McAfee
Together is power.

McAfee Labs Threat Report

December 2017

THREATS STATISTICS

Malware

Incidents

Web and Network Threats

The McAfee Labs count of new malware in Q3 reached an all-time high of 57.6 million new samples, an increase of 10% from Q2.

Introduction

Welcome to the McAfee Labs Threats Report. In this edition, we highlight the statistics gathered by McAfee Labs in Q3 of 2017. The biggest number of the quarter is our count of new malware, which reached an all-time high of 57.6 million new samples, an increase of 10% from Q2. The total count in the McAfee Labs sample database is now more than 780 million. New ransomware rose by 36% this quarter, largely from widespread Android screen-locking malware. The easy availability of exploit kits and dark web sources fuel the rapid creation of new malware.

Some of the biggest malware stories that McAfee covered in Q3 include the data breach at the Equifax credit reporting company; another data breach, through a misconfigured AWS server, at a Verizon customer support supplier; and a remote code execution vulnerability in Apache Struts, a popular component of many websites across the world.

Every quarter, the McAfee Global Threat Intelligence cloud dashboard allows us to see and analyze real-world attack patterns that lead to better customer protection. This information provides insight into attack volumes that our customers experience. See Page 9 for Q3 results.

—Raj Samani, Chief Scientist and McAfee Fellow, Advanced Threat Research Team

Stay Informed

Our Q3 report demonstrates an escalation in threats, not only in these stories and other reports but also in our statistics, which show increases across multiple categories. Staying informed of emerging threats and the tactics employed by malicious actors is essential. McAfee Labs is committed to helping our customers keep up to date. For more information on threats, follow us @McAfee_Labs.

This report was researched and written by:

- Niamh Minihane
- Francisca Moreno
- Eric Peterson
- Raj Samani
- Craig Schmugar
- Dan Sommer
- Bing Sun

Follow

Share

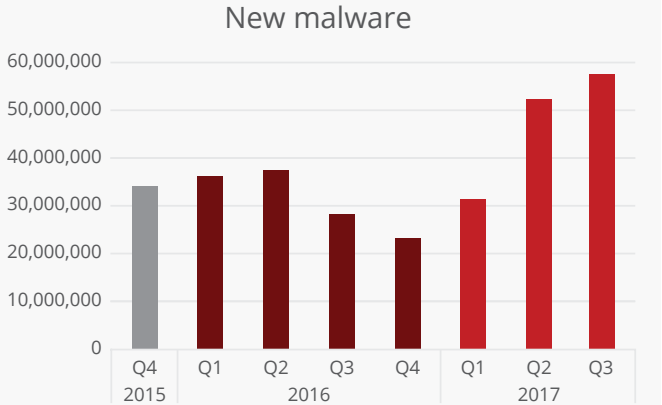
Threats Statistics

4 Malware

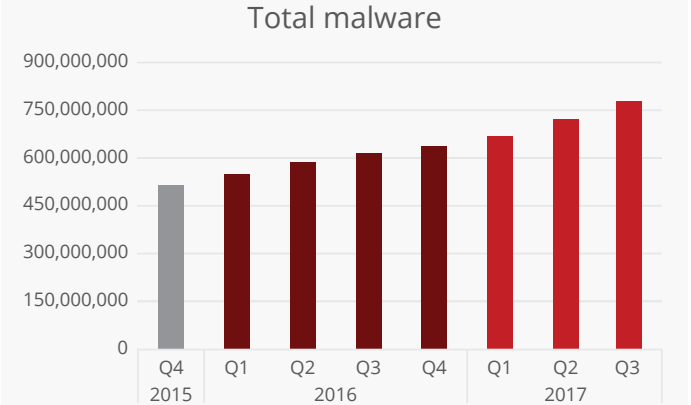
9 Incidents

11 Web and Network Threats

Malware

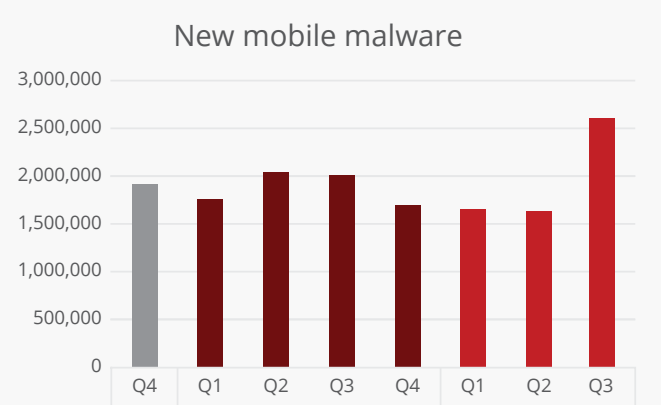


Source: McAfee Labs, 2017.

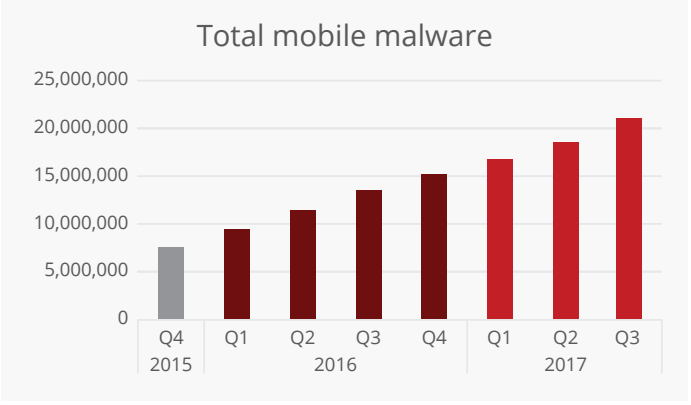


Source: McAfee Labs, 2017.

New malware increased by 10% in Q3, to a record high of 57.6 million samples.



Source: McAfee Labs, 2017.

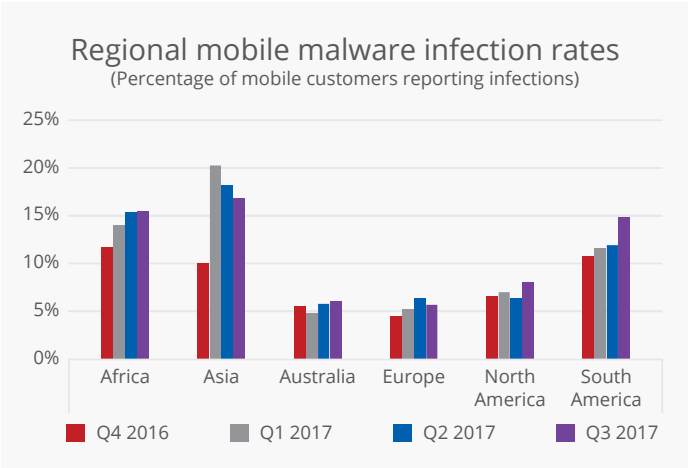


Source: McAfee Labs, 2017.

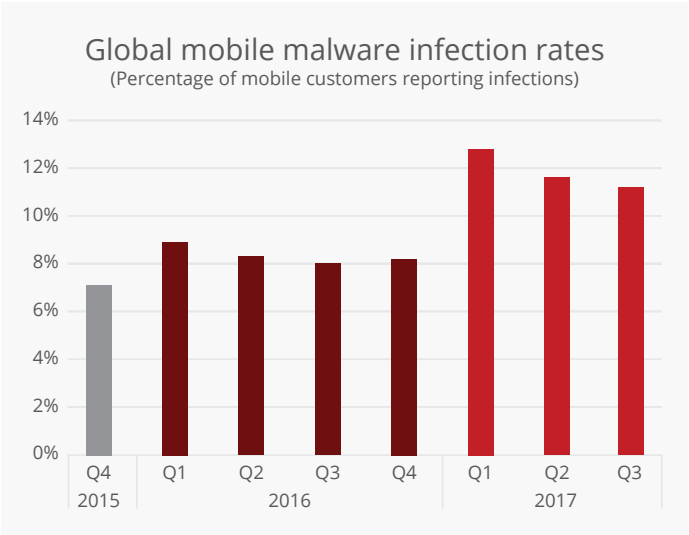
New mobile malware jumped by 60% in Q3, fueled by a big increase in Android screen-locking ransomware.

Follow

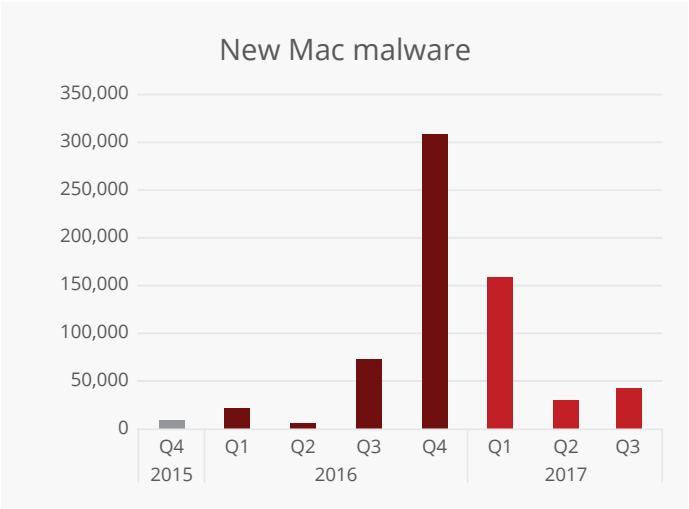
Share



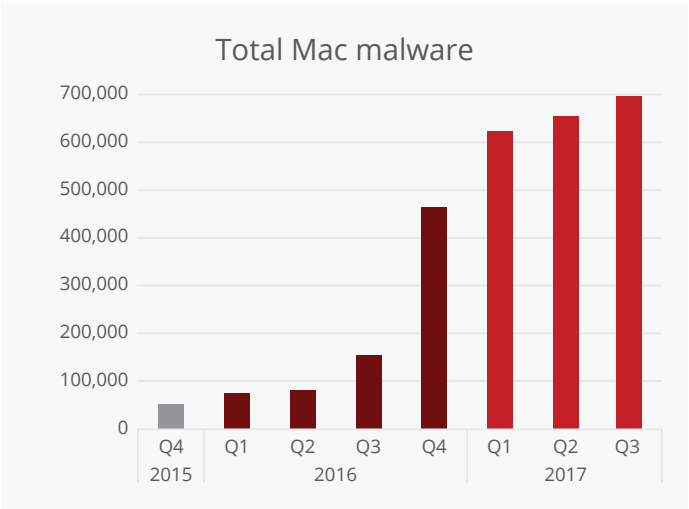
Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.



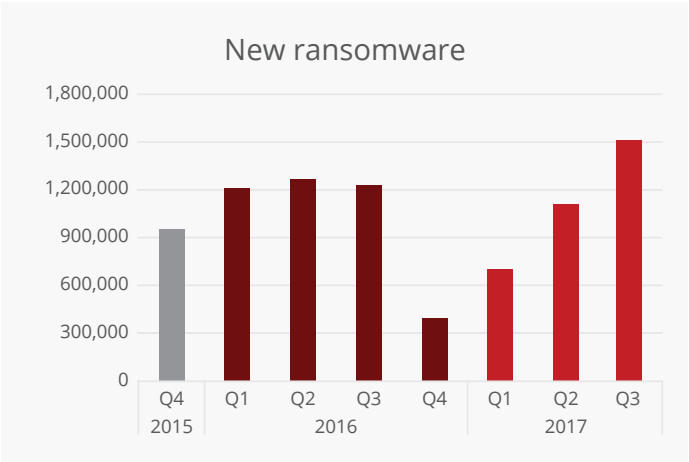
Source: McAfee Labs, 2017.



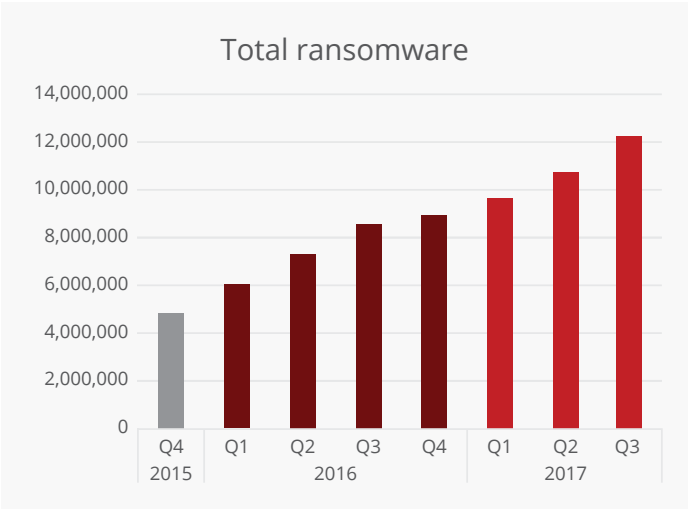
Source: McAfee Labs, 2017.

Follow

Share

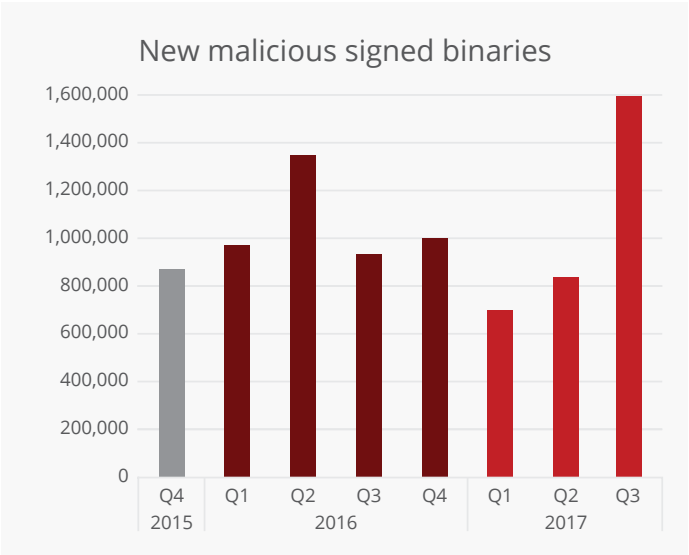


Source: McAfee Labs, 2017.

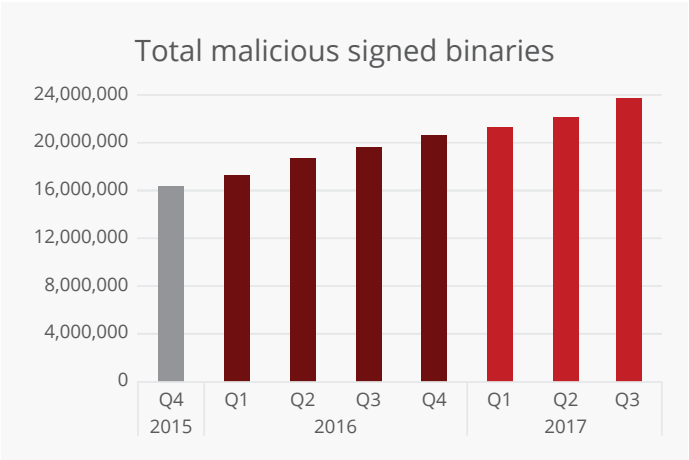


Source: McAfee Labs, 2017.

New ransomware rose by 36% in Q3, boosted by a big increase in Android screen-locking threats.



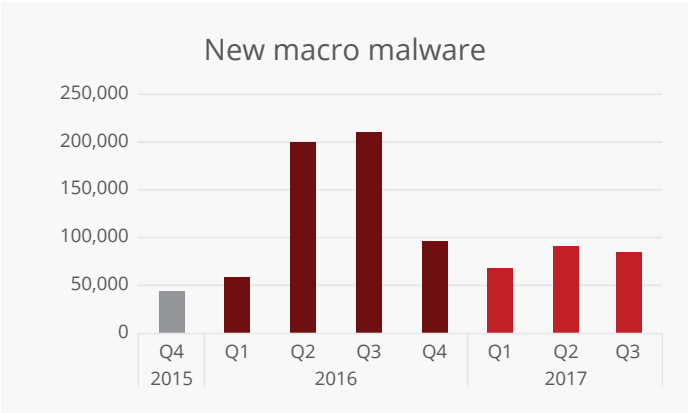
Source: McAfee Labs, 2017.



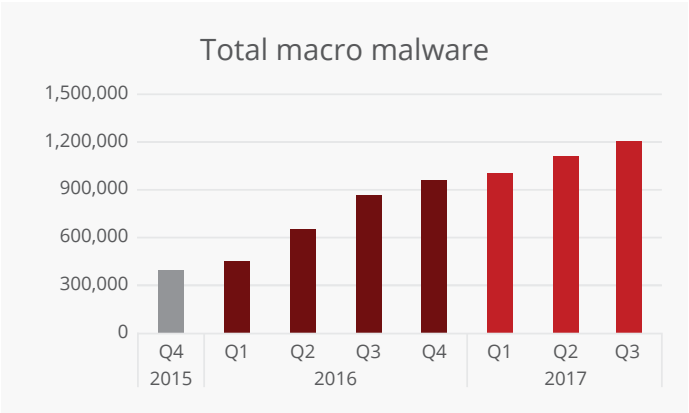
Source: McAfee Labs, 2017.

Follow

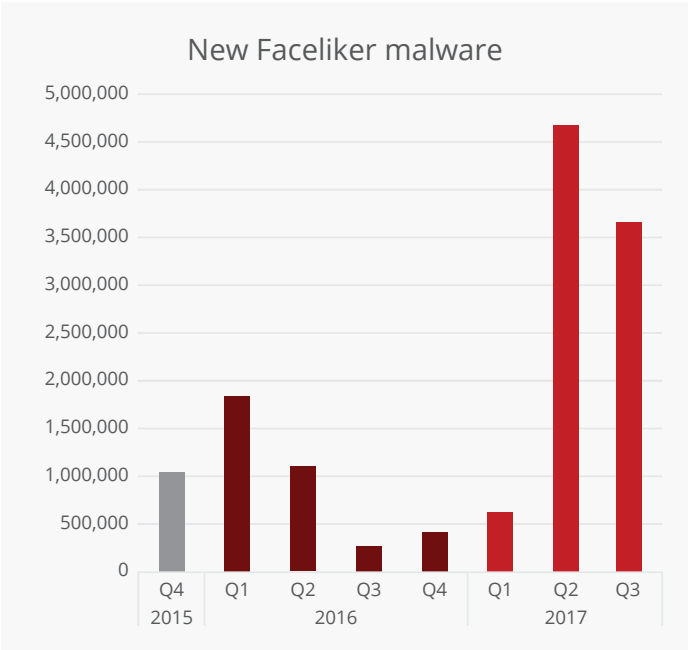
Share



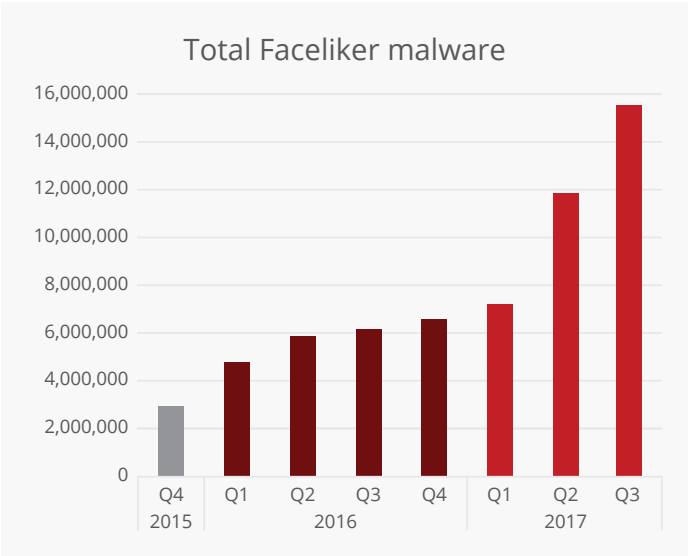
Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.

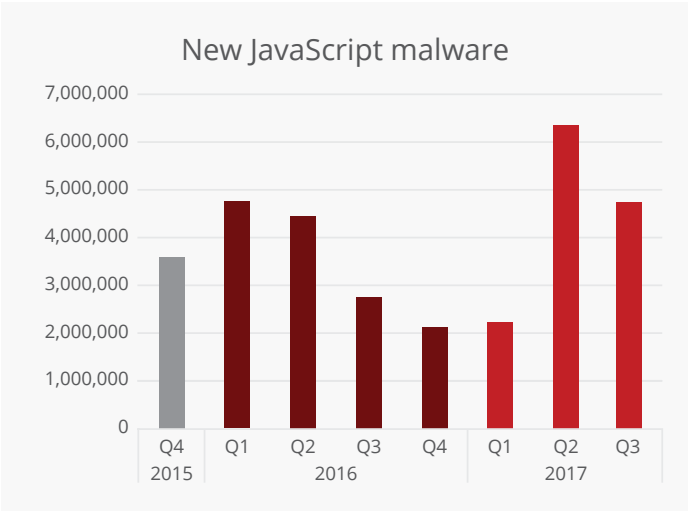


Source: McAfee Labs, 2017.

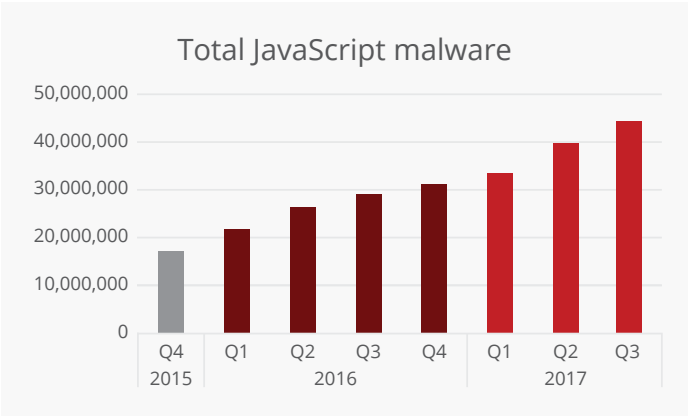
The Faceliker Trojan manipulates Facebook clicks to artificially "like" certain content. To learn more, read this post from McAfee Labs.

Follow

Share

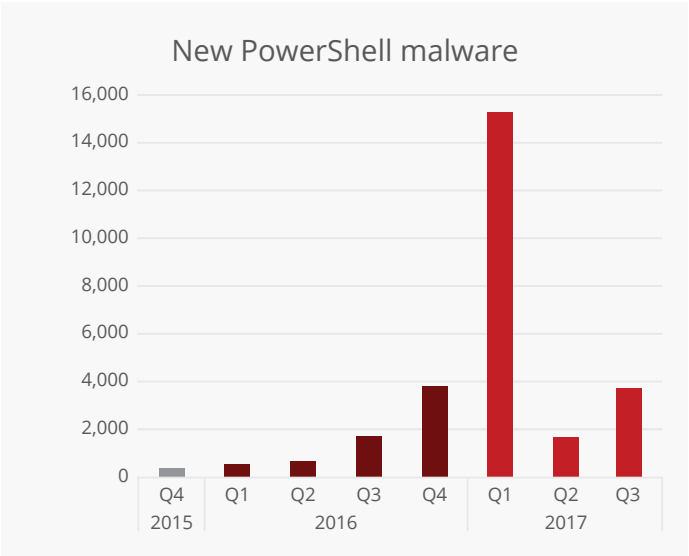


Source: McAfee Labs, 2017.

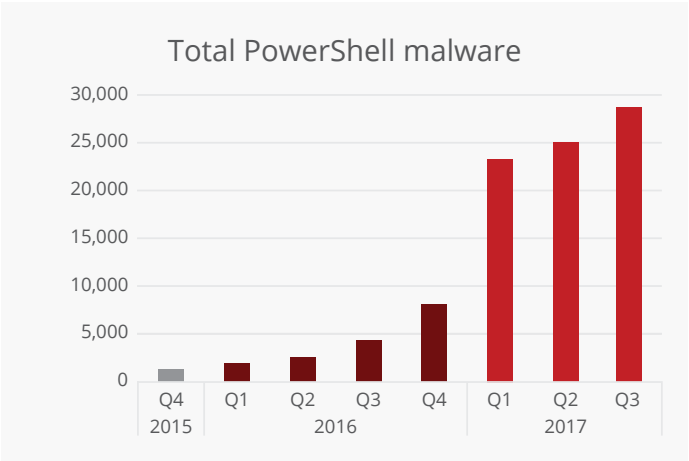


Source: McAfee Labs, 2017.

JavaScript malware fell by 26% in Q3 from an all-time high in Q2. For more on JavaScript threats, see "The rise of script-based malware," in the *McAfee Labs Threats Report, September 2017.*



Source: McAfee Labs, 2017.



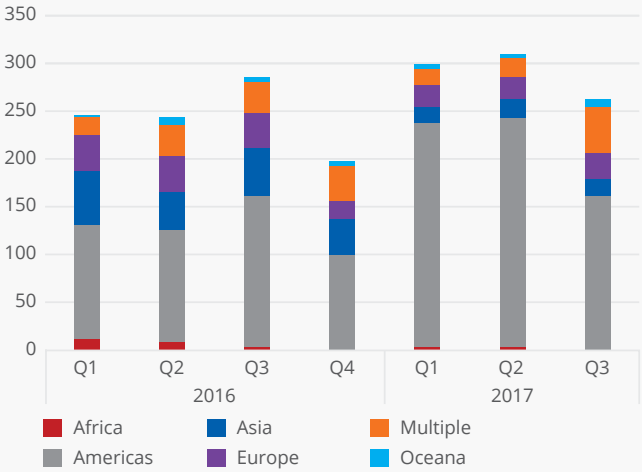
Source: McAfee Labs, 2017.

PowerShell malware more than doubled in Q3 compared with Q2. For more on PowerShell threats, see "The rise of script-based malware," in the *McAfee Labs Threats Report, September 2017.*

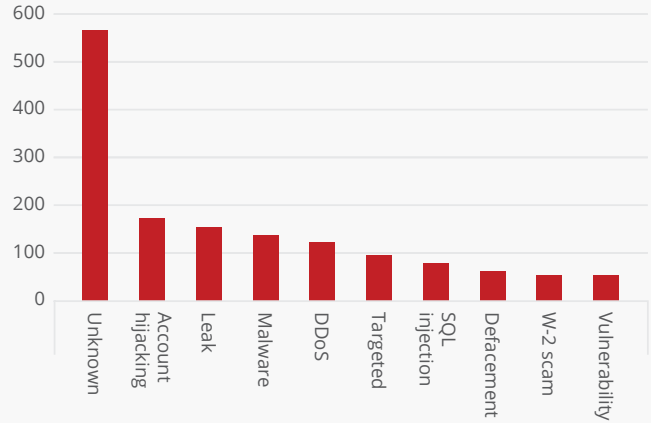
Follow

Share

Incidents



Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.

McAFEE GLOBAL THREAT INTELLIGENCE

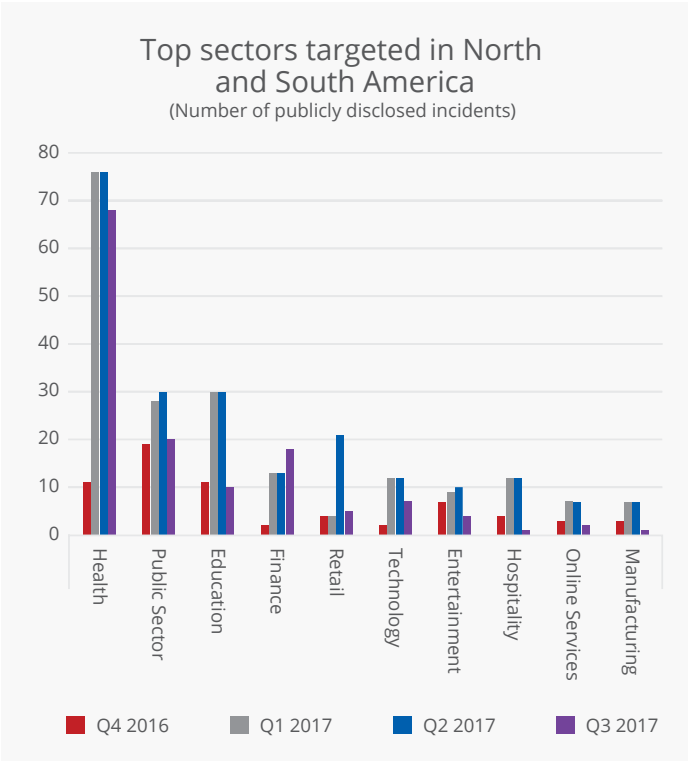
Every quarter, the McAfee Global Threat Intelligence cloud dashboard allows us to see and analyze real-world attack patterns that lead to better customer protection. This information provides insight into attack volumes that our customers experience. In Q3, our customers saw the following attack volumes:

- McAfee GTI received on average 45 billion queries per day in Q3.
- McAfee GTI protections against malicious files increased to 40 million per day in Q3 from 36 million in Q2.

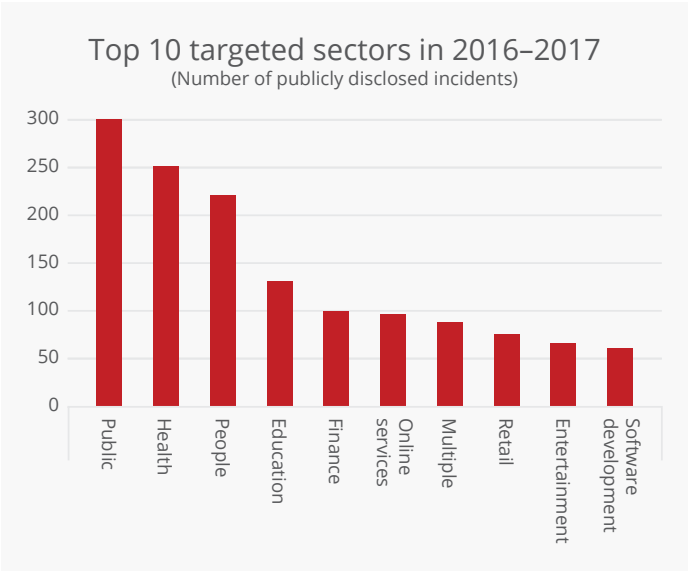
Continued on page 10.

Follow

Share



Source: McAfee Labs, 2017.



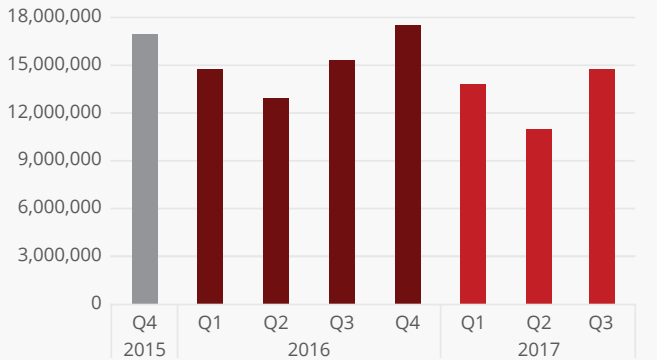
Source: McAfee Labs, 2017.

- McAfee GTI protections against potentially unwanted programs (PUPs) shows a decrease back to typical levels at 45 million per day in Q3 from an abnormal high of 77 million in Q2.
- McAfee GTI protections against medium-risk URLs shows an increase to 43 million per day in Q3 from 42 million in Q2.
- McAfee GTI protections against high-risk URLs shows an increase to 56 million per day in Q3 from 41 million in Q2.
- McAfee GTI protections against risky IP addresses shows a decrease to 48 million per day in Q3 from 58 million per day in Q2.

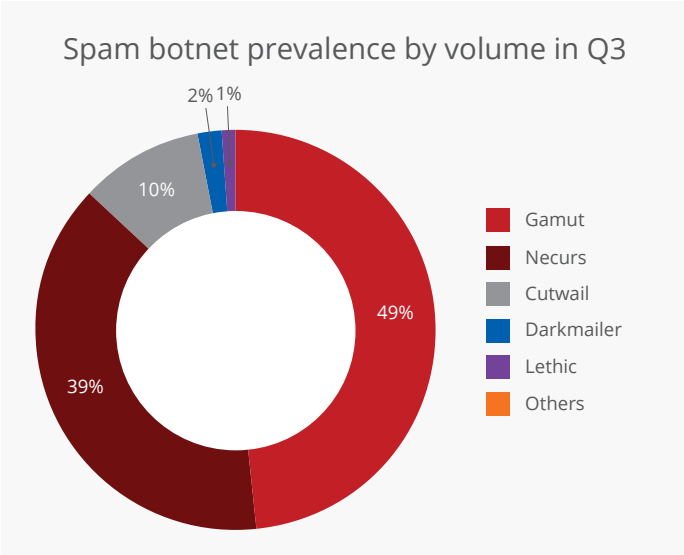
Follow

Share

Web and Network Threats

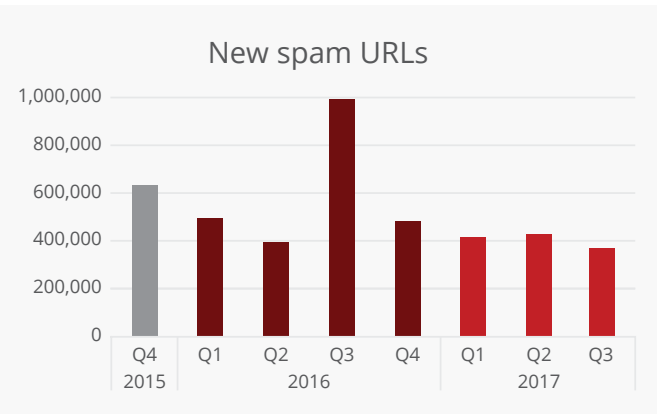


Source: McAfee Labs, 2017.

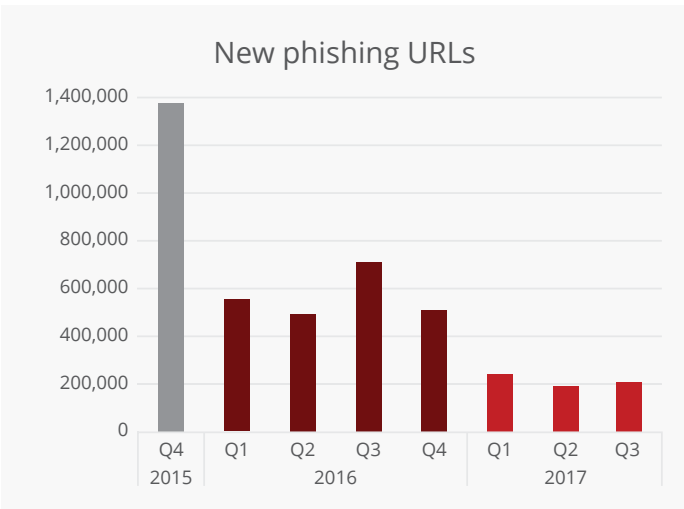


Source: McAfee Labs, 2017.

Gamut remains the most prevalent spamming botnet during Q3, with Necurs a close second. Necurs proliferated several Ykcol (Locky) ransomware campaigns with themes such as "Status Invoice," "Your Payment," and "Emailing: [Random Numbers] .JPG" during the quarter.



Source: McAfee Labs, 2017.

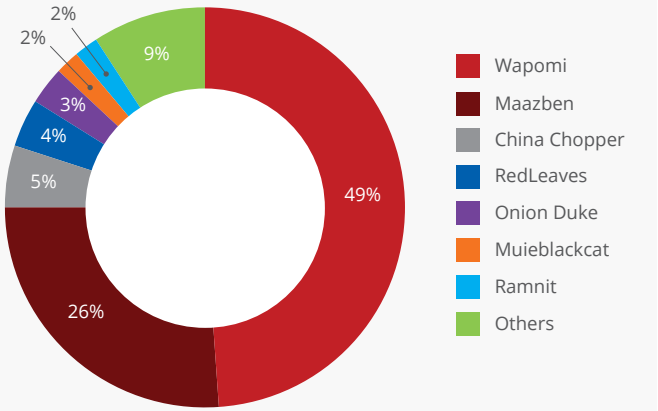


Source: McAfee Labs, 2017.

Follow

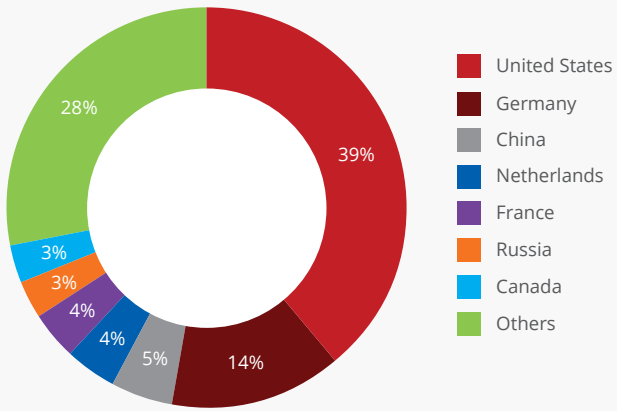
Share

Top malware connecting to control servers in Q3



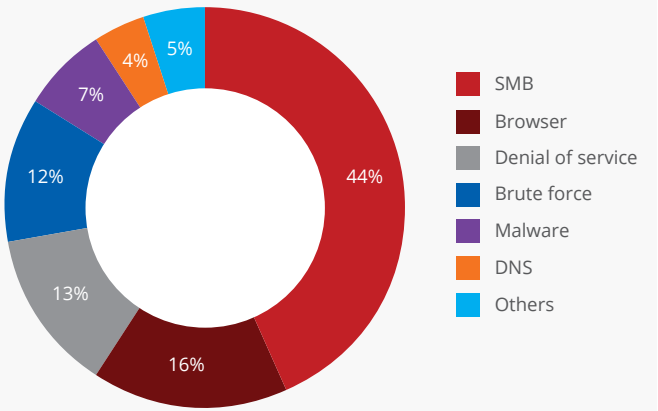
Source: McAfee Labs, 2017.

Top countries hosting botnet control servers in Q3



Source: McAfee Labs, 2017.

Top network attacks in Q3



Source: McAfee Labs, 2017.

Follow

Share

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

3708_1117_rp-threats-dec-2017
December 2017