Symantec

SYMANTEC INTELLIGENCE REPORT

OCTOBER 2015

Welcome to the October 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 number of vulnerabilities disclosed increased in October, from 349 in September to 441 reported during this month. However, vulnerability disclosures have trended lower over the last three months when comparing the last year's worth of monthly disclosures.

The number of new malware variants also appears to be lower than what has been seen over the last 12 month period. There were 21.7 million new pieces of malware created in October, which is down from the high for 2015 of 57.6 million seen back in June.

However, not everything is trending downward. Crypto-ransomware was up once again during October, setting another high for 2015, with 44 thousand instances seen during the month.

Spam also appears to have been increasing slightly over the last few months, reaching a six-month high of 53.5 percent. Spam rates appeared to have bottomed out during June, which saw the lowest spam levels seen in over a decade, but have increased slightly since.

In terms of targeted attacks, the Finance, Insurance, & Real Estate sector was the most targeted sector during October, comprising 69 percent of all targeted attacks. Large enterprises were the target of 67.9 percent of spear-phishing attacks as well, up from 45.7 percent in September.

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

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

Dridex Takedown Sinks Botnet Infections

International police action hits gang that specialized in stealing banking credentials.

By Symantec Security Response

An international law enforcement crackdown against the Dridex botnet has seen one man charged and a coordinated effort to sinkhole thousands of compromised computers, cutting them off from the botnet's control. The operation, which involved the FBI in the US, the UK National Crime Agency, and a number of other international agencies, may seriously disrupt a cybercrime enterprise which has stolen tens of millions of dollars from victims worldwide.

Potent financial threat

Dridex, which is detected by Symantec as W32.Cridex and also known as Bugat, is a financial threat that adds the infected computer to a botnet and injects itself into the victim's web browser in order to steal information, including banking credentials.

The malware is usually spread through phishing emails designed to appear to come from legitimate sources in order to lure the victim into opening a malicious attachment. It is also capable of self-replication by copying itself to mapped network drives and attached local storage such as USB keys. As is common with most financial attackers, the Dridex group regularly changed its tactics and most recently has been observed using malicious macros in Microsoft Office documents attached to emails to infect computers.

As reported in Symantec's State of financial Trojans 2014 whitepaper, Dridex was the third largest financial threat last year, accounting for some 29,000 detections. Nevertheless, this represented a decrease, with the number of infections down 88 percent since 2012.

Recent telemetry suggests that the threat has enjoyed something of a resurgence in activity, with detections beginning to increase again in the past few months.

The attackers behind Dridex have targeted a broad range of countries. The largest number of detections in 2015 was in the US. This was followed by Japan and Germany, with significant numbers of infections also seen in the UK, Canada, Australia, and a number of other European countries.

Law enforcement swoop

Yesterday's operation saw a 30-year-old Moldovan man charged by prosecutors in the US for offenses including criminal conspiracy, unauthorized computer access with intent to defraud, damaging a computer, wire fraud, and bank fraud. His extradition to the US is currently being sought following his arrest in Cyprus in August.

The FBI also obtained an injunction permitting it to start sinkholing Dridex infections by redirecting traffic from infected computers away from command-and-control (C&C) servers to benign substitute servers. This sinkholing operation is also being supported by the UK National Crime Agency.

This is the latest in a series of recent takedowns against major financial fraud cybercrime groups, following earlier operations against Gameover Zeus, Shylock, and Ramnit.

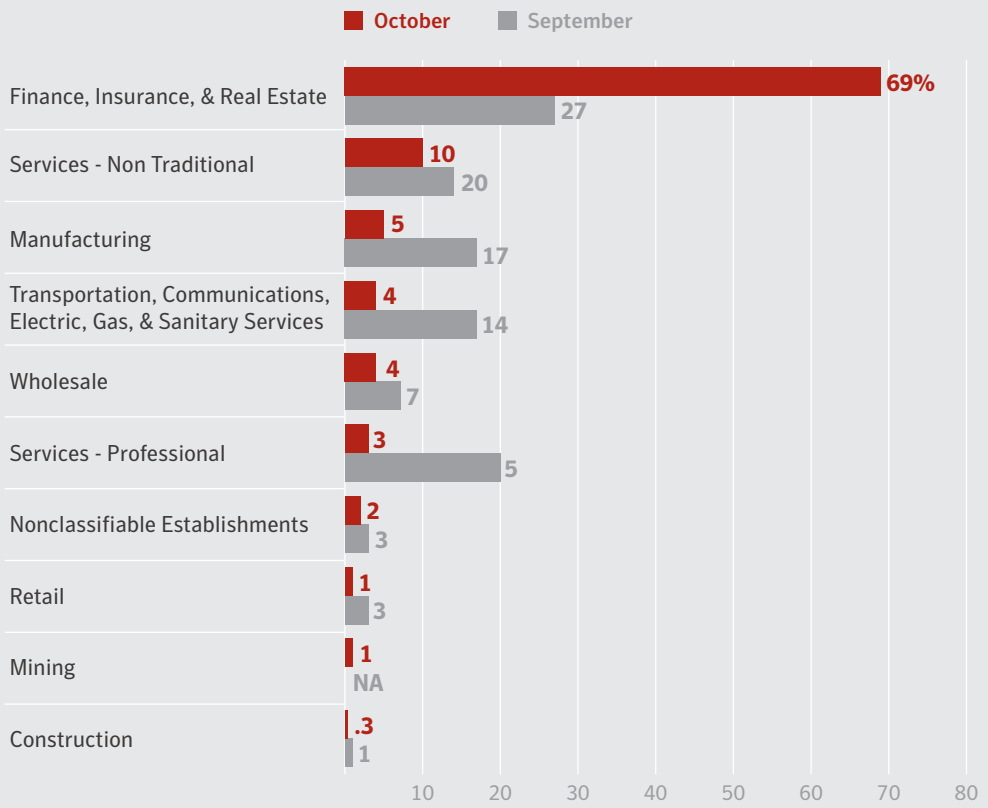
About the Security Response blog

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

OCTOBER IN NUMBERS

Targeted Attacks & Phishing



Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec

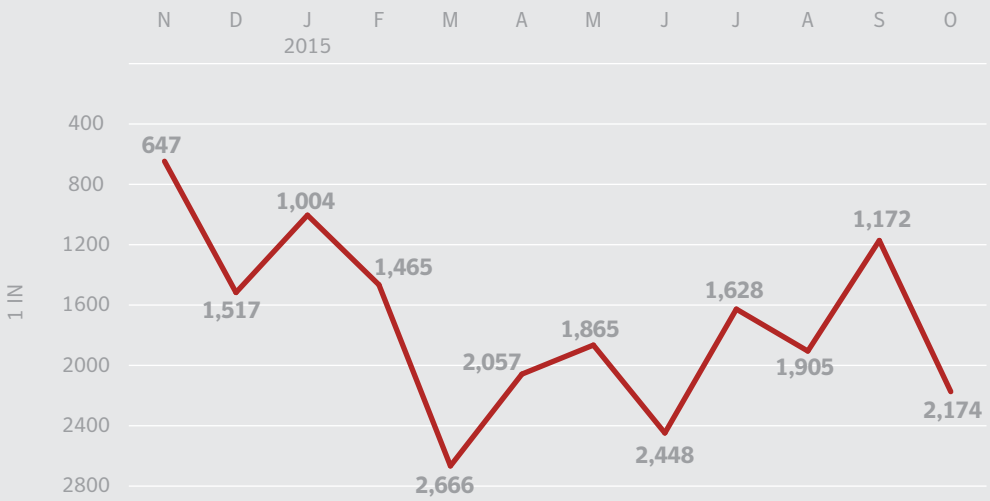
- *The Finance, Insurance, & Real Estate sector was the most targeted sector during October, comprising 69 percent of all targeted attacks.*

Company Size	October	September
1-250	19.7%	34.5%
251-500	5.2%	6.6%
501-1000	2.6%	7.2%
1001-1500	3.7%	3.8%
1501-2500	0.9%	2.1%
2501+	67.9%	45.7%

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec

- *Large enterprises were the target of 67.9 percent of spear-phishing attacks in October, up from 45.7 percent in September. Similarly, 19.7 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 2,174 emails was a phishing attempt.*

Industry	October	September
Nonclassifiable Establishments	1 in 1,036.9	1 in 1,006.4
Agriculture, Forestry, & Fishing	1 in 1,082.9	1 in 988.0
Public Administration	1 in 1,397.0	1 in 1,353.2
Mining	1 in 1,957.6	1 in 2,062.9
Services - Professional	1 in 2,011.3	1 in 1,194.4
Finance, Insurance, & Real Estate	1 in 2,262.6	1 in 1,888.1
Wholesale	1 in 2,431.5	1 in 2,303.3
Services - Non Traditional	1 in 2,466.1	1 in 2,210.3
Construction	1 in 2,486.5	1 in 2,324.9
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 3,016.4	1 in 2,828.2

Proportion of Email Traffic Identified as Phishing by Industry Sector

Source: Symantec.cloud

- *Nonclassifiable Establishments topped the list of industries with the highest proportion of phishing attempts during the month of October.*

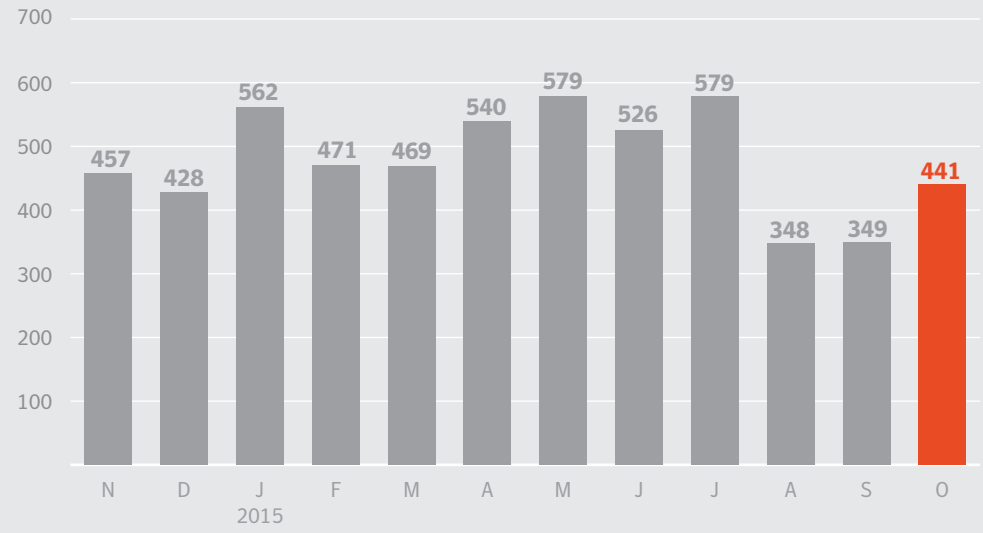
Company Size	October	September
1–250	1 in 2,015.2	1 in 723.4
251–500	1 in 1,856.5	1 in 1,703.2
501–1000	1 in 2,028.0	1 in 1,874.8
1001–1500	1 in 2,609.2	1 in 2,169.5
1501–2500	1 in 1,654.4	1 in 1,998.8
2501+	1 in 2,421.4	1 in 1,715.3

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 October for phishing attempts.*

Vulnerabilities

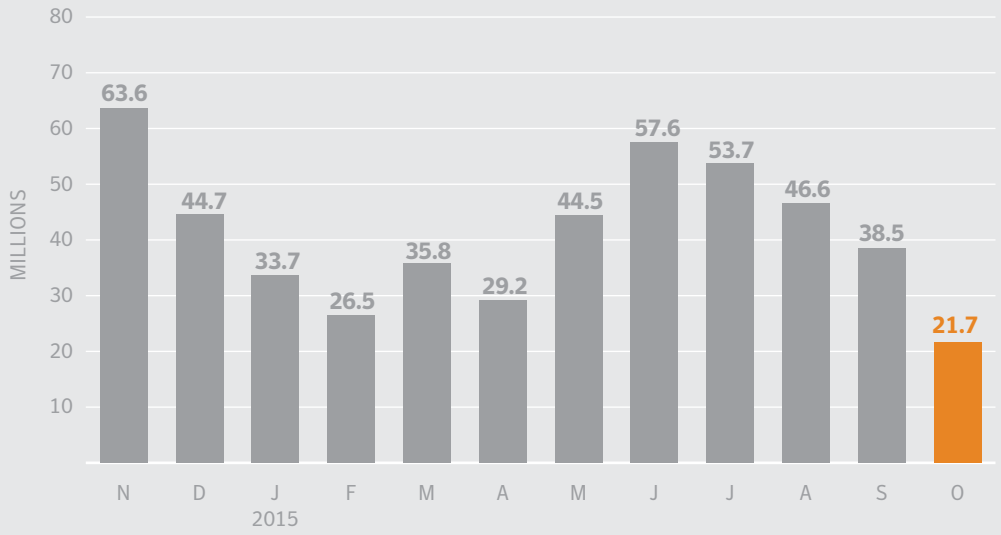


Total Number of Vulnerabilities

Source: Symantec

- *The number of vulnerabilities disclosed increased in October, from 349 in September to 441 reported during this month.*

Malware



New Malware Variants

Source: Symantec

- *There were 21.7 million new pieces of malware created in October, down from the high for 2015 of 57.6 million seen in June.*

Rank	Malware Name	October Percentage	Malware Name	September Percentage
1	W32.Ramnit!html	7.0%	W32.Ramnit!html	7.8%
2	W32.Almanahe.B!inf	5.8%	W32.Almanahe.B!inf	6.3%
3	W32.Sality.AE	5.7%	W32.Sality.AE	5.6%
4	W32.Downadup.B	4.0%	W32.Downadup.B	4.1%
5	W32.Ramnit.B	4.0%	W32.Ramnit.B	3.9%
6	W32.Ramnit.B!inf	2.8%	W32.Ramnit.B!inf	3.5%
7	W32.Virut.CF	1.7%	W32.Virut.CF	1.8%
8	W97M.Downloader	1.6%	W32.Chir.B@mm(html)	1.6%
9	W32.SillyFDC.BDP!lnk	1.4%	Trojan.Swifi	1.4%
10	W32.Chir.B@mm(html)	1.4%	W97M.Downloader	1.3%

Top 10 Malware

Source: Symantec

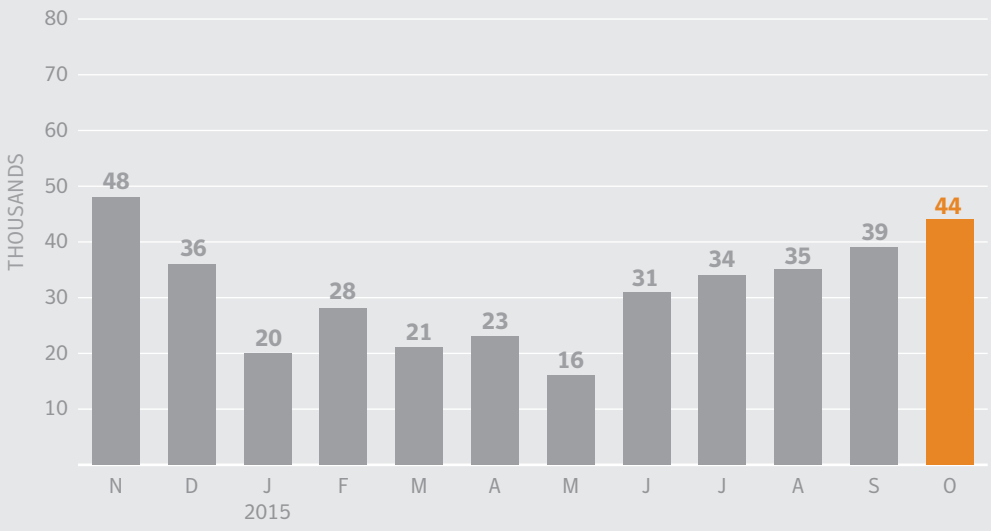
- *W32.Ramnit!html and W32.Almanahe.B!inf continue to be the most commonly seen malware detections in October.*

Rank	Malware Name	October Percentage	Malware Name	September Percentage
1	OSX.Sudoprint	42.0%	OSX.Sudoprint	81.6%
2	OSX.RSPlug.A	9.9%	OSX.RSPlug.A	3.1%
3	OSX.Klog.A	6.1%	OSX.Klog.A	2.5%
4	OSX.CnetDownloader	5.8%	OSX.Wirelurker	1.9%
5	OSX.Wirelurker	5.5%	OSX.Keylogger	1.7%
6	OSX.Flashback.K	5.4%	OSX.Flashback.K	1.4%
7	OSX.Luaddit	3.9%	OSX.Luaddit	1.4%
8	OSX.Keylogger	3.6%	OSX.Remoteaccess	1.1%
9	OSX.Exploit.Launchd	3.0%	OSX.Netweird	0.7%
10	OSX.Okaz	2.4%	OSX.Okaz	0.6%

Top 10 Mac OS X Malware Blocked on OS X Endpoints

Source: Symantec

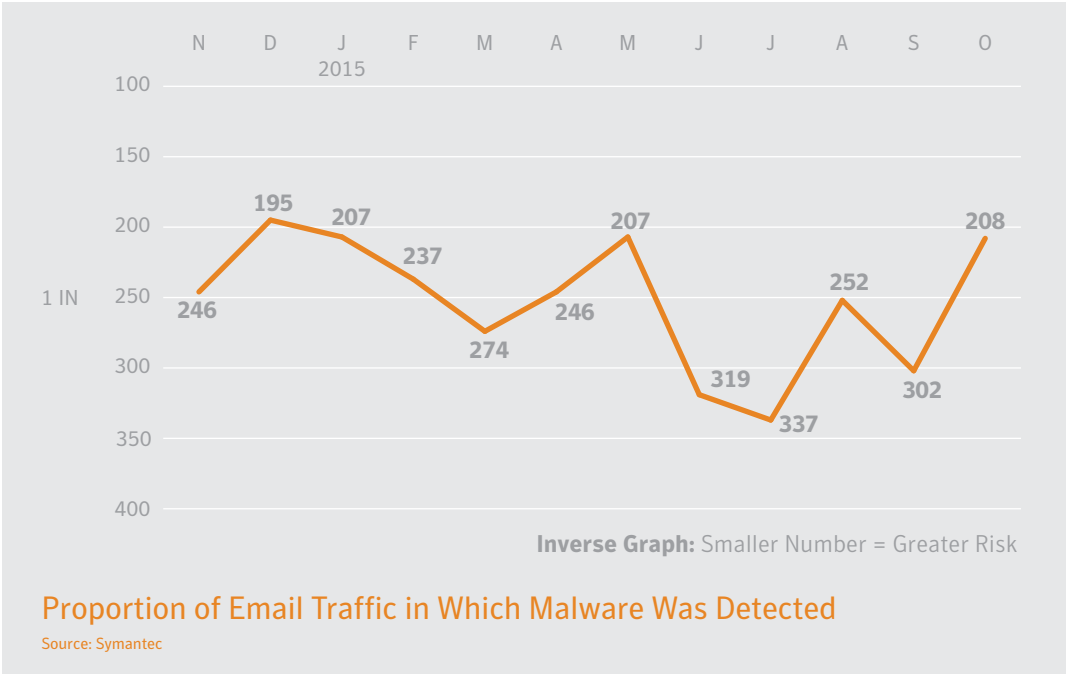
- *OSX.Sudoprint was again the most commonly seen OS X threat on OS X endpoints in October. This threat takes advantage of a vulnerability targeting the OS X operating system that was patched in August.*



Crypto-Ransomware Over Time

Source: Symantec

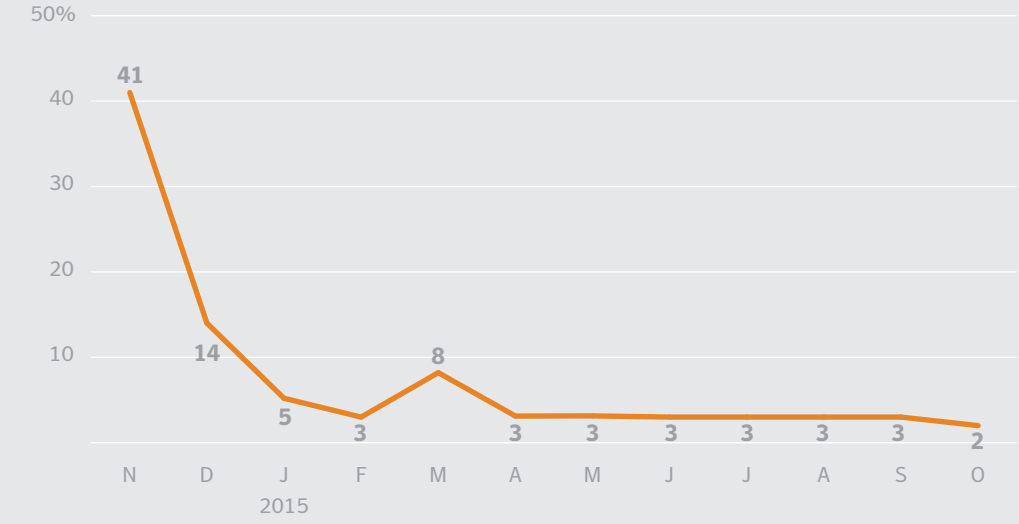
- *Crypto-ransomware was up during October, setting another high for 2015.*



Proportion of Email Traffic in Which Malware Was Detected

Source: Symantec

- *The proportion of email traffic containing malware increased this month, where one in 208 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	October	September
Public Administration	1 in 148.0	1 in 422.3
Agriculture, Forestry, & Fishing	1 in 172.3	1 in 307.9
Services - Professional	1 in 188.5	1 in 400.7
Wholesale	1 in 195.5	1 in 455.5
Services - Non Traditional	1 in 209.6	1 in 603.0
Construction	1 in 220.2	1 in 441.1
Finance, Insurance, & Real Estate	1 in 288.3	1 in 394.1
Mining	1 in 296.7	1 in 471.5
Nonclassifiable Establishments	1 in 340.3	1 in 586.2
Transportation, Communications, Electric, Gas, & Sanitary Services	1 in 345.7	1 in 606.1

Proportion of Email Traffic Identified as Malicious by Industry Sector

Source: Symantec.cloud

- *Public Administration was the most targeted sector in October for email malware, where one in every 148 emails contained malware.*

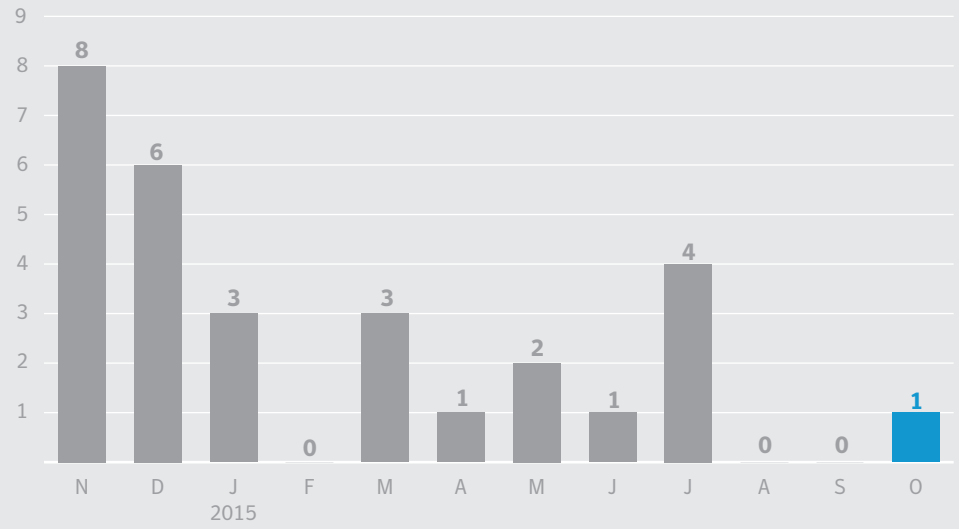
Company Size	October	September
1-250	1 in 144.3	1 in 165.0
251-500	1 in 158.9	1 in 374.4
501-1000	1 in 200.5	1 in 460.6
1001-1500	1 in 228.4	1 in 489.2
1501-2500	1 in 236.8	1 in 542.2
2501+	1 in 307.1	1 in 596.6

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 October, where one in 144.3 emails was malicious.*

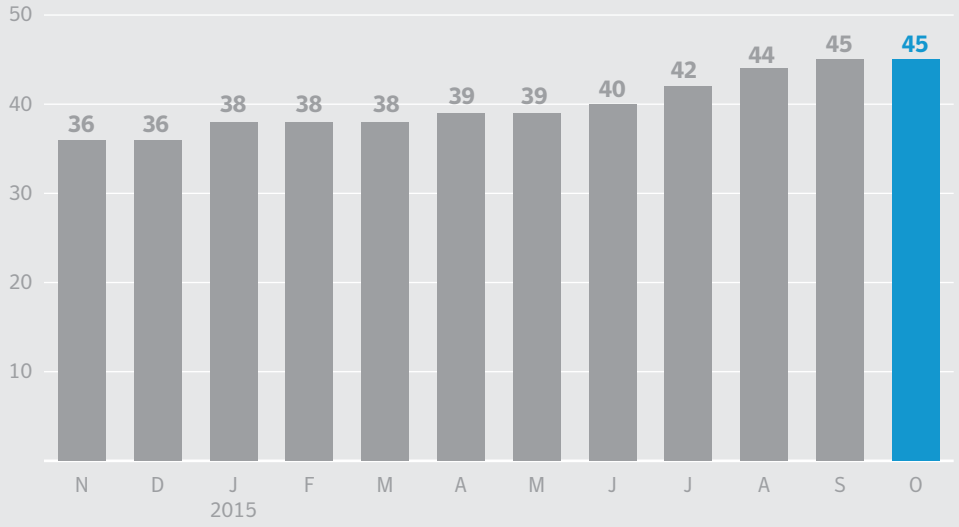
Mobile & Social Media



Android Mobile Malware Families by Month

Source: Symantec

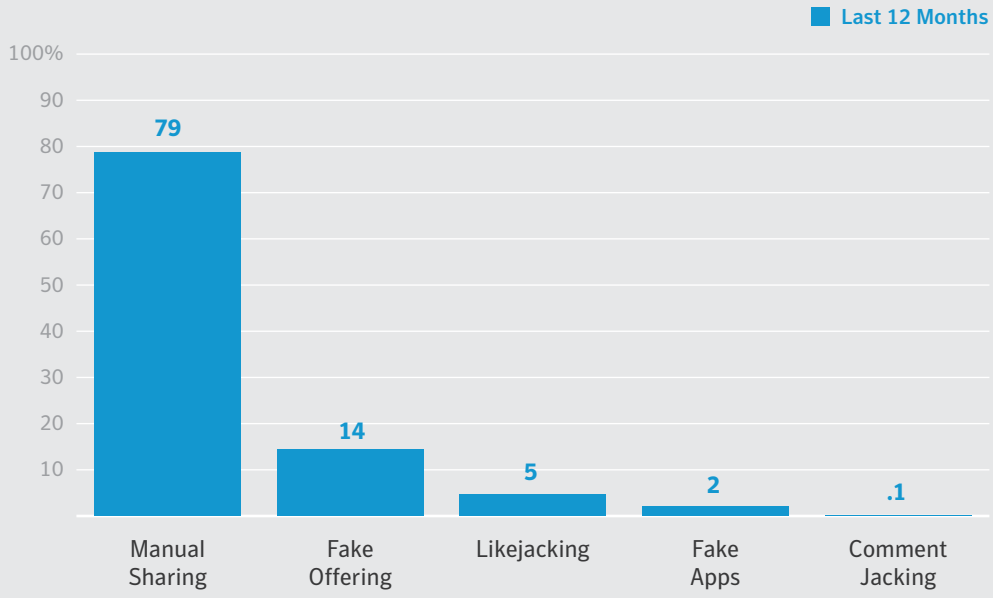
- *In October there was one new mobile malware family discovered.*



New Android Variants per Family by Month

Source: Symantec

- *There was an average of 45 Android malware variants per family in the month of in October.*



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

53.5%
+1.3% pts
October

52.2%
-.5% pts
September

52.7%
+2.4% pts
August

Overall Email Spam Rate

Source: Symantec

- *The overall email spam rate in October was 53.5 percent, up 1.3 percentage points from September.*

Industry	October	September
Mining	57.8%	55.7%
Manufacturing	55.4%	53.7%
Retail	54.2%	52.6%
Construction	54.0%	52.7%
Services - Professional	53.9%	52.7%
Agriculture, Forestry, & Fishing	53.9%	52.1%
Nonclassifiable Establishments	53.6%	51.7%
Wholesale	53.2%	52.1%
Services - Non Traditional	52.7%	51.8%
Public Administration	52.7%	–

Proportion of Email Traffic Identified as Spam by Industry Sector

Source: Symantec.cloud

- *At 57.8 percent, the Mining sector again had the highest spam rate during October. The Manufacturing sector came in second with 55.4 percent.*

Company Size	October	September
1–250	53.4%	52.3%
251–500	54.4%	52.5%
501–1000	53.8%	52.4%
1001–1500	53.2%	51.9%
1501–2500	53.7%	52.1%
2501+	53.3%	52.2%

Proportion of Email Traffic Identified as Spam by Organization Size

Source: Symantec.cloud

- *While most organization sizes had around a 53 percent spam rate, organizations with 251-500 employees had the highest rate at 54.4 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