McAfee
Together is power.

# McAfee Labs Threats Report

**September 2018**

**TOP STORIES OF THE QUARTER**

Want to Break Into a Locked Windows 10 Device? Ask Cortana (CVE-2018-8140)

Threat Report: Don't Join Blockchain Revolution Without Ensuring Security

AsiaHitGroup Gang Again Sneaks Billing-Fraud Apps Onto Google Play

# McAfee Global Threat Intelligence analyzed, on average, 1,800,000 URLs, 800,000 files, and another 200,000 files in a sandbox each day in Q2.

**This report was researched and written by:**

- Christiaan Beek
- Carlos Castillo
- Cedric Cochin
- Ashley Dolezal
- Steve Grobman
- Charles McFarland
- Niamh Minihane
- Chris Palm
- Eric Peterson
- Steve Povolny
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

## Introduction

Welcome to the McAfee® Labs Threats Report September 2018. In this edition, we highlight the notable investigative research and trends in threats statistics gathered by the McAfee Advanced Threat Research and McAfee Labs teams in Q2 of 2018.

Cybercriminals continue to follow the money. Although this statement is familiar, our latest Threats Report clearly shows the migration from certain older attacks to new threat vectors as they become more profitable. Just as in Q1, we see the popularity of cryptocurrency mining continue to rise.

In this report we detail recent findings from three McAfee Labs analyses that appeared in Q2. You can read summaries of each on pages 5-7. One area of investigation by our research teams is in digital assistants. In Q2 we analyzed a vulnerability in Microsoft's Cortana. This flaw allowed an attacker to log into a locked Windows device and execute code. Following our vulnerability disclosure policy, we communicated our findings to Microsoft; the analysis resulted in CVE-2018-8140. We also examined the world of cryptocurrency attacks with an in-depth view of blockchain technology. Our report detailed many of the vulnerabilities being exploited by threat actors looking for a quick return on their investment.

Turning to malware, our report details an area of cybercrime that is often poorly reported compared with the large-scale and "noisy" ransomware attacks of the past 18 months. Billing fraud has been the modus operandi of multiple threat actor groups for some time. We examine a campaign by the AsiaHitGroup that has attempted to charge 20,000 victims using apps from official stores such as Google Play.

In Q2, McAfee Global Threat Intelligence received an average of 49 billion queries per day. Meanwhile, the amount of new malware has fallen for the second successive quarter; however, this may not be significant because we saw a spike in Q4 of 2017, and new samples have been relatively flat for four of the past five quarters. New mobile malware samples increased 27% in Q2; this is the second successive quarter of growth. Coin miner malware remains very active; total samples grew by 86% in Q2, with more than 2.5 million new files added to the malware database.

We are pleased to let you know that all of our research is now available on the McAfee ePolicy Orchestrator® (McAfee ePO™) platform, starting with Version 5.10.0. This is in addition to our usual social channels, detailed below, plus the home pages of McAfee Labs and McAfee Advanced Threat Research.

Stay Safe. Stay Informed.

—Steve Grobman, Chief Technology Officer

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

Twitter

@SteveGrobman

@Raj_Samani

Follow

Share

# Table of Contents



## Top stories of the quarter

### Want to Break Into a Locked Windows 10 Device? Ask Cortana (CVE-2018-8140)

McAfee Labs and the Advanced Threat Research team discovered a vulnerability in the Cortana voice assistant in Microsoft Windows 10. The flaw, for which Microsoft provided a fix in June, can lead to unauthorized code execution. We explain how this vulnerability can be used to execute code from the locked screen of a fully patched Windows 10 machine (RS3 and RS4 before the June patch). In this analysis, we address three vectors of research that have been combined by Microsoft and together represent CVE-2018-8140. The first of these is an information leak; we finish with a demo showing full code execution to log in to a locked Windows device! We submitted the vulnerability to Microsoft in April as part of the Advanced Threat Research team's responsible disclosure policy. Attribution for this vulnerability submission goes to Cedric Cochin, Cyber Security Architect and Senior Principal Engineer.

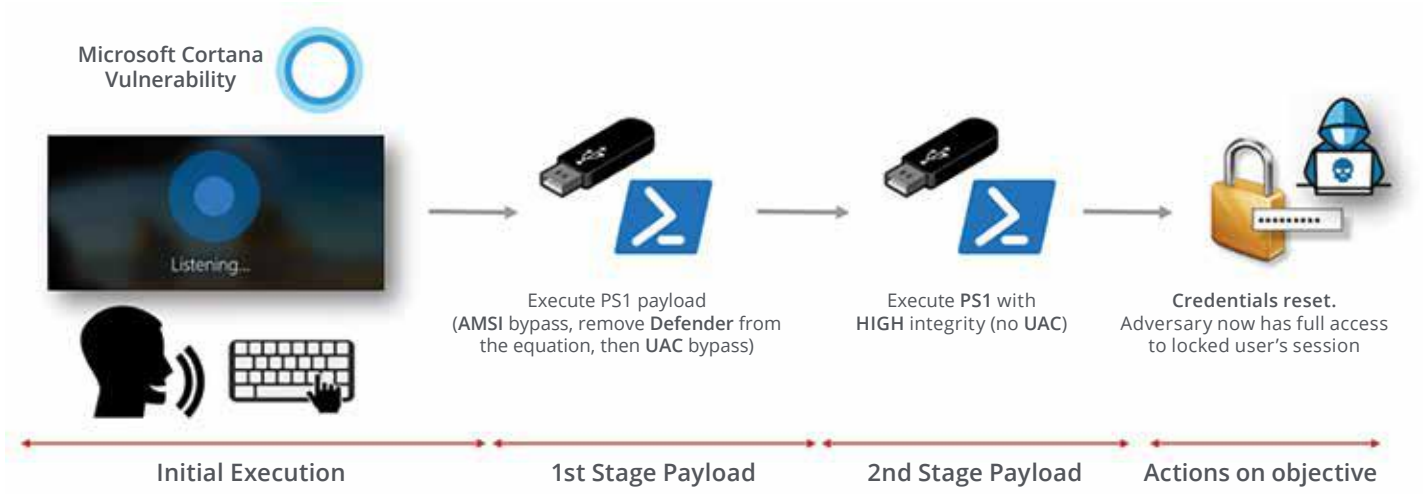



Figure 1. With four basic steps, an attacker can exploit Cortana and gain full control of a Windows 10 system.

Follow

Share

## Threat Report: Don't Join Blockchain Revolution Without Ensuring Security

Due to the increasing popularity of cryptocurrencies, the blockchain revolution is in full swing. Cybercriminals have also found new angles including illegal coin mining and theft leading to profits. The McAfee Advanced Threat Research team published in June a blockchain threat report to explain current threats against the users and implementers of blockchain technologies.

Even if you have not heard of blockchain, you have likely heard of cryptocurrencies, especially Bitcoin, the most popular implementation. Cryptocurrencies are built on top of blockchain, which records transactions in a decentralized way and enables a trusted "ledger" between trustless participants. Each block in the ledger is linked to the next block, creating a chain. The chain enables anyone to validate all transactions without going to an outside source. From this, decentralized currencies such as Bitcoin are possible. In this report, we examine the primary attack vectors: phishing, malware, implementation vulnerabilities, and technology.

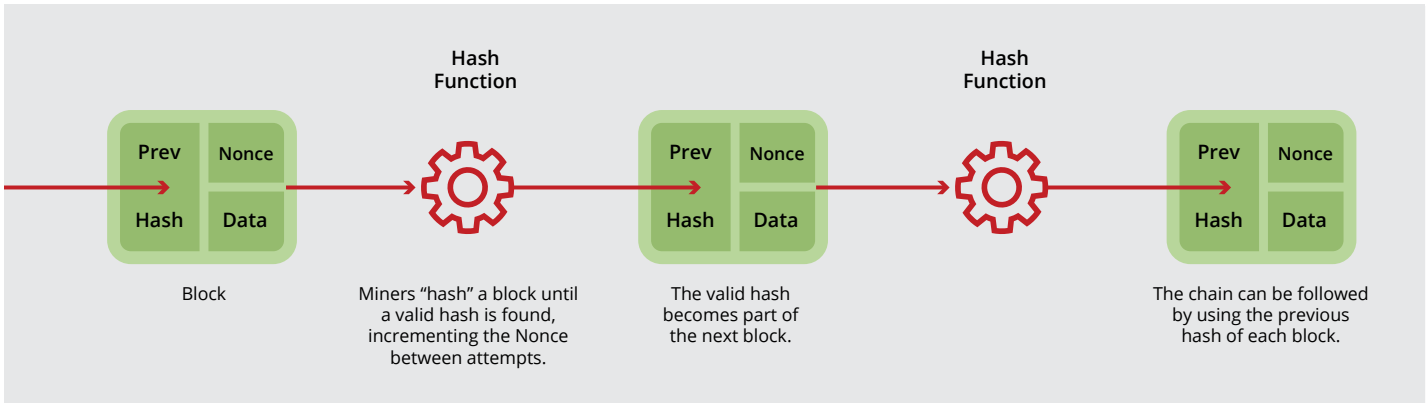



Figure 2. A proof-of-work blockchain, building on each previous hash. Source: https://bitcoin.org/bitcoin.pdf

Follow

Share

## AsiaHitGroup Gang Again Sneaks Billing-Fraud Apps Onto Google Play

The McAfee Mobile Research team found a new billing-fraud campaign of at least 15 apps published in 2018 on Google Play. Toll fraud (which includes billing fraud) is a leading category of potentially harmful apps on Google Play, according to the report "Android Security 2017 Year in Review." This new campaign demonstrates that cybercriminals keep finding new ways to steal money from victims using apps on official stores such as Google Play. The actors behind this campaign, the AsiaHitGroup Gang, has been active since at least late 2016 with the distribution of the fake-installer applications Sonvpay.A, which attempted to charge at least 20,000 victims from primarily Thailand and Malaysia for the download of copies of popular applications. One year later, in November 2017, a new campaign was discovered on Google Play, Sonvpay.B, which used IP address geolocation to confirm the country of the victim and added Russian victims to the billing fraud to increase its potential to steal money from unsuspected users. Our investigation explains how the malware in these campaigns works.


Figure 3. Malicious apps from the AsiaHitGroup Gang formerly found on Google Play.

Follow

Share

STATISTICS

# McAfee Global Threat Intelligence

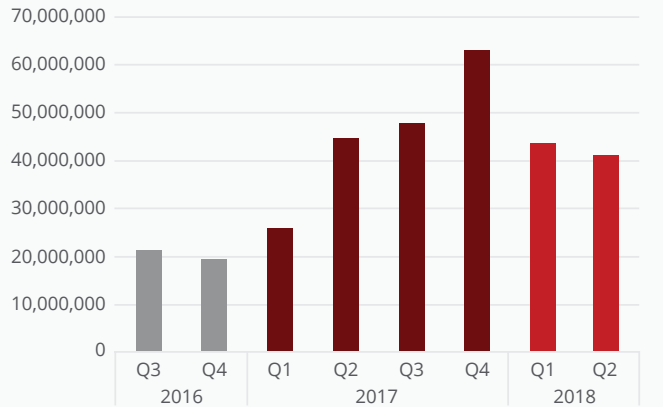
Every quarter, the McAfee® Global Threat Intelligence (McAfee GTI) cloud dashboard allows us to see and analyze real-world attack patterns that lead to better customer protection. This information provides insights into attack volumes that our customers experience. Each day, on average, McAfee GTI received 49 billion queries and 13 billion lines of telemetry, while analyzing 1,800,000 URLs and 800,000 files, plus another 200,000 files in a sandbox.

- McAfee GTI protections against malicious files reported 86,000 (0.1%) of them risky in Q2, out of 86 million tested files.
- McAfee GTI protections against malicious URLs reported 365,000 (0.5%) of them risky in Q2, out of 73 million tested URLs.
- McAfee GTI protections against malicious IP addresses reported 268,000 (0.4%) of them risky in Q2, out of 67 million tested IP addresses.

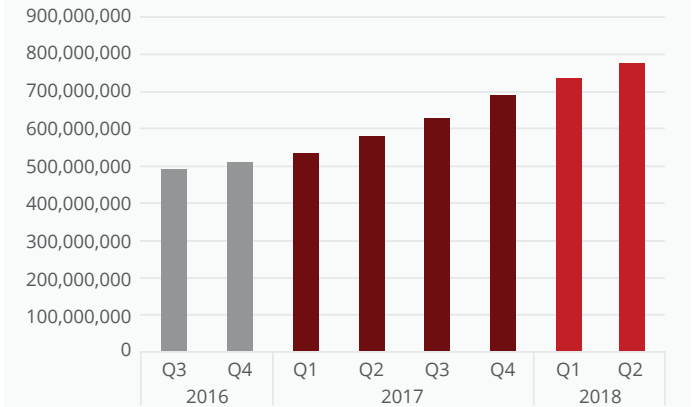
# Threats Statistics



## Malware

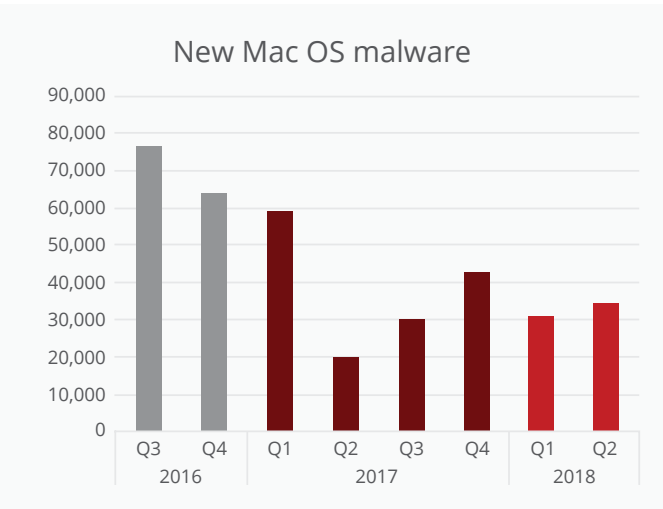



Source: McAfee Labs, 2018.

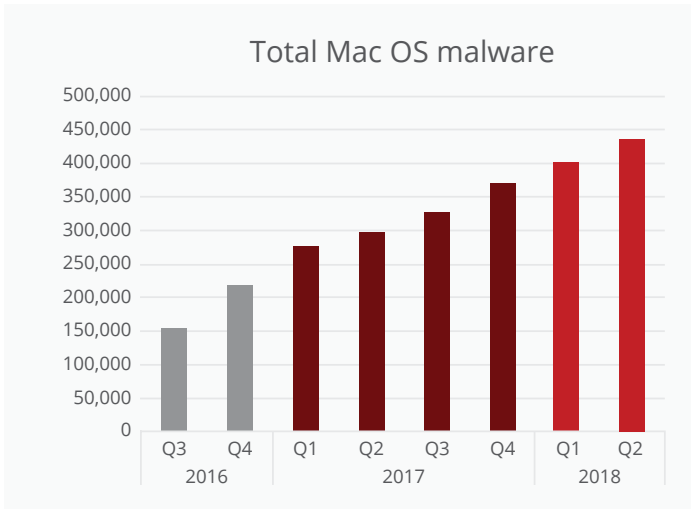



Source: McAfee Labs, 2018.

**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.**



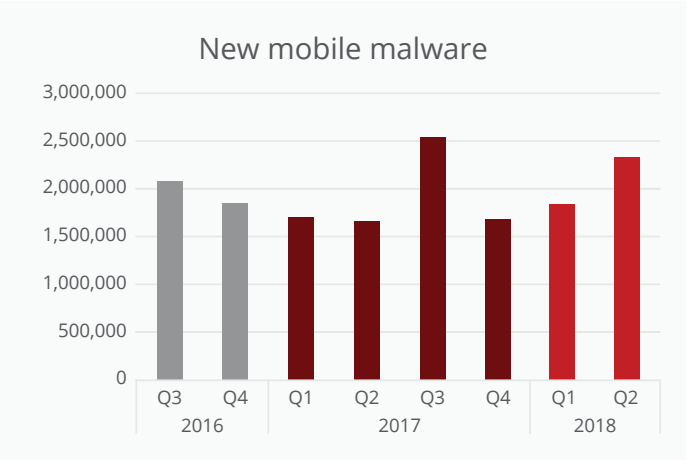

Source: McAfee Labs, 2018.



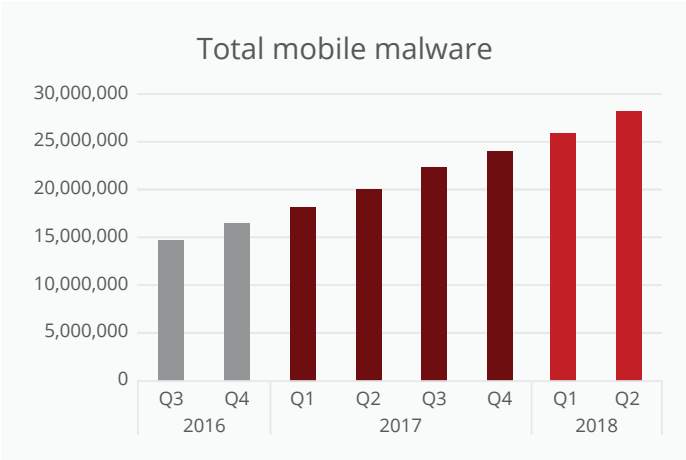

Source: McAfee Labs, 2018.

Follow

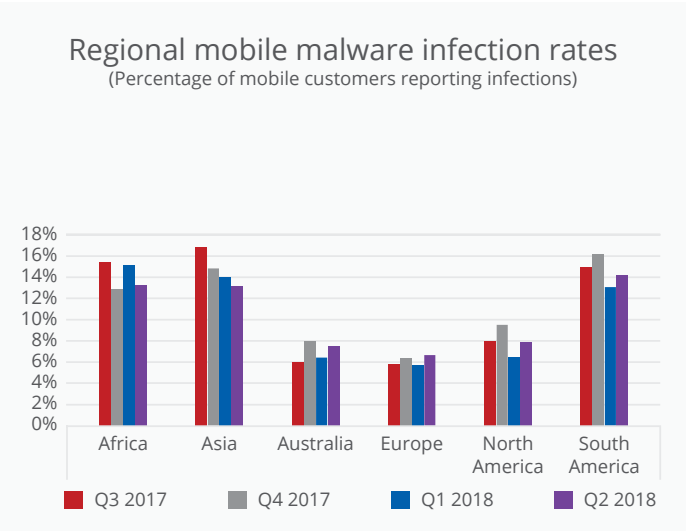
Share



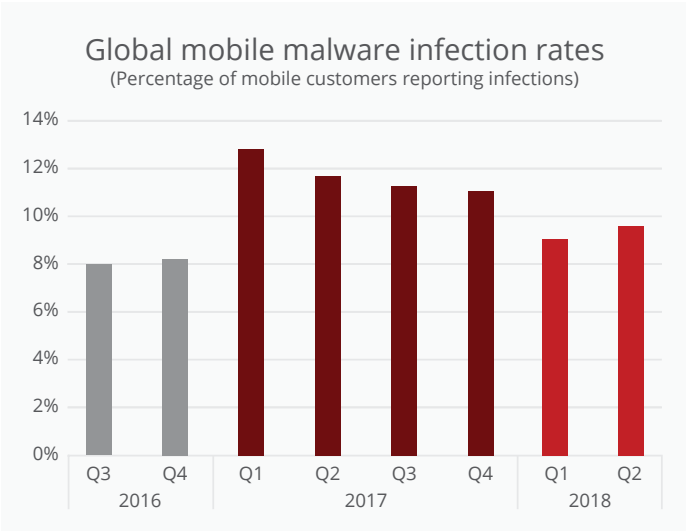

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.



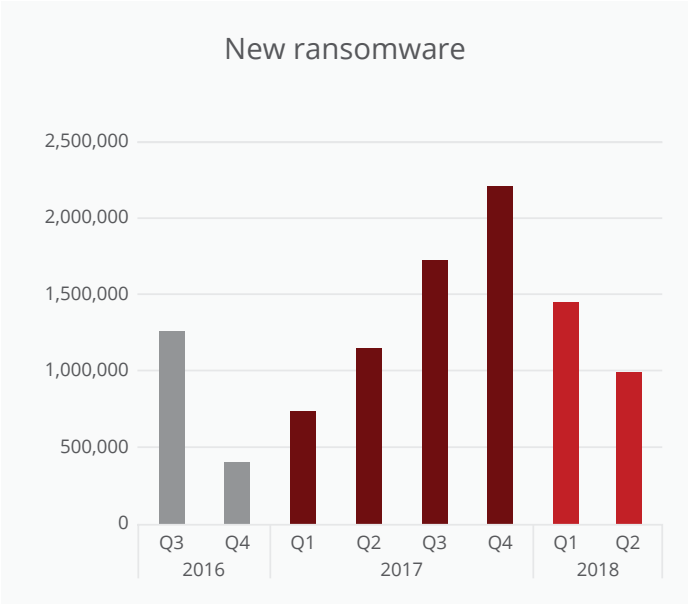

Source: McAfee Labs, 2018.



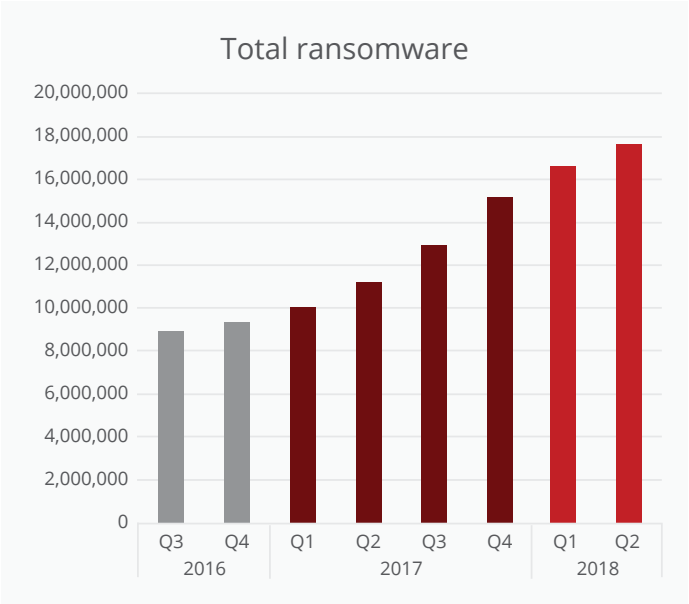

Source: McAfee Labs, 2018.

Follow

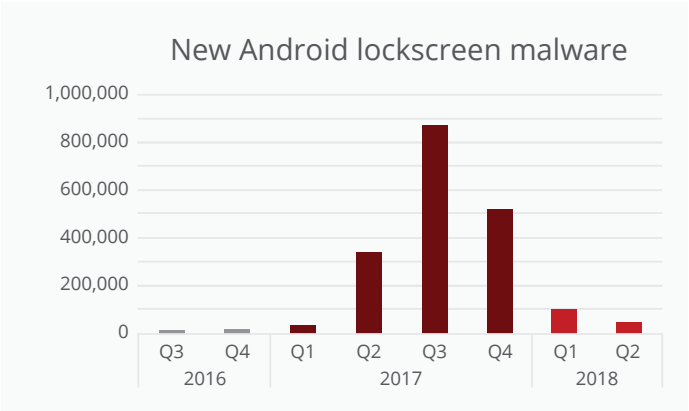
Share



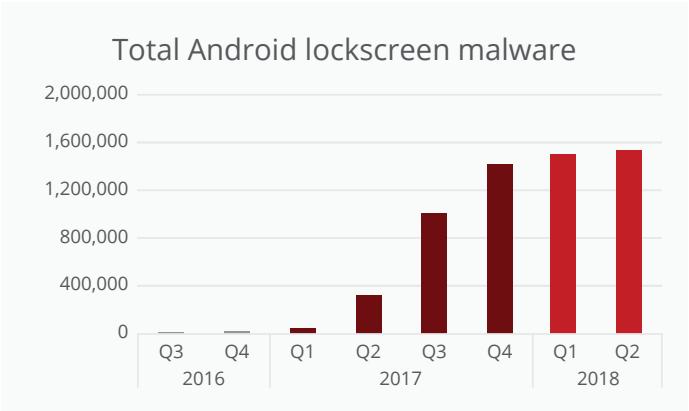

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.



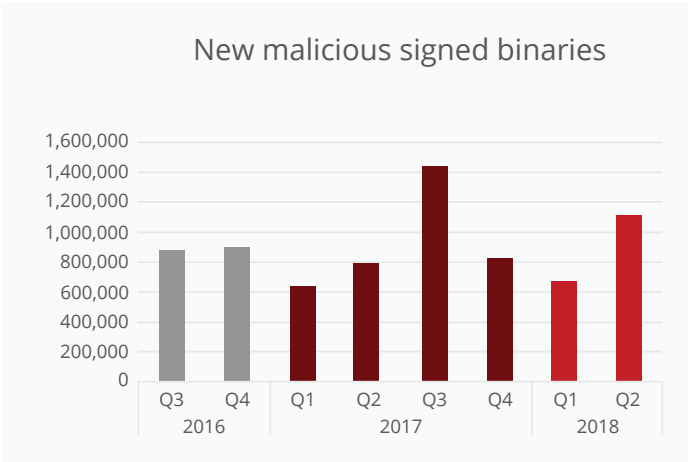

Source: McAfee Labs, 2018.



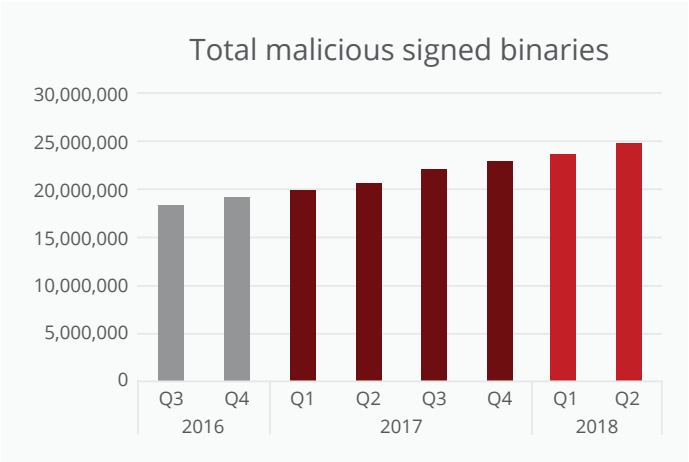

Source: McAfee Labs, 2018.

Follow

Share

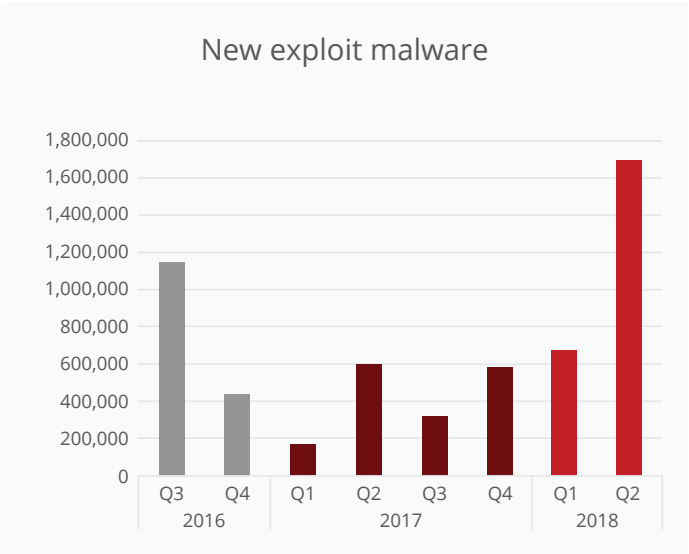



Source: McAfee Labs, 2018.

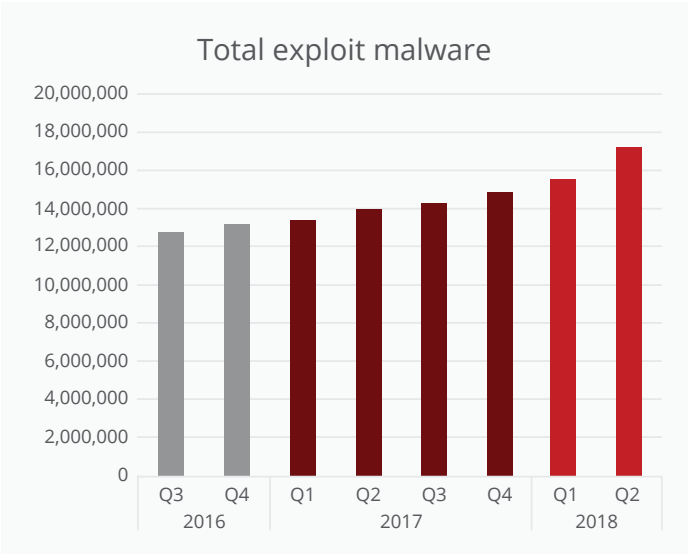



Source: McAfee Labs, 2018.

**Certificate authorities provide digital certificates that deliver information once a binary (application) is signed and validated by the content provider. When cybercriminals obtain digital certificates for malicious signed binaries, attacks are much simpler to execute.**




Source: McAfee Labs, 2018.

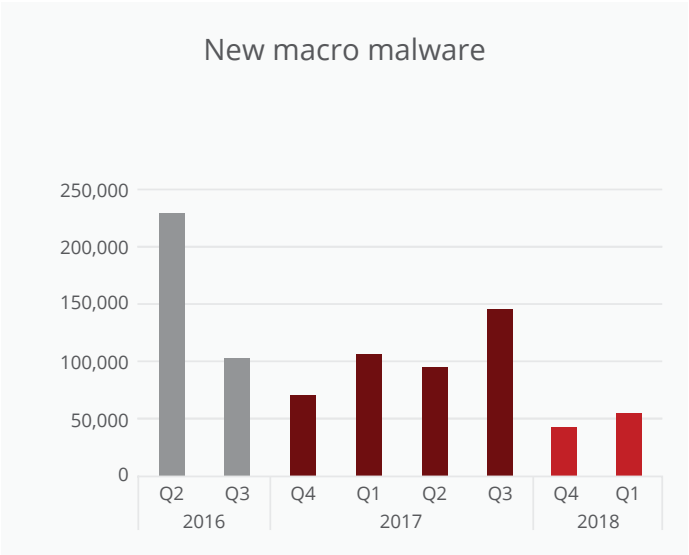



Source: McAfee Labs, 2018.

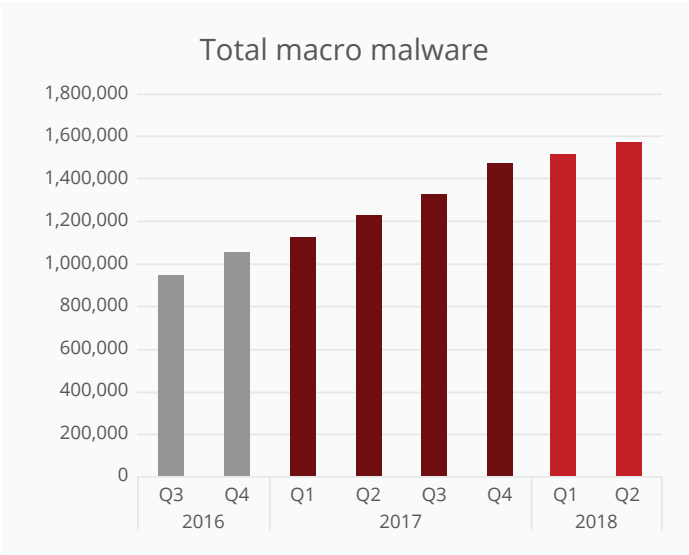
**Exploits take advantage of bugs and vulnerabilities in software and hardware. Zero-day attacks are examples of successful exploits. For an example, see the McAfee Labs post "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability."**

Follow

Share

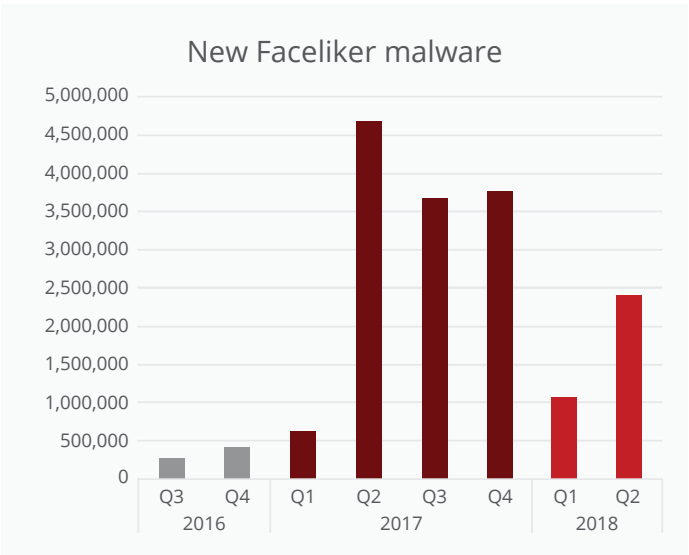



Source: McAfee Labs, 2018.

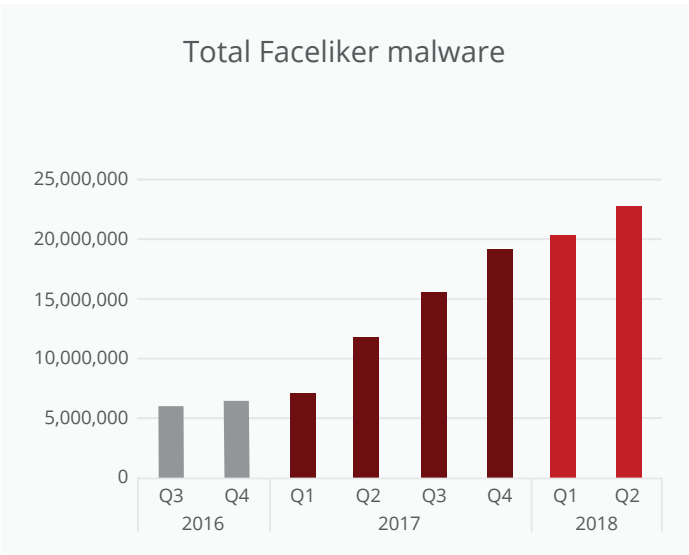



Source: McAfee Labs, 2018.

**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.

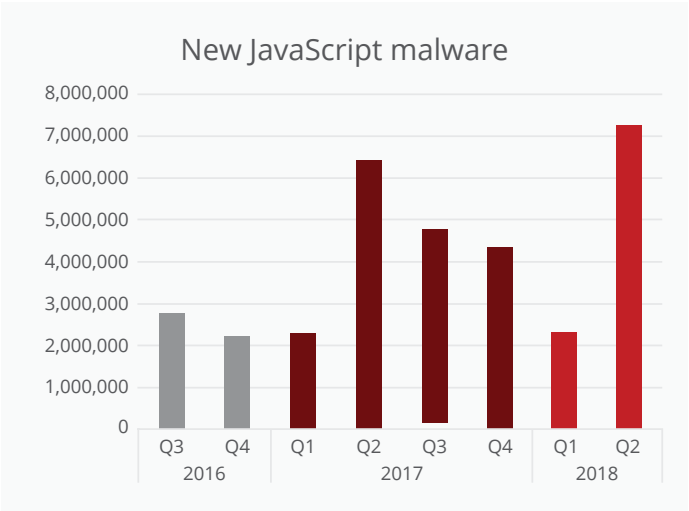



Source: McAfee Labs, 2018.

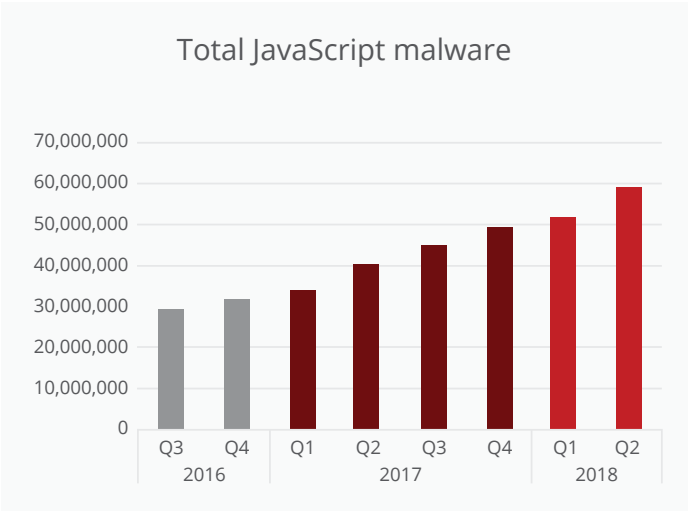
**The Faceliker Trojan manipulates Facebook clicks to artificially "like" certain content. To learn more, read this post from McAfee Labs.**

Follow

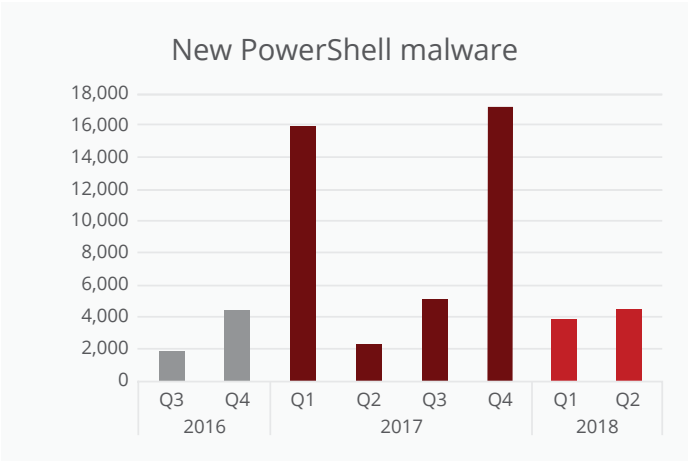
Share



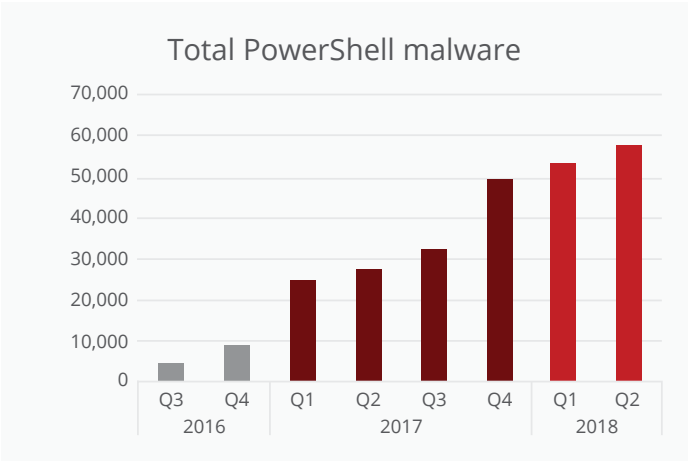

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.

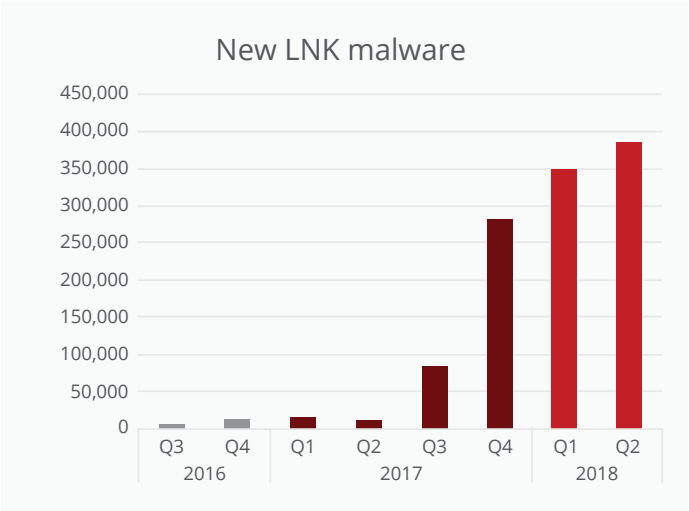



Source: McAfee Labs, 2018.

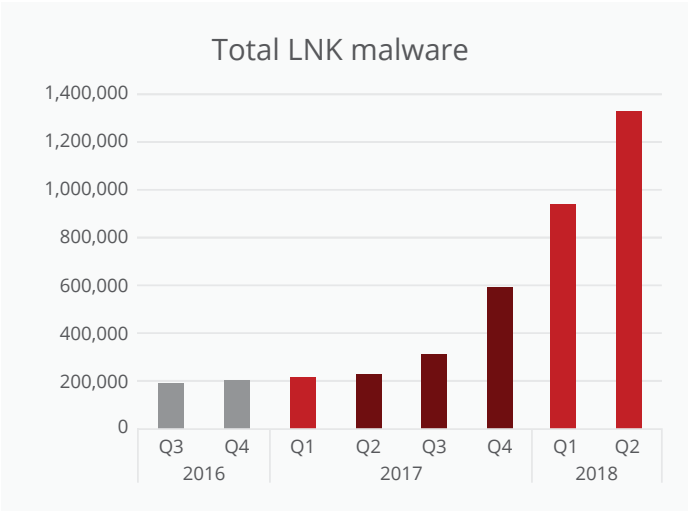
**For more on JavaScript and PowerShell threats, read "The rise of script-based malware," from an earlier *McAfee Labs Threats Report.***

Follow

Share

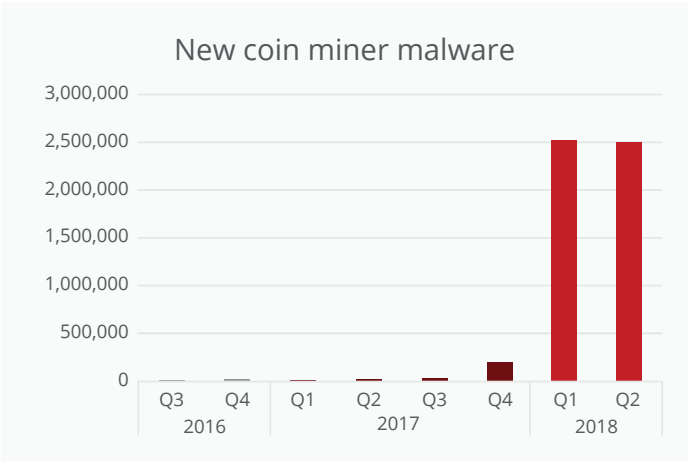



Source: McAfee Labs, 2018.

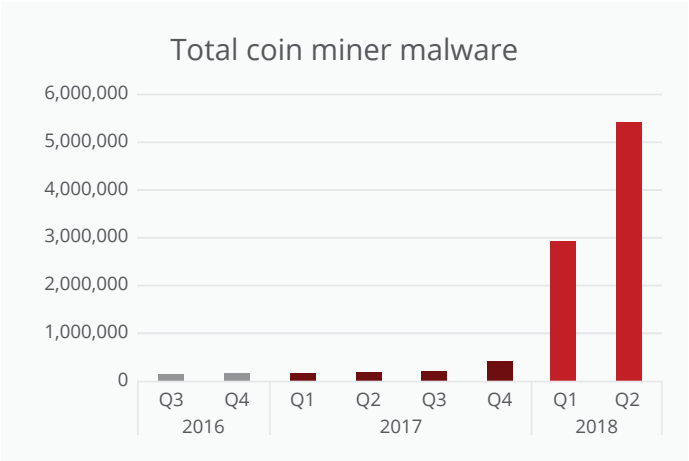



Source: McAfee Labs, 2018.

**Cybercriminals are increasingly using .lnk shortcuts to surreptitiously deliver malicious PowerShell scripts and other malware.**



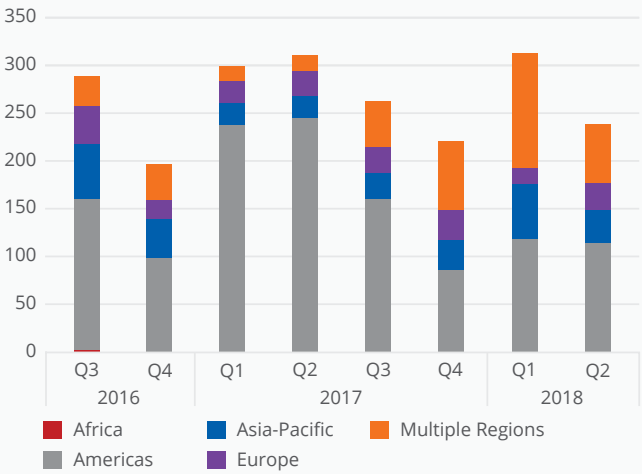

Source: McAfee Labs, 2018.



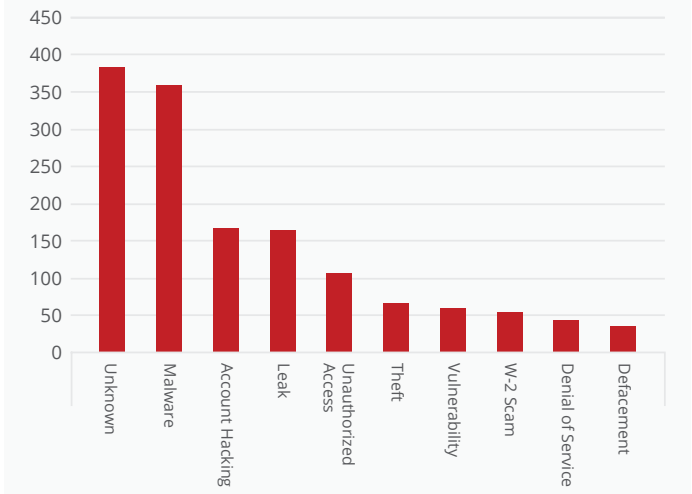

Source: McAfee Labs, 2018.

**Coin miner malware hijacks systems to create ("mine") cryptocurrency without victims consent or awareness. New coin miner threats have jumped massively in 2018.**

## Incidents




Source: McAfee Labs, 2018.



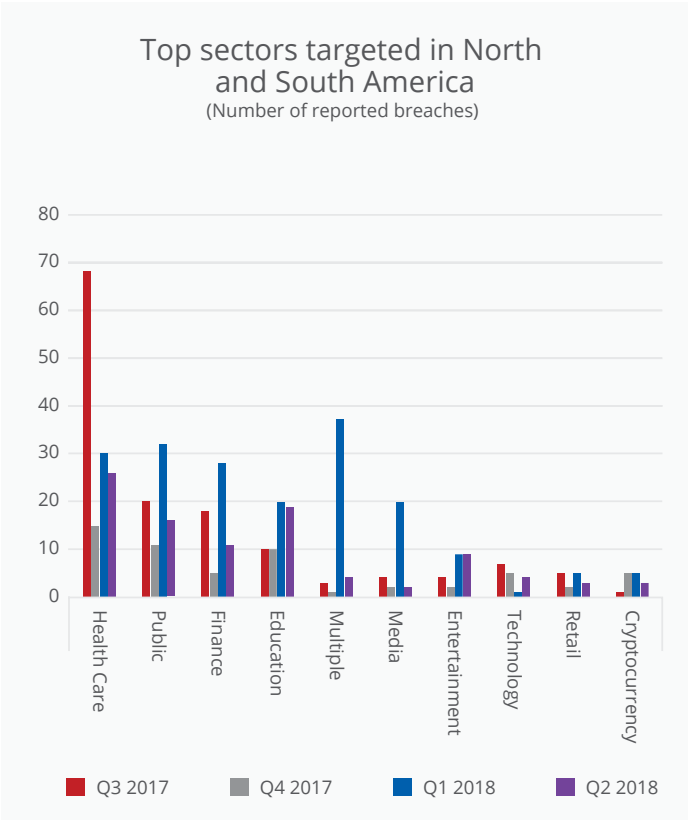

Source: McAfee Labs, 2018.

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

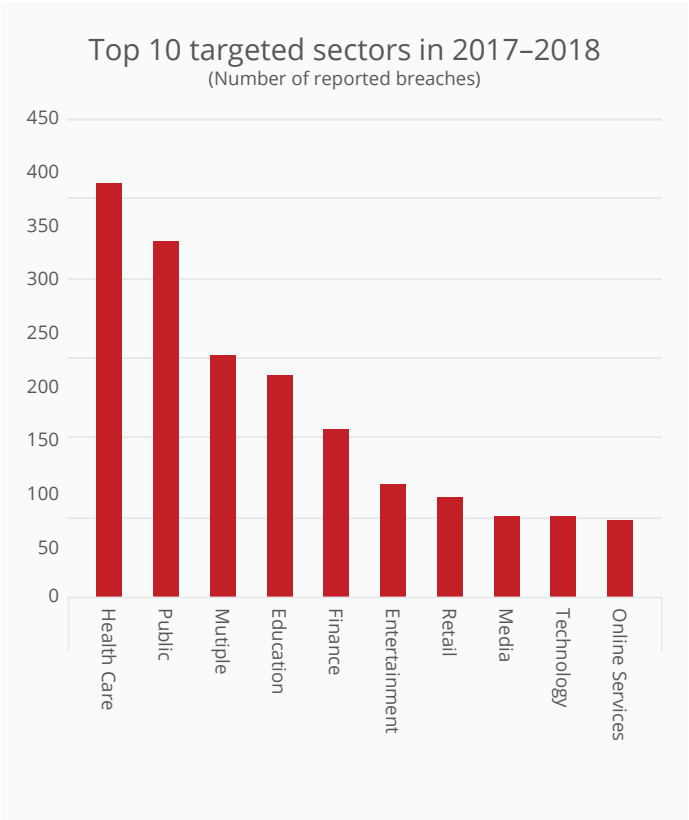
**The majority of attack vectors are either not known or not publicly reported.**

Follow

Share




Source: McAfee Labs, 2018.

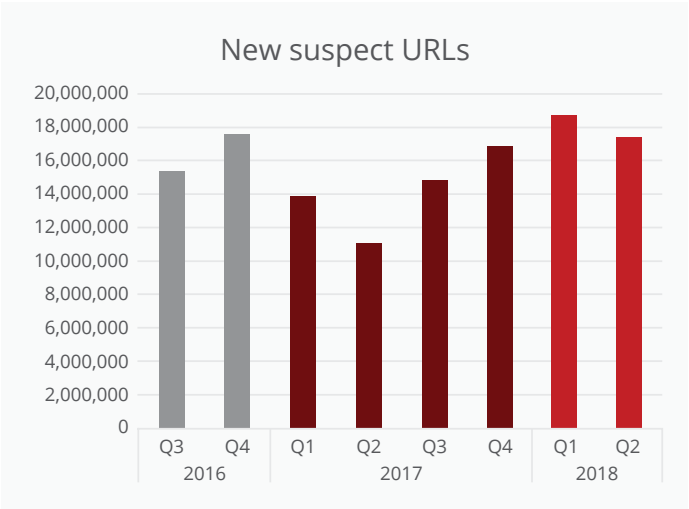



Source: McAfee Labs, 2018.

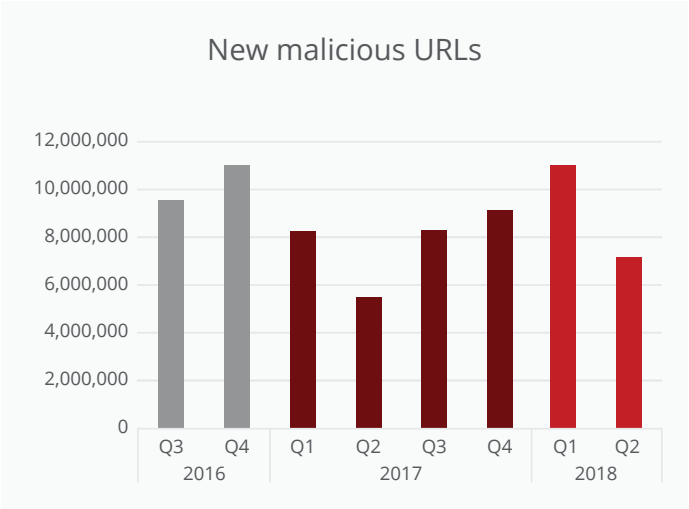
Follow

Share

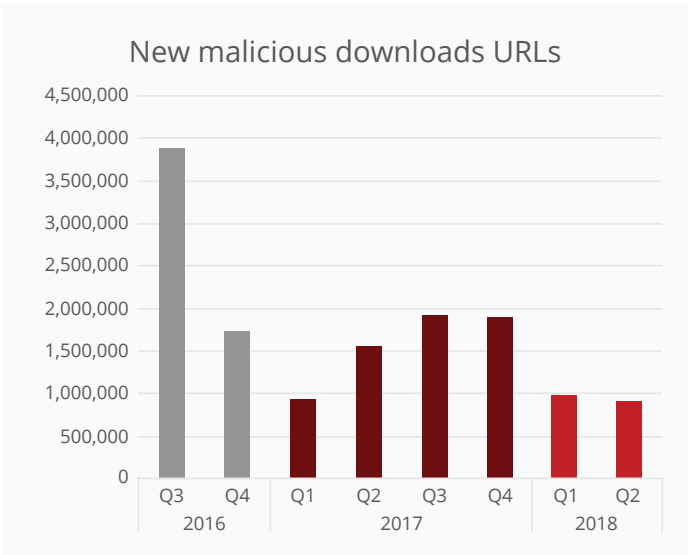
## Web and Network Threats



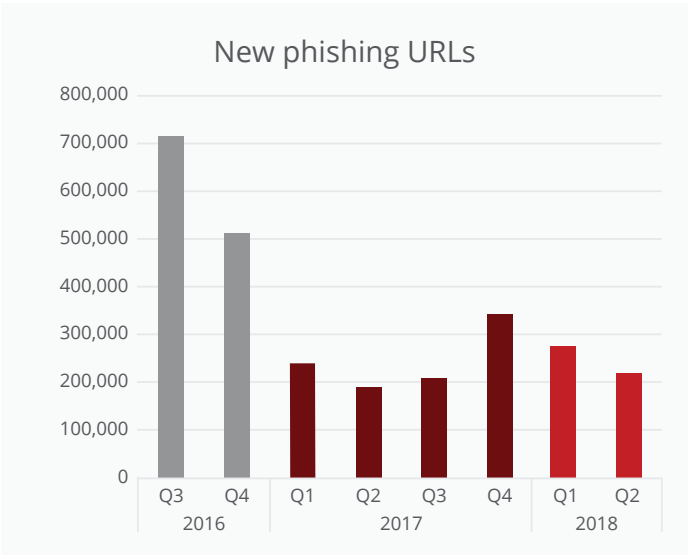

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.



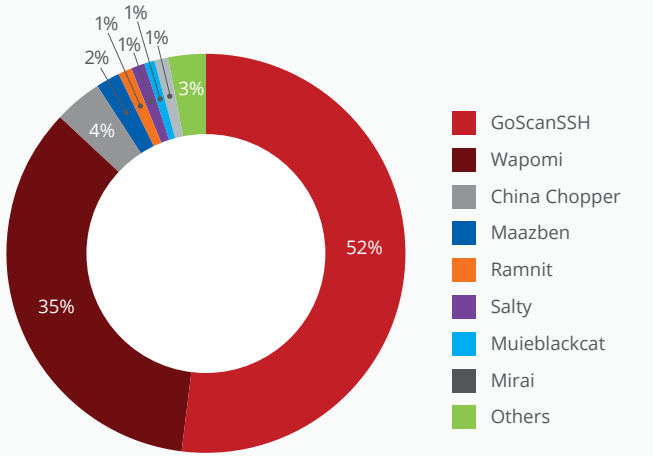

Source: McAfee Labs, 2018.

**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 URLs deploy code, including "drive-by" executables and Trojans, designed to hijack a computer's settings or activity. Malicious downloads come from sites that allow users, sometimes without their knowledge, to inadvertently download code that is harmful or annoying. Phishing URLs are web pages that typically arrive in hoax emails to steal user account information.**

Follow

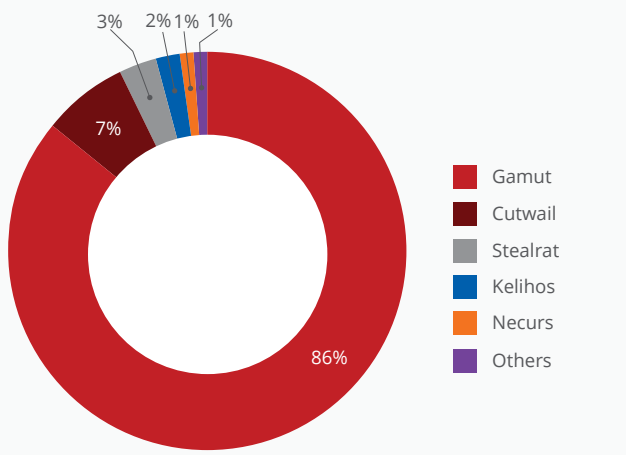
Share

## Top malware connecting to control servers in Q2




Source: McAfee Labs, 2018.

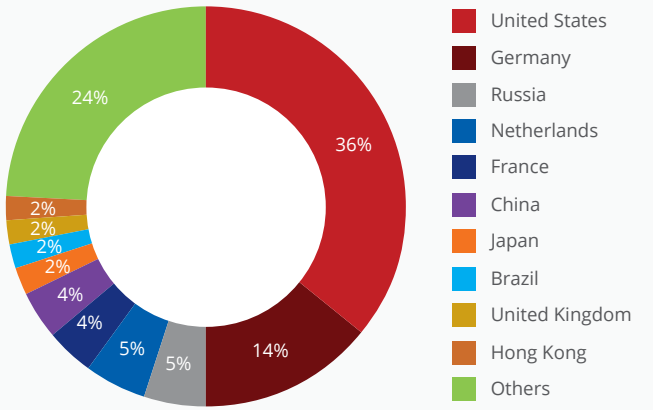
## Spam botnet prevalence by volume in Q2




Source: McAfee Labs, 2018.

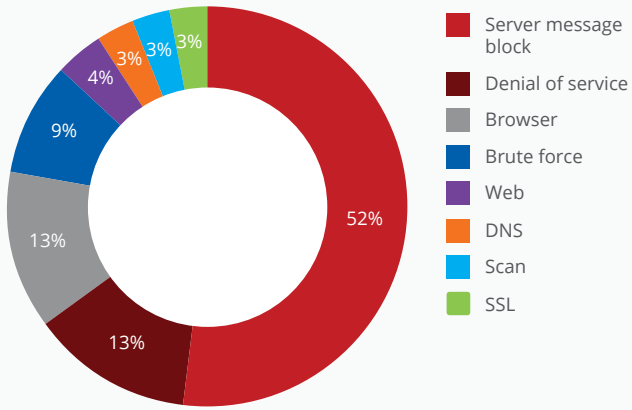
**The Gamut spam botnet outpaced all others during Q2. Most notably, it pushed "Canada Revenue Agency" phishing scams in high volume. Recent campaigns were related to bogus job offers that are commonly used as a "money mule" recruitment tactic.**

## Top countries hosting botnet control servers in Q2




Source: McAfee Labs, 2018.

## Top network attacks in Q2




Source: McAfee Labs, 2018.

Follow

Share

## About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our 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 and Advanced Threat Research

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