REPORT

McAfee
Together is power.

# McAfee Labs Threats Report

June 2018

KEY CAMPAIGNS

Gold Dragon Expands the Reach of Olympics Attacks

Lazarus Rises Again, Targeting Cryptocurrency Users

Advanced Data-Stealing Implants GhostSecret and Bankshot Have Global Reach and Implications

# The McAfee Labs count of total coin miner malware rose by 629% in Q1, to more than 2.9 million samples.

## Introduction

Welcome to the *McAfee® Labs Threats Report June 2018.* In this edition, we highlight the notable investigative research and threat trend statistics gathered by the McAfee Advanced Threat Research and McAfee Labs teams in Q1 of 2018.

In the first quarter, new revelations surfaced concerning complex nation-state threat campaigns that targeted users and enterprise systems worldwide. These campaigns were driven by many objectives—from profit-motivated cybercrime to political subversion to surveillance and espionage. Since our exploration of cryptojacking in the previous issue, we have seen continued expansion of this criminal endeavor during the quarter. The goal of the perpetrators is to monetize their criminal activity by expending the least amount of effort, using the fewest middlemen, and executing their crimes in the shortest time possible and with the least risk of discovery. We also observed that bad actors are demonstrating a remarkable level of technical agility and innovation. Many of the attack schemes that surged toward the end of 2017 have been improved upon in creative and complex ways to avoid detection and mitigation.

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

- Christiaan Beek
- Taylor Dunton
- Steve Grobman
- Mary Karlton
- Niamh Minihane
- Chris Palm
- Eric Peterson
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

Follow

Share

## Key campaigns

### Gold Dragon and the winter Olympic games

In early Q1, McAfee Advanced Threat Research reported an attack targeting organizations involved in the Pyeongchang Winter Olympics in South Korea. The attack was executed via a malicious Microsoft Word attachment containing a hidden PowerShell implant script. The script was embedded within an image file and executed from a remote server.

Our team of analysts also observed several secondary implants that extended the persistence of the initial fileless implant to enable continuous data exfiltration and access. Among those identified was a Korean-language implant, dubbed Gold Dragon, which served as a secondary payload and appeared on the first day of the attack. Gold Dragon had two primary functions: It served as a reconnaissance tool and downloaded and executed subsequent payloads in the attack chain; and it encrypted the data appropriated by other implants and sent the data to the control server. Gold Dragon is a particularly slippery instance of fileless malware because it is designed to be evasive, checking on processes related to antimalware solutions.

### Lazarus and cryptocurrency campaigns

The Lazarus cybercrime ring has reared its head again, launching a new, highly sophisticated Bitcoin-stealing phishing campaign—HaoBao—which targets global financial organizations and Bitcoin users. When recipients open malicious attachments, an implant scans for Bitcoin activity and establishes an implant for persistent data gathering. These techniques bear a strong similarity to other attacks that are believed to have been perpetrated by Lazarus.

Follow

Share

In early 2017, Lazarus was responsible for a Korean- and English-language phishing email campaign, in which attackers posed as employment recruiters. The primary targets were defense contractors and financial institutions, and the object of the campaigns was to obtain sensitive military information or to steal money. A key component of the campaign, which appeared to have ended in October 2017, was the use of malicious attachments.

Investigations of several attacks that delivered documents via Dropbox revealed the use of two implants—the first for data gathering and the second to establish persistence. These were typically embedded in older versions of Word documents that were launched via a Visual Basic macro. Once these actions were performed, the malware sent the data to a control server.

These techniques, tactics, and procedures bear a strong resemblance to 2017 campaigns targeting US defense contractors, US energy sector, financial organizations, and cryptocurrency exchanges. Stay tuned for the unfolding of the HaoBao cryptocurrency attacks.

## GhostSecret/Bankshot

McAfee Advanced Threat Research uncovered yet another global campaign targeting multiple sectors—from health care and finance to entertainment and telecommunications. Operation GhostSecret, which is currently active, is believed to be associated with the international cybercrime group known as Hidden Cobra. This extremely complex campaign, which employs a series of implants to appropriate data from infected systems, is also characterized by its ability to evade detection and throw forensic investigators off its trail. Our analysis also uncovered an infrastructure with servers based in India that are part of a covert network which collects the data and appears to be used for launching other attacks.

The first signs of this campaign targeted Turkish financial organizations and employed the Bankshot implant, which was first reported by the US Department of Homeland Security in December 2017. As with most threats of this type, phishing emails with malicious Word attachments were used to launch the attack. This new Bankshot variation uses an embedded Adobe Flash exploit to enable the execution of an implant.

The latest variant of GhostSecret not only uses Bankshot implant techniques, but it also incorporates elements of the Destover malware, which was used in the 2014 Sony Pictures attack, and the Proxysvc implant, a previously undocumented implant, which has operated undetected since mid-2017.

The combination of these data-gathering implants indicates that attackers such as Hidden Cobra are continually refining and honing their tools and scaling up their capabilities. GhostSecret will likely continue to target organizations worldwide.

## Key trends: Bad actors strive to do better

In Q1 2018, McAfee Labs recorded, on average, five new malware samples per second—a decrease from eight new samples per second in Q4. Despite a quarter-over-quarter decline in new malware of 31%, Q1 2018 saw notable technical developments among bad actors seeking to improve upon the latest successful technologies and tactics to outmaneuver their targets' defenses.

**From PowerShell to LNK:** In 2017 we saw a surge in the exploitation of benign technologies for malicious purposes, such as PowerShell. In Q1 2018, we saw malicious actors turn away from PowerShell exploits, which dropped 77%, and take advantage of LNK capabilities. New LNK malware rose 59% in Q1.

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 analyzed 2,400,000 URLs and 700,000 files.

In Q1, our customers saw the following attack volumes:

- An average of 51 billion queries received per day
- Protections against malicious files increased to 79 million per day in Q1, up from 45 million in Q4
- Protections against high-risk URLs increased to 49 million per day in Q1, up from 37 million in Q4
- Protections against high-risk IP addresses increased to 35 million per day in Q1, up from 26 million in Q4

**From Locky to Gandcrab:** Technical agility was also demonstrated by Gandcrab ransomware activity. Although overall new ransomware growth slowed by 32% in Q1, Gandcrab infected 50,000 systems in the first three weeks of the quarter, supplanting the Locky ransomware strains as the quarter's ransomware leader. Gandcrab uses new criminal methodologies, such as transacting ransom payments through the Dash cryptocurrency rather than through Bitcoin.

**Cryptojacking—infect and collect:** Cryptocurrencies also continued to shape the cyberthreat landscape in Q1, as cybercriminals extended their activity into the area of cryptojacking, the infection of user systems for the purpose of hijacking and using them to mine for cryptocurrencies.

Coin miner malware grew a stunning 629% to more than 2.9 million known samples in Q1 from almost 400,000 samples in Q4. This suggests that cybercriminals are warming to the prospect of monetizing infections of user systems without prompting victims to make payments, as is the case with popular ransomware schemes. Compared with well-established cybercrime activities such as data theft and ransomware, cryptojacking is simpler, more straightforward, and less risky. All criminals must do is infect millions of systems and start monetizing the attack by mining for cryptocurrencies on victims' systems. There are no middlemen, there are no fraud schemes, and there are no victims who need to be prompted to pay and who, potentially, may back up their systems in advance and refuse to pay.

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.

*—Steve Grobman, Chief Technology Officer*

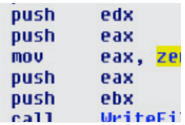
*—Raj Samani, Chief Scientist and McAfee Fellow, Advanced Threat Research*

Twitter @Raj_Samani

Follow

Share

# Table of Contents



```
push    edx
push    eax
mov     eax, ze
push    eax
push    ebx
call    WriteFi
```

## Gold Dragon Expands the Reach of Olympics Attacks

The Gold Dragon implant, first discovered by McAfee Advanced Threat Research analysts as part of a fileless malware attack targeting organizations involved in the Pyeongchang Winter Olympics in South Korea, is indicative of a new breed of tools and techniques that is gaining ground among attackers. Many fileless malware campaigns leverage PowerShell to launch an attack in memory to create a backdoor into a system. Gold Dragon stands out because it was customized for the Olympics attack, it persisted on infected systems, and it has shown up in subsequent attacks, notably on hacked servers in Chile slightly over a week after the Olympics incident. Gold Dragon is a particularly slippery instance of fileless malware because it is designed to be evasive, checking on processes related to antimalware solutions.

Like most attacks, the point of entry is via the user. Socially engineered emails were sent with a malicious Word attachment containing a hidden PowerShell implant script. When recipients clicked on the attachment, they were asked to enable a process that allowed them to view the content in their version of Word. The malware launched a Visual Basic macro that executed the PowerShell script from a remote server. This script then downloaded an image file and embedded additional PowerShell scripts into the pixels of the image. Further techniques add another layer of obfuscation, making Gold Dragon extremely difficult to detect, particularly after it found its way into a command line and made a connection to the attacker's control server, gathering system-level data that profiled targeted machines.

The Korean-language implant Gold Dragon is a secondary implant that extended persistence to the initial fileless implant to enable continuous data exfiltration and access. It has many similarities to implants such as Ghost419 and Brave Prince, which we have observed since mid-2017.

Follow

Share

Gold Dragon served multiple functions in the Olympics attack:

- It is believed to have been a second-stage payload in the Olympics attack
- It acted as both a reconnaissance tool and a downloader for other payloads
- It profiled the targeted device, gathering information such as directories on the desktop, recently accessed files, and program file folder; registry key and value information for the user's run key; and more
- It encrypted this data and sent it to the remote server
- To evade detection, it scouted for and terminated processes related to antimalware or antivirus solutions
- It was also capable of downloading and executing other components of the attack from the remote server

Gold Dragon is just one of many implants used in fileless malware attacks that provided attackers with distinct advantages: the ability to establish persistence and to enable continuous data exfiltration.

Follow

Share

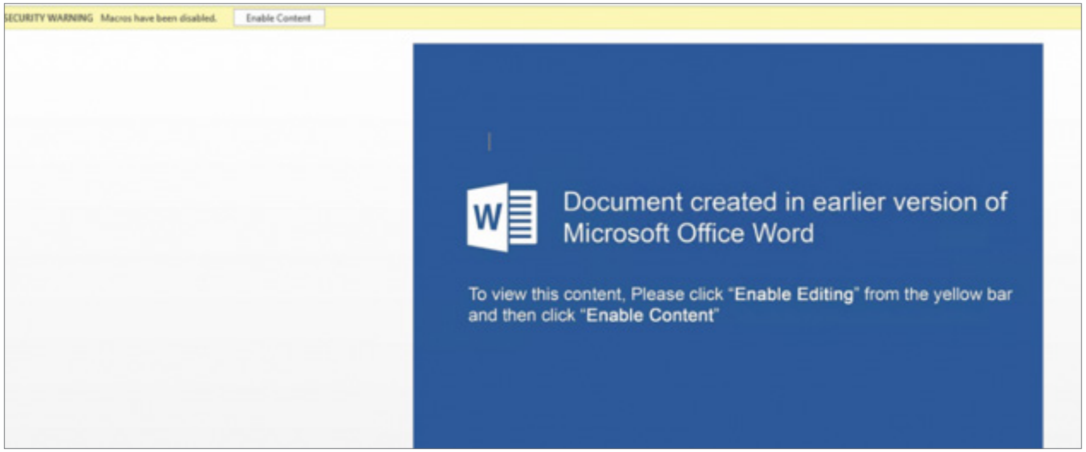
## Lazarus Rises Again, Targeting Cryptocurrency Users

Dormant for a short while during the latter part of 2017, the international cybercrime group known as Lazarus has resurfaced in Q1 2018—this time with a highly sophisticated and complex cryptocurrency scheme known as HaoBao. In the previous issue of the McAfee Labs Threats Report, we commented on how the increase in the valuation of Bitcoin prompted cybercriminals to expand their activities beyond demanding ransomware payments with cryptocurrency to cryptojacking, or mining for cryptocurrency.

Prior to the HaoBao campaign, McAfee researchers uncovered a spear-phishing campaign associated with Lazarus that targeted employees who worked at defense contractors and financial institutions. The object of the campaign was to appropriate sensitive data or steal funds. This campaign appeared to have run its course by October 2017.

In Q1 2018, McAfee Advanced Threat Research analysts discovered a new campaign, which ostensibly recruited for a business development executive of a large multinational bank located in Hong Kong.

The email enticed recipients to download infected Word documents from Dropbox. Much like the Gold Dragon attack described in the previous section, the documents were embedded in older versions of Word documents launched via a Visual Basic macro that presumably enabled the user to see the document in the current



Document created in earlier version of Microsoft Office Word

To view this content, Please click "**Enable Editing**" from the yellow bar and then click "**Enable Content**"

Figure 1. Example of the attack lure: a Microsoft Word document that appears to be an older version.

Follow

Share

version of Word. Once the user performed these actions, the malware exfiltrated system data and sent it to a control server.

This type of implant had not been detected before. This campaign used a one-time data-gathering implant that relied on downloading a second-stage implant to gain persistence. The implants contained the hardcoded word *haobao,* which triggered the execution of the data exfiltration mechanism by way of the Visual Basic macro. The purpose of the collected data was to identify targets for future attacks, specifically those who were running Bitcoin-related software through certain system scans.

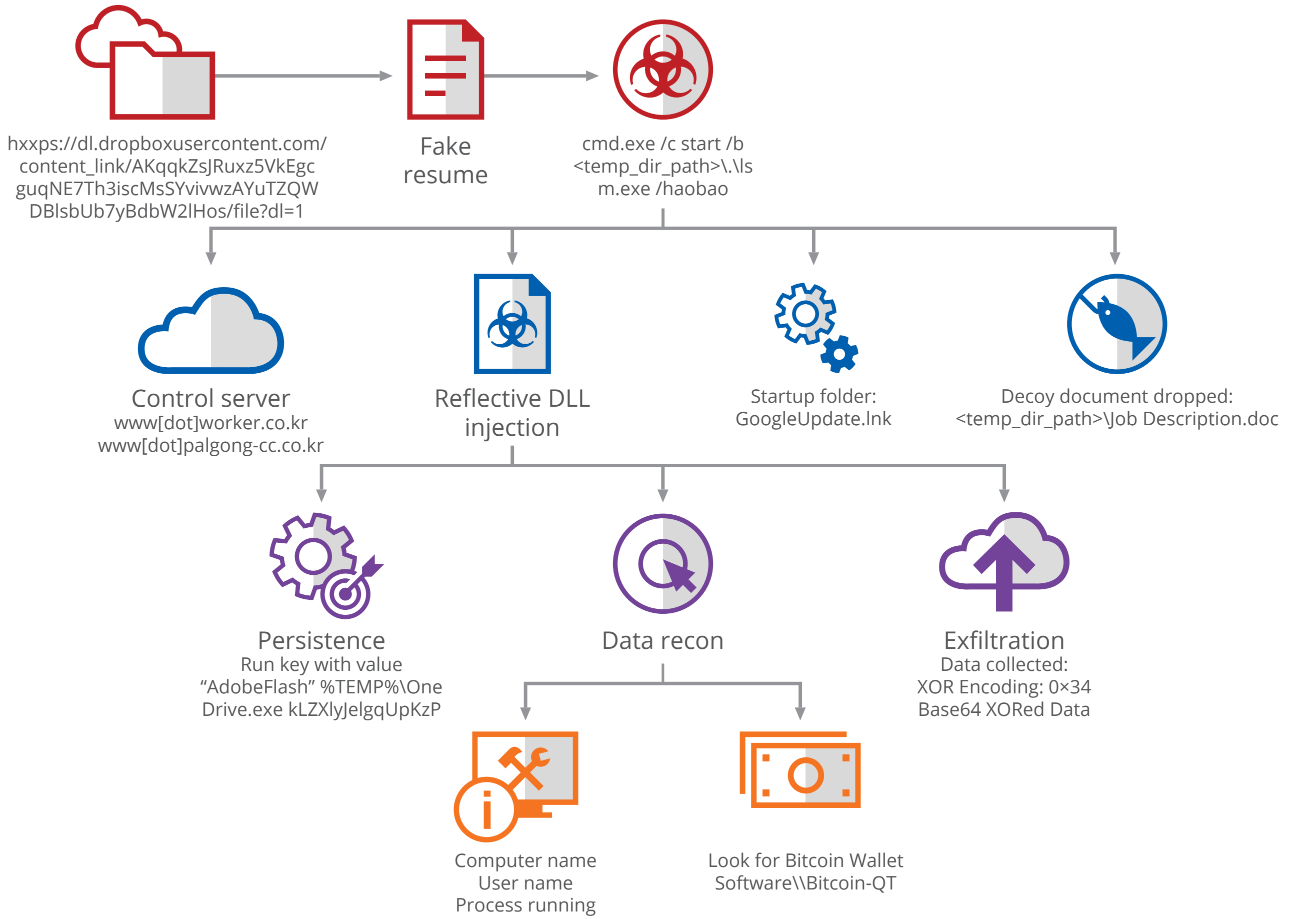


Figure 2. The trajectory of the HaoBao implant.

Follow

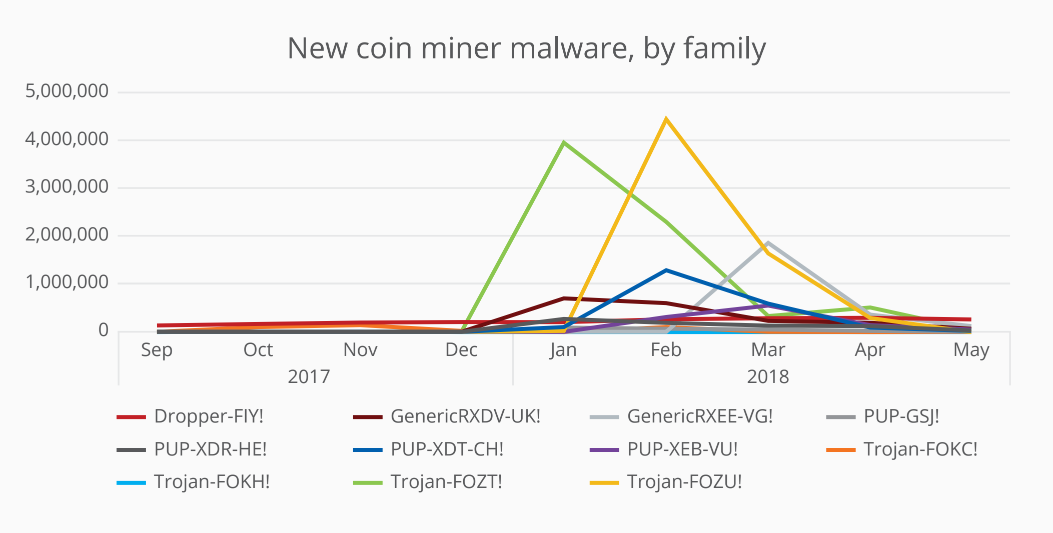
Share

McAfee analysts established a connection to Lazarus based on techniques that are similar to 2017 campaigns targeting the US Department of Defense, US Department of Energy, financial institutions, and cryptocurrency exchanges. They came to this conclusion with a high degree of confidence based on these observations:

- Attackers contact an IP address or domain that was used to host a malicious document from a previous Lazarus campaign in 2017
- The same author appears in these recent malicious documents who also appeared in the Lazarus 2017 campaigns
- HaoBao uses the same malicious document structure and similar job recruitment ads as in previous Lazarus campaigns
- The techniques are in alignment with the Lazarus group's interest in cryptocurrency theft

We expect to see cryptocurrency mining campaigns gain more traction and perhaps even overtake ransomware. Cybercriminals find campaigns such as HaoBao to be highly advantageous because they are more profitable and more difficult to detect with no apparent damage being done.

For a deeper look at the growing prevalence of CoinMiner, a malware variant that takes control of a victim's computer to mine new coins by infecting user executables, injecting Coinhive JavaScript into HTML files, and blocking the security products to halt signature updates, read the McAfee Labs post "Parasitic Coin Mining Creates Wealth, Destroys Systems."



Follow

Share

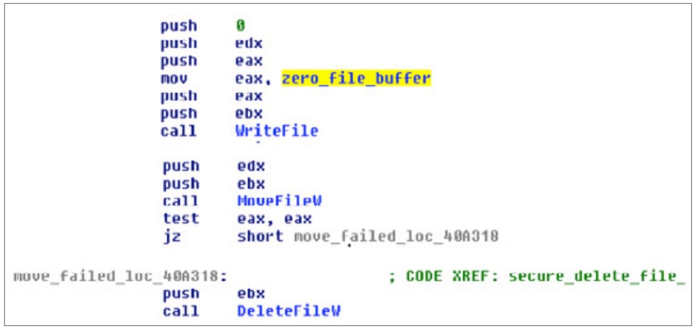
## Advanced Data-Stealing Implants GhostSecret and Bankshot Have Global Reach and Implications

The state-sponsored cybercrime group, Hidden Cobra, has recently launched data reconnaissance campaigns of global proportions. It appears that no sector has been spared by Operation GhostSecret. Hidden Cobra has attacked critical infrastructure organizations, financial institutions, health care, telecommunications, and the entertainment industry. The new implants leveraged in this campaign bear some resemblance to those used in other attacks, such as Bankshot and Proxysvc.

The key takeaway is that the threat actors continue to evolve their tools, increasing complexity and functionality. In addition to discovering these capabilities, our investigation uncovered an infrastructure connected to these operations with servers in India. The main objective of Operation GhostSecret appears to be covert data gathering in preparation for large-scale future attacks.

The first detectable activity targeted Turkish financial and trade institutions. In this campaign, we saw the return of the Bankshot implant, which first surfaced in 2017. The objective appears to be data gathering from financial institutions for possible future heists. Bankshot takes advantage of an unpatched zero-day vulnerability in Adobe Flash. The implants are distributed from a domain that looks similar to the legitimate cryptocurrency-lending platform Falcon Coin.

Initiated with a spear-phishing email employing a Word document, the campaign introduces the Bankshot implant, embedded in a Flash file that executes when the recipient opens the document. This version of the Bankshot implant both gives attackers complete remote access to systems and enables them to wipe files and content to remove all traces of destructive or malicious activity. Reconnaissance capabilities range from



```
                push    0
                push    edx
                push    eax
                mov     eax, zero_file_buffer
                push    eax
                push    ebx
                call    WriteFile

                push    edx
                push    ebx
                call    MoveFileW
                test    eax, eax
                jz      short move_failed_loc_40A318

move_failed_loc_40A318:                         ; CODE XREF: secure_delete_file_
                push    ebx
                call    DeleteFileW
```

Figure 3. A file-wiping technique used in Operation GhostSecret.

Follow

Share

generating a list of files in a directory that are forwarded to the control server to gathering domain and account names for all running processes. In addition, Bankshot can create a process by impersonating a logged-on user, overwrite files with zeros and mark them for deletion on reboot, or completely terminate processes.

In Operation GhostSecret, Hidden Cobra has taken this level of activity beyond the financial sector with a new class of implant that derives some coding structures and functionality from previous implants. The newly discovered, more advanced implant can accept extensive commands from the control server, making it a robust framework for data reconnaissance and data exfiltration. In addition to wiping and deleting files, the implant can execute other implants, read data out of files, and more.

Our observations and analysis corroborate our strong belief that as the capabilities of malware authors increase in sophistication, campaigns such as Operation GhostSecret will usher in bigger and more malicious cross-sector attacks in the near future.

### Trojan-Bankshot2: MITRE Adversarial Tactics, Techniques, and Common Knowledge

- **Exfiltration over control server channel:** Data is exfiltrated over the control server channel using a custom protocol
- **Commonly used port:** The attackers used common ports, such as port 443, for control server communications
- **Service execution:** The implant is registered as a service on the victim's machine
- **Automated collection:** The implant automatically collects data about the victim and sends it to the control server
- **Data from local system:** The malware discovers the local system and gathers data
- **Process discovery:** Implants can list processes running on the system
- **System time discovery:** As part of the data reconnaissance method, the system time is sent to the control server
- **File deletion:** Malware can wipe files indicated by the attacker

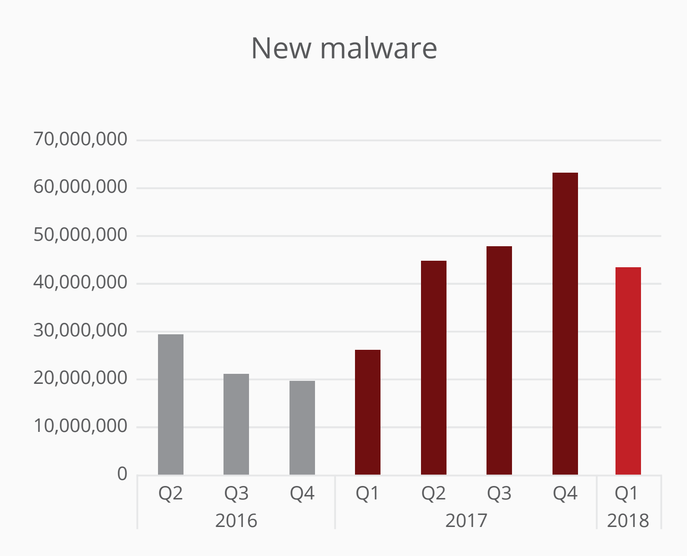
Figure 4. Indicators of compromise of the Bankshot implant.

Follow

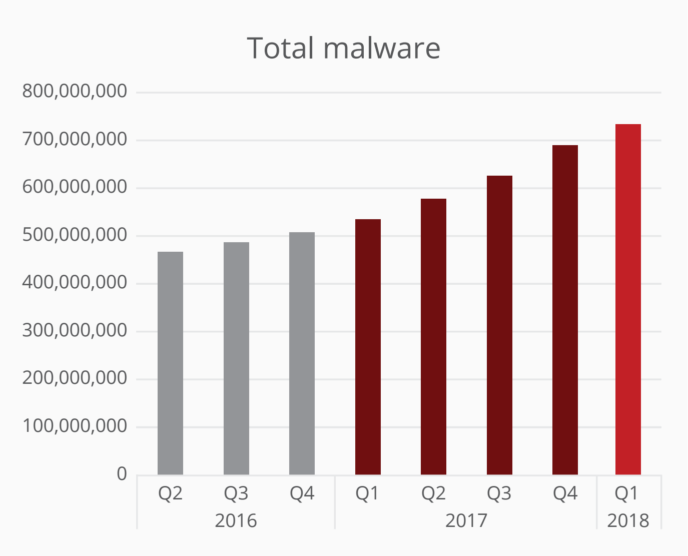
Share

# Threats Statistics

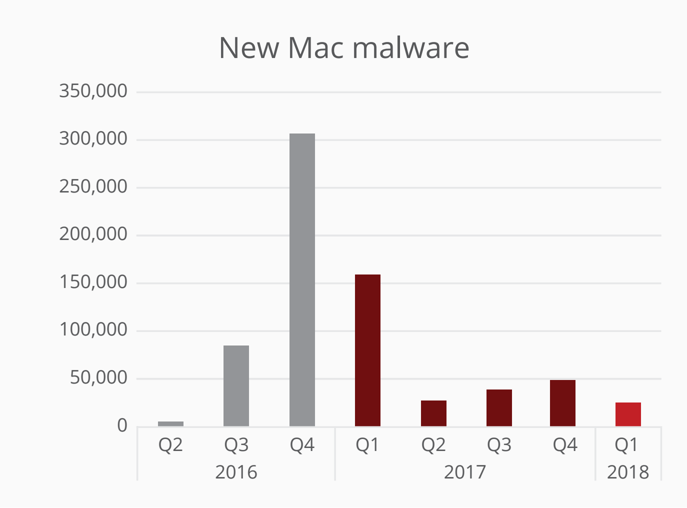
## Malware



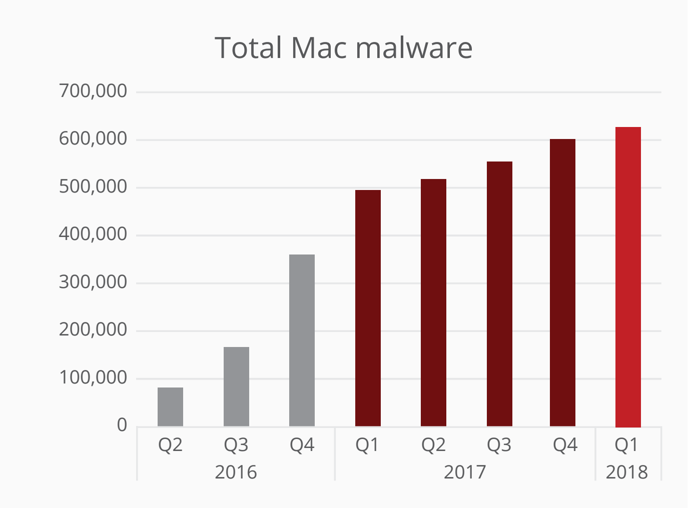
Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

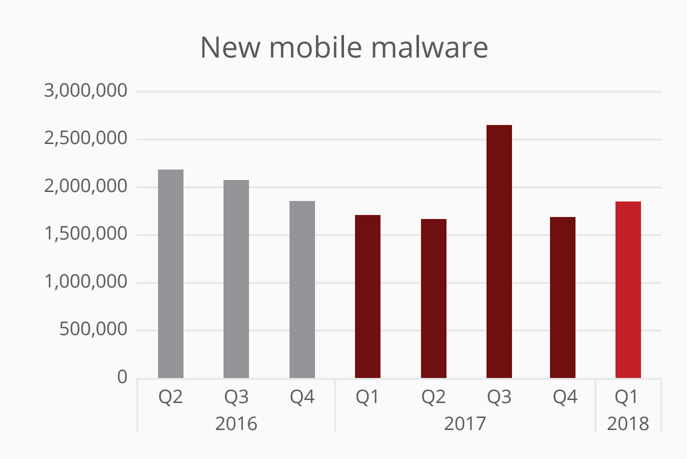


Source: McAfee Labs, 2018.

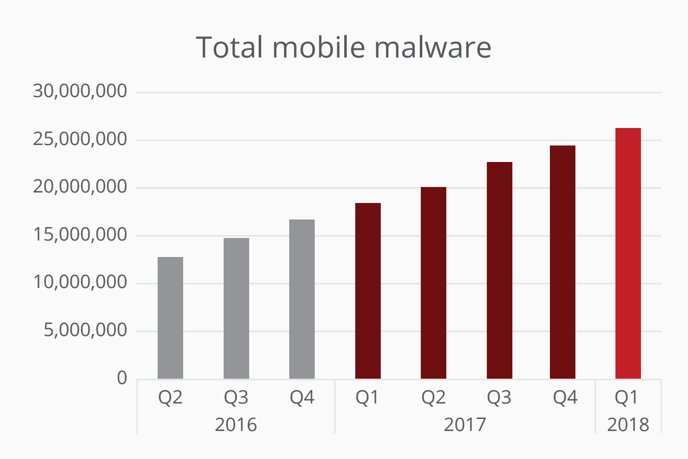
Malware data comes from the McAfee Sample Database, which includes malicious files gathered by McAfee spam traps, crawlers, and customer submissions, as well as from other industry sources.

Follow

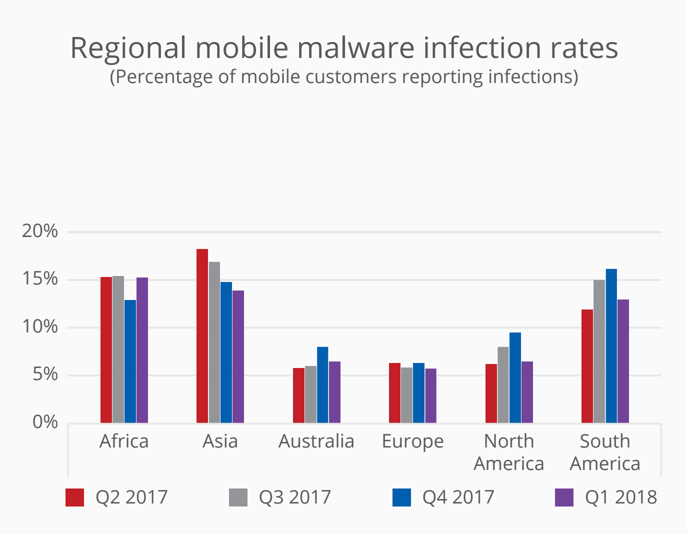
Share


New mobile malware

Source: McAfee Labs, 2018.

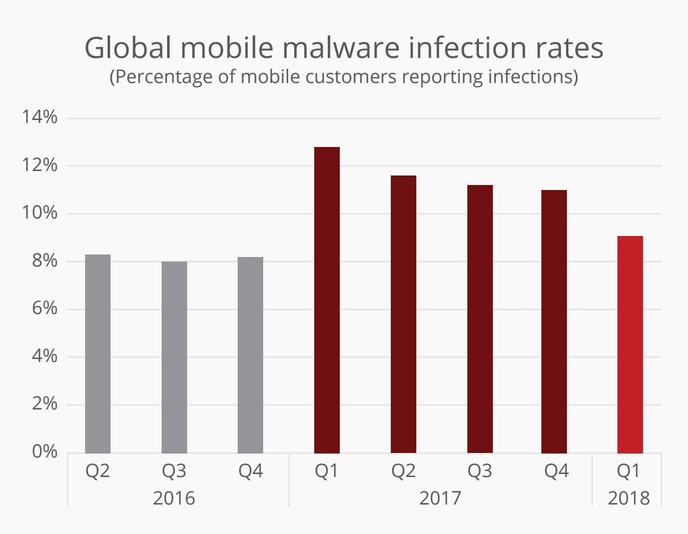

Total mobile malware

Source: McAfee Labs, 2018.


Regional mobile malware infection rates

(Percentage of mobile customers reporting infections)

Source: McAfee Labs, 2018.

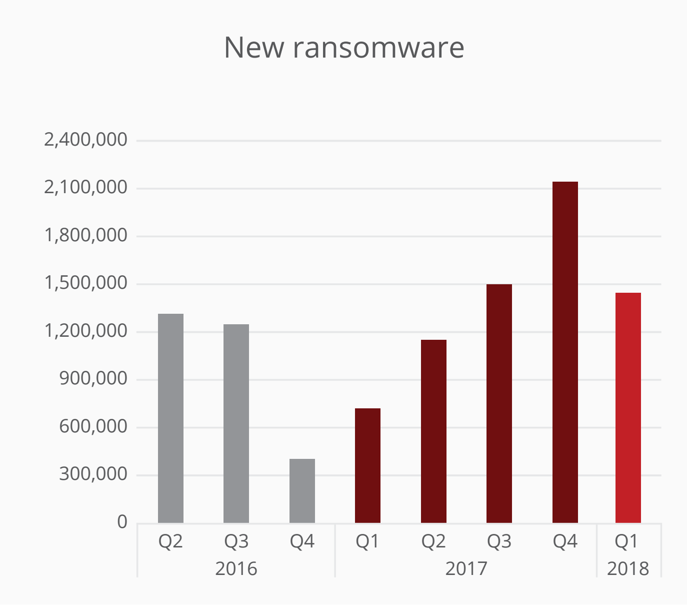

Global mobile malware infection rates

(Percentage of mobile customers reporting infections)

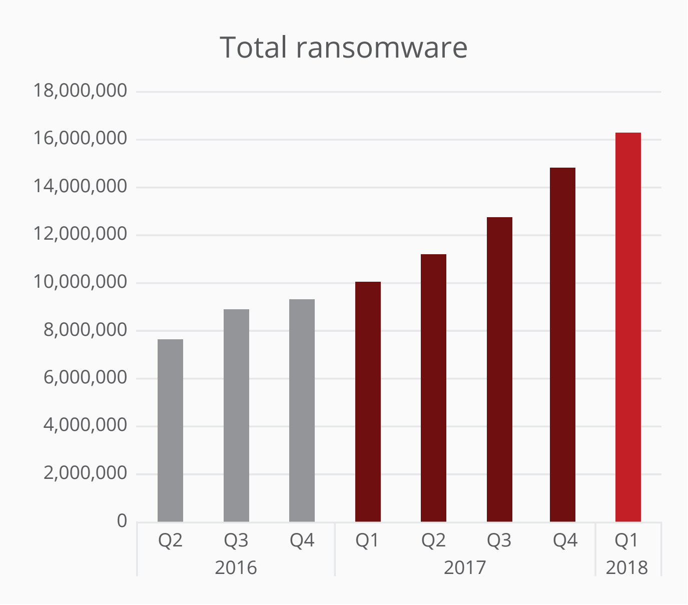
Source: McAfee Labs, 2018.

Follow

Share

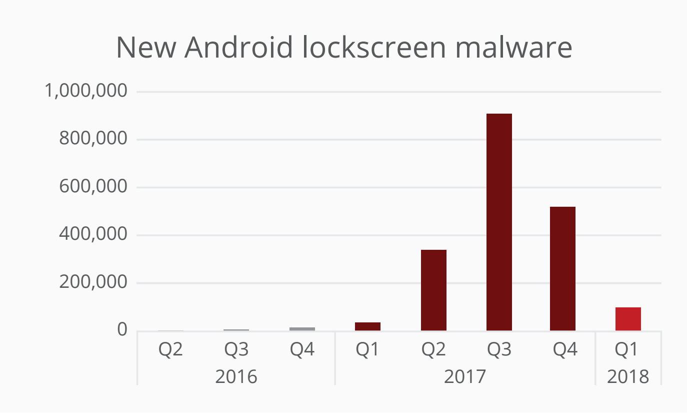


Source: McAfee Labs, 2018.

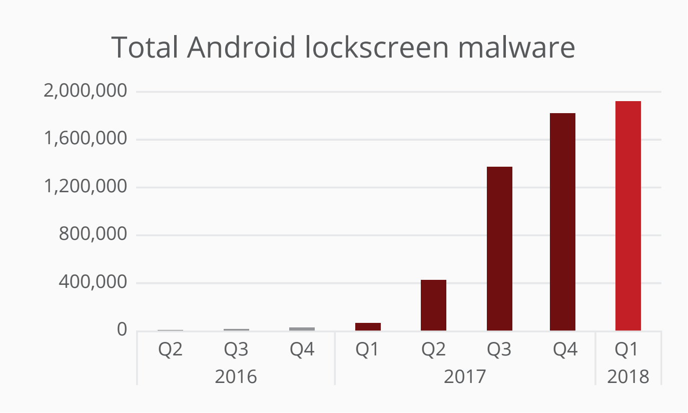


Source: McAfee Labs, 2018.

The 81% decline in new Android lockscreen malware made a significant contribution to the drop in new ransomware in Q1.



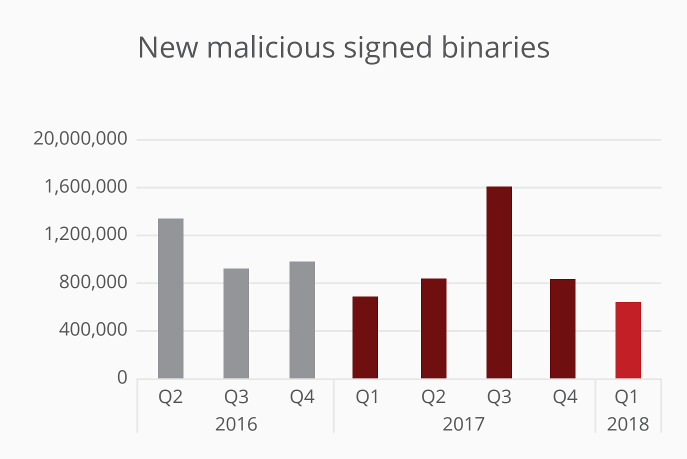
Source: McAfee Labs, 2018.



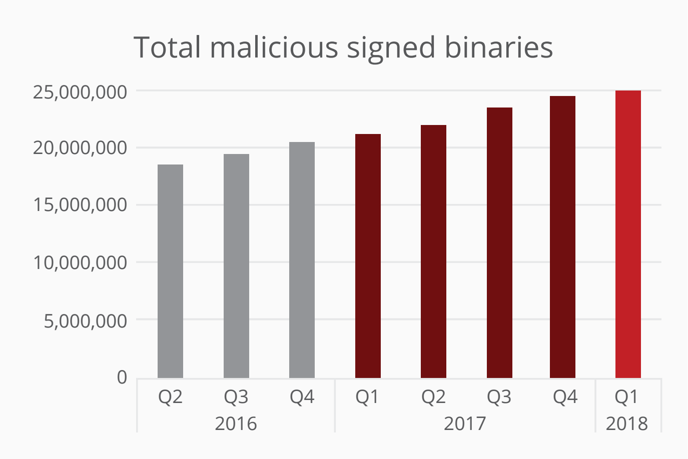
Source: McAfee Labs, 2018.

Follow

Share

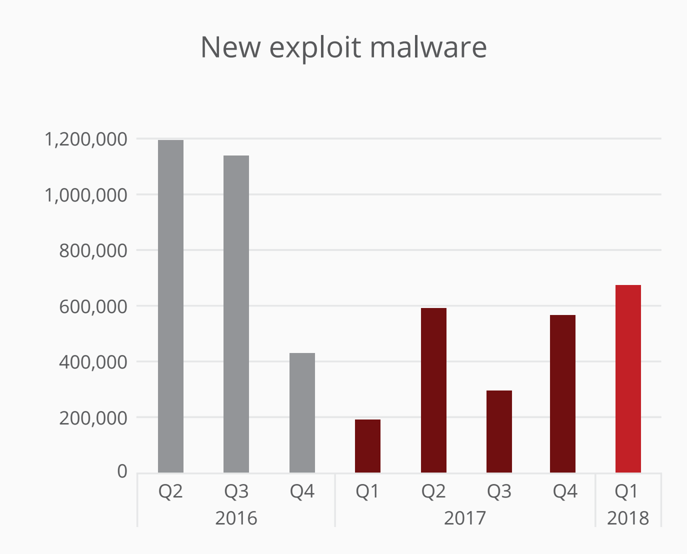


Source: McAfee Labs, 2018.

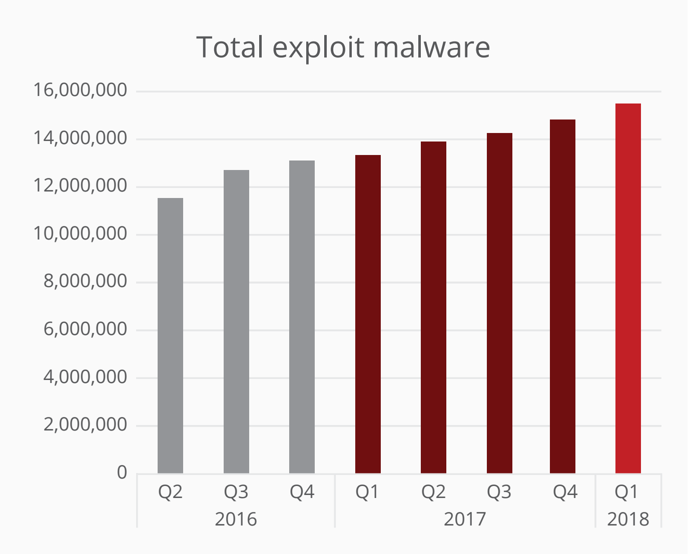


Source: McAfee Labs, 2018.

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.

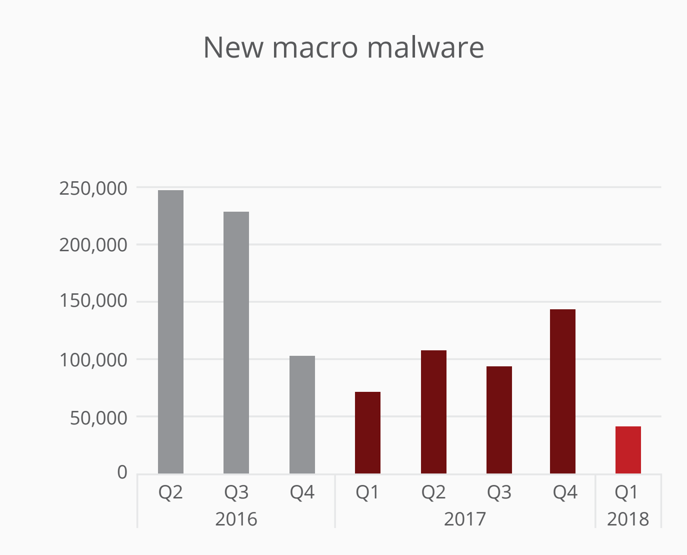


Source: McAfee Labs, 2018.

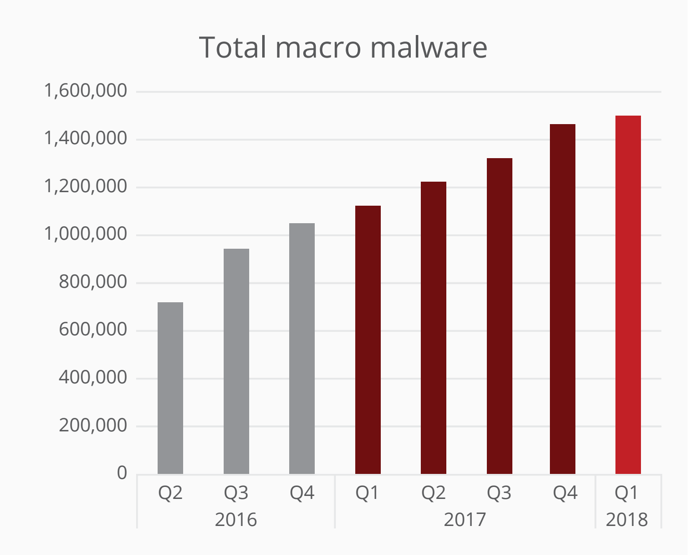
Exploits take advantage of bugs and vulnerabilities in software and hardware. Zero-day attacks are examples of successful exploits. For a recent example, see the McAfee Labs post "Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability."

Follow

Share

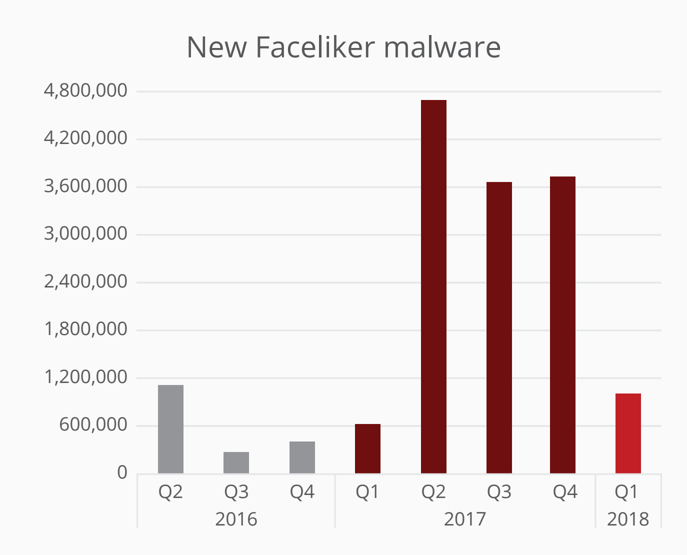


Source: McAfee Labs, 2018.

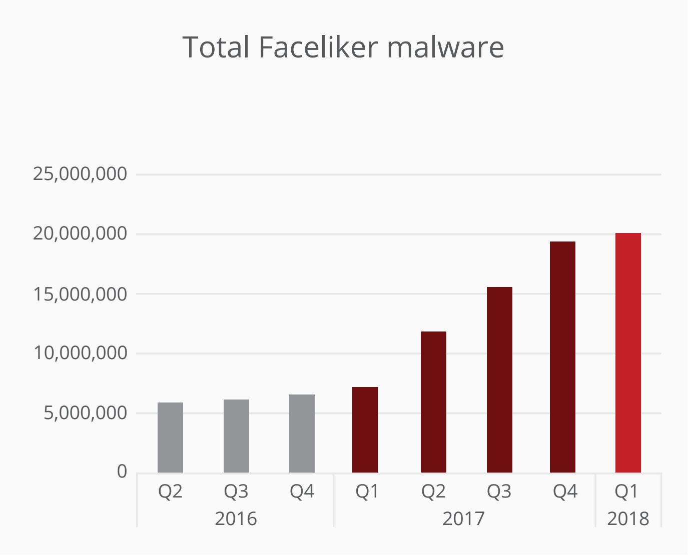


Source: McAfee Labs, 2018.

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.

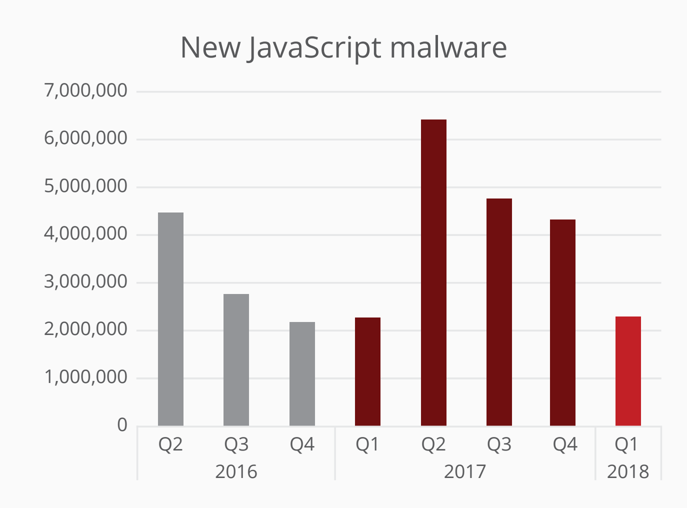


Source: McAfee Labs, 2018.

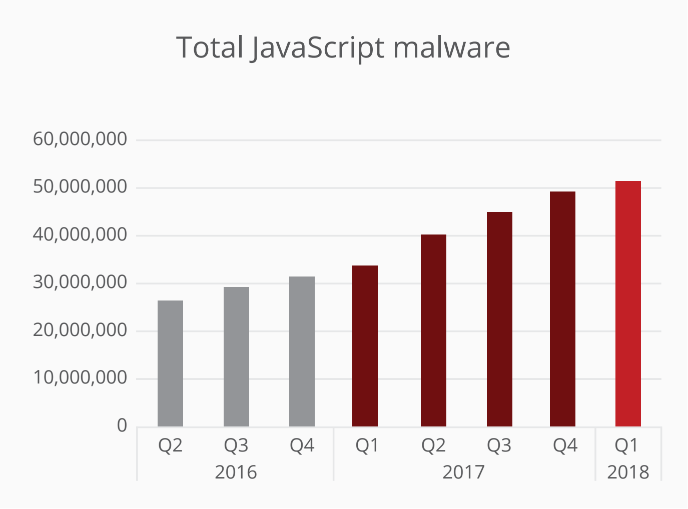
The Faceliker Trojan manipulates Facebook clicks to artificially "like" certain content. To learn more, read this post from McAfee Labs.

Follow

Share

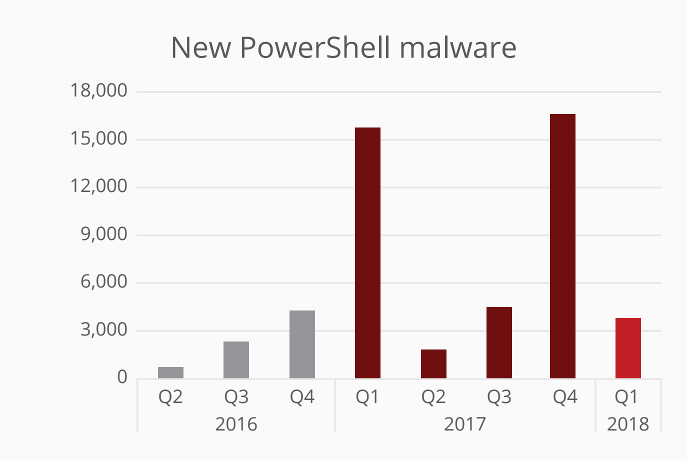


Source: McAfee Labs, 2018.

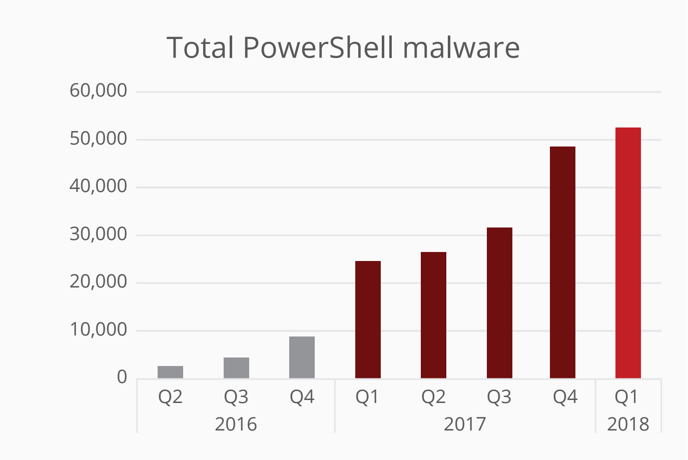


Source: McAfee Labs, 2018.

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



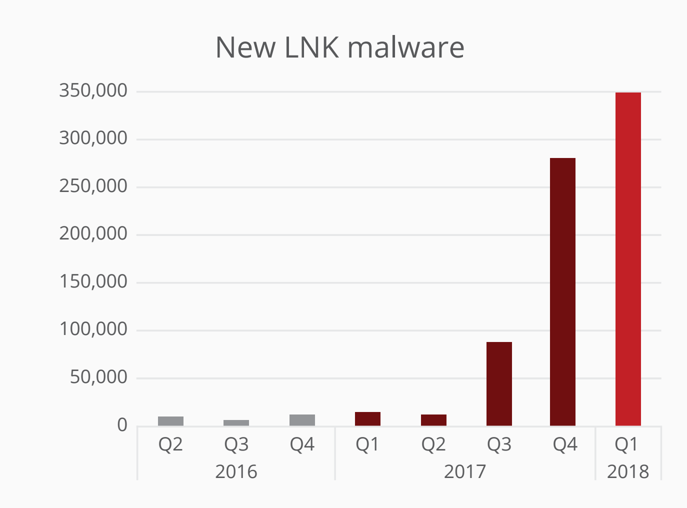
Source: McAfee Labs, 2018.



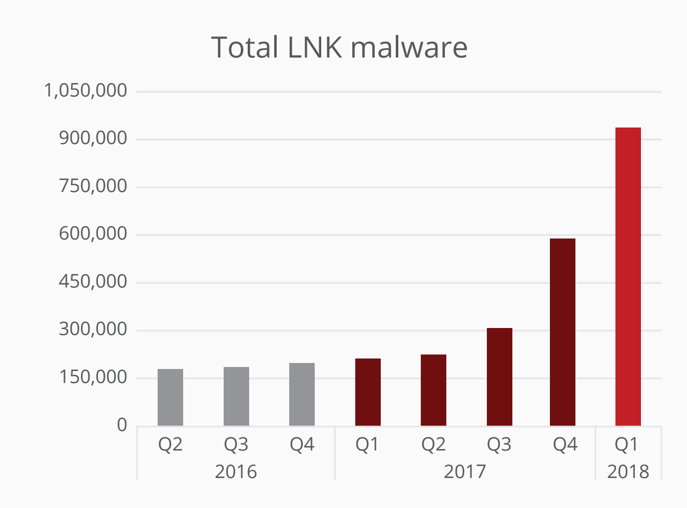
Source: McAfee Labs, 2018.

Follow

Share

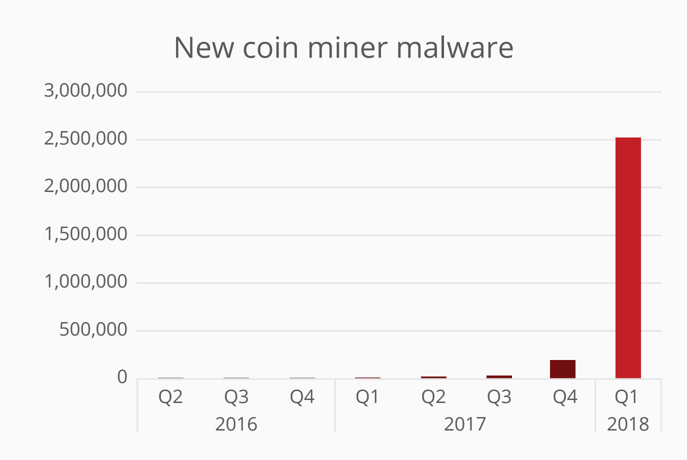


Source: McAfee Labs, 2018.

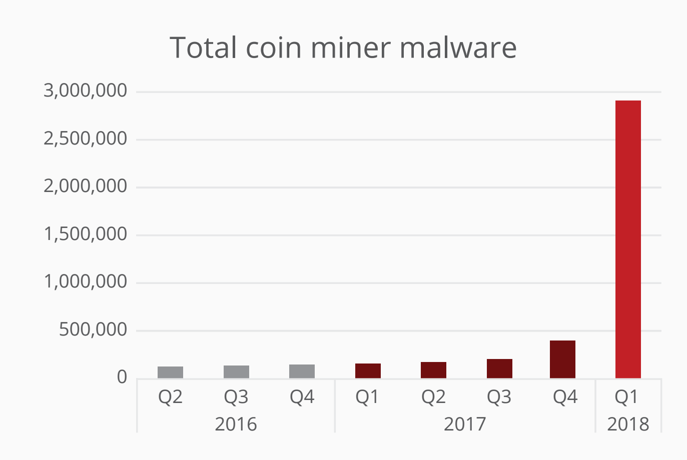


Source: McAfee Labs, 2018.

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



Source: McAfee Labs, 2018.



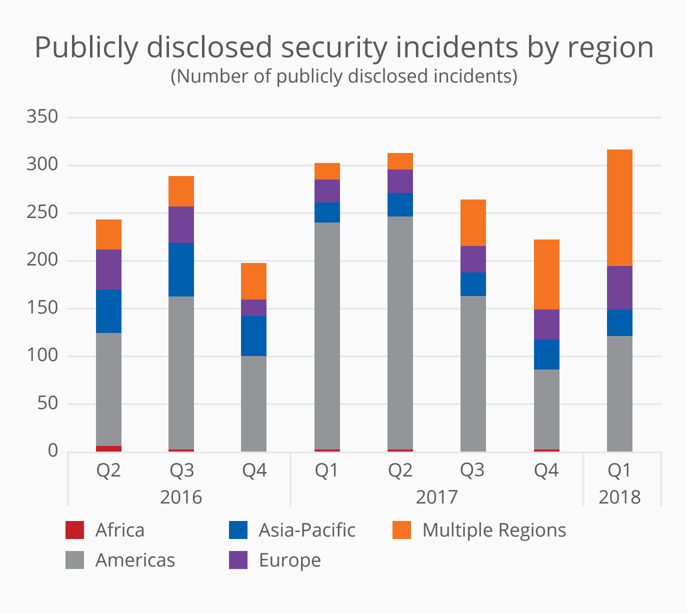
Source: McAfee Labs, 2018.

Coin miner malware hijacks systems to create ("mine") cybercurrency without victims consent or awareness. New coin miner threats jumped by 1,189% in Q1.

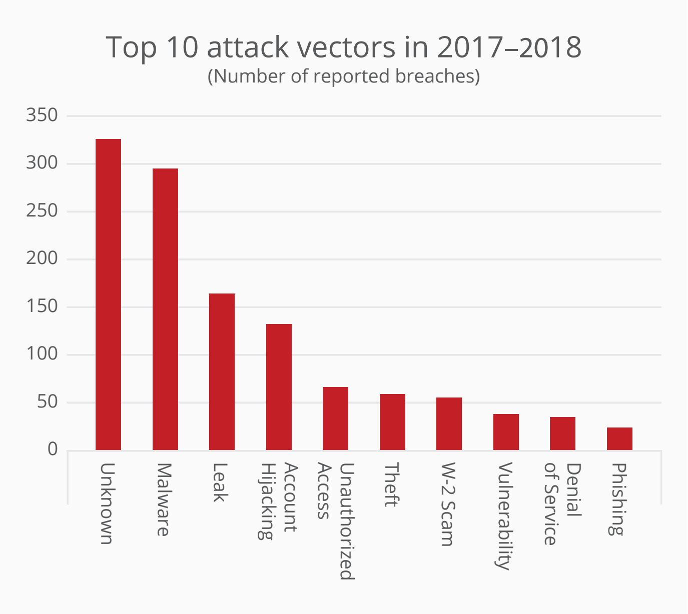
Follow

Share

## Incidents



Source: McAfee Labs, 2018.



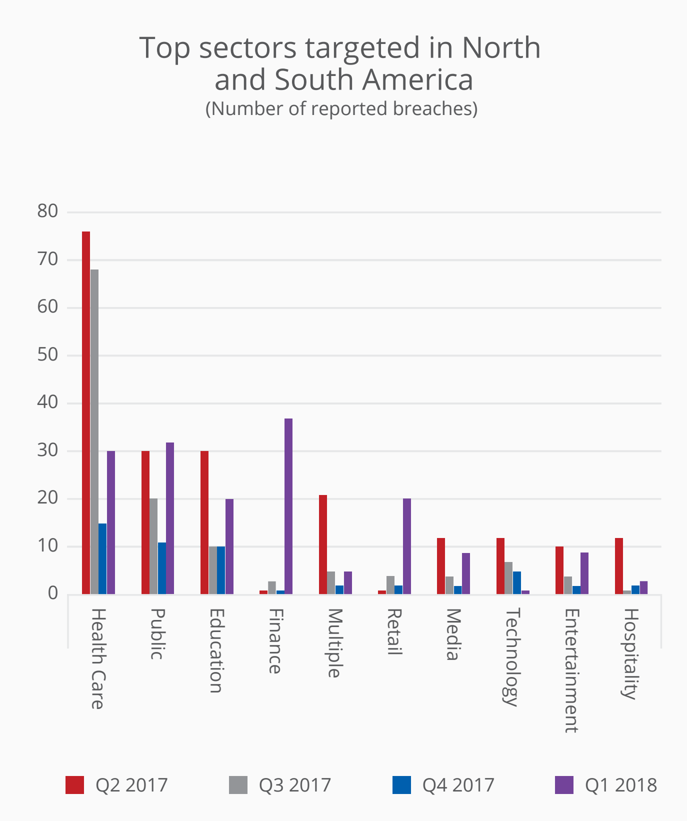
Source: McAfee Labs, 2018.

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

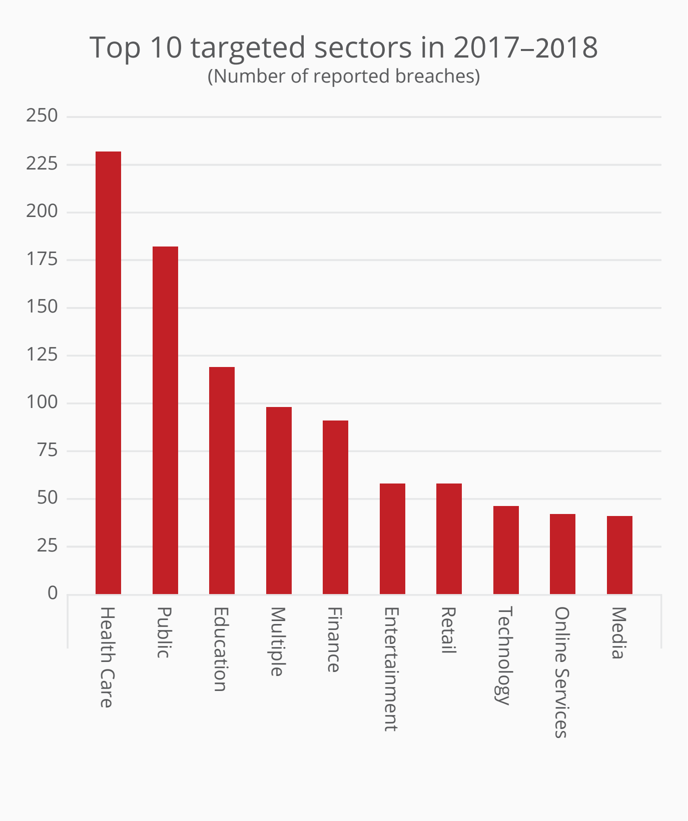
The majority of attack vectors are either not known or not publicly reported.

Follow

Share



Source: McAfee Labs, 2018.

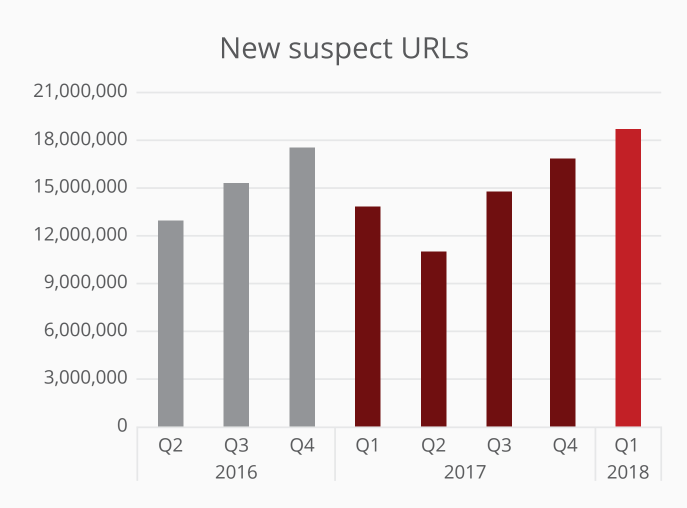


Source: McAfee Labs, 2018.

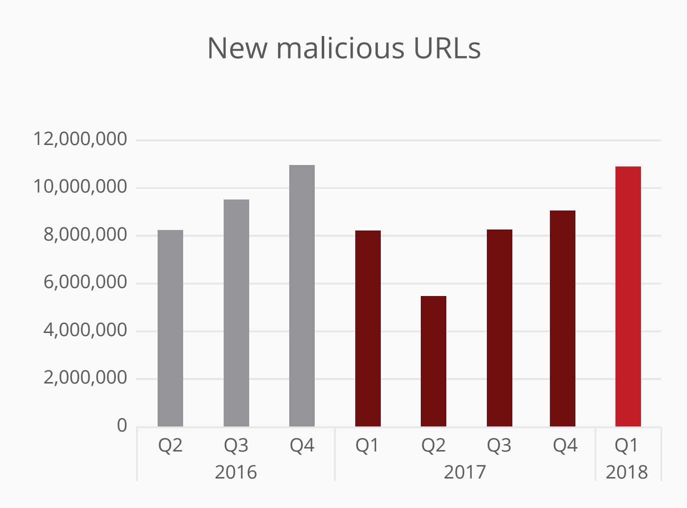
Follow

Share

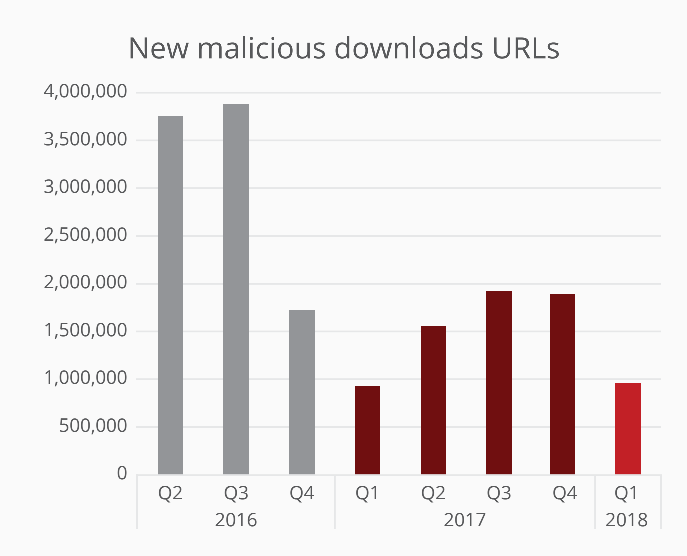
## Web and Network Threats



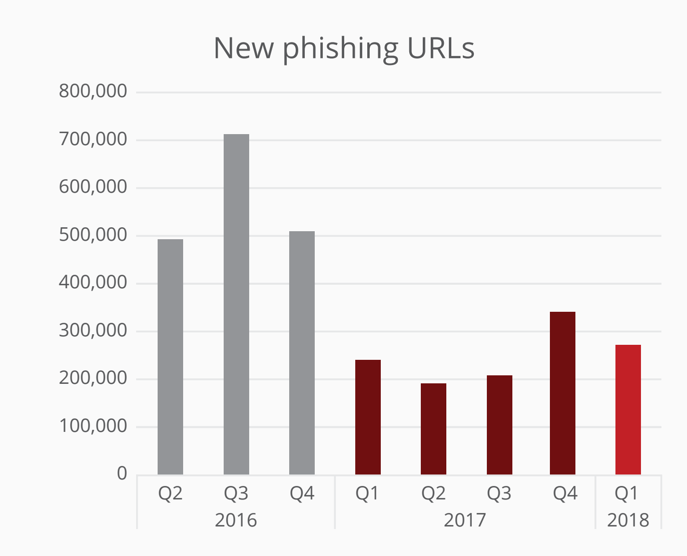
Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.



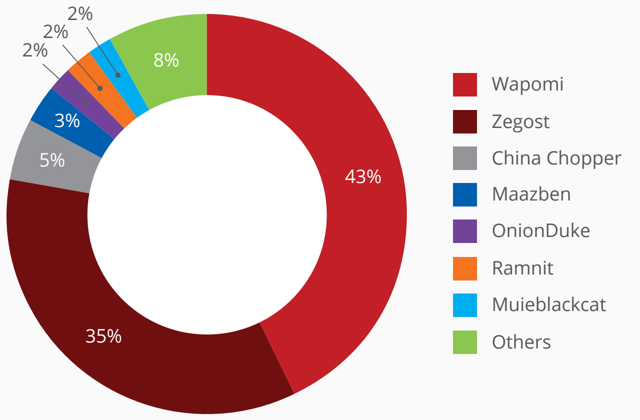
Source: McAfee Labs, 2018.

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

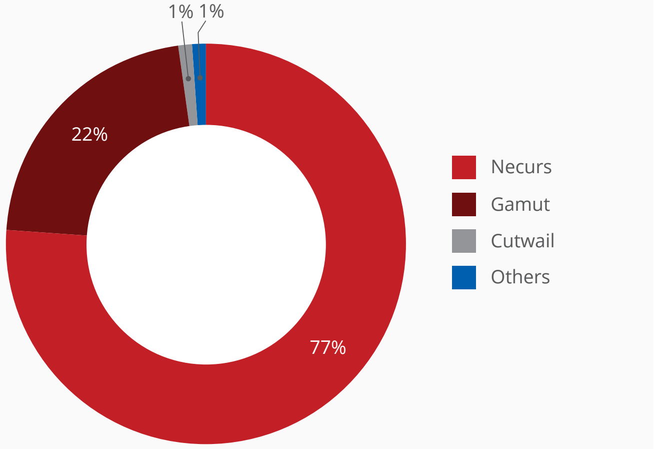
Share

Top malware connecting to control servers in Q1



Source: McAfee Labs, 2018.

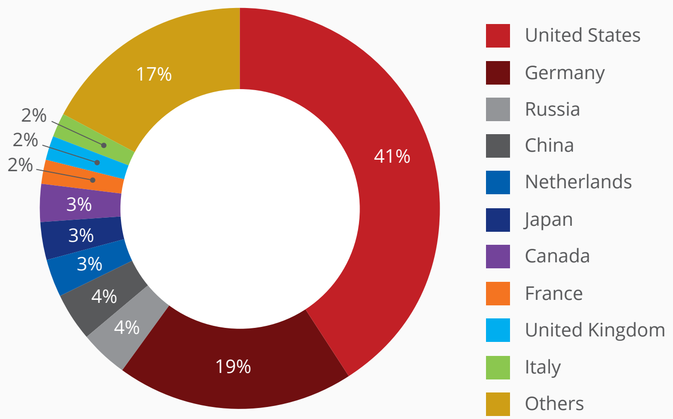
Spam botnet prevalence by volume in Q1



Source: McAfee Labs, 2018.

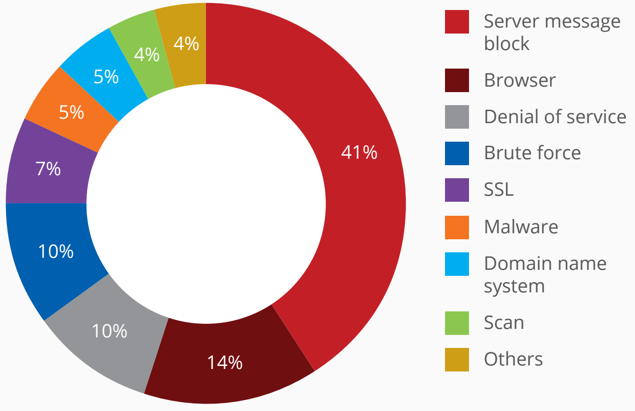
**Responsible for roughly three-quarters of botnet spam observed during Q1, the Necurs botnet again takes the top rank. Romance scams, ransomware, and downloaders were popular threats. Gamut remains second, despite a nearly 50% decrease in volume from Q4 2017.**

Top countries hosting botnet control servers in Q1



Source: McAfee Labs, 2018.

Top network attacks in Q1



Source: McAfee Labs, 2018.

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 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