McAfee
Together is power.

# McAfee Labs Threats Report

**December 2018**

**TOP STORIES OF THE QUARTER**

Underground Forums Boost the Effectiveness of Cybercriminals

Cryptomining Boom Times Continue

Exploit Kits Add Support for Vulnerabilities, Ransomware

Targeted Attacks Motivated by Cyber Espionage

## Introduction

Welcome to the *McAfee® Labs Threats Report, December 2018*. In this edition, we highlight the notable investigative research and trends in threats statistics and observations gathered by the McAfee Advanced Threat Research and McAfee Labs teams in Q3 of 2018.

We are very excited to present to you new insights and a new format in this report. We are dedicated to listening to our customers to determine what you find important and how we can add value. In recent months we have gathered more threat intelligence, correlating and analyzing data to provide more useful insights into what is happening in the evolving threat landscape. McAfee is collaborating closely with MITRE Corporation in extending the techniques of its MITRE ATT&CK™ knowledge base, and we now include the model in our report. We have just started to refine our process and reports. You can expect more from us, and we welcome your feedback.

Although the aftermath of takedowns of underground markets were still apparent in Q3, many other underground markets have eagerly filled the gaps. With the services on offer, the effectiveness of cybercriminals is increasing. During this quarter we also noticed greater activity from the GandCrab ransomware family. Using an affiliate program, demonstrating agile development, and mixing with other cybercrime services such as exploit kits have resulted in a big wave of attacks from this family.

The third quarter was also highlighted by major security conferences. Representatives of the McAfee Advanced Threat Research team shared insights from their research at several of these events. At DEF CON we demonstrated how an attacker could manipulate medical devices. During Black Hat USA, the team released research into code reuse by North Korean malware families that revealed previously undiscovered links.

We also welcomed many customers and partners as we shared our latest research at the McAfee MPOWER conferences in Las Vegas, Sydney, Tokyo, and Rome. During this quarter, we have stayed busy analyzing threats, welcoming new researchers to the team, and especially publishing our findings. You can read our results on our blogs page and our team's page.

We hope you enjoy the new format and we look forward to your reactions.

—Raj Samani, Chief Scientist and McAfee Fellow
Twitter: @Raj_Samani

—Christiaan Beek, Lead Scientist
Twitter: @ChristiaanBeek

**Dark web marketplaces focus on selling narcotics and other illicit goods. These markets offer hacking tools, hackers for hire, and data records.**

Follow

Share

# Table of Contents




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

- Alexandre Mundo Alguacil
- Christiaan Beek
- Carlos Castillo
- Taylor Dunton
- John Fokker
- Steve Grobman
- Tim Hux
- Niamh Minihane
- Lee Munson
- Eric Peterson
- Marc Rivero
- Thomas Roccia
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

## Underground Forums Boost the Effectiveness of Cybercriminals

### Dark web markets

The ripple effect of the takedowns of the Hansa and AlphaBay dark web markets were still apparent in Q3. Competing marketplaces, such as Dream Market, Wall Street Market, and Olympus Market eagerly filled the gap left by law enforcement actions last year.

Wall Street and Dream Markets have become the largest marketplaces. Olympus Market, which was well on its way to being one of the top markets, suddenly disappeared in Q3. There is speculation that the disappearance was an exit scheme initiated by the market's administrators to steal money from their own vendors and customers.

The McAfee Advanced Threat Research team has noticed a shift in dark web platforms. Several individual sellers have moved away from large markets and have opened their own specific marketplaces. They hope to fly under the radar of law enforcement and build a trusted relationship with their customers without the fear of a quick exit by the market owners. This shift has sparked a new line of business: Defiant website designers who offer to build hidden marketplaces for aspiring vendors. Other vendors are moving away from the TOR network, choosing platforms such as Telegram to offer their goods and services.

Dark web marketplaces, generally accessible via TOR, focus on selling narcotics and other illicit goods. These markets also offer hacking tools, hackers for hire, and data records. The accessibility of these marketplaces to a large public make them a force to be reckoned with. Stolen digital data, which drives much of the profits, will continue to be a key motivator. As long as there are markets, we must secure our data.

### Underground hacker forums

Different from dark web markets, underground hacker forums are less accessible to the public and focus on cybercrime-related topics. McAfee researched several of these meeting places in Q3 to determine the hot topics.

**Leaked user credentials:** Credential abuse is one of the most popular topics on the underground scene, and the large data breaches we read about help maintain this popularity. The use of valid accounts makes it child's play for cybercriminals to access and take over an individual's personal life. Cybercriminals often show an interest in email accounts because these are regularly used to restore login credentials for other online services. Password reuse, not enabling two-factor authentication, and failing to change passwords on a regular basis are the main factors that make these attacks so effective.

**CVE discussions:** We have seen numerous mentions of Common Vulnerabilities and Exposures. The most recently published CVEs were hot topics in discussions of browser exploit kits—RIG, Grandsoft, and Fallout—and of ransomware, especially GandCrab. In the English-speaking, less technical underground forums we observed several discussions of old CVE implementations in familiar tools such as Trillium MultiSploit. These threads show that cybercriminals are eager to weaponize both new and old vulnerabilities. The popularity of these topics in underground forums should warn organizations to make vulnerability management a priority in their cyber resilience plans.

**Credit card–stealing malware targeting e-commerce sites:** Large-scale credit card theft has shifted from point-of-sale systems to (third-party) payment platforms on large e-commerce sites. Groups such as Magecart have been responsible for many headlines in recent months, successfully skimming thousands of credit card details directly from the victims' websites. These breaches have fueled an underground demand for malicious tools such as MagentoCore that are being used to steal credit card data by injecting malicious JavaScript code into vulnerable Magento platforms.

**Credit card shops:** In spite of a decrease of point-of-sale fraud such as skimming, recent big credit card thefts maintain a steady supply of "fresh" card details offered on "dump sites" such as JokerStash, Trump's Dumps, and Blackpass.

Credit card companies and e-commerce sites are making good strides on fraud detection, for example, by implementing geographic IP location checks for online purchases. Every action triggers a reaction, however; we have noticed an increased demand for compromised machines that are in the same zip code as stolen credit card information. Underground markets that sell remote desktop protocol (RDP) access make good use of this.


Figure 1. Trump's Dumps login page.

## RDP shops

Early in Q3 we published an extensive report on online platforms that sell RDP access to hacked machines. Criminals offer logins to computer systems worldwide, ranging from home to medical to even government systems. RDP shops remained popular throughout this quarter and continue to serve criminals looking to commit credit card fraud, cryptomining, ransomware, and account fraud. RDP shops such as Blackpass provide one-stop access to all the tools used to commit fraud; in addition to RDP access they sell social security numbers, bank details, and online accounts.

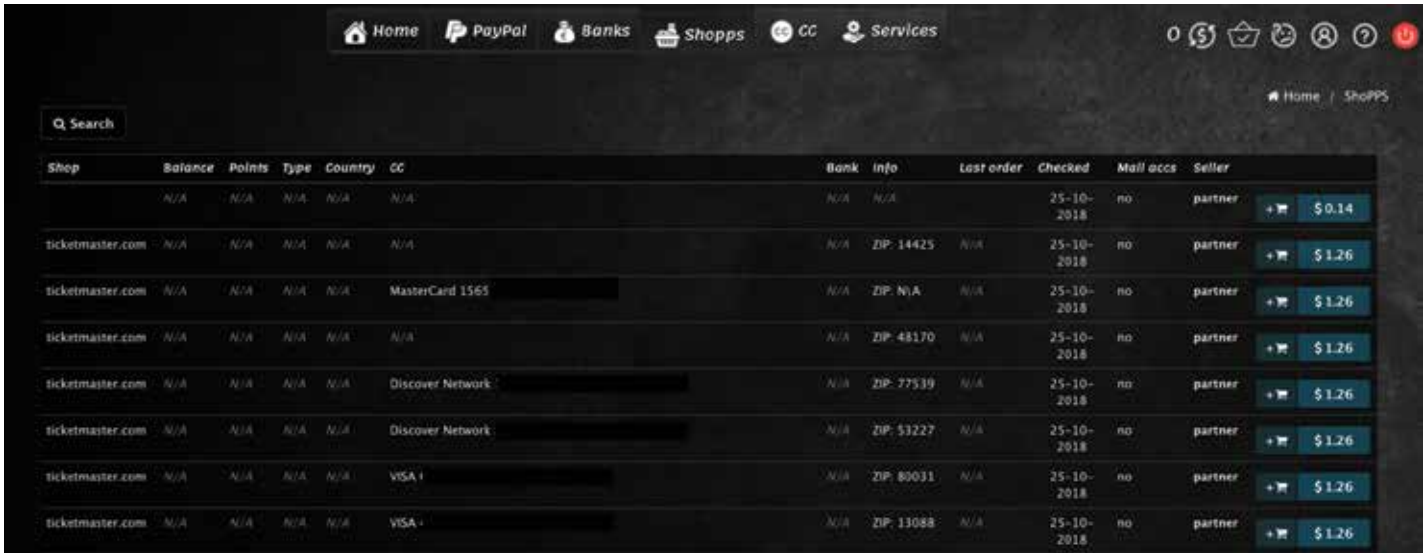



Figure 2. RDP-shop Blackpass offers online accounts and credit cards possibly connected to one of the Magecart breaches.

Fraudsters continue to demand RDP-accessible systems with several active online accounts. Criminals can use this access to order goods online through their victims' accounts and have them shipped elsewhere. RDP continues to be an Achilles heel for many organizations, judging by the amount of targeted ransomware attacks, such as SamSam, BitPaymer, and GandCrab, that leverage RDP as an entry method.

### Ransomware-as-a-service

On underground forums there is a strong interest for the leading ransomware-as-a-service families such as GandCrab. These developers are forming strategic partnerships with other essential services, such as crypter services and exploit kits, to better service their customers and increase infection rates. At the end of the Q3 we published research on how the latest version of GandCrab partnered with the relatively new crypter service NTCrypt. This partnership was formed after NTCrypt won a crypter contest launched by the group behind GandCrab. A crypter service provides malware obfuscation to evade antimalware security products.


Figure 3. The NTCrypt-GandCrab partnership announcing a special price for GandCrab users.

**Android malware:** We saw an increase in discussions of mobile malware, mostly targeting Android and focused on botnets, banking fraud, ransomware, and bypassing two-factor authentication.

**Other malware and botnets:** These two subjects form the backbone of cybercrime; they are regular topics for discussion in the cybercriminal underground. In addition to threads on well-known malware families and large botnets, we have seen numerous discussions of small, unnamed botnets, cryptocurrency mining malware, and remote access Trojans. Apart from GandCrab and its partnered services, no other specific malware families stood out in underground discussions.

**Distributed denial of service:** DDoS attack methods and booter/stresser services remained hot topics among young cybercriminals; we saw these mostly discussed in English-speaking, less technical forums.

## Ransomware Families Decline in Number

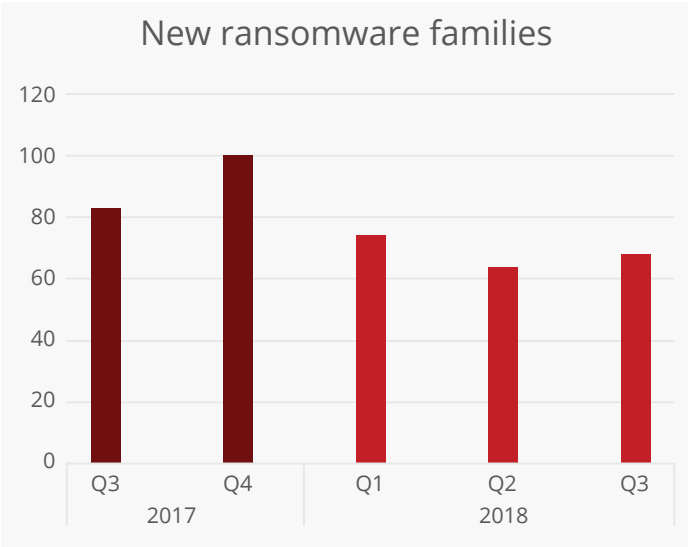
Although we have seen a decline in the number of unique families during recent months, ransomware remained active in Q3. The decline in new families may be due to many ransomware actors switching to a more lucrative business model: cryptomining.

One of the most active ransomware families in Q3 was GandCrab. Due to its affiliate scheme, several participants launched their campaigns when new versions were released. Many versions appeared as the developers tried to stay ahead of the security industry's responses. The sheer volume of GandCrab samples contributed to the increase in new ransomware in Q3.

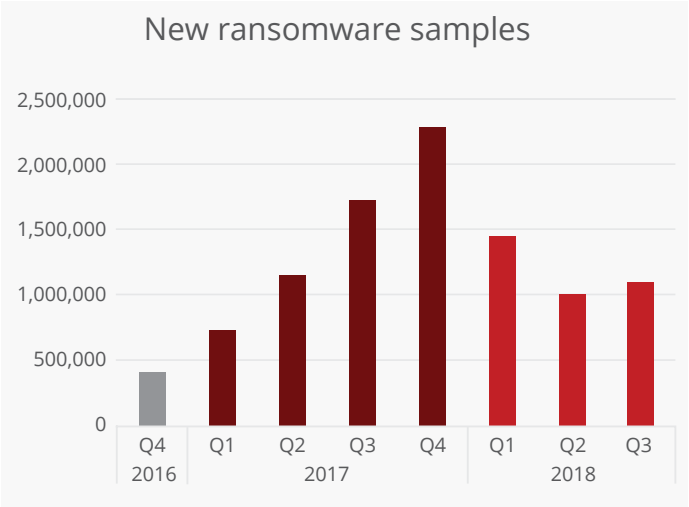
Some of the changes we observed:

- Added to the Fallout exploit kit to boost infections
- Used the CVE-2018-8440 vulnerability (a patch was released in September) to boost infections
- Added a random five-character extension to encrypt files
- Added the ability to kill processes related to Word, Excel, SQL Server, Oracle, PowerPoint, Outlook, and others

The biggest change we noticed was the increase in size of the ransom payment. GandCrab Version 5 requires the victim to pay US $2,400 for the decryption key. Past versions required $1,000.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.

Follow

Share

Similarities in Version 5 with previous versions:

- Does not infect Russian users
- Contains a hardcoded list of URLs that it contacts to send the victims' system information
- The ransom/payment/decryption site is still on the dark web at hxxp://gandcrabmfe6mnef[.]onion
- Uses the hardcoded key "jopochlen" to encrypt victims' information with the RC4 algorithm

The Advanced Threat Research team wrote an extensive report on GandCrab Version 5 and its changes.

Another active ransomware family in Q3 was Scarab, which released six new variants along with numerous updates to current variants (new extension(s) added to encrypted files, new ransomware notes, etc.). The ransomware does not appear to target a specific sector or region.

New variants in Q3:

- Scarab-Omerta—July
- Scarab-Bin—July
- Scarab-Recovery—July
- Scarab-Turkish—July
- Scarab-Barracuda—July
- Scarab-CyberGod—August

Updated in Q3:

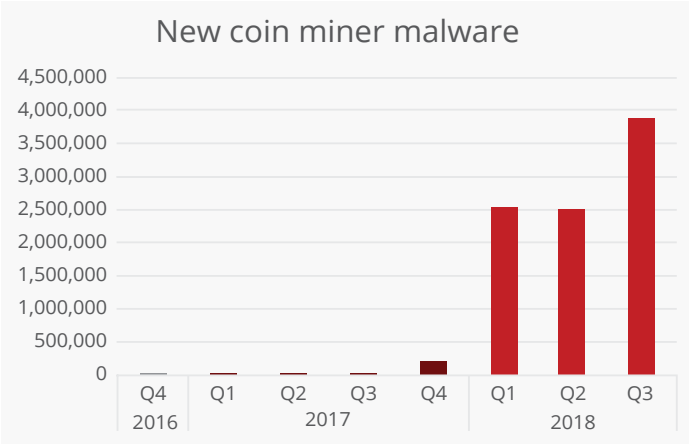
- Scarab-Please—Ransomware
- Scarab-Bitcoin—Ransomware
- Scarab-Crypt000—Ransomware
- Scarab-DiskDoctor—Ransomware
- Scarab-Bomber—Ransomware

| Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery |
|---|---|---|---|---|---|
| Windows Management Instrumentation | Startup Items | Process Injection | Process Injection | Hooking | File and Directory Discovery |
| | Hooking | Scheduled Task | Bypass User Account Control | Input Capture | |
| | Registry Run Keys/ Startup Folder | Bypass User Account Control | Disabling Security Tools | | |
| | Scheduled Task | DLL Search Order Hijacking | File Deletion | | |

Figure 4. The Advanced Threat Research team mapped malware and other attacks in Q3 to the MITRE ATT&CK™ framework. We have removed techniques that were not present. The darker the background, the more frequently the technique was used.

## Cryptomining Boom Times Continue

Mining cryptocurrency via malware is one of the big stories of 2018. Total "coin miner" malware has grown more than 4,000% in the past year.




Source: McAfee Labs, 2018.

Security researcher Remco Verhoef discovered a Mac OS threat later named OSX.Dummy, which was distributed on cryptomining chat groups. The exploitation is simple, requiring victims to execute a one-line command in the OSX terminal to download and execute the payload.

The actor wrote messages on the Slack, Telegram, and Discord channels suggesting users download software to fix crypto problems. The fake software executes with a single line in Bash. The users essentially infected their own devices instead of falling victim to an unknown exploit or an exploit kit. In execution, OSX.Dummy opens a reverse shell on a malicious server, giving an attacker access to the compromised system.

Cryptominers will take advantage of any reliable scenario. Some security researchers discovered that unofficial repositories of the open-source media player Kodi have served a modified add-on that delivers cryptominer malware. This operation started in 2017.

Another campaign takes advantage of the vulnerability CVE-2018-14847, exploiting unpatched MikroTik routers. Security researcher Troy Mursch detected more than 3,700 compromised devices serving as miners. The campaign primarily targeted North America and Brazil.

We would not usually think of using routers or IoT devices such as IP cameras or videorecorders as cryptominers because their CPUs are not as powerful as those in desktop and laptop computers. However, due to the lack of proper security controls, cybercriminals can benefit from volume over CPU speed. If they can control thousands of devices that mine for a long time, they can still make money.

| Execution | Persistence | Privilege Escalation | Defense Evasion | Discovery | Command and Control |
|---|---|---|---|---|---|
| Execution through Module Load | Registry Run Keys/ Startup Folder | Bypass User Account Control | Bypass User Account Control | Query Registry | Data Obfuscation |
| Local Job Scheduling | Hooking | Hooking | | | Uncommonly Used Port |
| Scheduled Task | | Process Injection | | | |
| Third-Party Software | | Scheduled Task | | | |
| | | Startup Items | | | |

Figure 5. MITRE ATT&CK™ framework. The darker the background, the more frequently the technique was used.

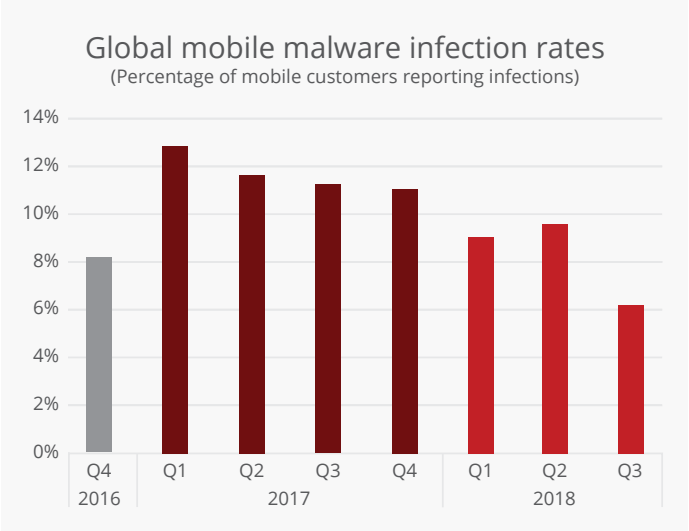
**Coin miner malware hijacks systems to create ("mine") cryptocurrency without victims consent or awareness. New coin miner threats have jumped massively in 2018.**

Follow

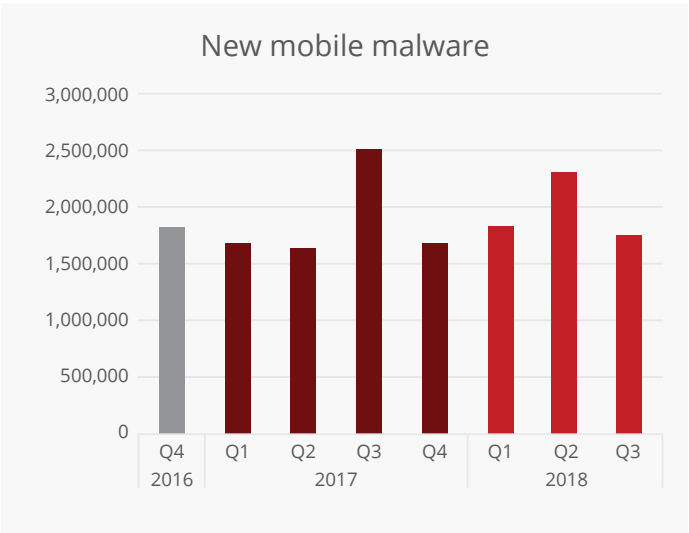
Share

## Mobile Threats Fueled by Fake Apps

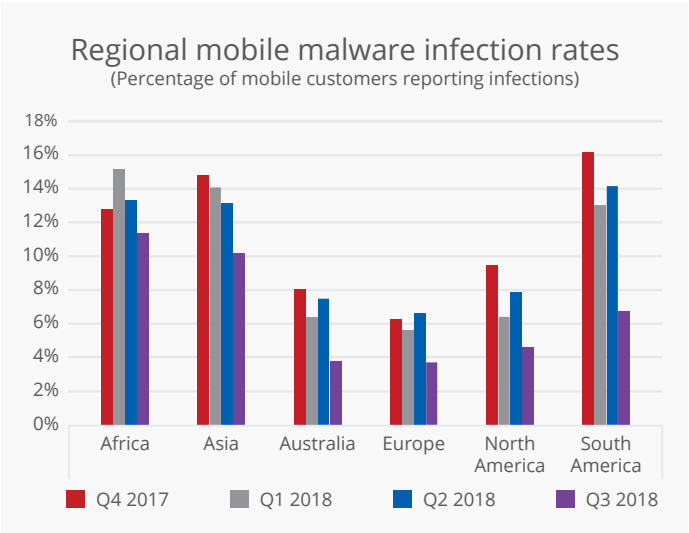
Overall, new mobile malware declined by 24% in Q3, and McAfee mobile security customers reported 36% fewer infections in the quarter. In spite of the downward trend, the mobile security landscape detected some unusual threats in Q3. New threats ranged from a fake "cheats" app for the Fortnite game that installed malware, to mobile banking Trojans and apps that served unwanted advertisements. We observed an attack targeting members of the Israel Defense Forces that installed fake dating apps to infect their devices. The fake app exfiltrated data including location, contact list, listening to phone calls, and using the camera.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.

Follow

Share

In Q3 the McAfee Mobile Research team detected a threat that infected at least 5,000 devices. Android/TimpDoor spreads via phishing, using text messages to trick victims into downloading and installing a fake voice-message app that allows cybercriminals to use infected devices as network proxies without users' knowledge. If the fake application is installed, a background service starts a Socks proxy that redirects all network traffic from a third-party server via an encrypted connection through a secure shell tunnel—allowing potential access to internal networks and bypassing network security mechanisms such as firewalls and network monitors.

Devices running TimpDoor could serve as mobile backdoors for stealthy access to corporate and home networks because the malicious traffic and payload are encrypted. Worse, a network of compromised devices could also be used for more profitable purposes such as sending spam and phishing emails, performing ad click fraud, or launching distributed denial-of-service attacks.

The malicious app appears to be a legitimate voice application, but the buttons and functions are fake.

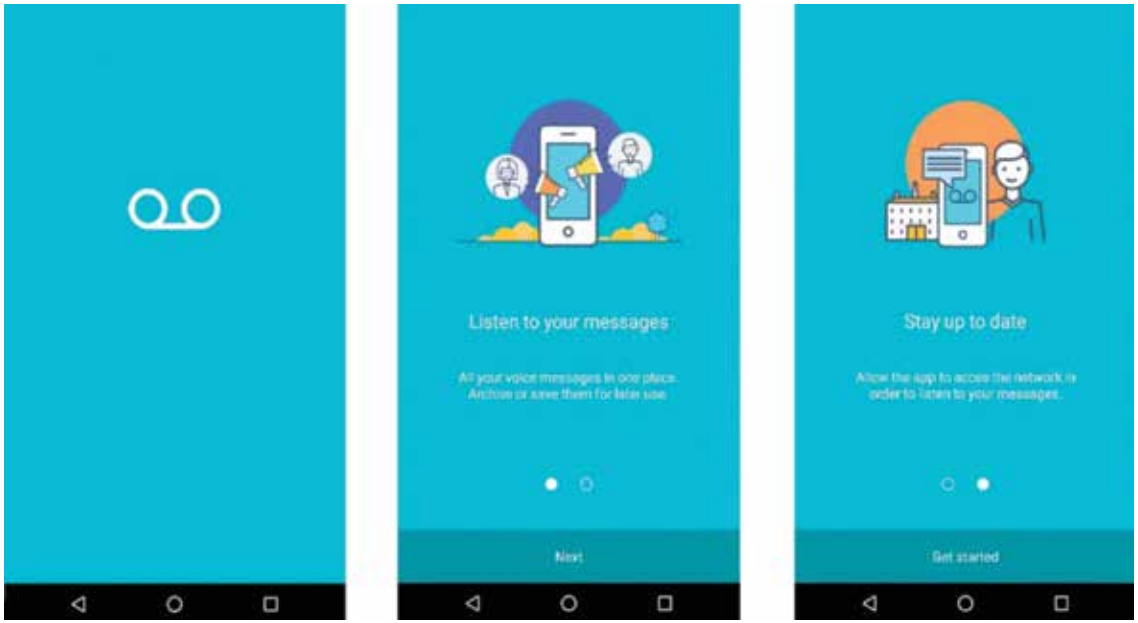



Figure 6. The fake voice-message app Android/TimpDoor.

```
this.mHandler.postDelayed(new Runnable() {
    public void run() {
        AppService.this.startSsh();
        AppService.this.startNetworkConnectionMonitor();
        AppService.this.setupAlarmManager();
        AppService.this.startPoolSshConnection();
    }
}, 3000);
```

Figure 7. One of the most interesting characteristics of Android/Timpdoor is the capability to keep the SSH connection open.

The app has an alarm to keep the connection established and constantly upload information regarding the device.

Cisco's Talos group uncovered a campaign that infected 13 iPhones with a malicious mobile device manager. The infection method is still unknown; the attackers would have required physical access or social engineering techniques to deploy the device managers. The infection workflow and capabilities:

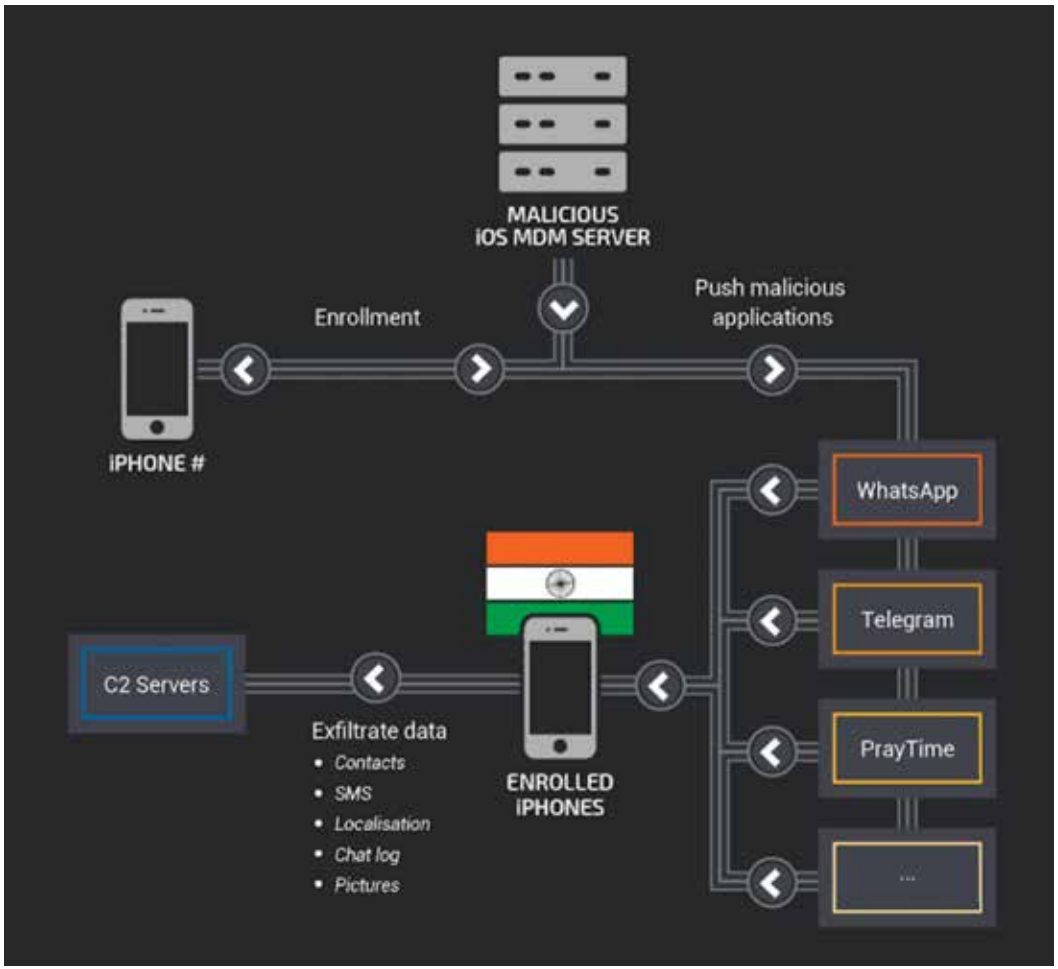



Figure 8. Source: Cisco Talos Intelligence Group.

The attackers used BOptions sideloading techniques to inject a dynamic library and add features to installed legitimate applications. This attack reminds us that development and framework environments are also vulnerable if they are not properly secured.

| Initial Access | Persistence | Defense Evasion | Discovery | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|
| Spearphishing Attachment | Dylib Hijacking | Access Token Manipulation | Account Discovery | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Spearphishing Link | | Code Signing | Application Window Discovery | Automated Collection | Data Compressed | Remote File Copy |
| Spearphishing via Service | | | Browser Bookmark Discovery | Clipboard Data | Data Encrypted | Standard Application Layer Protocol |
| | | | File and Directory Discovery | Data from Information Repositories | Data Transfer Size Limits | |
| | | | System Owner/User Discovery | Data from Local System | Exfiltration Over Alternative Protocol | |
| | | | System Service Discovery | Email Collection | Exfiltration Over Command and Control Channel | |
| | | | System Time Discovery | Input Capture | Exfiltration Over Other Network Medium | |
| | | | | Screen Capture | Exfiltration Over Physical Medium | |
| | | | | | Scheduled Transfer | |

Figure 9. MITRE ATT&CK™ framework. The darker the background, the more frequently the technique was used.

## Banking Trojans Turn to Uncommon File Types

Banking malware remained a constant threat during the year due to the effectiveness of campaigns and the profits that cybercriminals can enjoy. In Q3 we observed an increase in uncommon file types used in spam campaigns. Those attacks relied on bypassing email protection systems, which are configured to stop and analyze common Office, archive, scripting, and other files. This quarter, we observed IQY files (an Excel format) sent in separate waves that delivered different malware families to infected devices. These campaigns prompted users to click on emails while using conventional social engineering phrases: “photos sent,” “payment,” “please confirm.” These campaigns accounted for around 500,000 emails sent worldwide.

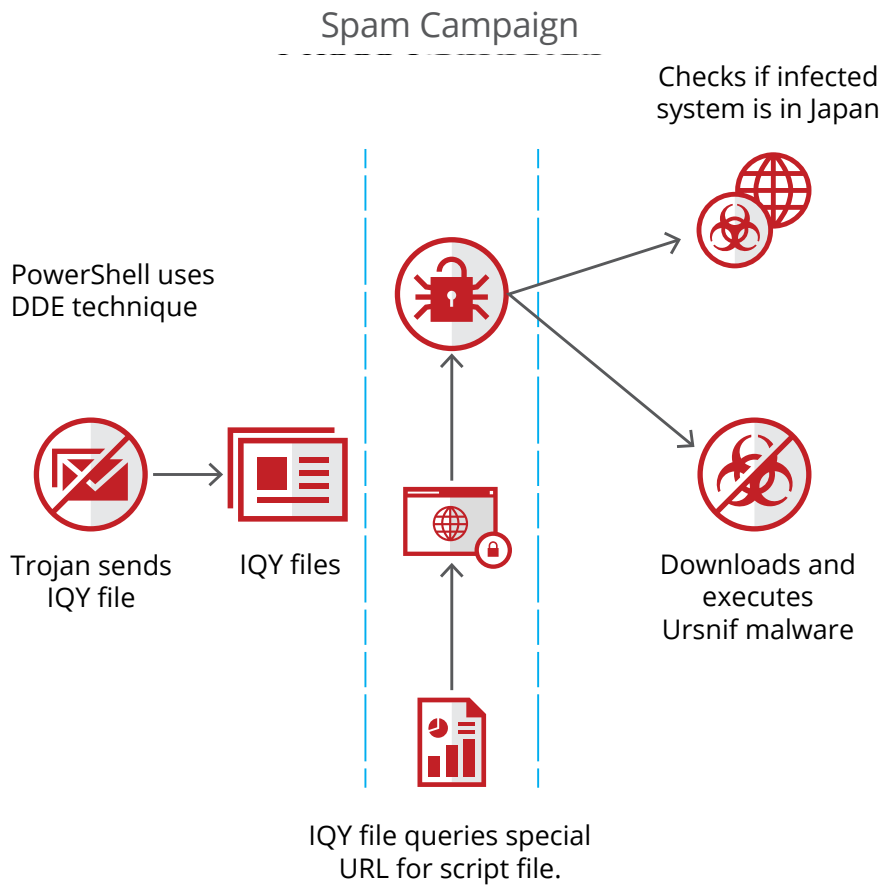



Figure 10. The infection chain employs a combination of IQY files plus DDE, and PowerShell to deliver Ursnif or Bleboh malware.

In Q3 we observed many campaigns using convincing emails, focused on their selected sectors and enticing users to click on them.

Financial institutions have added protections in recent years to protect their customers. One effective method is two-factor authentication for operations such as transferring funds to other accounts or logging into bank accounts. In Q3, the Advanced Threat Research team observed a well-known banking malware family had updated its "web injects" to include two-factor operations to attack certain financial companies.

```
function removeTrf()
{
    if (typeof(DrInfo) == 'undefined') return false;
    var dr_arr = DrInfo.split('::');
    var temp = dr_arr[dr_arr.length-1].split(':');
    dr_arr[dr_arr.length-1]=temp[0];
    dr_arr[dr_arr.length]=temp[1];
    if (!$('#listaMov').length) return false;
    if (!$('#main:contains("'+dr_arr[dr_arr.length-1]+'")').length) return false;

    if ($('#listaMov tr:contains("'+floatToTxt(parseFloat(dr_arr[dr_arr.length-2]))+'")'))
    {
        if ($('#listaMov tr:contains("'+floatToTxt(parseFloat(dr_arr[dr_arr.length-2]))+'")').length) top.sendComm('RemoveTrf');
        $('#listaMov tr:contains("'+floatToTxt(parseFloat(dr_arr[dr_arr.length-2]))+'")').prev(':contains("COMMISS")').remove();
        $('#listaMov tr:contains("'+floatToTxt(parseFloat(dr_arr[dr_arr.length-2]))+'")').remove();
    }
}
```

Figure 11. A web inject file for the Zeus Panda malware. Source: Cofense.

Zeus Panda often changes its web injects to include new techniques to bypass the latest protections applied by the financial sector.

In Q3, some well-known malware families updated their versions with slight modifications. The banking Trojan Kronos became popular in 2014, when it was discovered. This year, a new version hosted its control server on the TOR network and renamed the banking malware Osiris to sell on the underground market. Another new campaign targeted users in Germany with malicious .doc files carrying macros that downloaded Kronos. Kronos was also delivered in Q3 by the RIG exploit kit, which previously dropped Zeus Panda.

Banking malware has long been popular in Brazil. In Q3, McAfee detected a new family targeting the country: CamuBot attempts to camouflage itself as a security module required by the banks it targets. Compared with other Brazilian malware families, CamuBot shares few similarities. CamuBot has taken on characteristics from non-Brazilian malware families such as TrickBot, Ursnif, Dridex, and Qakbot. This is a major change in malware targeting Brazilians; most threats are less sophisticated compared with the banking malware affecting other continents. Organized cyber gangs in Brazil are very active in targeting their own population. They have learned a lot from their Eastern Europe peers and have adapted their malware to include techniques used elsewhere.

| Execution | Persistence | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|
| Exploitation for Client Execution | Bootkit | Code Signing | Hooking | Application Window Discovery | Distributed Component Object Model | Clipboard Data | Data Compressed | Data Encoding |
| PowerShell | Kernel Modules and Extensions | DCShadow | Input Capture | File and Directory Discovery | Pass the Hash | Email Collection | Exfiltration Over Alternative Protocol | Uncommonly Used Port |
| Windows Management Instrumentation | Local Job Scheduling | File Deletion | | Network Service Scanning | Remote Desktop Protocol | | | |
| | Office Application Startup | Modify Registry | | Peripheral Device Discovery | | | | |
| | Registry Run Keys/ Startup Folder | Process Injection | | Process Discovery | | | | |
| | Service Registry Permissions Weakness | | | Query Registry | | | | |
| | | Software Packing | | Security Software Discovery | | | | |
| | | | | System Information Discovery | | | | |
| | | | | System Time Discovery | | | | |

Figure 12. MITRE ATT&CK™ framework. The darker the background, the more frequently the technique was used.

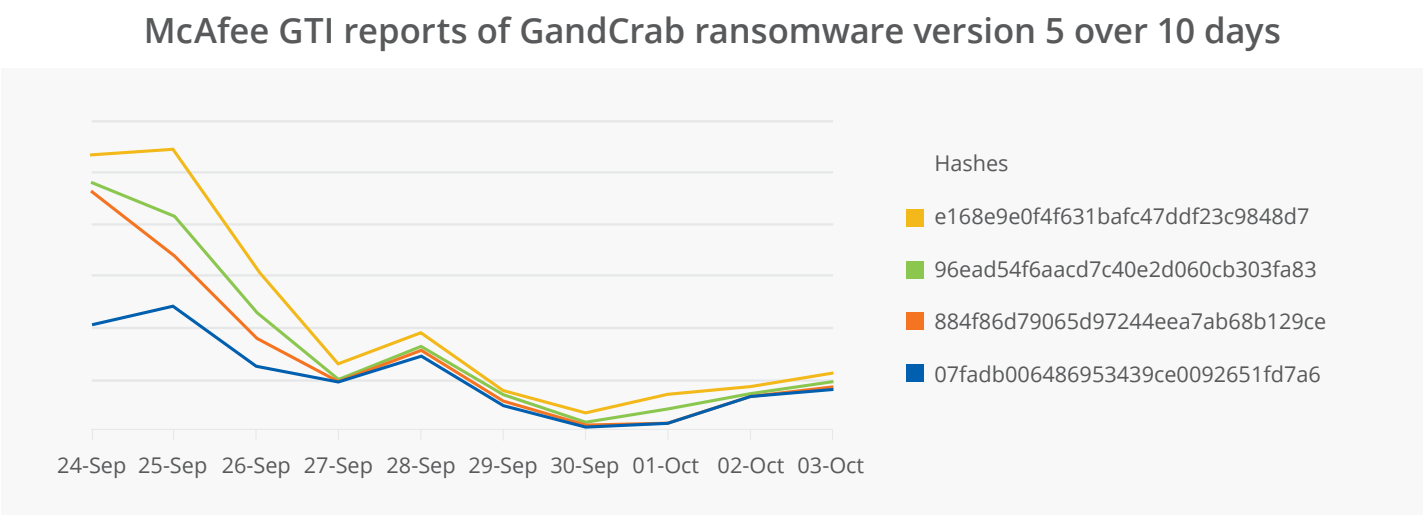
## Exploit Kits Add Support for Vulnerabilities, Ransomware

Exploit kits are the delivery vehicles for many cybercrime operations. Some can remain in business, while others are taken out by law enforcement actions. In Q3 we found two new exploit kits on the scene.

**Fallout:** This exploit kit was discovered in August. It takes advantage of flaws in Adobe Flash Player and Microsoft Windows. A successful infection will allow an attacker to download malware onto the victim's computer. This exploit kit shares similarities with the Nuclear exploit kit. Fallout was found during an investigation at some Japanese organizations, although it targets no specific region. CVE-2018-4878 and CVE-2018-8174 are the only two vulnerabilities included in this kit, which used the latter flaw to spread GandCrab Version 5.

The following chart is based on telemetry from McAfee® Global Threat Intelligence. It shows the distribution of four samples of the GandCrab Version 5 ransomware we measured in late September and early October. These samples were most likely spread via the Fallout exploit kit. The chart displays a typical exploit kit infection rate, with a high level

of hits at the beginning and a rapid decrease over a short time. This is a common business model for exploit kits; a customer pays either by installations or for a fixed time. The September 28 increase was probably due to the release of another round of samples by affiliates.




**Underminer:** This exploit kit was discovered in July. It protects its own code and control server traffic with RSA encryption and takes advantage of flaws in Microsoft Internet Explorer and Flash Player to infect users with a range of malware, including cryptominers and boot kits. The exploit kit targets users in the Asia-Pacific region. Two vulnerabilities were added to this kit in Q3: CVE-2018-4878 (Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution) and CVE-2018-8174 (Windows VBScript Engine Remote Code Execution Vulnerability; for more, see the next section).

| Initial Access | Execution | Privilege Escalation | Defense Evasion |
|---|---|---|---|
| Drive-By Compromise | Exploitation for Client Execution | Exploitation for Privilege Escalation | Bypass User Account Control |
| Exploit Public-Facing Application | Scripting | | Exploitation for Defense Evasion |

Figure 13. MITRE ATT&CK™ framework. The darker the background, the more frequently the technique was used.

## Vulnerabilities Open Door to Shellcode, Privilege Escalation

In Q3 three vulnerabilities stood out for their use of new malware families or campaigns.

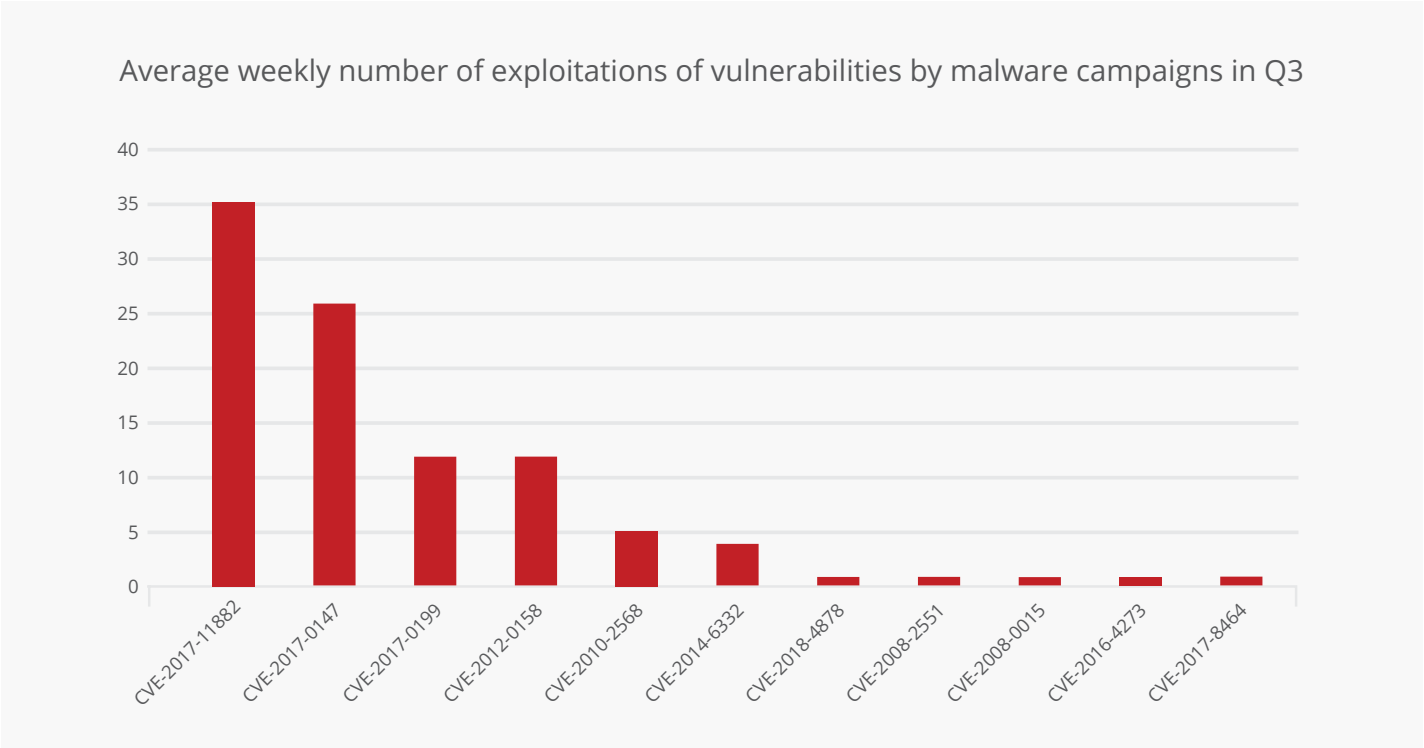
**Windows VBScript Engine Remote Code Execution Vulnerability** (CVE-2018-8174). This flaw was patched in May but was exploited in Q3 by "Operation Personality Disorder." The attackers used malicious RTF documents containing VBScript to exploit a flaw in Internet Explorer and launch shellcode. The code dropped a backdoor payload and gave control of the infected systems. The campaign was carried out by the Cobalt Gang, whose alleged leader was arrested in Spain this year.

This vulnerability was added in Q3 to two new exploit kits, Fallout and Underminer. The flaw was also used to infect users with GandCrab Version 5 via Fallout. The threat actors behind the malvertising campaign used legitimate advertising sites to redirect victims to a landing page containing the exploit kit. The landing page contained Base64-encoded VBScript code that is decoded by a JavaScript function. The decoded code executes shellcode by exploiting the defect in the VBScript engine. The shellcode then downloads the payload, which loads GandCrab into memory on the infected system.

**Windows ALPC Elevation of Privilege Vulnerability** (CVE-2018-8440). This was patched in September. The zero-day flaw made headlines after the security researcher who found the defect posted proof-of-concept details to Twitter and GitHub in late August—causing Microsoft to include a patch in the September updates. The flaw allowed anyone with local access rights to gain system privileges. The vulnerability was used to infect users with GandCrab by exploiting a privilege escalation flaw in Windows, allowing the ransomware to gain elevated privileges and encrypt as many files as possible. The attack tries to exploit a problem with the Windows Task System in which the operating system improperly handles calls to an advanced local procedure call. Due to how the malware author compiled the code, one version of the exploit code worked only on Windows 7 through Windows 10 Server. The compiled code would not run on Windows XP or Vista because a file needed for some calls, xpsprint.dll, does not exist on these older versions.

**Scripting Engine Memory Corruption Vulnerability** (CVE-2018-8373). A variant of a remote code execution vulnerability with Internet Explorer's scripting engine delivered QuasarRAT. The exploit did not work perfectly in all environments and did not always succeed in delivering the malware. Several groups of security analysts, including the McAfee Advanced Threat Research team, published information on the campaign and how the malware works. According to one team, VBScript!AccessArray stores the address of an array's element in the stack. VBScript!AssignVar then triggers the call of the Default Property Get function in the script to modify the length of the array. This frees the element's memory, whose address has been saved in the stack by VBScript!AccessArray. After patching, the SafeArrayLock function is added to lock the current array before VBScript!AssignVar, so that the array length can no longer be modified in the Default Property Get function.

The following diagram represents the frequency of exploitation of vulnerabilities used in malware campaigns during an average week in Q3. Attackers employed most of these vulnerabilities to weaponize a document and install and launch a malicious program:




Source: McAfee Labs, 2018.

## Targeted Attacks Motivated by Cyber Espionage

In Q3, the Advanced Threat Research team recorded more than 35 publicly known targeted attacks. Cyber espionage was the biggest motivator for these attacks. The activities were mostly related to political tensions in several regions that inspired nation-state groups to conduct cyber operations to gather intelligence.

Adversary groups sponsored by the Russian government conducted several operations during Q3, McAfee believes. The most active during this period were the groups APT28, Dragonfly, and Sandworm, which targeted government, laboratory, energy, and military sectors.

Researchers from ESET discovered the first rootkit that exploits the Unified Extensible Firmware Interface (UEFI); the malware was developed and used by APT28, ESET says. The threat, dubbed LoJax, infects the UEFI. When the UEFI is infected, LoJax can survive both a reboot of the machine and even a hard disk replacement. To distribute the malware, the adversaries used Trojanized versions of the antitheft software LoJack. The victims were government entities in the Balkans as well as Central and Eastern Europe, according to the researchers telemetry.

Some of these groups are now using more open-source tools, as well as macros and scripting. Otherwise, their code does not offer much that is new, apart from basic improvements.

Two campaigns are examples of attacks targeting financial institutions.

Operation Double Infection**:** This campaign was discovered in August; spear phishing emails containing two malicious URLs attempt to install two backdoors. The emails appear to come from financial institutions and attempt to steal funds from the victims. The attackers behind the operation focused on companies in Eastern Europe and Russia.

Operation Personality Disorder**:** This campaign uses either a malicious attachment or a URL contained in an email to drop the backdoor More_eggs. Successful exploitation allows the threat actors to take control of the computer, gain access to system information, and install the final payload: Cobalt Strike. The phishing emails appear to come from legitimate financial organizations in Europe. Some of the malicious RTF files used in the attacks contain exploits for a range of vulnerabilities, including CVE-2018-8174. (For more, see the section on Vulnerabilities.)

Both campaigns have the following in common:

- Target financial organizations in Eastern Europe and Russia.
- Use phishing emails that appear to come from legitimate financial companies or vendors.
- Use malicious Word documents with VBA code to infect systems after the user allows macros to run.
- Use custom JavaScript binary backdoors disguised as text files to gain full access to the infected system.
- Use the command-line tool cmstp.exe (the Microsoft Connection Manager Profile Installer) with a malicious installation information file to bypass Microsoft Windows AppLocker and download and execute remote code
- Useregsvr32.exe to bypass Windows AppLocker.
- Are carried out by the well-known threat actor Cobalt Group. The group has been in operation since at least 2013 and is reported to have been behind more than 100 attacks against worldwide financial institutions.
- The group's suspected leader was arrested in March, but attacks are still being carried out.

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| Drive-By Compromise | CMSTP | Component Object Model Hijacking | Bypass User Account Control | Bypass User Account Control | Brute Force | Account Discovery | Exploitation of Remote Services | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Exploit Public-Facing Application | Command-Line Interface | Create Account | DLL Search Order Hijacking | CMSTP | Credential Dumping | File and Directory Discovery | Logon Scripts | Automated Collection | Data Compressed | Connection Proxy |
| Replication Through Removable Media | Execution through API | DLL Search Order Hijacking | Exploitation for Privilege Escalation | Code Signing | Credentials in Files | Network Service Scanning | Remote Desktop Protocol | Data from Information Repositories | Data Encrypted | Custom Command and Control Protocol |
| Spearphishing Attachment | Exploitation for Client Execution | Hidden Files and Directories | Hooking | Component Object Model Hijacking | Hooking | Network Share Discovery | Third-Party Software | Data from Local System | Exfiltration Over Alternative Protocol | Data Encoding |
| Spearphishing Link | Graphical User Interface | Hooking | New Service | Deobfuscate/ Decode Files or Information | Input Capture | Peripheral Device Discovery | Windows Admin Shares | Data Staged | Exfiltration Over Command and Control Channel | Data Obfuscation |
| Supply Chain Compromise | LSASS Driver | | Process Injection | DLL Search Order Hijacking | Input Prompt | Process Discovery | | Email Collection | Exfiltration Over Other Network Medium | Multi-Stage Channels |
| Trusted Relationship | PowerShell | LSASS Driver | Scheduled Task | Exploitation for Defense Evasion | | Query Registry | | Input Capture | | Multiband Communication |
| | Regsvr32 | Modify Existing Service | | File Deletion | | Security Software Discovery | | Man in the Browser | | Multilayer Encryption |
| | Rundll32 | New Service | | Hidden Files and Directories | | System Information Discovery | | Screen Capture | | Remote Access Tools |
| | Scheduled Task | Registry Run Keys/ Startup Folder | | Indicator Removal from Tools | | System Network Configuration Discovery | | Video Capture | | Remote File Copy |
| | Scripting | Scheduled Task | | Masquerading | | System Owner/User Discovery | | | | Standard Application Layer Protocol |
| | Service Execution | System Firmware | | Modify Registry | | System Service Discovery | | | | Standard Cryptographic Protocol |
| | Third-Party Software | | | Obfuscated Files or Information | | System Time Discovery | | | | |
| | User Execution | | | Process Doppelgänging | | | | | | |
| | Windows Management Instrumentation | | | Process Injection | | | | | | |
| | | | | Regsvr32 | | | | | | |
| | | | | Rootkit | | | | | | |
| | | | | Rundll32 | | | | | | |
| | | | | Scripting | | | | | | |
| | | | | Software Packing | | | | | | |
| | | | | Trusted Developer Utilities | | | | | | |
| | | | | Valid Accounts | | | | | | |

Figure 14. MITRE ATT&CK™ framework. The darker the background, the more frequently the technique was used.

# Threats Statistics



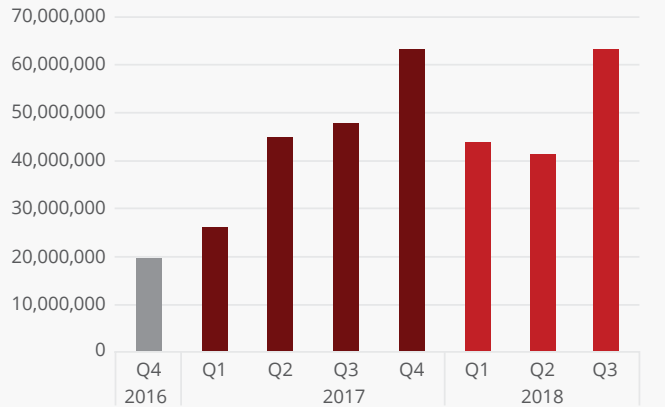
THREATS STATISTICS

# McAfee Global Threat Intelligence

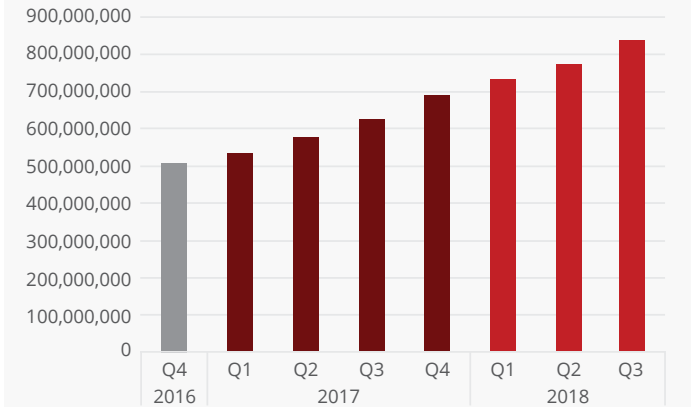
Every quarter, the McAfee® Global Threat Intelligence (McAfee GTI) cloud dashboard allows us to see and analyze real-world attack patterns that lead to better customer protection. This information provides insights into attack volumes that our customers experience. Each day, on average, McAfee GTI received 49 billion queries and 13 billion lines of telemetry, while analyzing 5,600,000 URLs and 700,000 files, plus another 200,000 files in a sandbox.

- McAfee GTI tested 77 billion suspicious files and reported 73 million (0.01%) as risky.
- McAfee GTI tested 16 billion potentially malicious URLs and reported 63 million (0.4%) as risky.
- McAfee GTI tested 15 billion potentially malicious IP address and reported 66 million (0.4%) as risky.

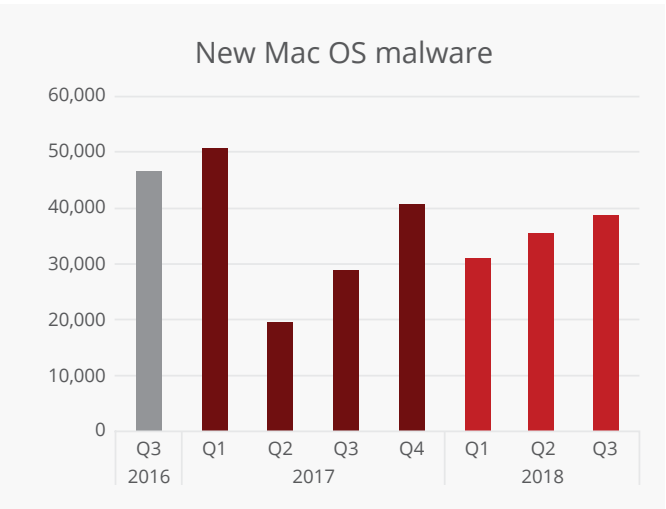
## Malware



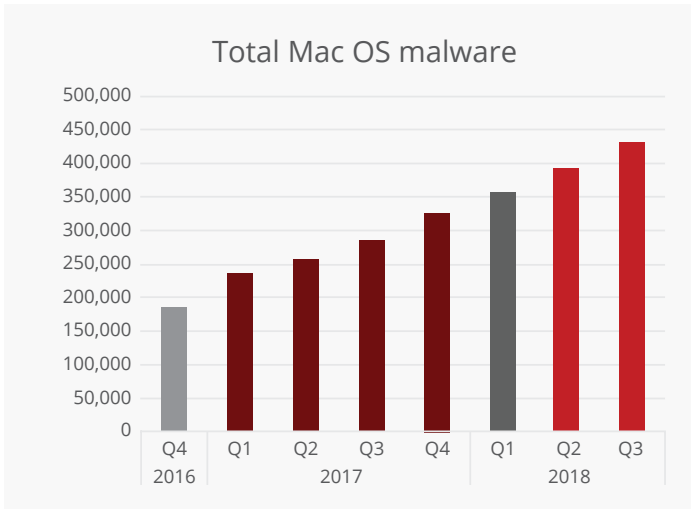

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.

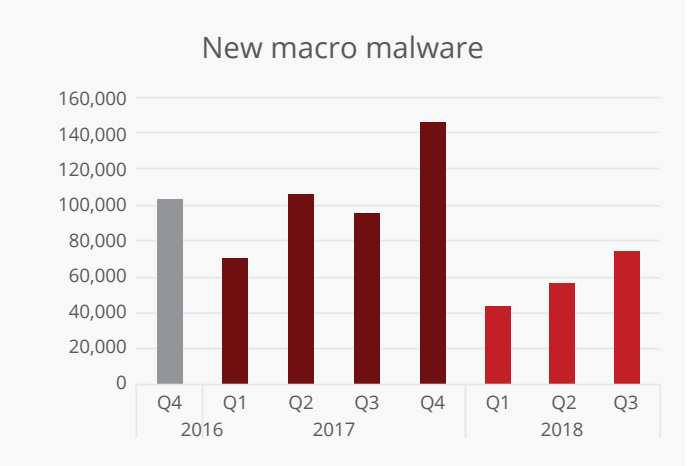



Source: McAfee Labs, 2018.

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




Source: McAfee Labs, 2018.

Many of the macros used in attachments are heavily obfuscated to make it difficult for analysts to understand the macro's function. With Vba2Graph, we can visualize the flow of a macro's execution to understand what could happen:

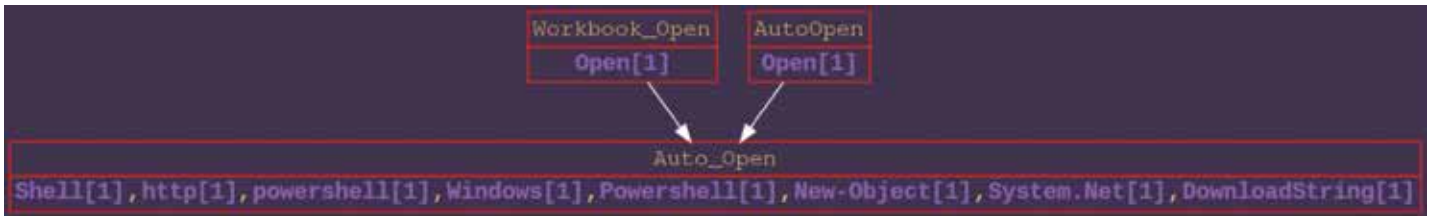



Figure 15. The AutoOpen function opens a shell on the victim's system, and then opens PowerShell to download a file.

**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.**

Follow

Share

The preceding example is typical; we see these embedded daily. Now let's look at a more obscure example:

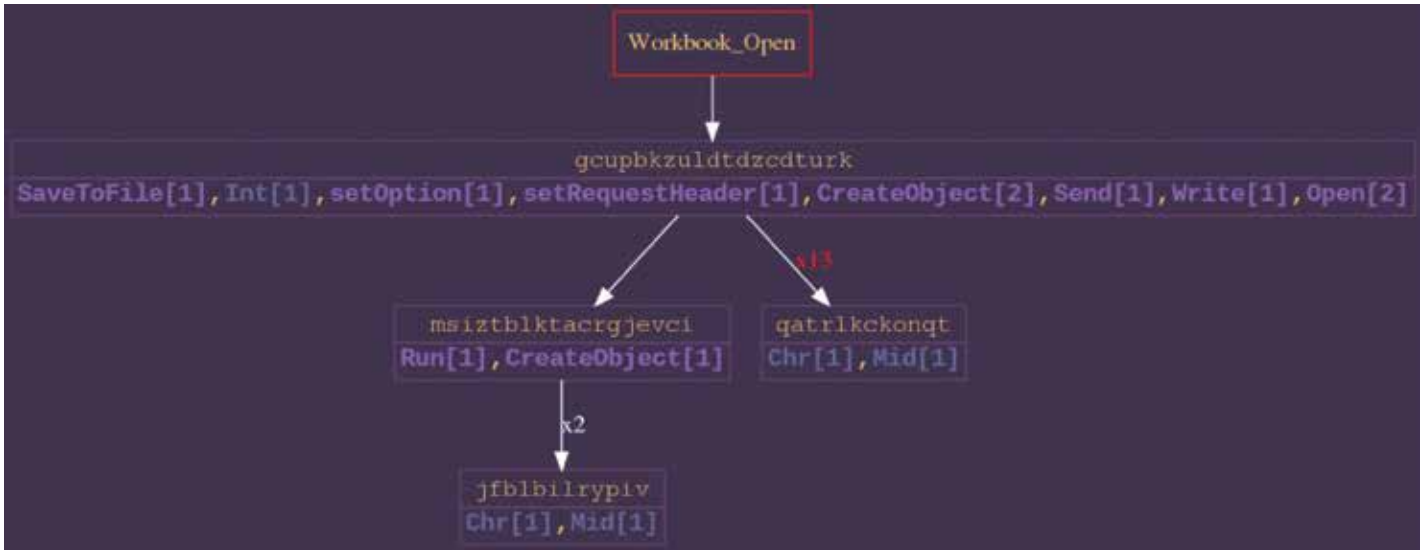
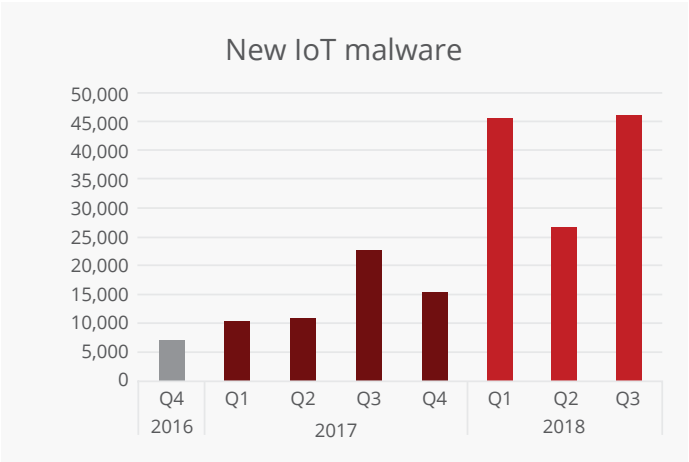
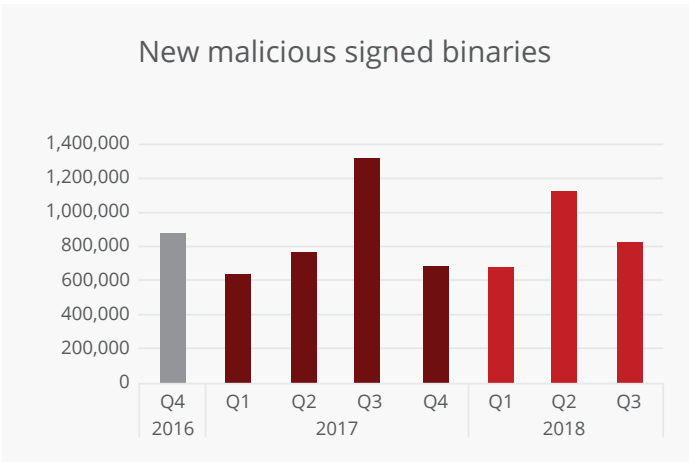



Figure 16. A macro creates a new file and runs it, but the function names are obfuscated.

In this example, we can still determine some of the actions, but an analyst researching this has to spend more effort to understand what is happening. Further, machine learning solutions that look only at function names (Auto_Open) fail because these names are obfuscated. By using multiple classifiers, however, we can create a successful a machine learning model to determine whether macros are malicious, as we do on the Advanced Threat Research team.




Source: McAfee Labs, 2018.



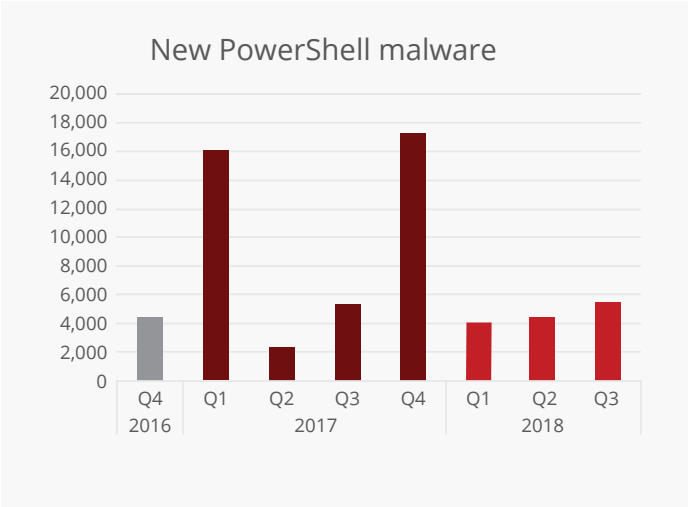

Source: McAfee Labs, 2018.

**Threats to the Internet of Things target a variety of hardware, including IP cameras, home routers, and smart devices. These threats generally affect Linux-based systems.**

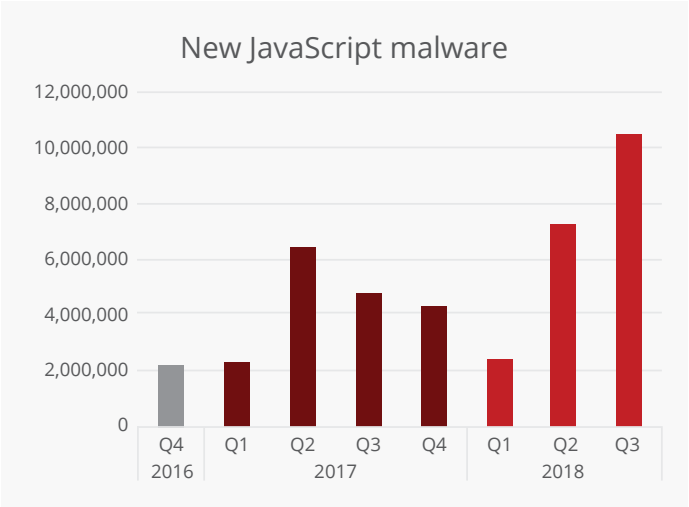
**Certificate authorities provide digital certificates that deliver information once a binary (application) is signed and validated by the content provider. When cybercriminals obtain digital certificates for malicious signed binaries, attacks are much simpler to execute.**

Follow

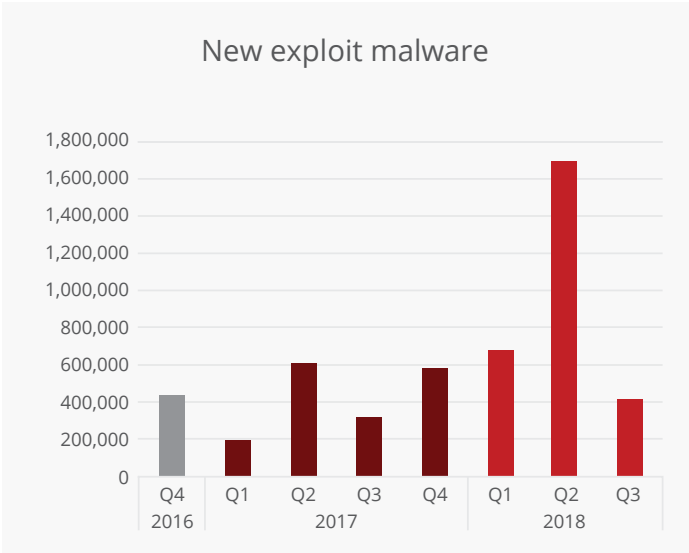
Share




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.

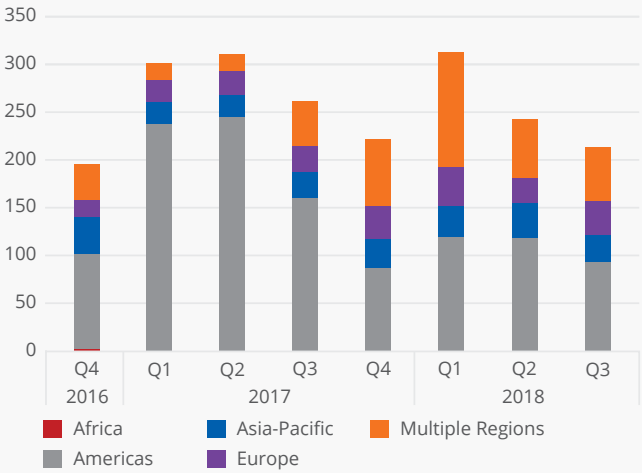
For more on JavaScript and PowerShell threats, read "The rise of script-based malware," from an earlier *McAfee Labs Threats Report.*

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."

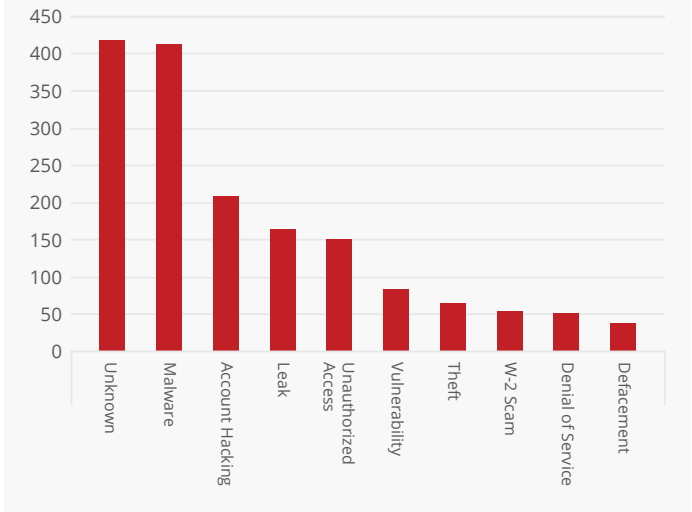
Follow

Share

## Incidents




Source: McAfee Labs, 2018.



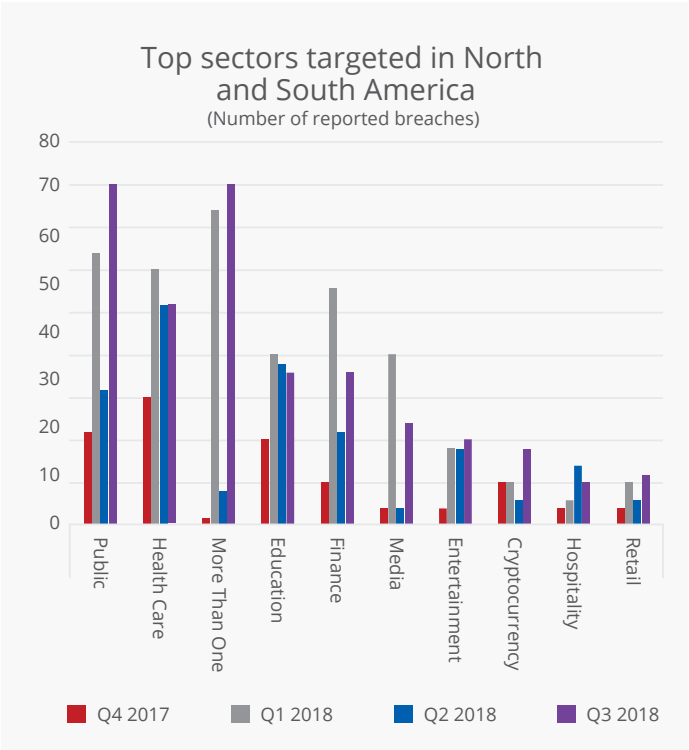

Source: McAfee Labs, 2018.

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

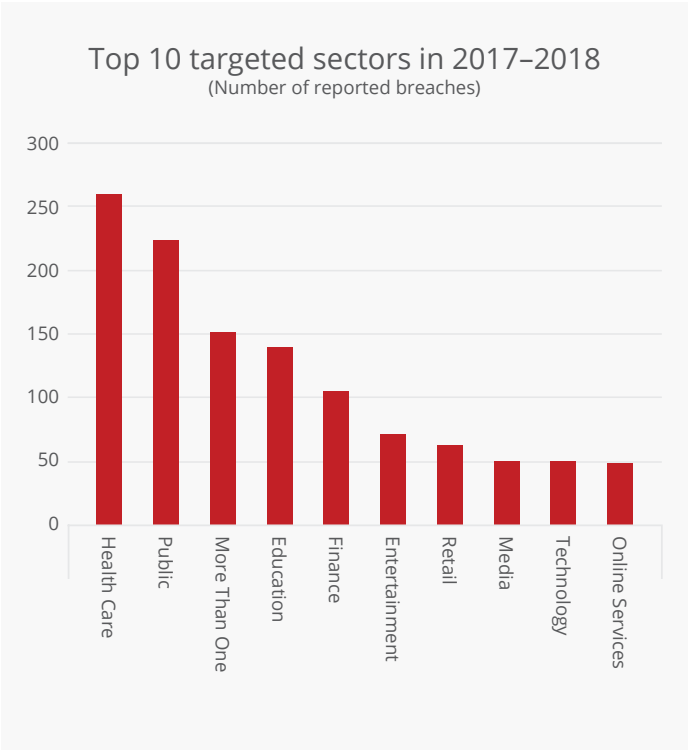
**The majority of attack vectors are either not known or not publicly reported.**

Follow

Share




Source: McAfee Labs, 2018.

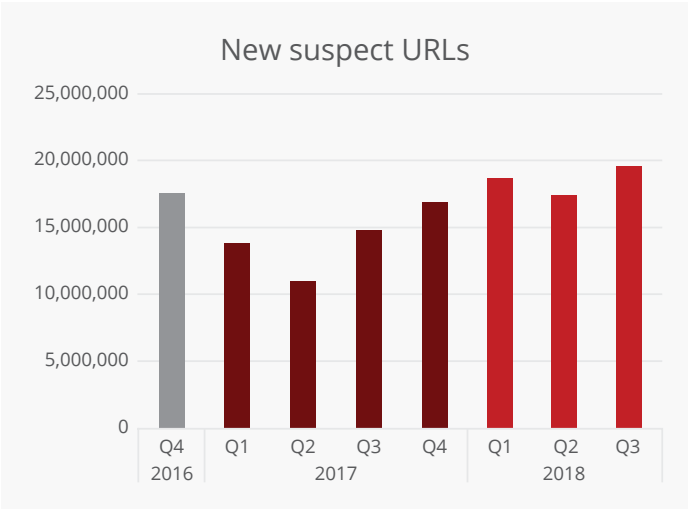



Source: McAfee Labs, 2018.

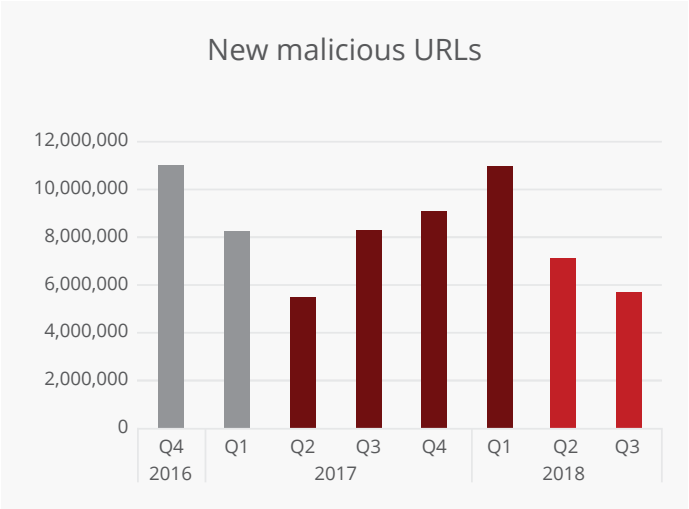
Follow

Share

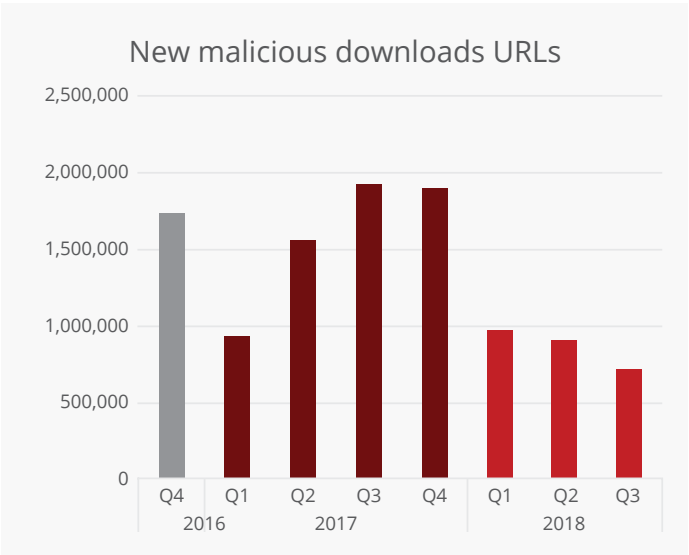
## Web and Network Threats



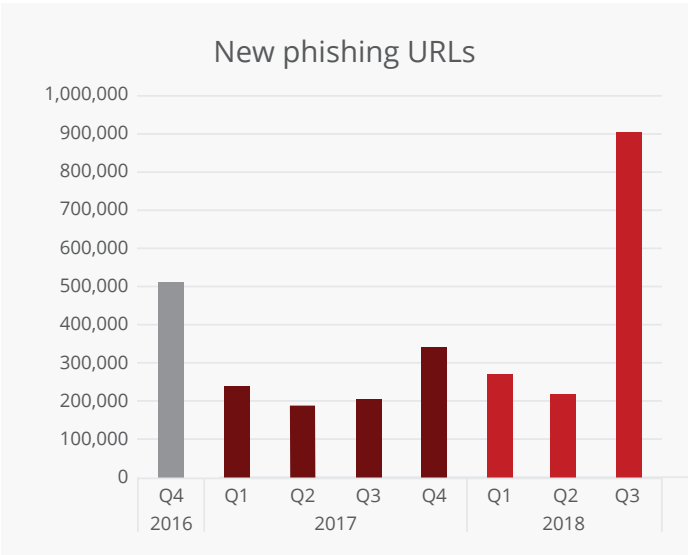

Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.




Source: McAfee Labs, 2018.



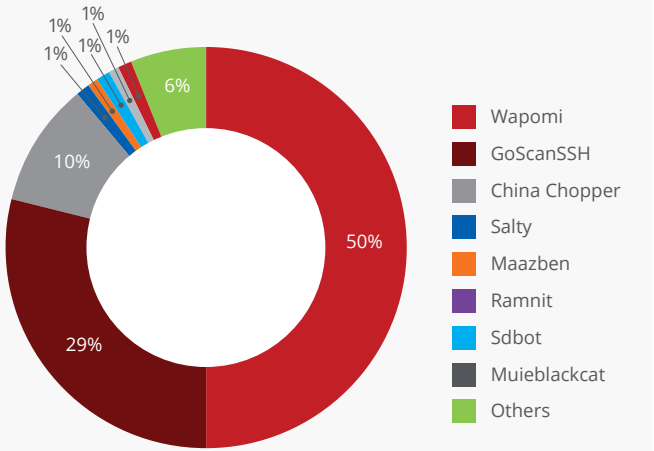

Source: McAfee Labs, 2018.

**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

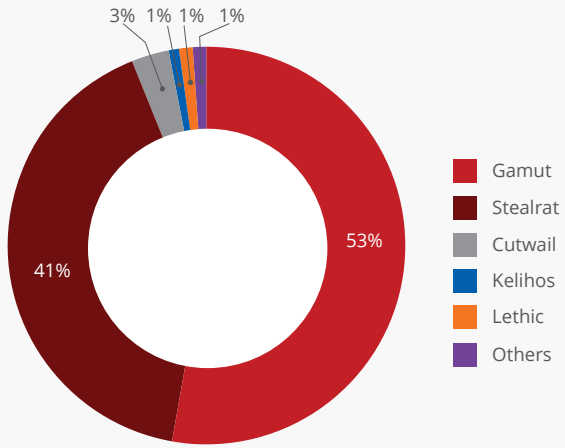
Share

## Top malware connecting to control servers in Q3



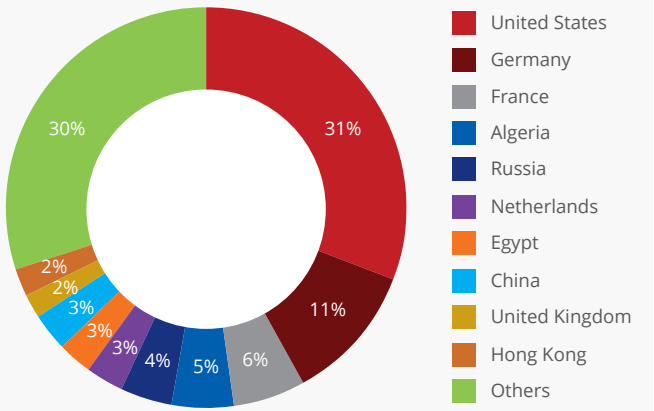

Source: McAfee Labs, 2018.

## Spam botnet prevalence by volume in Q3



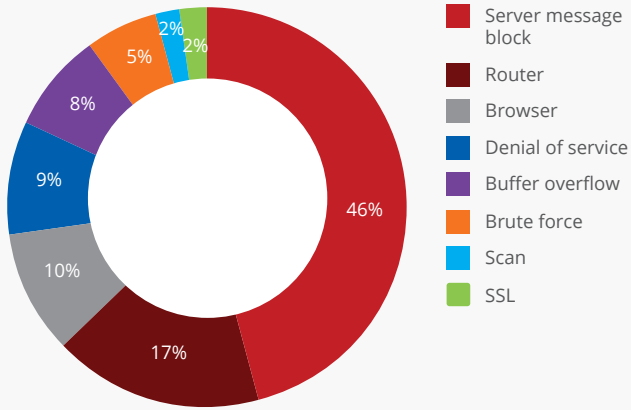

Source: McAfee Labs, 2018.

## Top countries hosting botnet control servers in Q3




Source: McAfee Labs, 2018.

## Top network attacks in Q3




Source: McAfee Labs, 2018.

**Gamut, the top spam-producing botnet, spews "sextortion" scams, which demand payment and threaten to reveal victims browsing habits. For the second time in 2018, StealRat was among the top botnets, with 41% of total volume; much of StealRat's spam is related to adult dating. The Necurs botnet failed to make the chart for the first time in nearly two years. Having been the highest-volume emitter during Q4 2017 and Q1 2018, this absence is unlikely to last.**

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