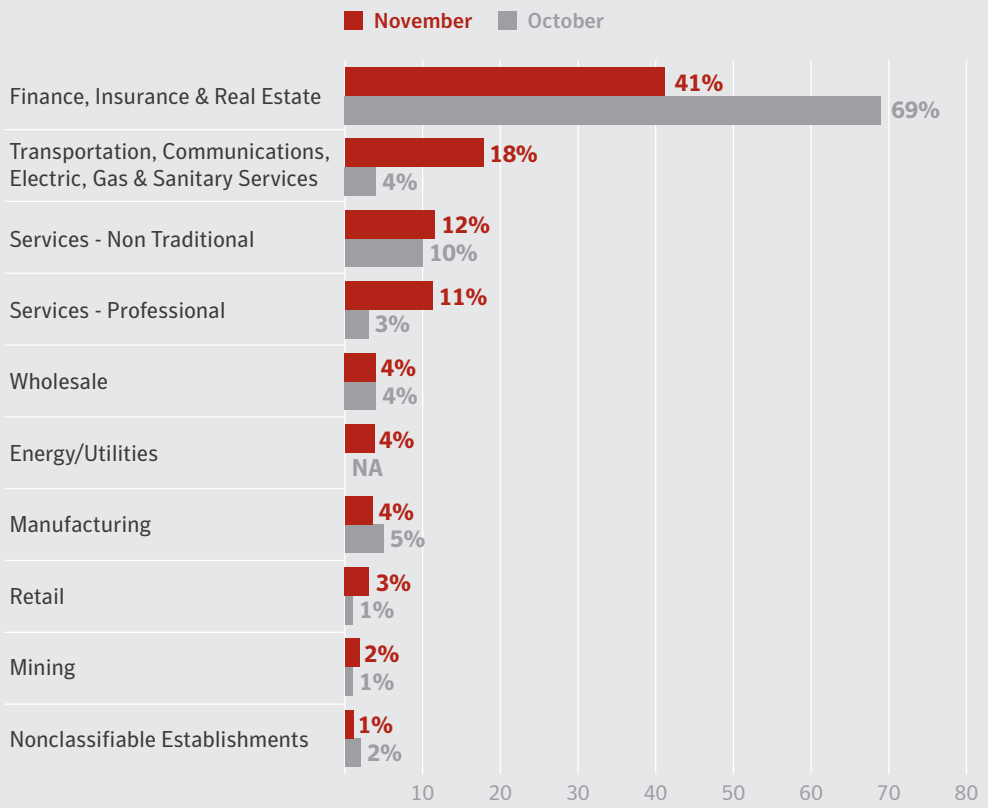
About the Security Response blog

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

NOVEMBER IN NUMBERS

Targeted Attacks & Phishing



Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec

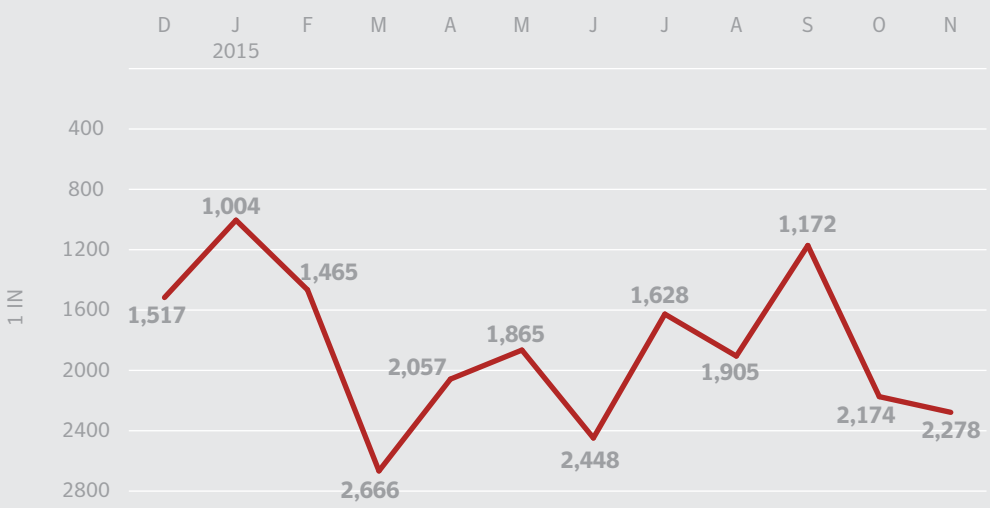
The Finance, Insurance, & Real Estate sector was the most targeted sector during November, comprising 41 percent of all targeted attacks.

Company Size	November	October
1-250	24.9%	19.7%
251-500	4.1%	5.2%
501-1000	12.9%	2.6%
1001-1500	4.5%	3.7%
1501-2500	3.8%	0.9%
2501+	49.9%	67.9%

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec

Large enterprises were the target of 49.9 percent of spear-phishing attacks in November. Similarly, 24.9 percent of attacks were directed at small businesses 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 2,278 emails was a phishing attempt.*

Industry	November	October
Agriculture, Forestry, & Fishing	1 in 1,224.4	1 in 1,082.9
Nonclassifiable Establishments	1 in 1,464.9	1 in 1,036.9
Public Administration	1 in 1,575.0	1 in 1,397.0
Services - Professional	1 in 1,787.8	1 in 2,011.3
Mining	1 in 2,104.3	1 in 1,957.6
Finance, Insurance, & Real Estate	1 in 2,377.8	1 in 2,262.6
Services - Non Traditional	1 in 2,539.8	1 in 2,466.1
Wholesale	1 in 2,603.3	1 in 2,431.5
Construction	1 in 2,983.3	1 in 2,486.5
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 3,717.1	1 in 3,016.4

Proportion of Email Traffic Identified as Phishing by Industry Sector

Source: Symantec.cloud

- *Agriculture, Forestry, & Fishing topped the list of industries with the highest proportion of phishing attempts during the month of November.*

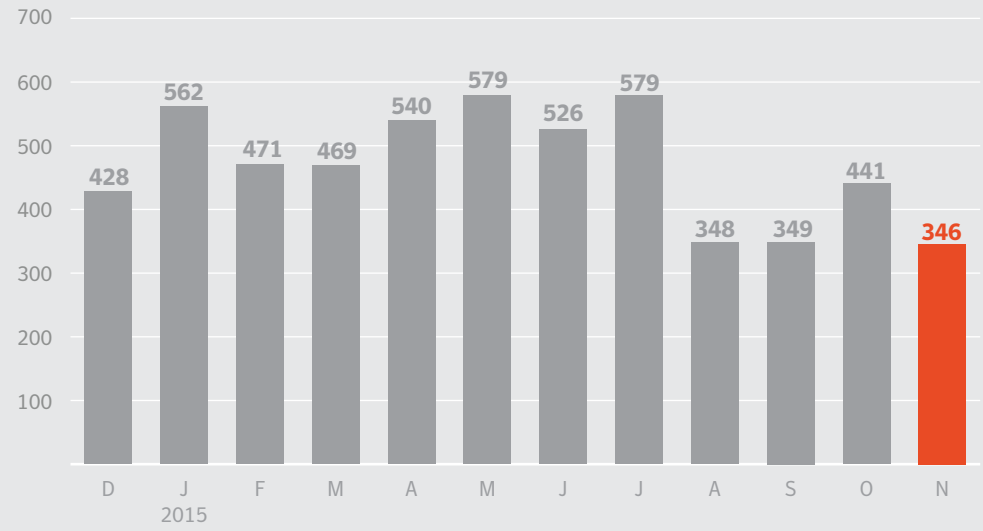
Company Size	November	October
1–250	1 in 2,131.3	1 in 2,015.2
251–500	1 in 1,765.7	1 in 1,856.5
501–1000	1 in 2,131.2	1 in 2,028.0
1001–1500	1 in 2,863.9	1 in 2,609.2
1501–2500	1 in 1,619.1	1 in 1,654.4
2501+	1 in 2,569.4	1 in 2,421.4

Proportion of Email Traffic Identified as Phishing by Organization Size

Source: Symantec.cloud

- *Companies with 1501-2500 employees were the most targeted organization size in November for phishing attempts.*

Vulnerabilities

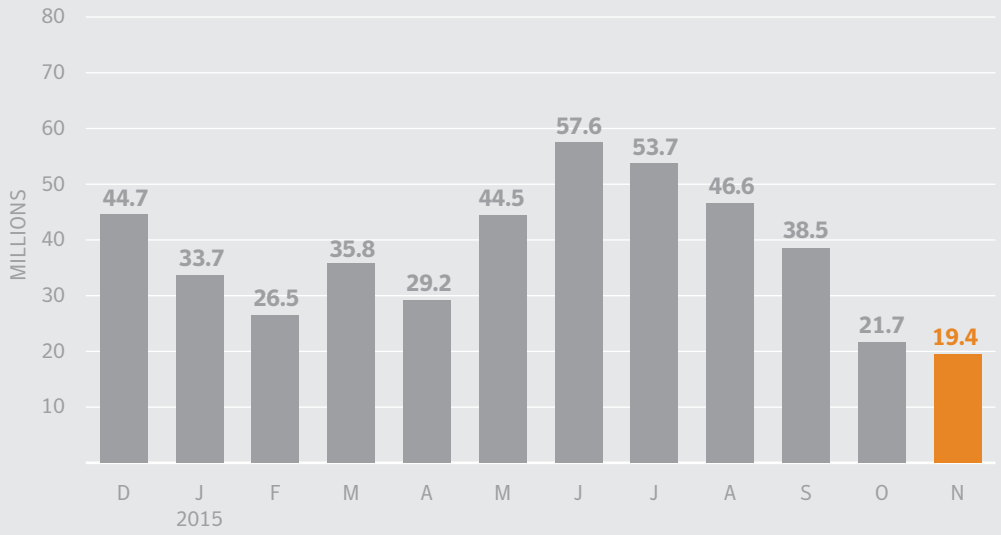


Total Number of Vulnerabilities

Source: Symantec

- *The number of vulnerabilities disclosed decreased in November, from 441 in October to 346 reported during this month.*

Malware



New Malware Variants

Source: Symantec

- *There were 19.4 million new pieces of malware created in November. This rate has steadily declined in the second half of 2015, from a high of 57.6 million seen in June.*

Rank	Malware Name	November Percentage	Malware Name	October Percentage
1	W32.Ramnit!html	7.6%	W32.Ramnit!html	7.0%
2	W32.Almanahe.B!inf	6.0%	W32.Almanahe.B!inf	5.8%
3	W32.Sality.AE	5.5%	W32.Sality.AE	5.7%
4	W32.Ramnit.B	4.0%	W32.Downadup.B	4.0%
5	W32.Downadup.B	3.6%	W32.Ramnit.B	4.0%
6	W97M.Downloader	3.1%	W32.Ramnit.B!inf	2.8%
7	W32.Ramnit.B!inf	3.0%	W32.Virut.CF	1.7%
8	W32.Virut.CF	1.7%	W97M.Downloader	1.6%
9	W32.Chir.B@mm(html)	1.7%	W32.SillyFDC.BDP!lnk	1.4%
10	Trojan.Swifi	1.3%	W32.Chir.B@mm(html)	1.4%

Top 10 Malware

Source: Symantec

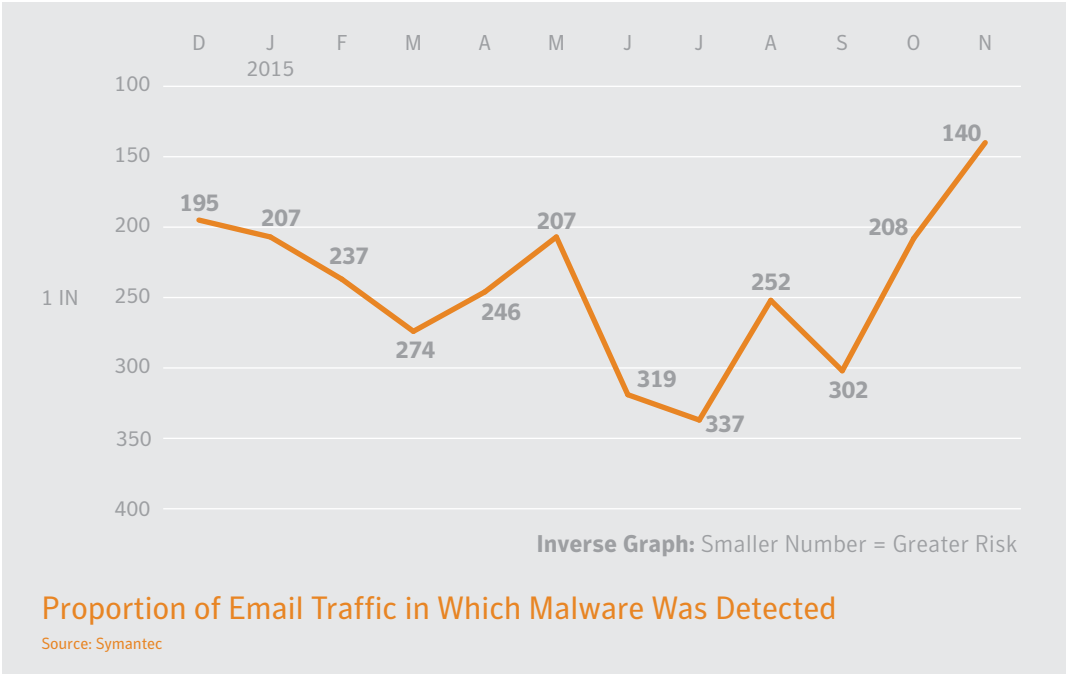
- *W32.Ramnit!html and W32.Almanahe.B!inf continue to be the most commonly seen malware detections in November.*

Rank	Malware Name	November Percentage	Malware Name	October Percentage
1	OSX.CnetDownloader	82.6%	OSX.Sudoprint	42.0%
2	OSX.Sudoprint	4.5%	OSX.RSPlug.A	9.9%
3	OSX.RSPlug.A	1.9%	OSX.Klog.A	6.1%
4	OSX.Klog.A	1.7%	OSX.CnetDownloader	5.8%
5	OSX.Sabpab	1.4%	OSX.Wirelurker	5.5%
6	OSX.Keylogger	1.4%	OSX.Flashback.K	5.4%
7	OSX.Okaz	0.9%	OSX.Luaddit	3.9%
8	OSX.Wirelurker	0.9%	OSX.Keylogger	3.6%
9	OSX.Luaddit	0.8%	OSX.Exploit.Launchd	3.0%
10	OSX.Remoteaccess	0.7%	OSX.Okaz	2.4%

Top 10 Mac OS X Malware Blocked on OS X Endpoints

Source: Symantec

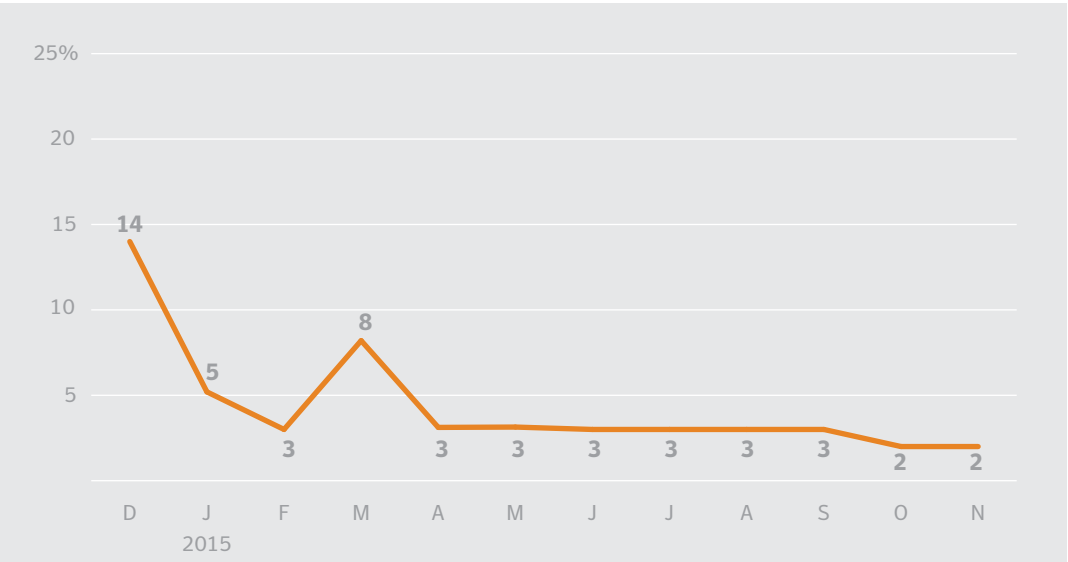
- *OSX.CnetDownloader was the most commonly seen OS X threat on OS X endpoints in November.*



Proportion of Email Traffic in Which Malware Was Detected

Source: Symantec

- *The proportion of email traffic containing malware increased this month, where one in 140 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 two percent.*

Industry	November	October
Public Administration	1 in 85.6	1 in 148.0
Services - Professional	1 in 103.2	1 in 188.5
Agriculture, Forestry, & Fishing	1 in 104.2	1 in 172.3
Wholesale	1 in 145.2	1 in 195.5
Construction	1 in 145.6	1 in 220.2
Services - Non Traditional	1 in 154.5	1 in 209.6
Finance, Insurance, & Real Estate	1 in 163.1	1 in 288.3
Mining	1 in 195.0	1 in 296.7
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 204.1	1 in 345.7
Nonclassifiable Establishments	1 in 206.9	1 in 340.3

Proportion of Email Traffic Identified as Malicious by Industry Sector

Source: Symantec.cloud

- *Public Administration was the most targeted sector in November for email malware, where one in every 85.6 emails contained malware.*

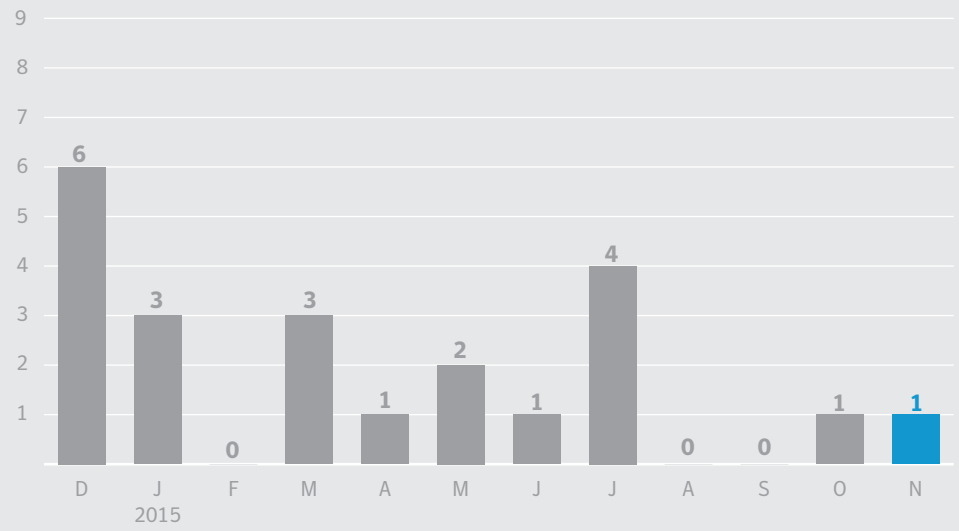
Company Size	November	October
1-250	1 in 109.3	1 in 144.3
251-500	1 in 93.7	1 in 158.9
501-1000	1 in 122.5	1 in 200.5
1001-1500	1 in 143.8	1 in 228.4
1501-2500	1 in 139.8	1 in 236.8
2501+	1 in 190.4	1 in 307.1

Proportion of Email Traffic Identified as Malicious by Organization Size

Source: Symantec.cloud

- *Organizations with 251-500 employees were most likely to be targeted by malicious email in the month of November, where one in 93.7 emails was malicious.*

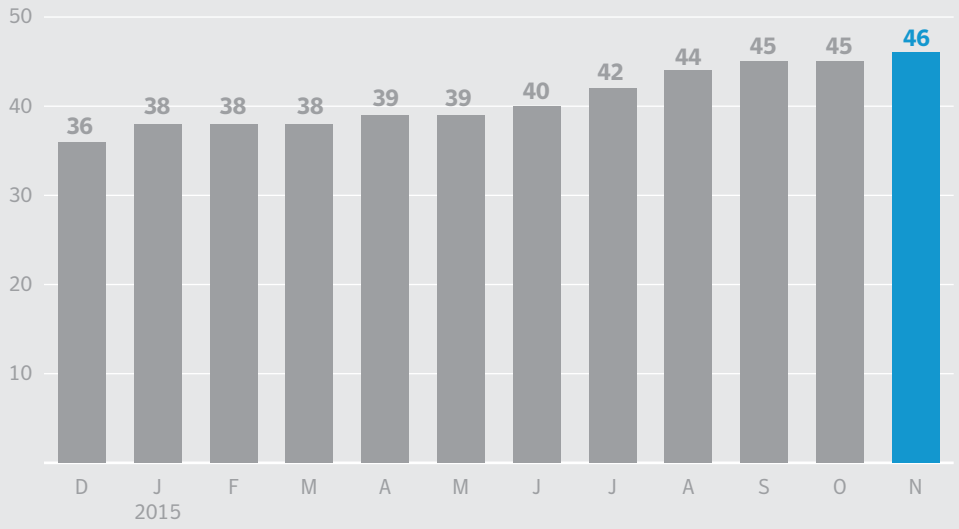
Mobile & Social Media



Android Mobile Malware Families by Month

Source: Symantec

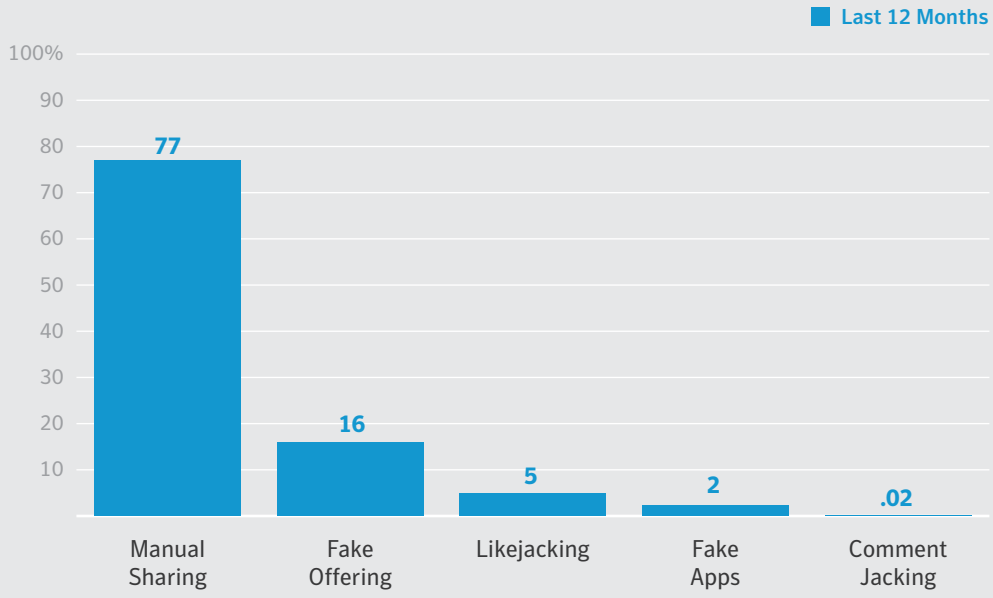
- *In November there was one new mobile malware family discovered.*



New Android Variants per Family by Month

Source: Symantec

- *There was an average of 46 Android malware variants per family in the month of in November.*



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, 77 percent of social media threats required end users to propagate them.*
- *Fake offerings comprised 16 percent of social media threats.*

Spam

54.1%
+.6% pts
November

53.5%
+1.3% pts
October

52.2%
-.5% pts
September

Overall Email Spam Rate

Source: Symantec

- *The overall email spam rate in November was 54.1 percent, up 0.6 percentage points from October.*

Industry	November	October
Mining	57.0%	57.8%
Manufacturing	55.5%	55.4%
Services - Non Traditional	55.2%	52.7%
Construction	55.0%	54.0%
Agriculture, Forestry & Fishing	54.7%	53.9%
Public Administration	54.7%	52.7%
Services - Professional	54.2%	53.9%
Retail	54.1%	54.2%
Nonclassifiable Establishments	53.6%	53.6%
Wholesale	53.4%	53.2%

Proportion of Email Traffic Identified as Spam by Industry Sector

Source: Symantec.cloud

- *At 57 percent, the Mining sector again had the highest spam rate during November. The Manufacturing sector came in second with 55.5 percent.*

Company Size	November	October
1–250	54.8%	53.4%
251–500	54.9%	54.4%
501–1000	54.0%	53.8%
1001–1500	54.2%	53.2%
1501–2500	54.0%	53.7%
2501+	53.5%	53.3%

Proportion of Email Traffic Identified as Spam by Organization Size

Source: Symantec.cloud

- *While most organization sizes had around a 54 percent spam rate, organizations with 251-500 employees had the highest rate at 54.9 percent.*

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

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