REPORT

McAfee Together is power.

McAfee Labs Threats Report

March 2018

THREATS STATISTICS

Malware

Incidents

Web and Network Threats

The McAfee Labs count of new malware in Q4 reached an all-time high of 63.4 million new samples.

This report was researched and written by:

- Alex Bassett
- Christiaan Beek
- Niamh Minihane
- Eric Peterson
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

Introduction

Welcome to the *McAfee Labs Threats Report March 2018.* In this edition we highlight the news and statistics gathered in Q4 of 2017 by the McAfee Advanced Threat Research and McAfee Labs teams. We have seen a remarkable end to the year, not only with the threat statistics presented within this report, but also with the findings of some of our recent research.

One of the biggest developments in cybercrime is an increasing emphasis on cryptocurrency hijacking, which coincided with the increased market interest in digital currencies. The Q4 spike in Bitcoin value, which peaked in December at more than US$19,000 per coin, prompted many actors to extend their activities into the hijacking of Bitcoin and Monero wallets. This shift reinforces the point that cybercriminals will always seek to combine the highest returns in the shortest time with the least risk. Security researchers have also recently discovered Android apps used for cryptocurrency mining. We currently see discussions in underground forums that suggest moving from Bitcoin to Litecoin because the latter is a safer model with less chance of exposure.

Some cybercriminals are still developing botnets exploiting the Internet of Things and borrowing and developing new code. For now, we see these botnets mostly used for denial of service attacks. The challenge to the security industry will be to adequately defend against such attacks as they increase in bandwidth and frequency.

Follow

Share

Key trends: Cybercriminals pivot, taking on new strategies and tactics

In Q4 of 2017, McAfee Labs recorded on average eight new malware samples per second—an increase from four new samples per second in Q3. Overall, the quarter was characterized by newer tools and schemes, such as PowerShell malware and cryptocurrency mining, which surged along with the value of Bitcoin.

PowerShell: In 2017, McAfee Labs saw PowerShell malware grow by 267% in Q4, and by 432% year over year, as the threat category increasingly became a go-to toolbox for cybercriminals. The scripting language was irresistible, as attackers sought to use it within Microsoft Office files to execute the first stage of attacks.

In December, Operation Gold Dragon, a malware campaign targeting the 2018 Winter Olympics, was uncovered. The campaign is an exemplary implementation of PowerShell malware in an attack.

Cryptocurrency mining: Online currency fuels much of cybercrime, including malware purchases and ransomware payments. Cybercriminals would rather find outside computing power instead of using their own equipment because the price of a dedicated mining machine could exceed $5,000. In Q4 McAfee Advanced Threat Research team analysts reported on this growth industry, explaining how cybercriminals often seek to maliciously introduce malware that will either use a victim's computing power to mine for coins or simply locate and steal the user's cryptocurrency.

Ransomware: In 2017, McAfee Labs observed 59% increase in ransomware year over year, including 35% growth in Q4 alone. This activity included new creative tactics from cybercriminals, who pushed the category past its typical objective of extorting money to disruption within corporate networks. Actors devised strategies to create "smoke and mirrors" by distracting defenders from actual attacks, such as the emergence of pseudoransomware, seen in NotPetya and a Taiwan bank heist.

In spite of ransomware's continued growth, Q4 featured law enforcement successes against cybercriminal networks, with the arrest of the actors allegedly responsible for the spread of CTB Locker ransomware.

Follow

Share

The health care sector target: In 2017 the health care sector experienced a 210% increase in publicly disclosed security incidents compared with 2016, though incidents decreased by 78% in Q4. In analyzing the attacks, McAfee Advanced Threat Research experts concluded that many of the incidents were caused by failures to comply with security best practices or to address vulnerabilities in medical software.

Necurs and Gamut: In Q4, 97% of spam botnet traffic was driven by just two botnets that allow cybercriminals to rent access: Necurs, a recent purveyor of "lonely girl" spam, pump-and-dump stock spam, and Locky ransomware downloaders, surpassed Gamut, sender of job offer–themed phishing and money mule recruitment emails, as most prevalent spamming botnet.

STATISTICS

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. On average McAfee GTI analyzed each day 400,000 URLs and 800,000 files. In Q4, our customers saw the following attack volumes:

- McAfee GTI received on average 48 billion queries per day in Q4.
- McAfee GTI protections against malicious files increased to 45 million per day in Q4 from 40 million in Q3.
- McAfee GTI protections against risky URLs fell to 57 million per day in Q4 from 99 million in Q3, in spite of a sharp increase in high-risk URLs after December 19.
- McAfee GTI protections against risky IP addresses rose to 84 million per day in Q4 from 48 million per day in Q3.

Key campaigns: Asymmetrical cyberwarfare continues to escalate

At the beginning of 2017, McAfee analysts predicted the hard-to-solve challenges the cybersecurity industry would face in the coming year, naming the asymmetry of information as a major hurdle. In short, adversaries have the luxury of access to research done by the technical community, and can download and use open-source tools to support their campaigns, while the defenders' level of insight into cybercriminal activities is considerably more limited, and identifying evolving tactics often must take place after malicious campaigns have begun. Major attacks in Q4 demonstrated that growing asymmetrical cyberwarfare is in full effect.

November 2017: APT28, also known as Fancy Bear, leveraged a Microsoft Office Dynamic Data Exchange technique that had been made public just a few weeks earlier to launch in a phishing email campaign citing the New York City terror attacks.

December 2017: Attacks targeting organizations involved in the Winter Olympic Games in Pyeongchang leveraged steganography and a new tool released days before the attack, Invoke-PSImage. Operation Gold Dragon gained a persistent presence on victim's systems, giving attackers the ability to search at will and access data stored on the device or in connected cloud accounts.

To stay up to date with our research, check out our social media channel—Twitter @McAfee_Labs—where we provide analysis into new campaigns, as well as describe new tools that you can use to better protect your environment.

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

Twitter @Raj_Samani

Follow

Share

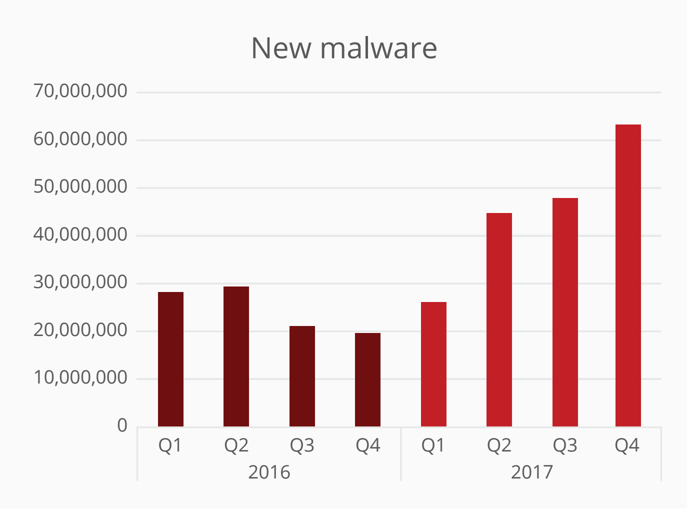
Threats Statistics

7 Malware

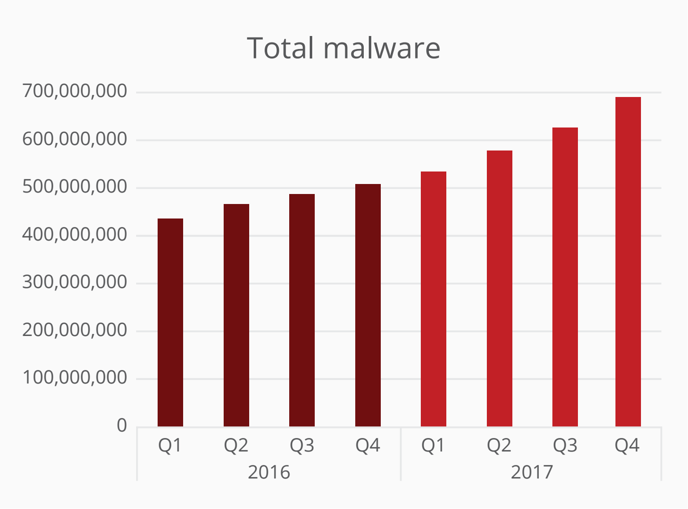
14 Incidents

16 Web and Network Threats

Malware

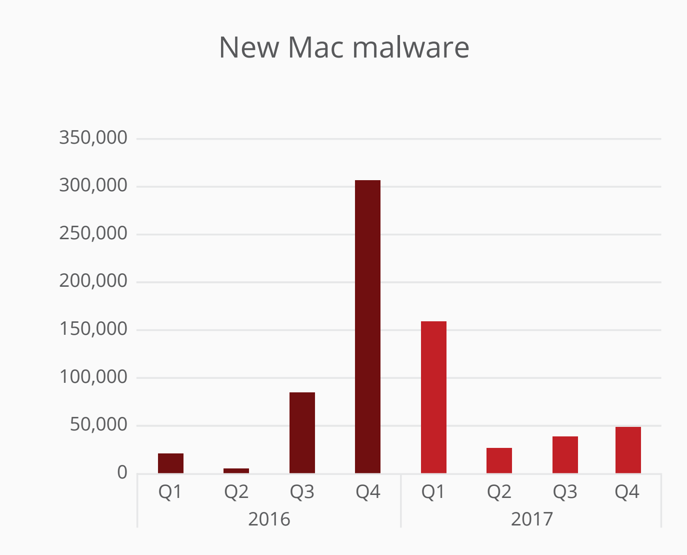


Source: McAfee Labs, 2018.

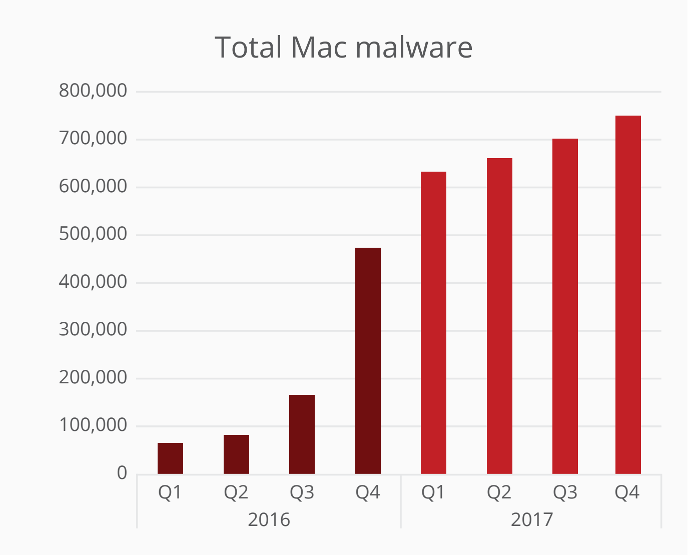


Source: McAfee Labs, 2018.

Malware data comes from the McAfee Sample Database, which includes malicious files gathered by McAfee spam traps, crawlers, and customer submissions, as well as from other industry sources. One of the leading threats this quarter was Waboot.



Source: McAfee Labs, 2018.

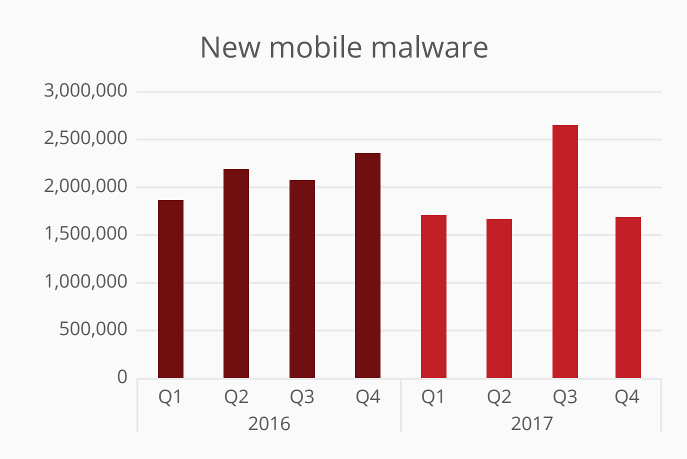


Source: McAfee Labs, 2018.

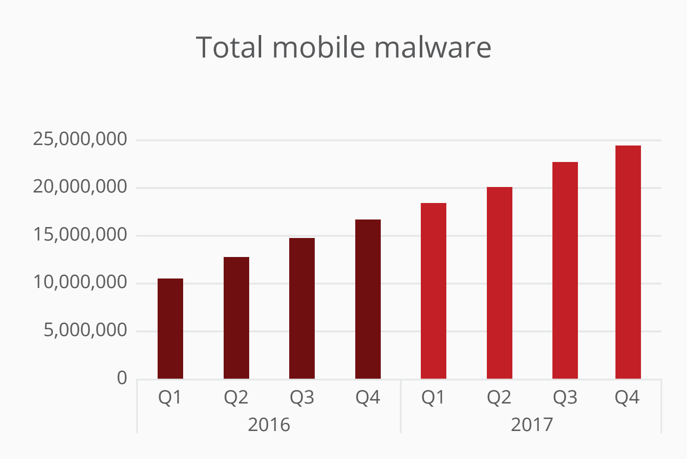
Two common forms of Mac malware this quarter were Flashback, which grabs passwords and other data through browsers, and Longage, which can give a hacker control of a system.

Follow

Share

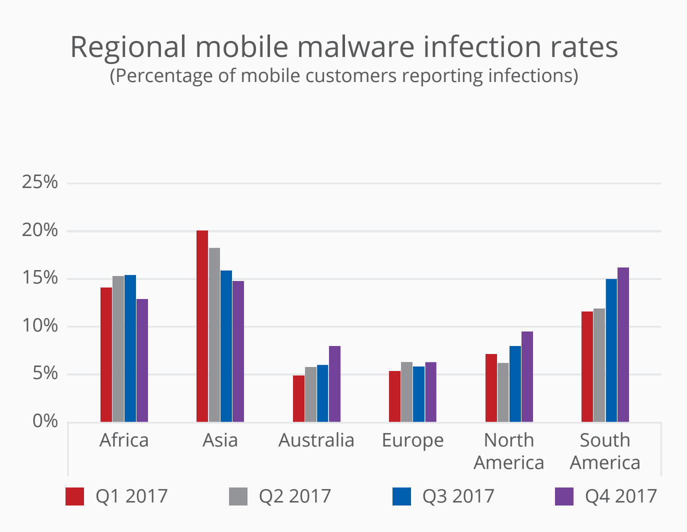


Source: McAfee Labs, 2018.

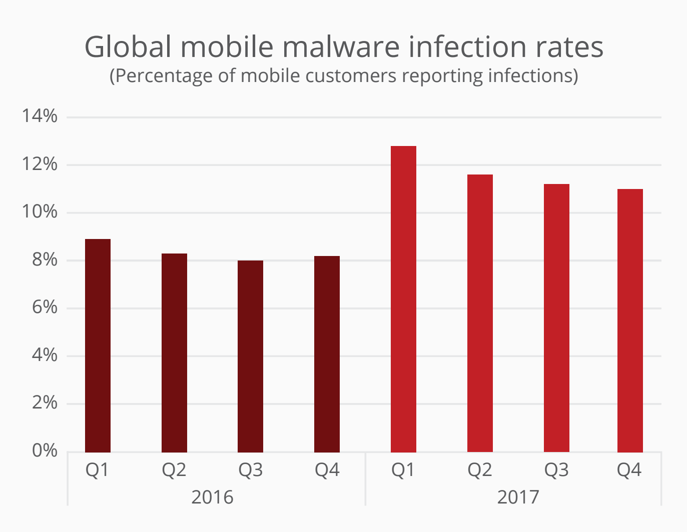


Source: McAfee Labs, 2018.

The growth of Android screen-locking ransomware declined significantly this quarter. (See separate charts on page 9.) The Piom Trojan dropper also slowed markedly.



Source: McAfee Labs, 2018.

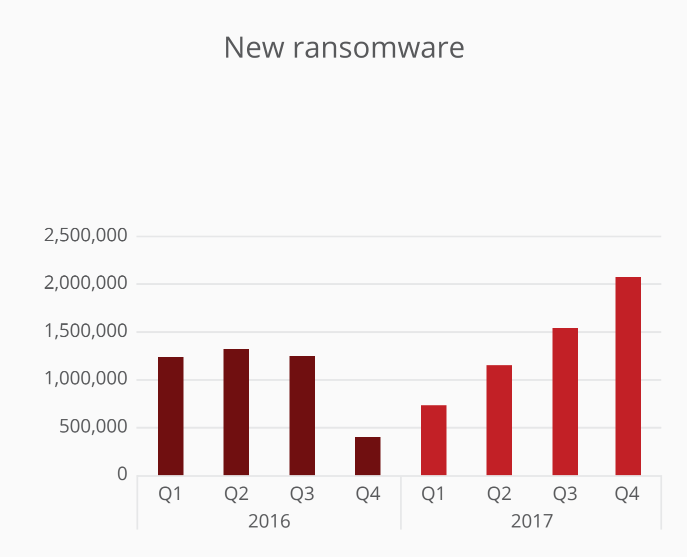


Source: McAfee Labs, 2018.

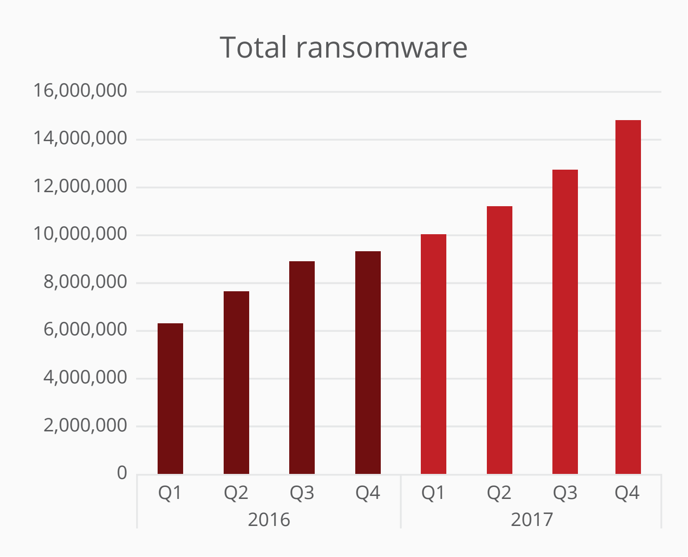
Global infection rates have declined slightly during the last three quarters, even as percentages have increased in Australia and the Americas.

Follow

Share

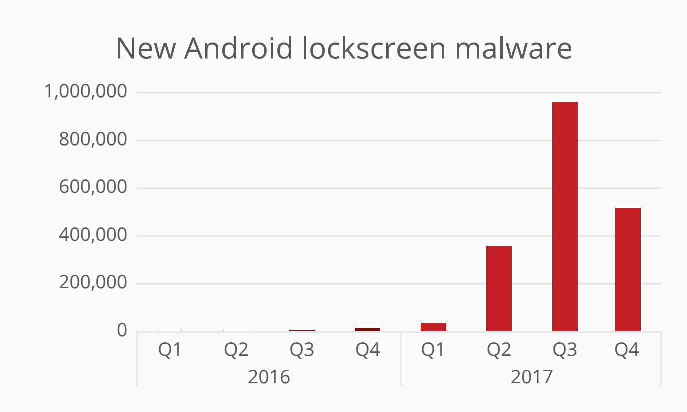


Source: McAfee Labs, 2018.

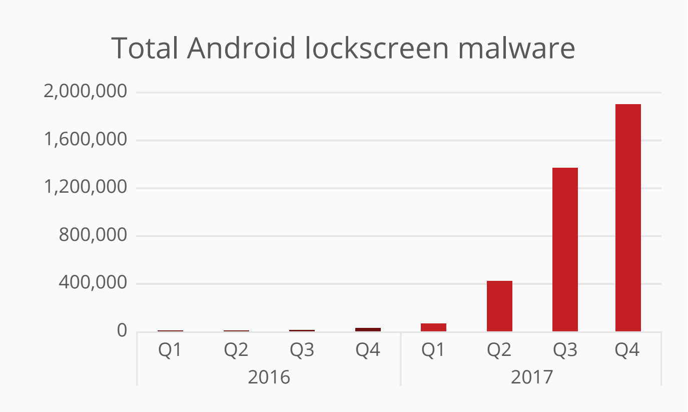


Source: McAfee Labs, 2018.

A big contributor to ransomware growth was Ransom:Win32/Genasom.



Source: McAfee Labs, 2018.

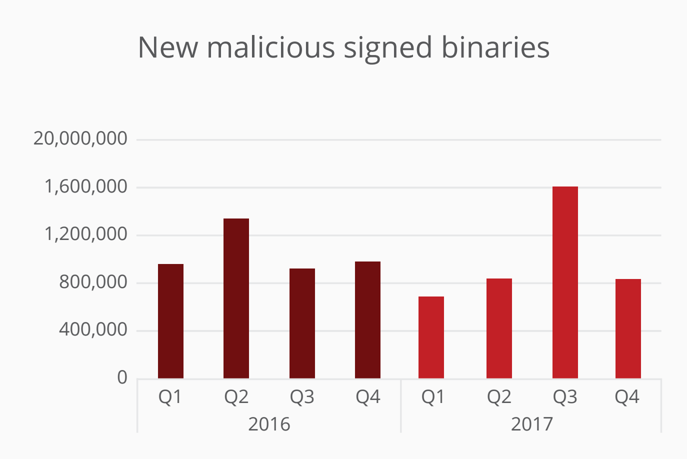


Source: McAfee Labs, 2018.

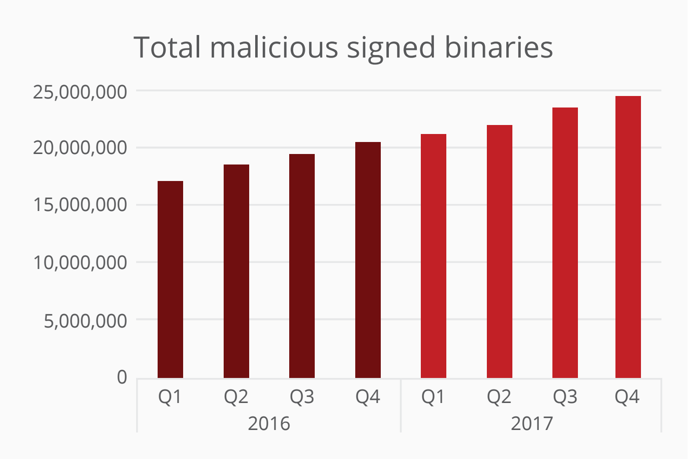
This form of ransomware started slowly in 2016, but burst into prominence last year.

Follow

Share



Source: McAfee Labs, 2018.

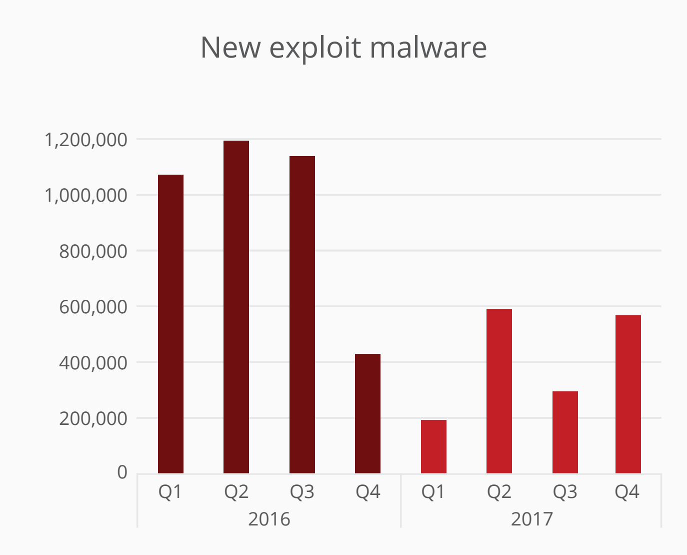


Source: McAfee Labs, 2018.

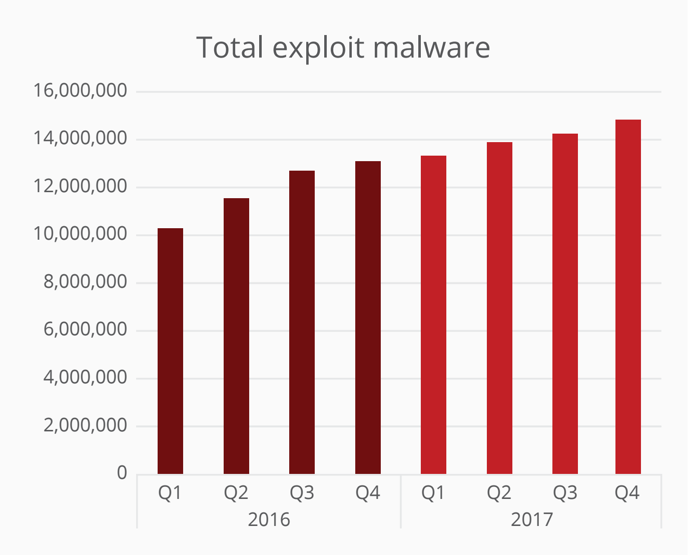
Certificate authorities provide digital certificates that deliver information online once an application, or binary, is signed and validated by the service provider that owns the content. This trust model is undermined when cybercriminals obtain certificates for malicious signed binaries, or malicious applications, which make attacks much simpler to execute.

Follow

Share



Source: McAfee Labs, 2018.

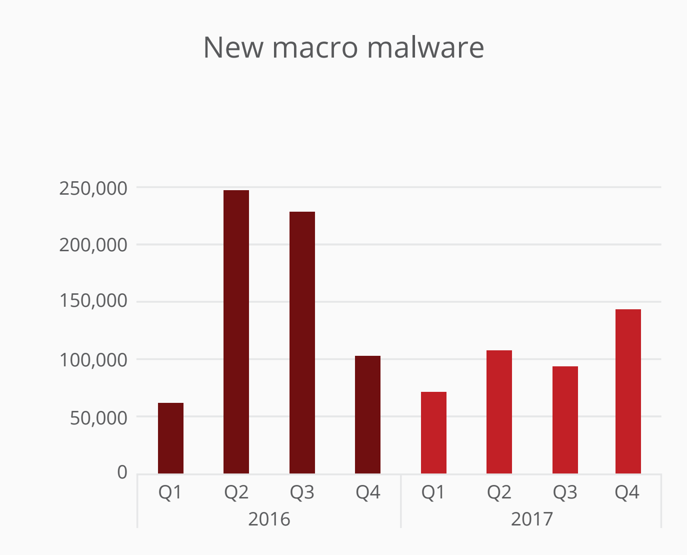


Source: McAfee Labs, 2018.

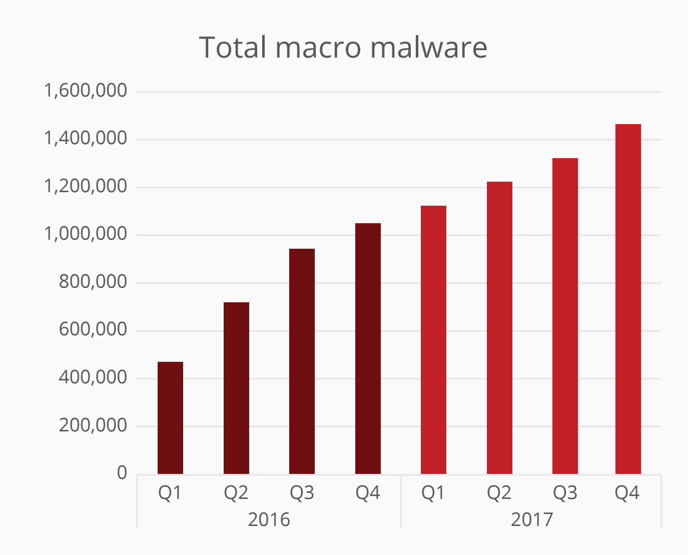
Exploits take advantage of bugs and vulnerabilities in software and hardware. Zero-day attacks are examples of successful exploits. For a recent example, see the McAfee Labs post "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability."

Follow

Share

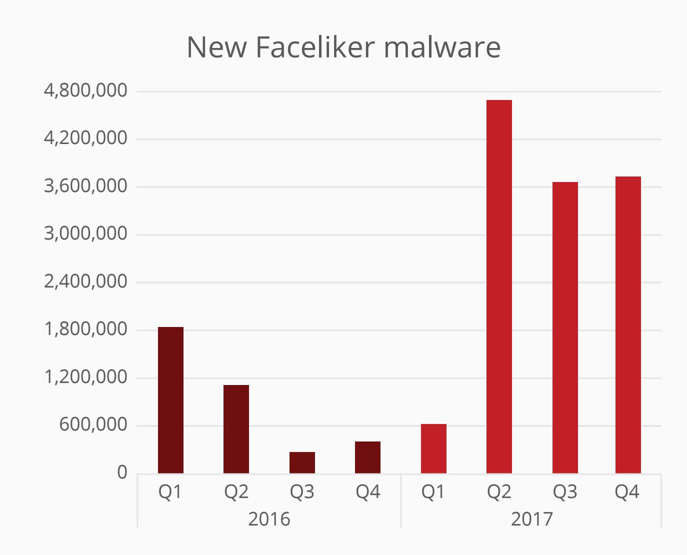


Source: McAfee Labs, 2018.

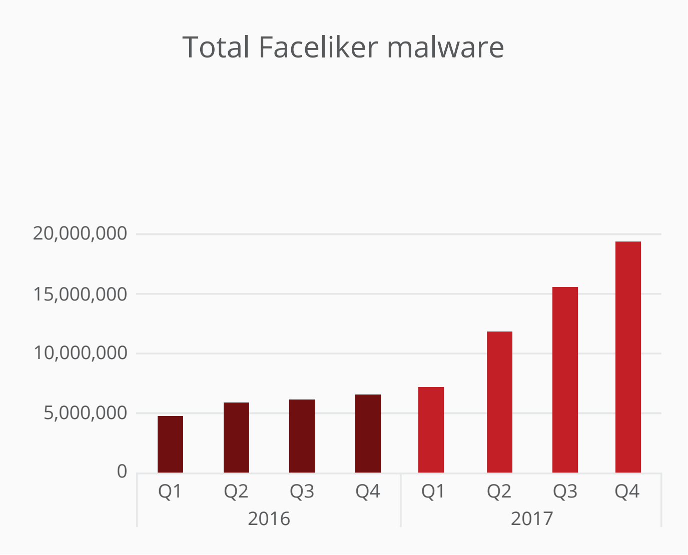


Source: McAfee Labs, 2018.

Macro malware usually arrives as a Word or Excel document in a spam email or zipped attachment. Bogus but tempting filenames encourage victims to open the documents, leading to infection if macros are enabled.



Source: McAfee Labs, 2018.

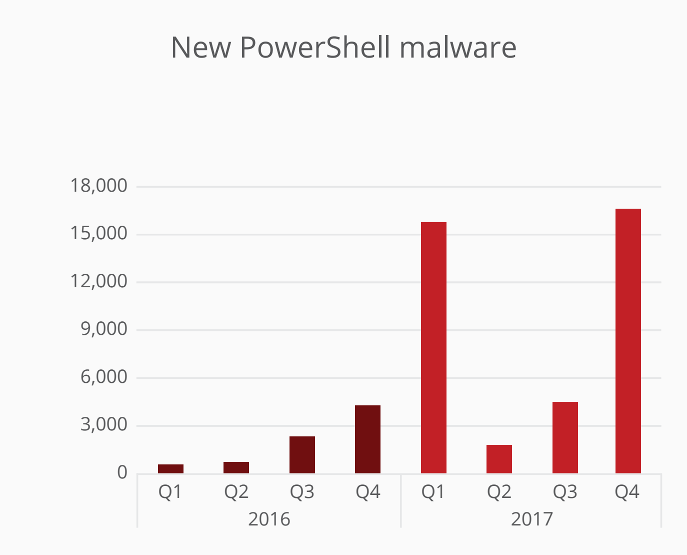


Source: McAfee Labs, 2018.

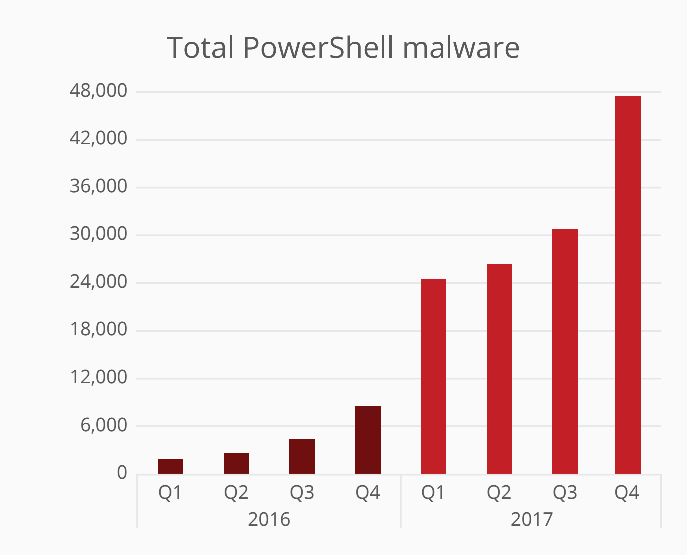
The Faceliker Trojan manipulates Facebook clicks to artificially "like" certain content. To learn more, read this post from McAfee Labs.

Follow

Share

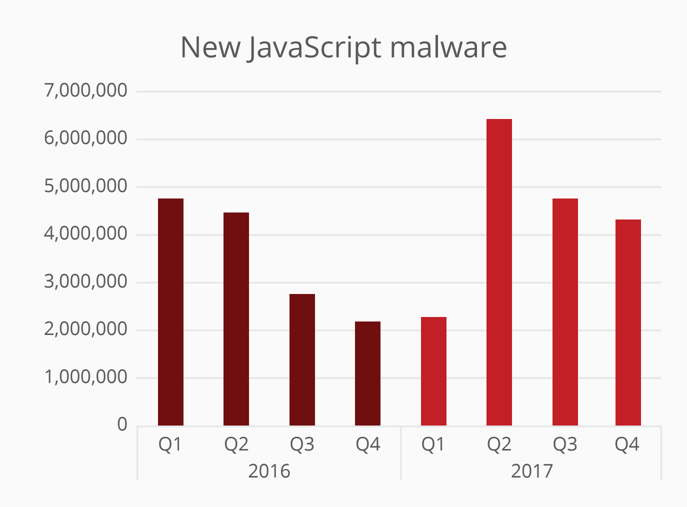


Source: McAfee Labs, 2018.

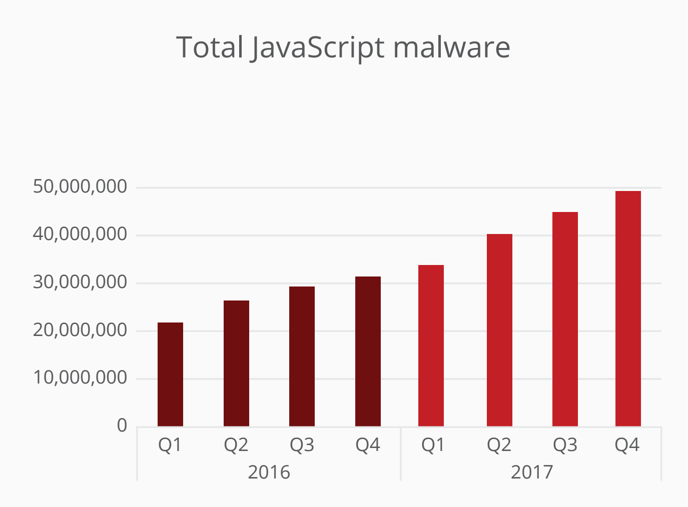


Source: McAfee Labs, 2018.

PowerShell threats were boosted by a rash of downloaders in Q4. For more on PowerShell and JavaScript threats, see "The rise of script-based malware," in the *McAfee Labs Threats Report, September 2017*.



Source: McAfee Labs, 2018.

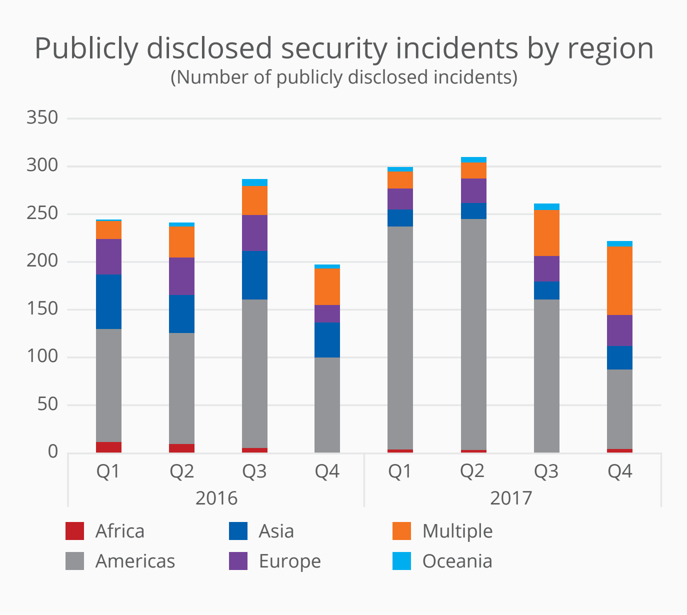


Source: McAfee Labs, 2018.

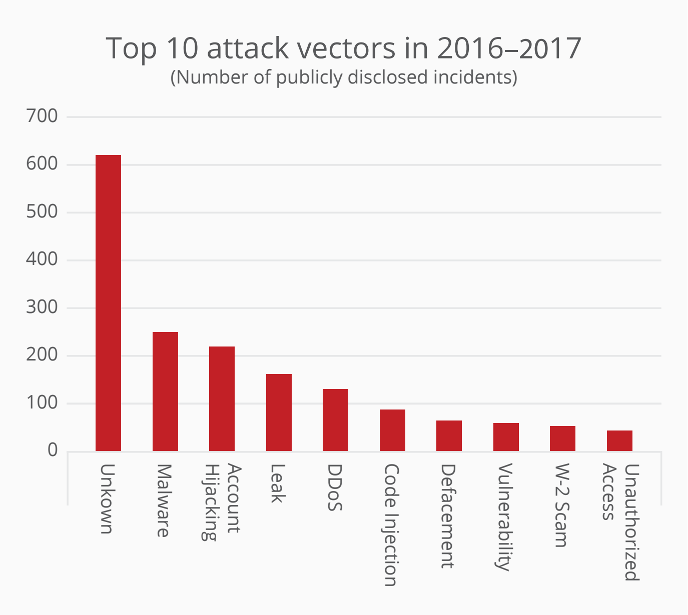
Follow

Share

Incidents



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

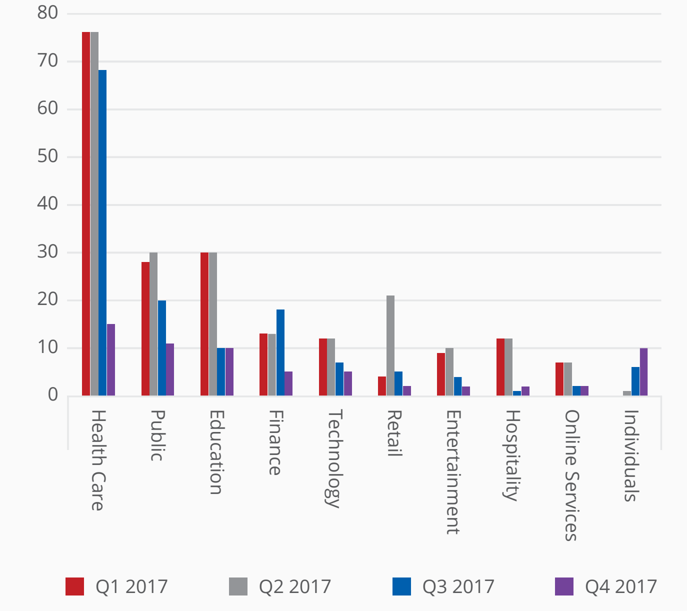
Security incidents data is compiled from several sources, including hackmageddon.com, privacyrights.org/data-breaches, haveibeenpwned.com, and databreaches.net.

The majority of attack vectors are either not known or not publicly reported.

Follow

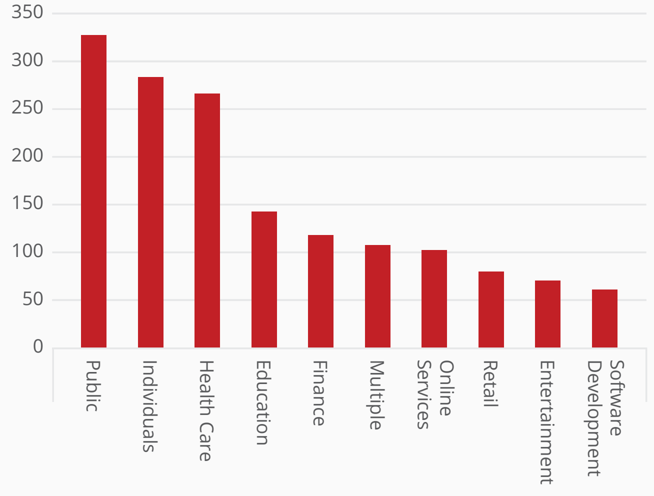
Share

Top sectors targeted in North and South America
(Number of publicly disclosed incidents)



Source: McAfee Labs, 2018.

Top 10 targeted sectors in 2016–2017
(Number of publicly disclosed incidents)

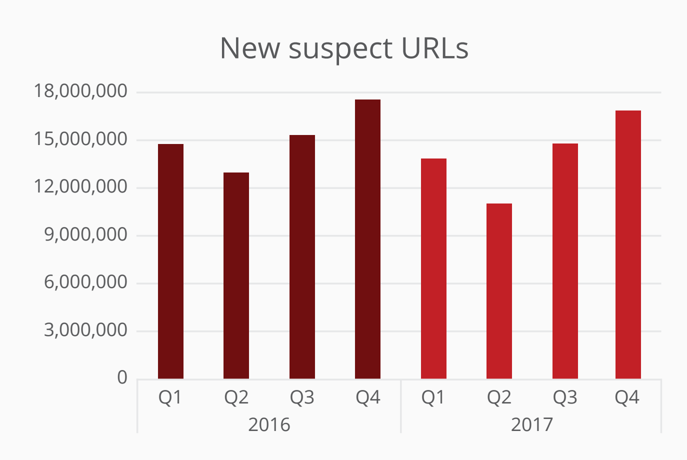


Source: McAfee Labs, 2018.

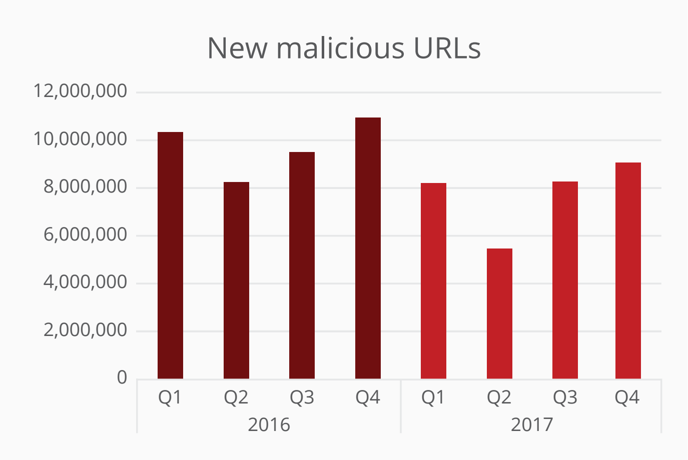
Follow

Share

Web and Network Threats



Source: McAfee Labs, 2018.



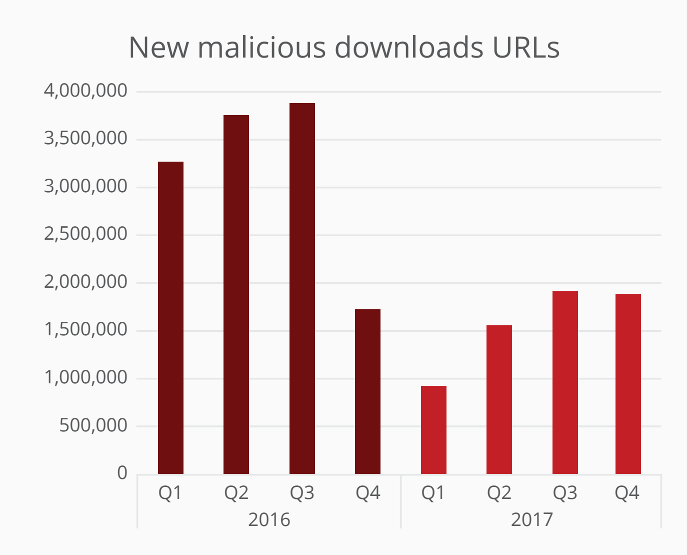
Source: McAfee Labs, 2018.

The McAfee® TrustedSource™ Web Database contains URLs (web pages) organized into categories, based on web reputation, to use with filtering policies to manage web access. Suspect URLs are the total number of sites that earn High Risk or Medium Risk scores.

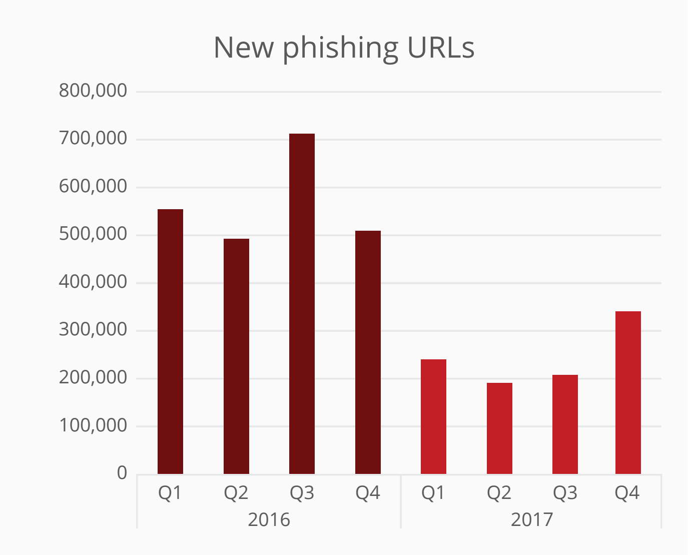
Malicious sites deploy code designed to hijack a computer's settings or activity. This category includes self-installing applications ("drive-by" executable files), Trojans, and other malware that exploit vulnerabilities in browsers or other applications.

Follow

Share



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

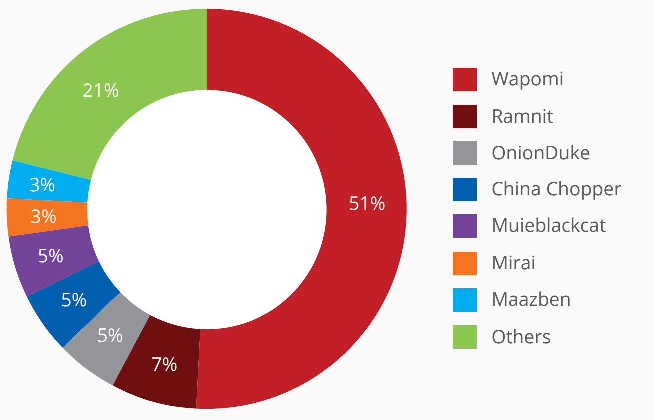
Malicious downloads come from sites that allow a user to inadvertently download code that is harmful or annoying. This category includes screensavers, toolbars, and file-sharing programs that contain adware, spyware, viruses, and other malicious code. Sometimes, the malware is added without users' knowledge, as when they click "Yes" or "I agree" without reading the full terms and conditions. The effects can include slower performance, theft of passwords, and the loss or damage of personal files.

Phishing URLs are web pages that typically arrive in hoax emails to steal user account information. These sites falsely represent themselves and appear as legitimate company web pages to deceive and obtain user data for perpetrating fraud or theft.

Follow

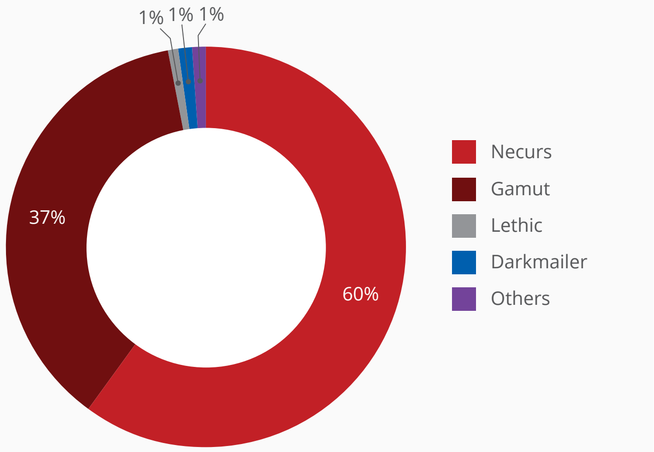
Share

Top malware connecting to control servers in Q4



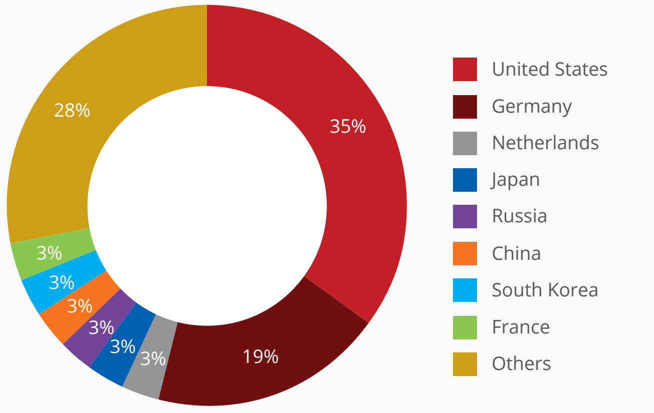
Source: McAfee Labs, 2018.

Spam botnet prevalence by volume in Q4



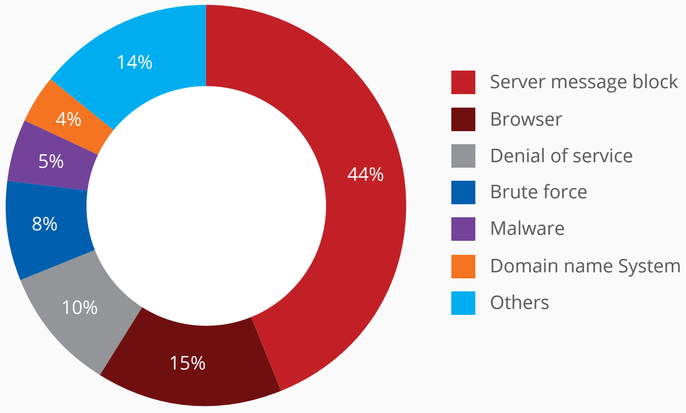
Source: McAfee Labs, 2018.

Top countries hosting botnet control servers in Q4



Source: McAfee Labs, 2018.

Top network attacks in Q4



Source: McAfee Labs, 2018.

Necurs—a recent purveyor of “lonely girl” spam, pump and dump stock spam, and Locky ransomware downloaders—and Gamut—sending job offer–themed phishing (and possible money mule recruitment), in English, German, and Italian— were responsible for 97% of spam botnet traffic in Q4.

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, led by McAfee Advanced Threat Research, 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 and McAfee Advanced Threat Research deliver 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