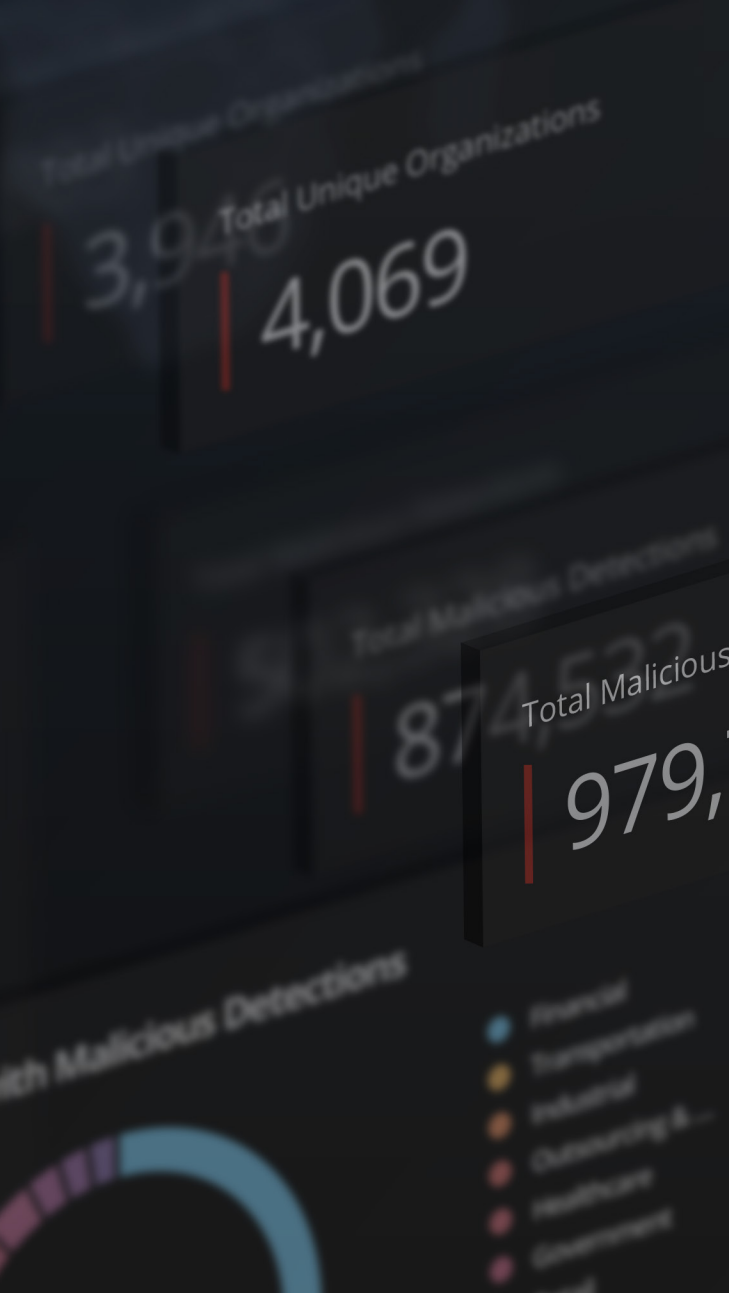


# McAfee Labs COVID-19 Threats Report

July 2020



---

# The dominant theme of 2020 has been the scale and impact cyber-related attacks have had on our wider society.

---

## Introduction

What a year so far. What started as a trickle of phishing campaigns and the occasional malicious app quickly turned into a deluge of thousands of malicious URLs and more-than-capable threat actors leveraging our thirst for more information as an entry mechanism into systems across the world.

In this “Special Edition” threat report we take a deeper dive into COVID-19 related attacks. Additionally, we have launched the [McAfee COVID-19 Threats Dashboard](#) to complement this threat report and extend its impact beyond the publication date.

Timeliness is a challenge for publishing any threat report, but through the development of [MVISION Insights](#), our threat reports will link to a live dashboard tracking the world’s top threats. We will also make available the IoCs, Yara rules, and mapping to the MITRE ATT&CK framework as part of our continuing commitment to sharing our actionable intelligence. I hope these McAfee resources will be useful to you, the reader.

This report was researched and written by:

- Christiaan Beek
- Taylor Dunton
- Dan Flaherty
- Lynda Grindstaff
- Steve Grobman
- Tracy Holden
- Tim Hux
- Abhishek Karnik
- Sriram P
- Tim Polzer
- Thomas Roccia
- Raj Samani
- Sekhar Sarukkai
- Craig Schmugar

---

Follow



Share



The dominant theme of 2020 has been the scale and impact cyber-related attacks have had on our wider society. All too often, we are called into investigations where businesses have been halted, or victims have lost considerable sums of money. While we all have had to contend with pandemic lockdown, criminals of all manner of capability have had a field day.

We hope you enjoy these new threat report approaches, and moreover we would appreciate you sharing these findings far and wide. These tools and insights could be the difference between a business remaining operational or having to shut its doors at a time when we have enough challenges to contend with.

Many thanks for your time.

—*Raj Samani, McAfee Fellow and Chief Scientist*

Twitter [@Raj\\_Samani](#)

---

Follow

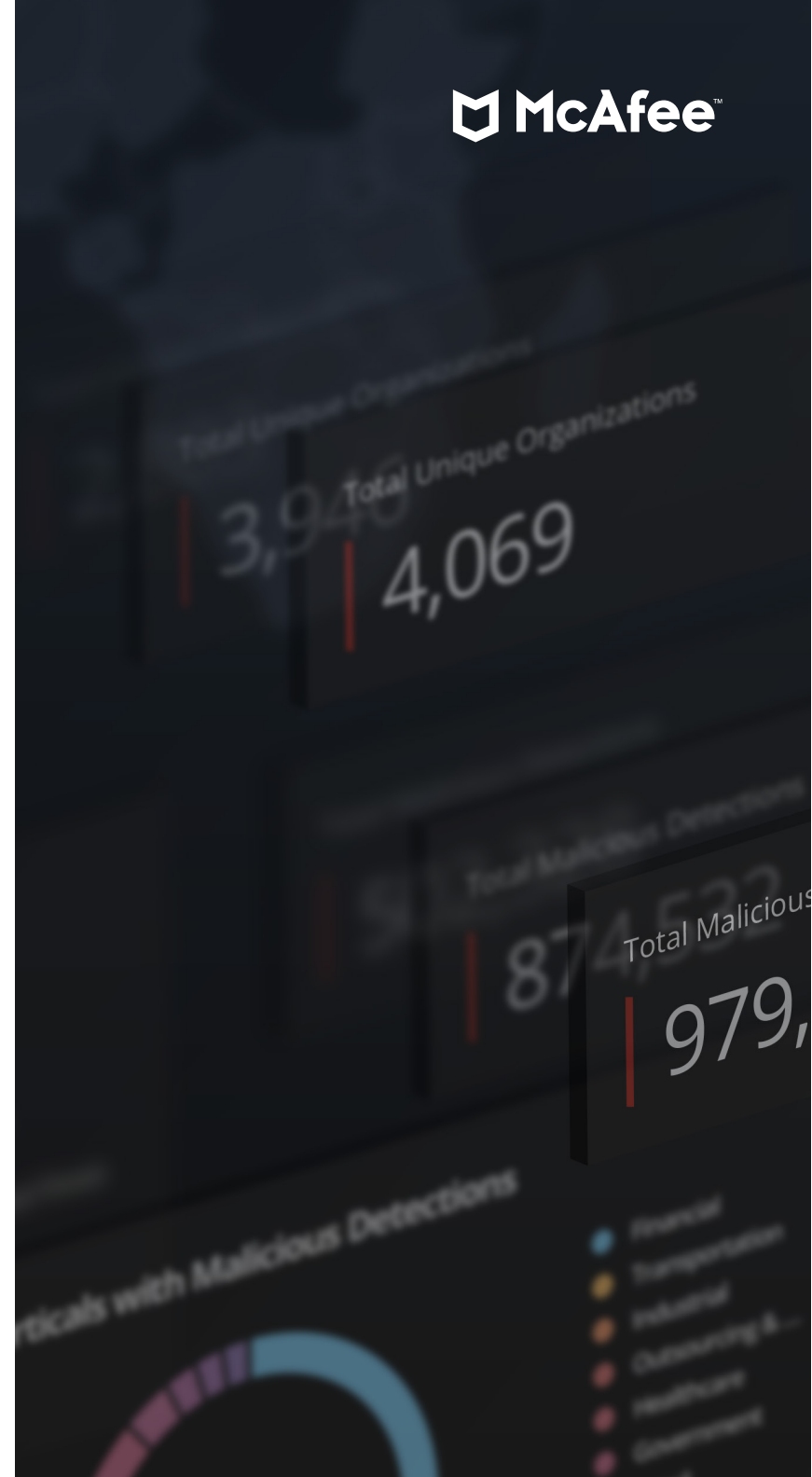


Share



## Table of Contents

<b>6</b>	COVID-19 Cyberthreat Timelines, Distribution, and Detection	<b>32</b>	Spams and Scams
<b>7</b>	Threats To Sectors and Vectors	<b>33</b>	Underground Marketplaces
<b>10</b>	Malware Threats Statistics	<b>35</b>	URL Scams
<b>14</b>	Threat Actors Target the Cloud	<b>39</b>	Recommendations
<b>18</b>	Malware Phishing and Trojans		
<b>30</b>	Ransomware		



It's no surprise that opportunistic cybercriminals are targeting employees working from home during the COVID-19 pandemic. The need for enterprises to quickly quarantine workforces has challenged SOCs and CTOs to adapt a secure work-from-home model the scope of which the security industry has never experienced.

Providing the collaboration and productivity systems sufficient to fuel a functioning work-from-home force has required a greater reliance on personal cyber hygiene as employees balance their everyday at-home bandwidth with the technical demands of their jobs. The workforce is also distracted by the anxieties created by a departure from normalcy and routine, dealing with their family's needs at a time when the requirements of quarantining such as social distancing, personal protection equipment requirements, supply-and-demand shortages, increasing unemployment, and a full stop on the mental benefits of expectations and routines. Cybercriminals see a remote, distracted, and vulnerable workforce as opportune targets.

Cybercriminals are using COVID-19-themed ransomware, RDP exploits, scam URLs and spam designed to lure remote workers into mishandling external engagement. Clicking an unverified link or opening an ill-advised

attachment, and other engagements designed to unleash their full arsenal of malware with tactics and techniques honed to target pandemic vulnerabilities and breach internal corporate resources.

Since early reports of the Coronavirus, McAfee researchers have focused our security research and resources on the tactics and techniques cybercriminals have wielded during the pandemic's progression. We have worked to keep our customers and security community safe through the monitoring and adaptation of our detection stack to better manage the COVID-19 threat landscape. Consult the [McAfee Threat Center](#) for the latest in evolving COVID-19 threats.

---

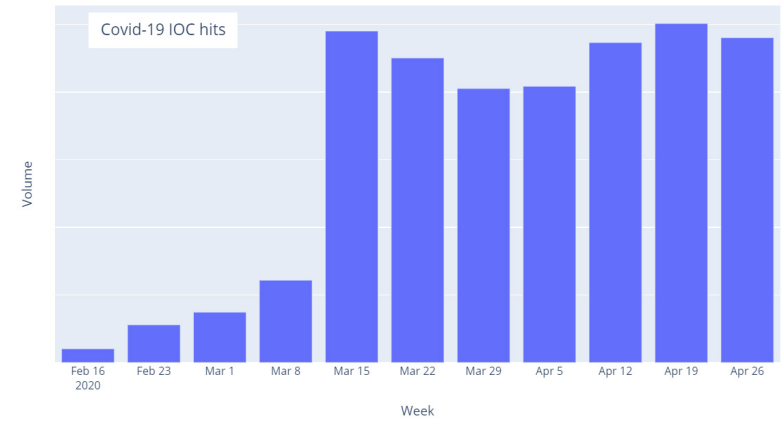
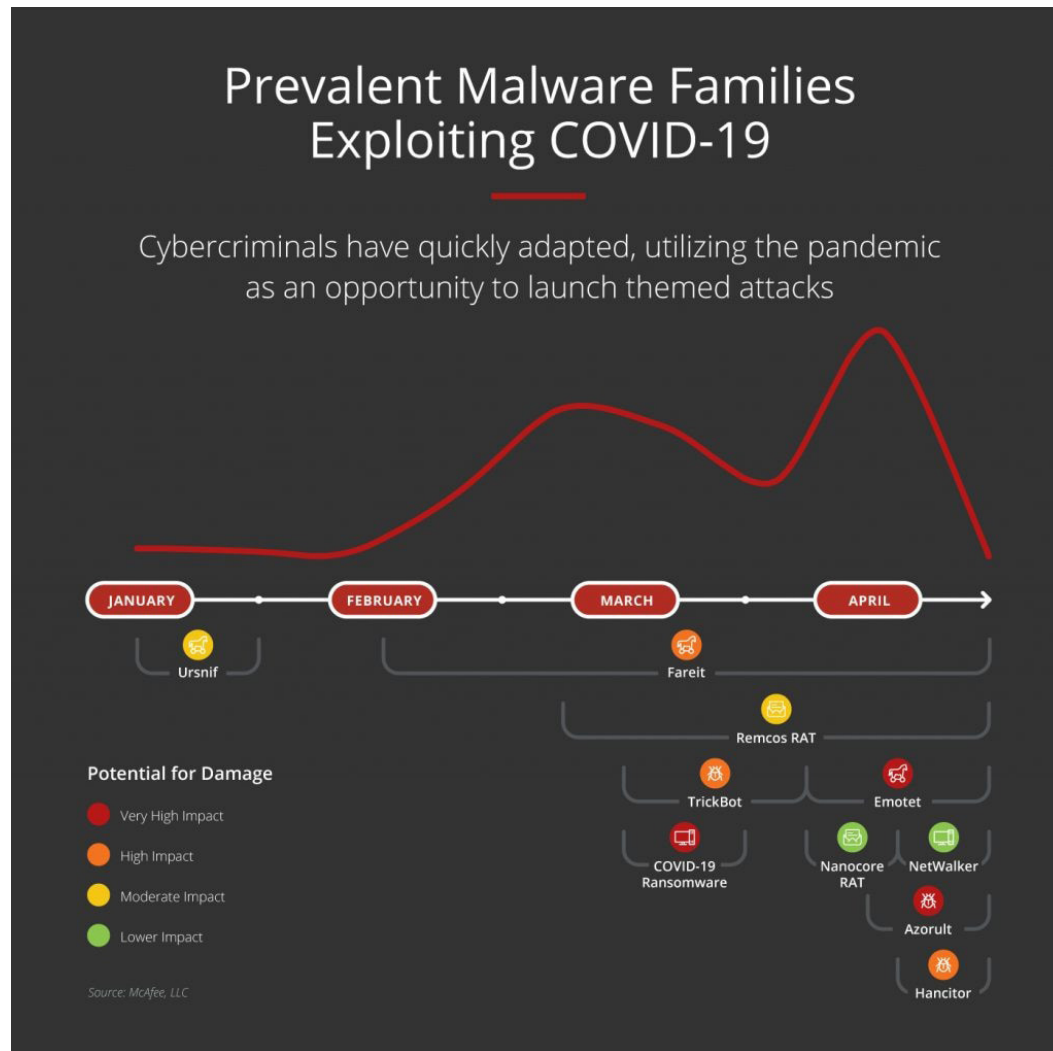
Follow



Share



COVID-19 Cyberthreat Timelines, Distribution, and Detection



Follow   

Share 

### Threats to Sectors and Vectors

The volume of threats related to COVID-19 has been significant, with lures used in all manner of attacks.

McAfee has observed malicious detections in almost all the countries impacted by the COVID-19 pandemic, although the volume differs greatly.

### Global Detection Heat Map

The [McAfee COVID-19 Threat Dashboard](#) uses intelligence gathered and updated daily by McAfee Advanced Programs Group (APG). McAfee first observed a detection for known IoCs in mid-January. We observed detections in almost all the countries which have been impacted by the COVID-19 pandemic.<sup>1</sup>

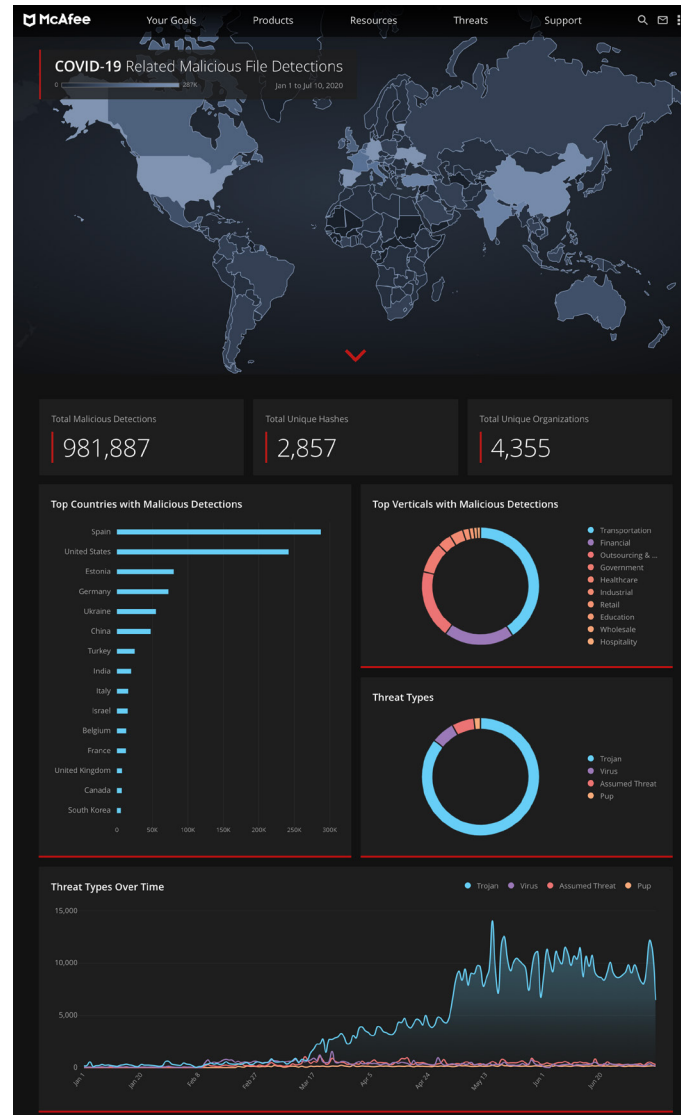


Figure 1. Our COVID-19 Threats Dashboard extends the impact of this report with daily updated intelligence provided by McAfee Advanced Programs Group (APG).

Follow



Share



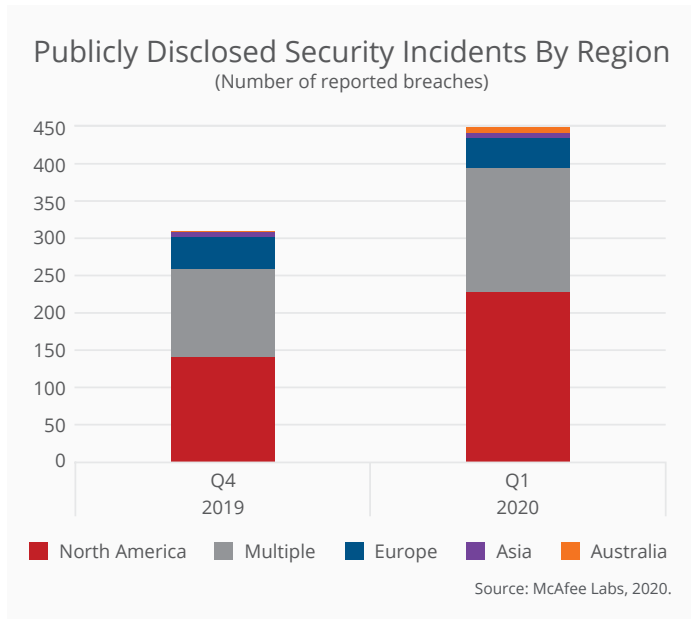


Figure 2. McAfee Labs counted 458 publicly disclosed security incidents in the first quarter of 2020, including those in which the region target was non-applicable, an increase of 41% from Q4 of 2019. Disclosed incidents targeting North America increased 60% over the previous quarter, while Europe decreased 7%.

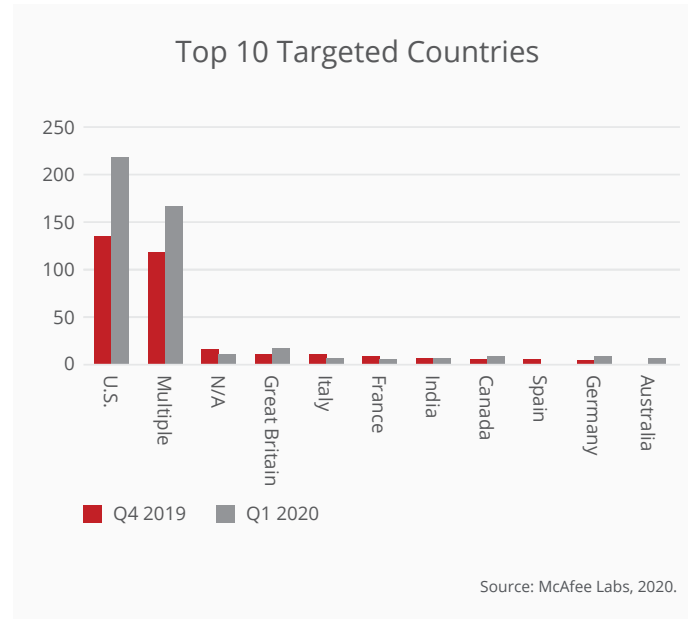


Figure 3. Disclosed incidents targeting the United States in Q1 2020 increased 61%, Great Britain increased 55%, and Canada increased 50% over the previous quarter.

Follow



Share





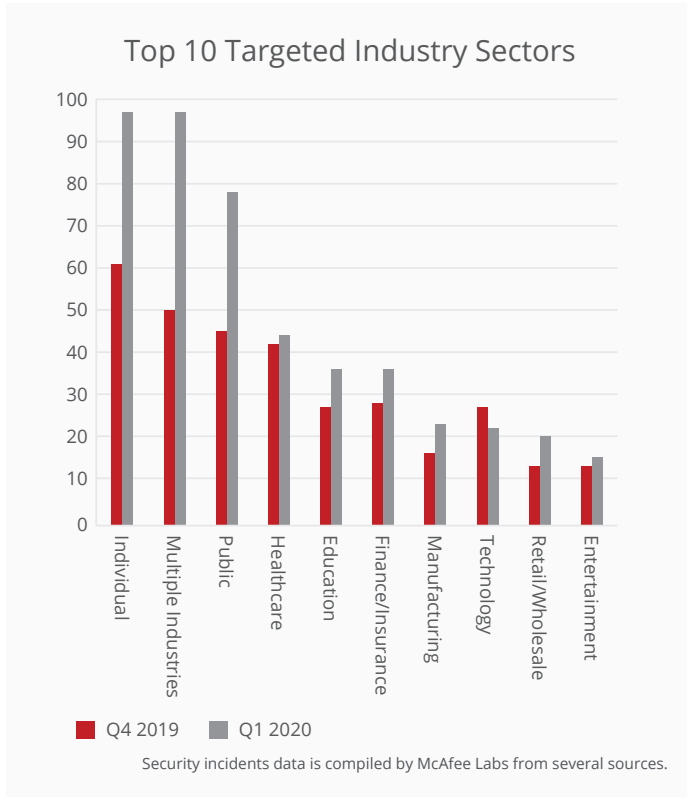


Figure 4. Disclosed incidents detected in the first quarter of 2020 targeting Multiple Industries increased 94%, the Public sector increased 73%, the Individual sector increased 59%, and Manufacturing increased 44%, while incidents in Science and Technical decreased 19%.

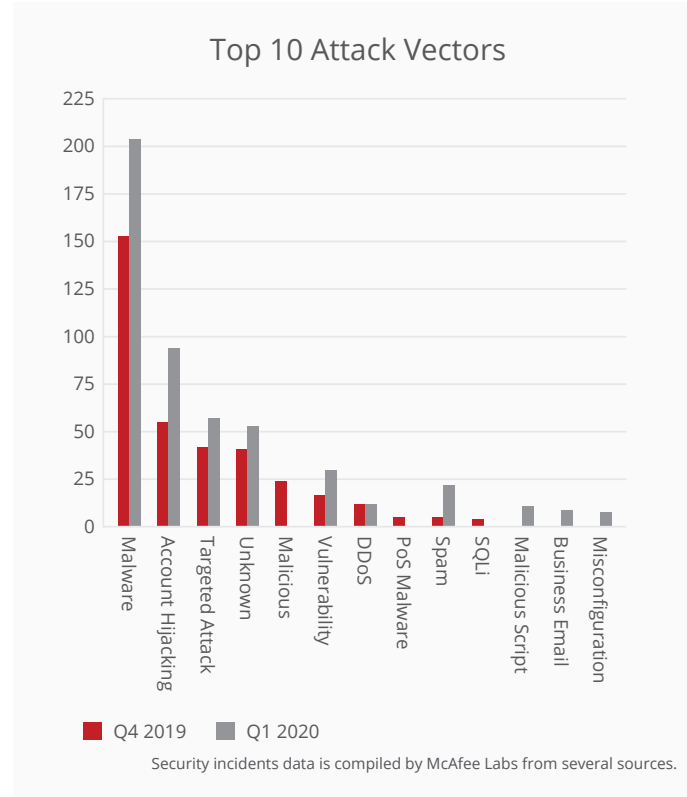


Figure 5. Overall, malware led disclosed attack vectors in the first quarter of 2020, followed by account hijacking and targeted attacks. Disclosed malware attacks increased by 33% from the previous quarter, account hijacking attacks increased by 71%, and Targeted Attacks increased by 60%.

Follow



Share



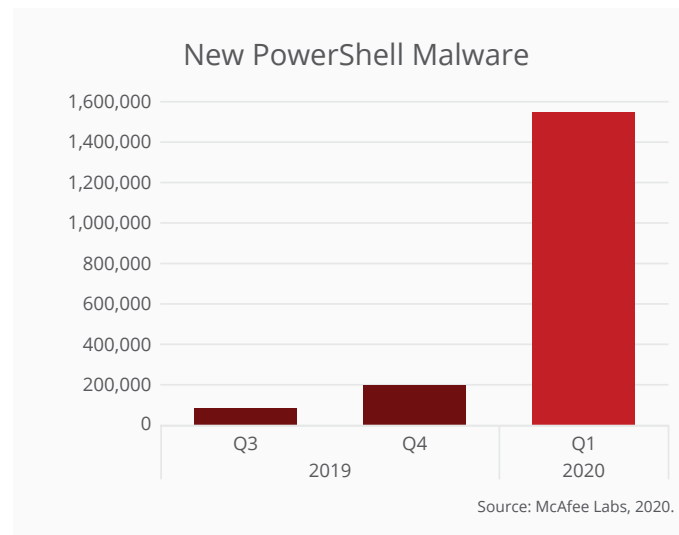
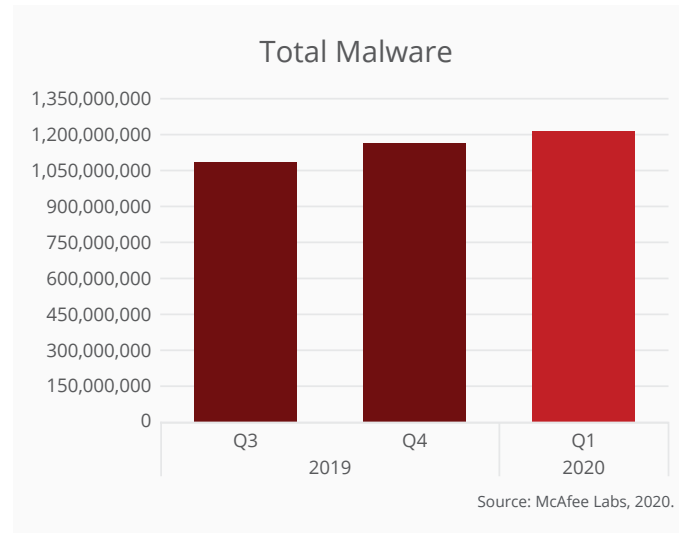
### Malware Threats Statistics

The first quarter of 2020 saw significant increases in several threat categories:

- McAfee Labs observed 375 threats per minute in Q1 2020.
- New PowerShell Malware increased 689% in Q1 2020 when compared to the previous quarter. This increase can largely be attributed to the Donoff family of TrojanDownloader. Donoff also played a significant role in a 412% increase of New Macro Malware during Q1 2020.
- Total PowerShell malware grew 1,902% over the previous four quarters.
- New Mobile Malware increased 71% during Q1 2020 compared to the previous quarter, primarily due to Trojans.
- Total mobile malware grew nearly 12% over previous four quarters.
- New IoT Malware (58%) and New MacOS Malware (51%) rose by more than 50%.
- New Coin Miner Malware increased 26%.
- New Linux rose 8%.

The following categories showed reductions in Q1 2020 compared to the previous quarter:

- New Exploit Malware decreased 56%.
- New JavaScript Malware decreased 38%.
- New Malware decreased 35%.
- New Ransomware decreased 12%.
- New Malicious Signed Binaries decreased 11%.

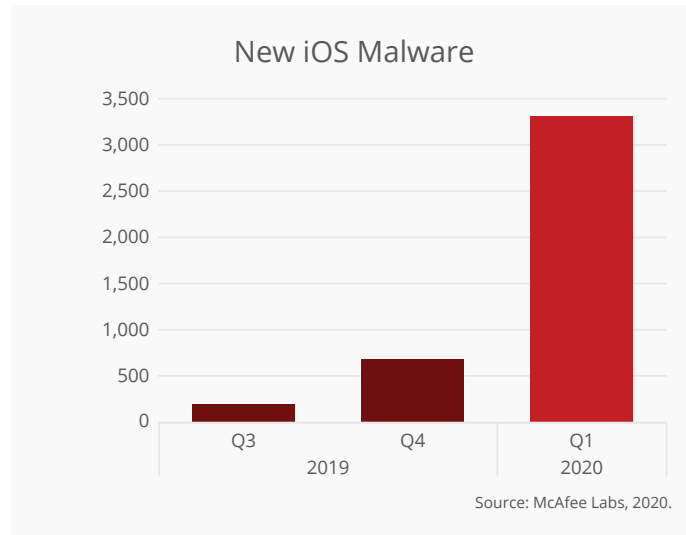
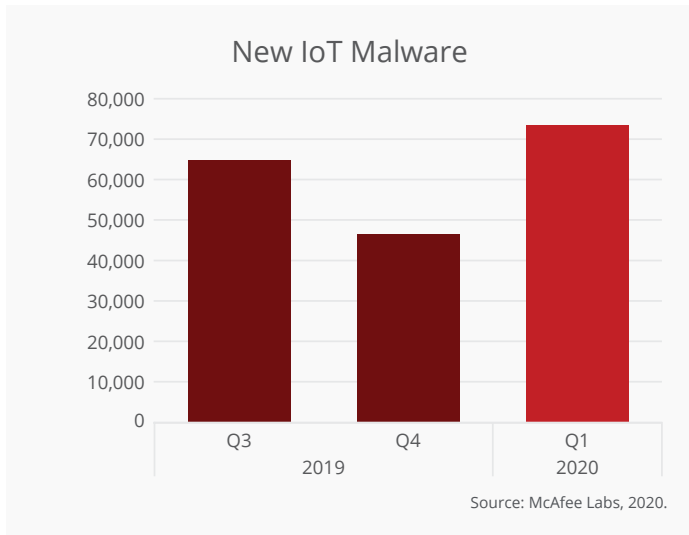
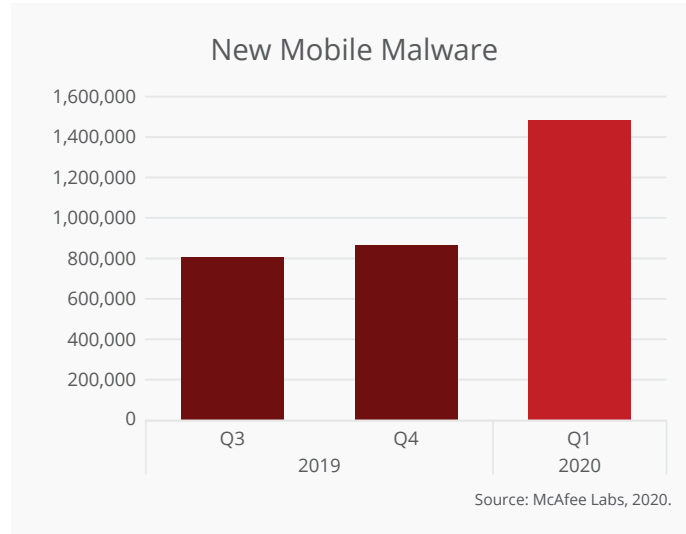
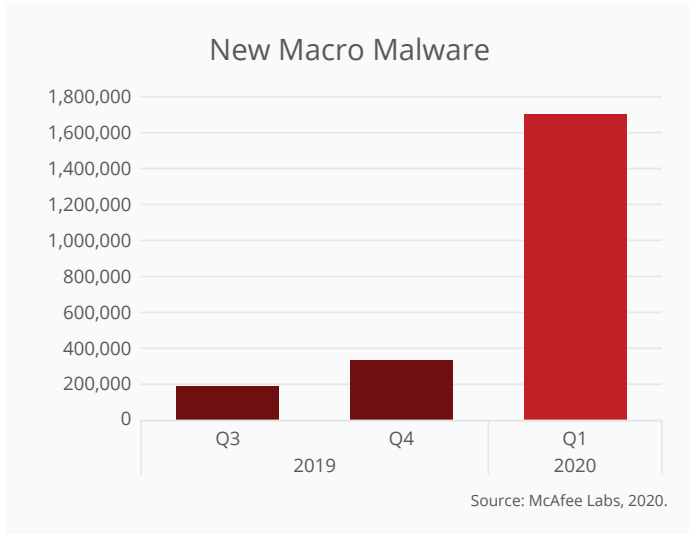


Follow



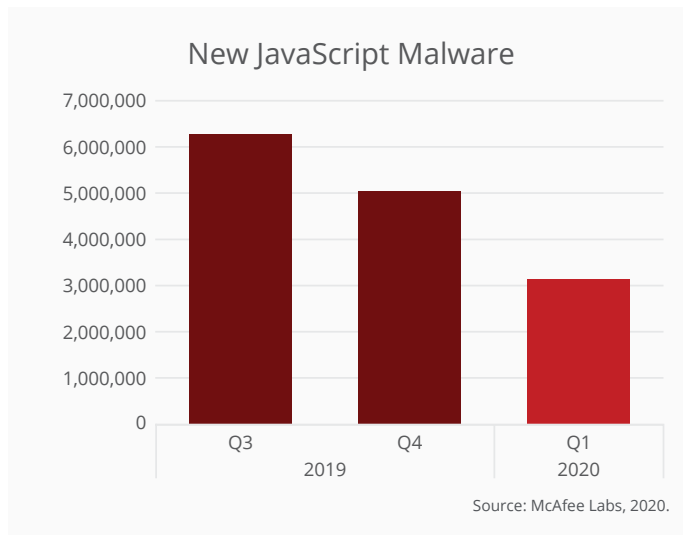
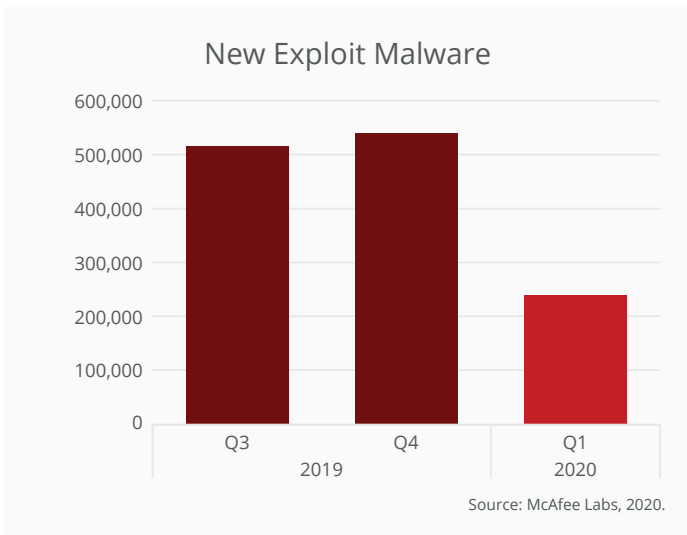
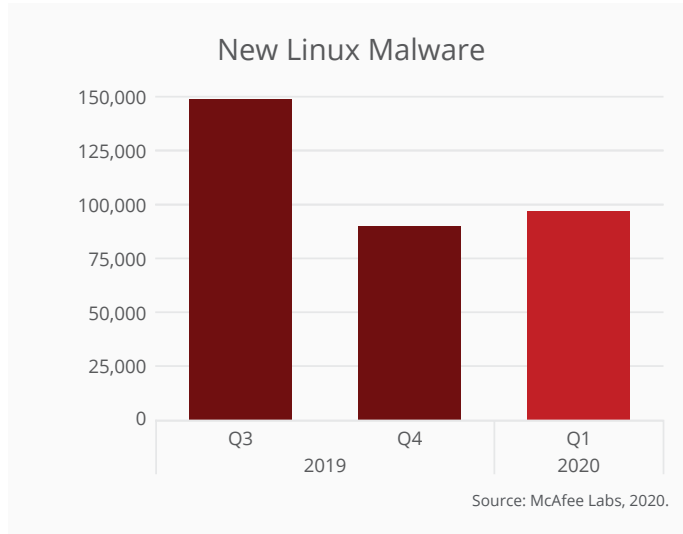
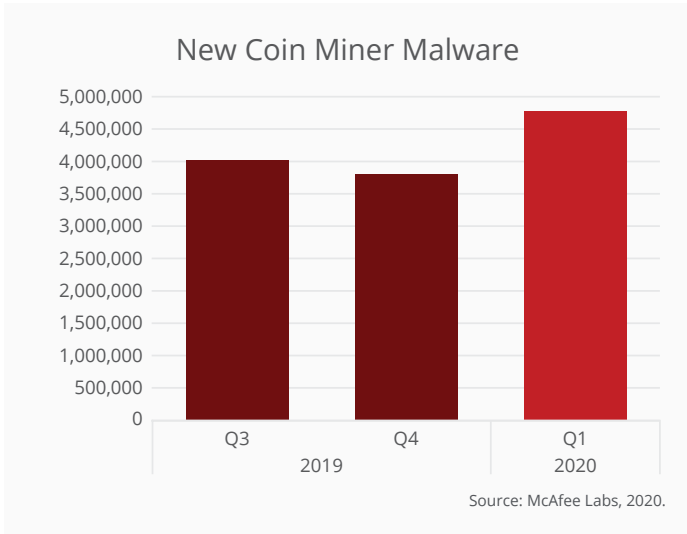
Share





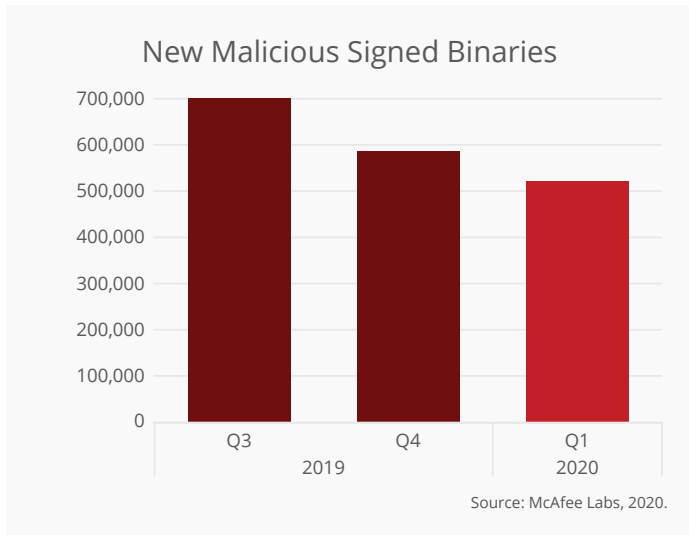
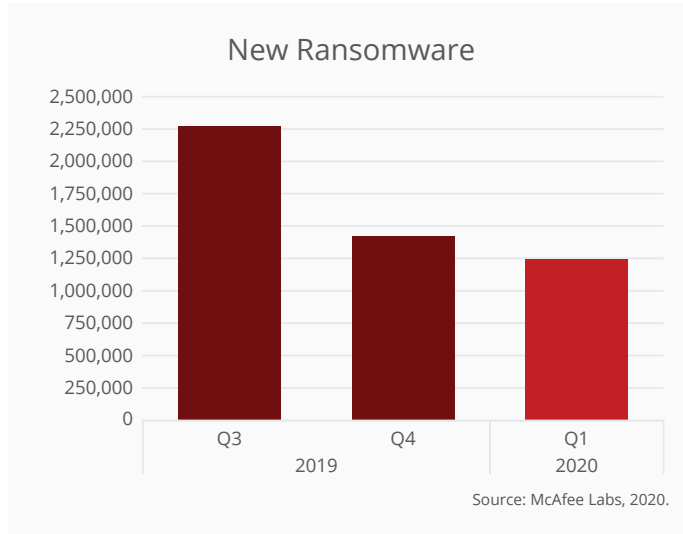
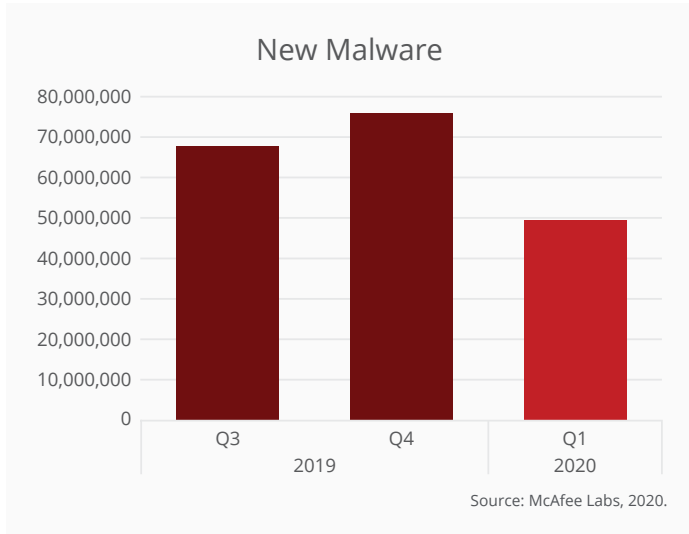
Follow   

Share 



Follow   

Share 



Follow   

Share 

### Threat Actors Target the Cloud

The sudden, large-scale shift of the global workforce to work from home included a growth as high as 775%<sup>2</sup> according to Microsoft. In compiling the [McAfee Cloud Adoption and Risk Report—Work From Home](#) edition, McAfee aggregated and anonymized cloud usage data from more than 30 million McAfee MVISION cloud users worldwide between January and April 2020. The amount of threats from external actors targeting cloud services increased 630% with the greatest concentration on collaboration services like Microsoft 365. McAfee separated external threats into two categories, both typically involving the use of stolen credentials:

- **Excessive Usage from Anomalous Location.** This begins with a login from a location that has not been previously detected and is anomalous to the user’s organization. The threat actor then initiates high-volume data access and/or privileges access activity.
- **Suspicious Superhuman.** This is a login attempt from more than one geographically distant location impossible to travel to within a given period of time. McAfee tracks this across multiple cloud services for example, if a user attempts to log into Microsoft 365 in Singapore, then logs into Slack in California five minutes later.

Internal or insider threat categories remained the same indicating that employees didn’t take advantage of working from home to attempt to steal more data. Most of the attacks McAfee observed were external cloud-native threats directly targeting cloud accounts.

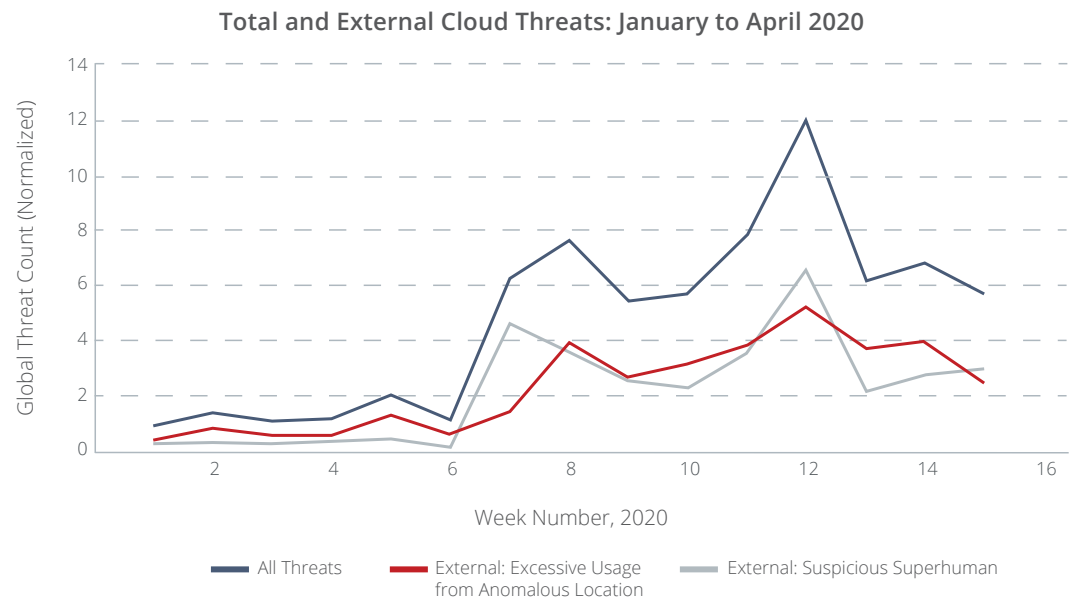


Figure 6. Cloud threat events across all industries.

Follow   

Share 

### Vertical Focus: Cloud Threats

Transportation and Logistics, Education, and Government experienced the largest increases in internal and external threat events in their cloud accounts. These industries increasingly depend on cloud services for productivity, and likewise, attackers followed the trend with attempts to access their accounts and exfiltrate data.

McAfee ran an analysis of the source IP addresses used in attacks from external actors to see the locations they were sourced from.

While source IP can't be used to determine attribution for an attack, it does offer a view of attack data that can assist with the implementation of security controls. The IPs monitored were not only used to attack cloud accounts, but also other malicious activity, pointing to the reuse of criminal infrastructure for multiple attacks.

The data in the following IP chart indicates the number of IP addresses used to launch attacks by size of circle, and the peak number of threat events targeting individual organizations from these IPs by depth of color.

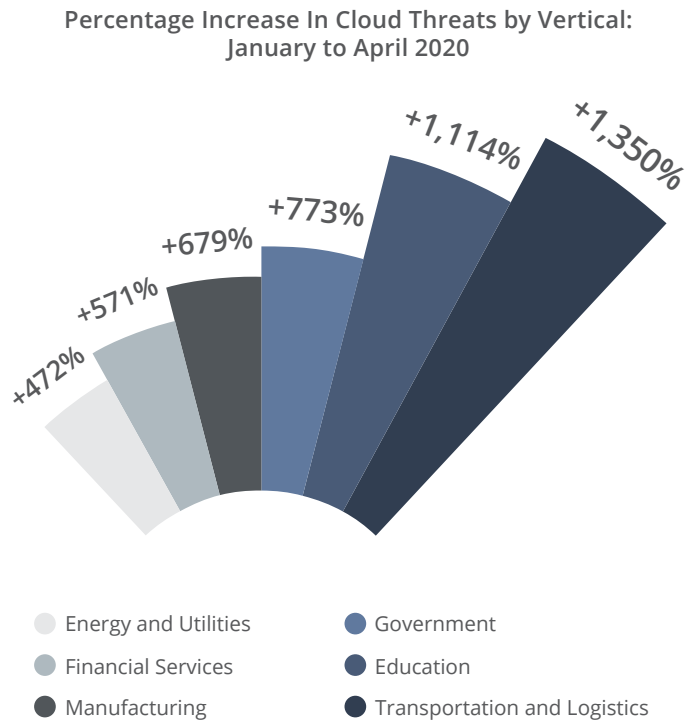


Figure 7. Increase in cloud threat events by industry.

Follow



Share



Source IP Geolocation for External Cloud Threats: January to April 2020



Figure 8. Global view of external attack sources on cloud accounts by source IP geolocation.

The top 10 source IP geolocations for external attacks on cloud accounts from January to April 2020 (sorted by number of IPs used) are:

- |                       |                  |
|-----------------------|------------------|
| 1. Thailand           | 7. Laos          |
| 2. USA                | 8. Mexico        |
| 3. China              | 9. New Caledonia |
| 4. India              | 10. Vietnam      |
| 5. Brazil             |                  |
| 6. Russian Federation |                  |

Note: None of the countries in our top 10 are in Europe, which wields some of the most stringent data protection regulations in the world. The majority originated from countries historically active in cybercrime and others lacking resources to enforce cybercrimes regulations.<sup>3</sup>

Follow



Share



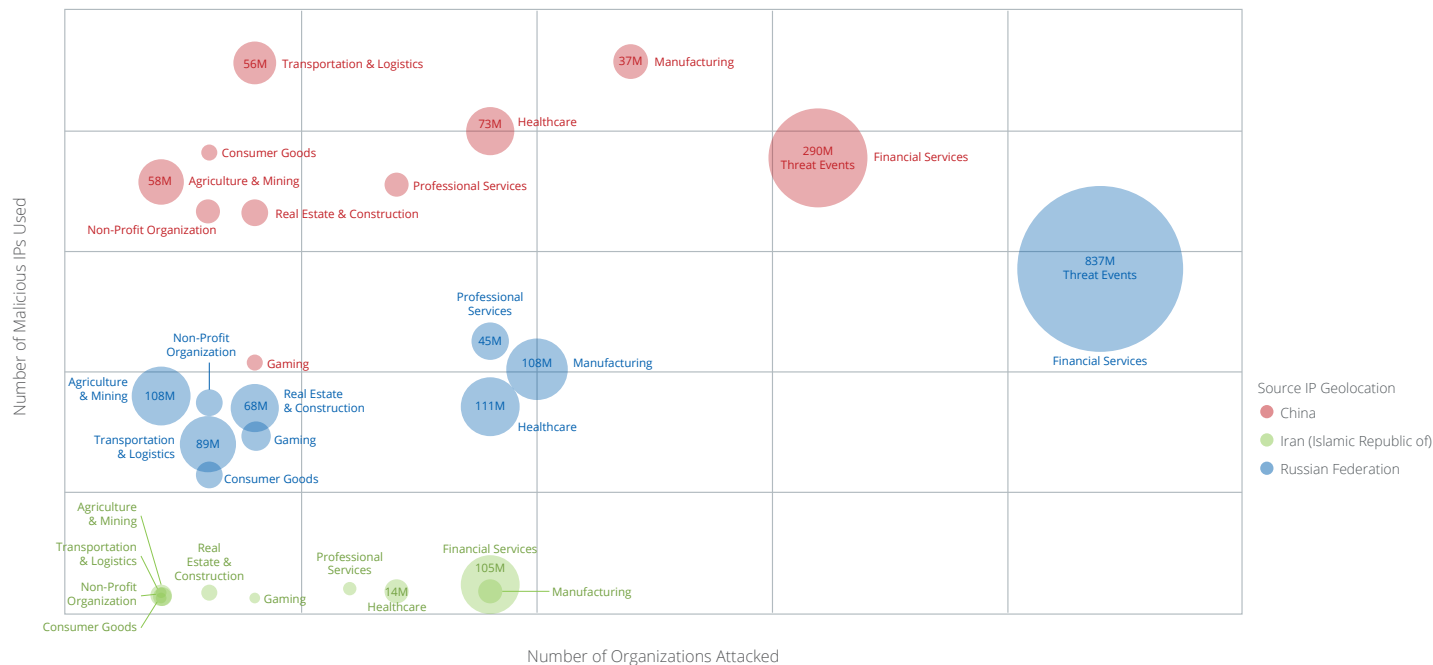


Many of these attacks are likely opportunistic, essentially “spraying” cloud accounts with access attempts using stolen credentials. However, several prominent industries are often targeted by external threat actors in particular Financial Services. These targeted attacks are often found to have a source in either China, Iran, or Russia.<sup>4</sup>

The IP geolocation of these three countries can provide a deeper view into how industries are being targeted by external cloud attacks. In the following chart, the

vertical axis shows the number of IPs used against each industry, with more IPs typically indicating more infrastructure and funding behind the attacks. The horizontal axis shows the number of organizations in a given industry being attacked, giving us a sense of the allocation attack infrastructure across vertical. Bubble size similarly shows us the volume of threat events targeting a specific industry, with color representing either Russia, China, or Iran.

Industry Comparison of Cloud Threat Volume from Common Targeted Attack Sources: January to April 2020



Follow



Share



While Financial Services experienced the fifth highest increase in attack volume that industry experienced the highest attack volume in a view of common locations for targeted attacks.

Healthcare is the second-most targeted industry, followed by Manufacturing. All organizations, but those in highly targeted industries in particular, need to continuously monitor their cloud activity to detect and block malicious access to their sensitive data.

### Malware Phishing and Trojans

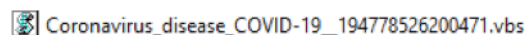
As a global workforce learned to adapt to remote work amidst COVID-19 quarantines, threat actors also adapted to opportunities offered by the security challenges and systemic stresses presented during the pandemic.

Cybercriminals have used phishing email delivery methods with pandemic themes and messages to entice employees and their family members into engaging with and enabling threats to gain a foothold on their systems.

Phishing campaigns based on bogus SBA Loans emails, scam COVID-19 tests, and antibody treatments have also been detected.

### Ursnif

In January, McAfee observed the emergence of a phishing campaign using a strain of Ursnif, a banking Trojan that steals banking credentials by collecting activities of the victims, records keystrokes and tracks network traffic and browser activity.



On executing the VBS file it drops a dll in C:\Programdata\FxrPLxT.dll and executes the .dll with rundll32.exe. The dll is injected into iexplorer.exe and communicates with its C&C server using http get requests.

### IOCs

Type	IOC	Comment
Sha256	e82d49c11057f5c222a440f05daf9a53e860455dc01b141e072de525c2c74fb3	Filename: Coronavirus_disease_COVID-19_194778526200471.vbs
Sha256	8bcdf1fbc8cee1058ccb5510df49b268dbfce541cfc4c83e135b41e7dd150e8d	Ursnif dll

Follow



Share



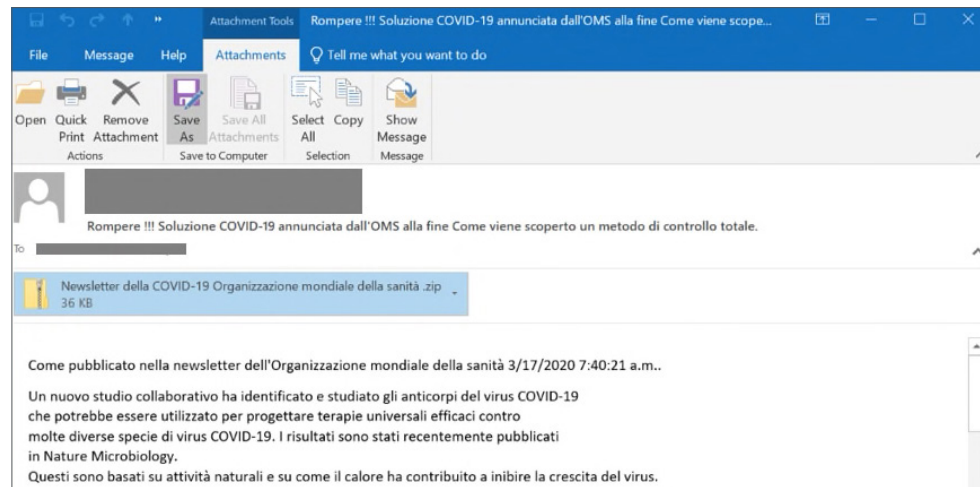
MITRE ATT&CK™ MATRIX

Technique ID	Tactic	Technique details
T1059	Execution	Command-Line Interface
T1129	Execution	Execution through Module Load
T1085	Defense Evasion, Execution	Rundll32
T1060	Persistence	Registry Run Keys / Startup Folder
T1055	Defense Evasion, Privilege Escalation	Process Injection

Fareit Trojan

Beginning in February, McAfee observed another campaign leveraging phishing emails referencing the terms “COVID-19” and “Coronavirus” to entice users to

click on links or attachments that then downloaded the information-stealing Fareit Trojan onto their computers.



Follow   

Share 

IOCs

Type	IOC	Comment
Sha256	2faf0ef9901b80a05ed77fc20b55e89dc0e1a23ae86dc19966881a00704e5846	Attachment
Sha256	38a511b9224705bfea131c1f77b3bb233478e2a1d9bd3bf99a7933dbe11dbe3c	Email

MITRE ATT&CK™ MATRIX

Technique ID	Technique	Technique details
T1193	Initial Access	Spear phishing Attachment
T1106	Execution	Execution through API
T1130	Defense Evasion	Install Root Certificate
T1081	Credential Access	Credentials in Files
T1012	Discovery	Query Registry
T1071	C & C	Standard Application Layer Protocol

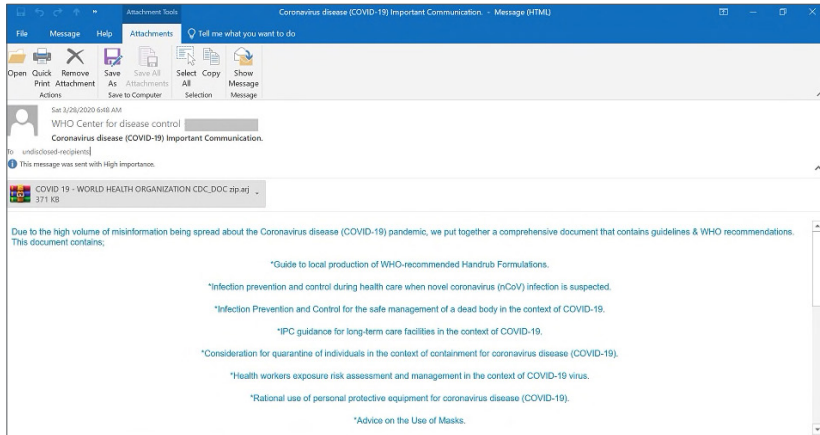
Follow



Share



## Fareit Spam 4



## IOCs

Type	IOC	Comment
Sha256	f8e041bed93783bbd5966bfba6273fe7183464035ea54fe1d59ff85a679b3e3e	Dropped Binary
Sha256	9e17f5e70c30ead347b68841fa137015d713269add98f0257fb30cc6afdea4fe	Attachment
Sha256	ada05f3f0a00dd2acac91e24eb46a1e719fb08838145d9ae7209b5b7bba52c67	Email

## MITRE ATT&CK™ MATRIX

Technique ID	Technique	Technique details
T1193	Initial Access	Spear phishing Attachment
T1204	Execution	User Execution
T1071	Command and Control	Standard Application layer Protocol

Follow



Share



## Emotet Trojan

By late March, McAfee had detected COVID-19-themed phishing campaigns using a strain of the Emotet Trojan to infect users' systems. One version of this email promises to provide information on Coronavirus antibody research and new treatments for the disease. Once established on the victim's system, Emotet can do a number of things on the system but it is almost always programmed to propagate itself by sending large numbers of spam emails to other user's systems.

We observed the following email being distributed which translated to English is:

### Subject:

Break !!! COVID-19 solution announced by WHO at the end How a total control method is discovered

### Email Body:

As published in the newsletter of the World Health Organization 3/17/2020 7:40:21 a.m. A new collaborative study identified and studied antibodies to the COVID-19 virus which could be used to design effective universal therapies against many different species of COVID-19 viruses. The results have recently been published in Nature Microbiology.

These are based on natural activities and how heat helped inhibit the virus from growing.

The COVID-19 virus causes a serious disease with high mortality badgers in humans. Several strategies have been developed to treat COVID-19 virus infection, including ZMapp, which has proven effective in non-human primates and has been used below compassionate treatment protocols in humans ...

Please download the full text in the attached document ...

Also share with all contacts to ensure quick epidermal control.

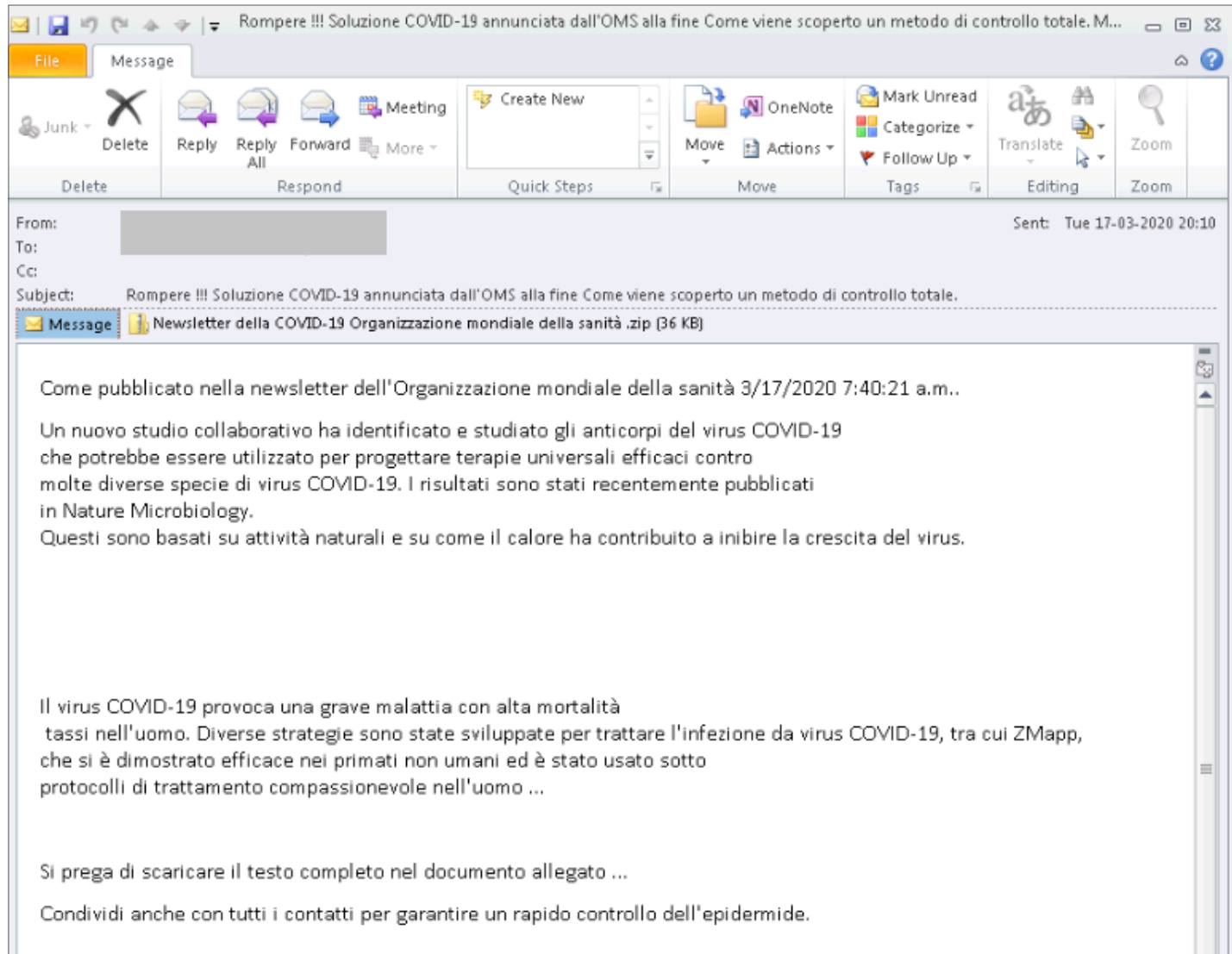
---

Follow



Share





Follow



Share



The email contains a zipped Emotet executable which once executed will use the process hollowing technique to inject into regasm.exe. It will then contact its C&C server and being to send spam email out.

IOCs

Type	IOC	Comment
Sha256	ca70837758e2d70a91fae20396dfd80f93597d4e606758a02642ac784324eee6	Attachment
Sha256	702feb680c17b00111c037191f51b9dad1b55db006d9337e883ca48a839e8775	Email

MITRE ATT&CK™ MATRIX

Technique ID	Tactic	Technique details
T1121	Defense Evasion, Execution	Regsvcs/Regasm
T1093	Defense Evasion	Process Hollowing

Follow   

Share 



### Azorult

Azorult is a malware mostly used to obtain usernames, passwords, cryptocurrencies, browsing history, and cookies. These lists are sold in the underground and bought by ransomware affiliates to break into companies. McAfee ATR has observed cases in which Azorult infections have advanced to a ransomware outbreak in a matter of hours to a few days. What sets Azorult apart from the other malware described in this report, is that the creators of Azorult created a fake Coronavirus infection map website (corona-virus-map[.]com). The fake website appears as below:

#### IOCs

Type	IOC	Comment
Sha256	c40a712cf1eec59efac42daada5d79c7c3a1e8ed5fbb9315bfb26b58c79bb7a2	Jar file from domain
URL	H**p://corona-virus-map.net/map.jar	
Sha256	63fcf6b19ac3a6a232075f65b4b58d69cfd4e7f396f573d4da46aaf210f82564	Dropped Binary

#### MITRE ATT&CK™ MATRIX

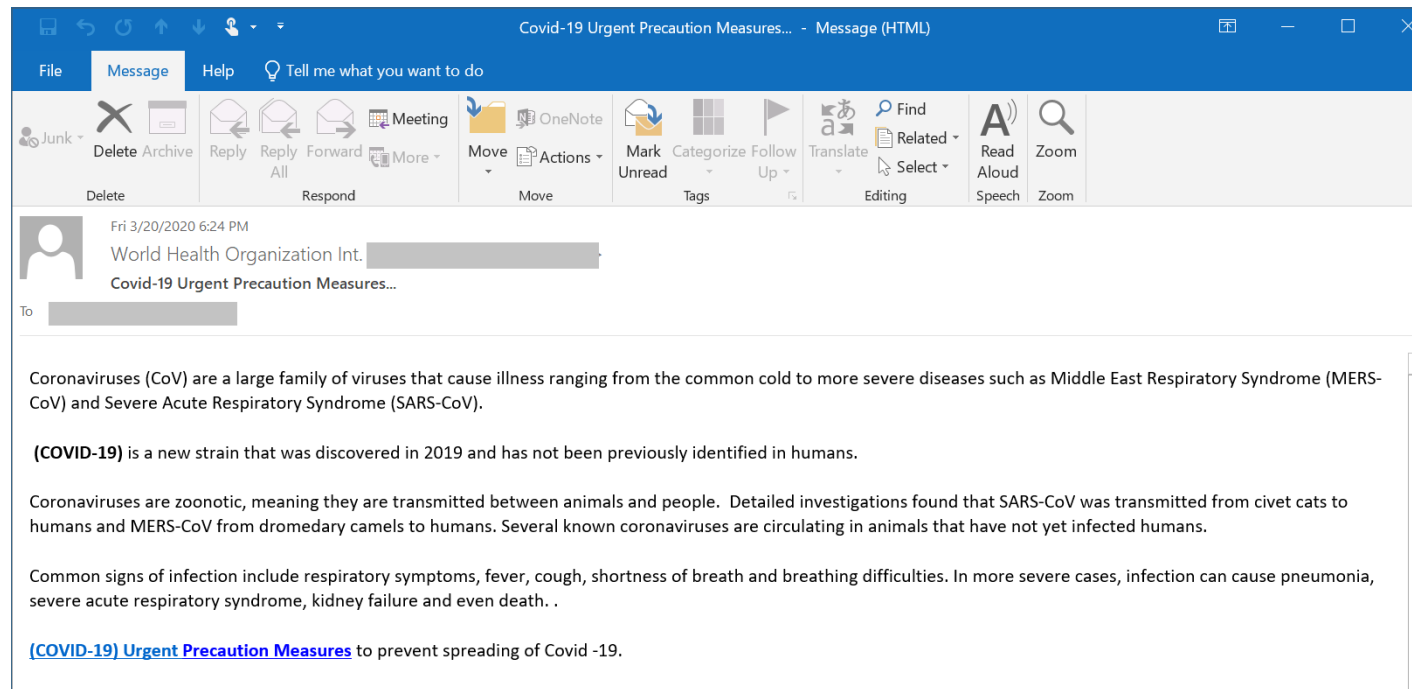
Technique ID	Technique	Technique details
T1059	Execution	Command-Line Interface
T1012	Discovery	Query Registry

Follow   

Share 

### Nanocore RAT

NanoCore is a Remote Access Trojan (RAT) and its highly customizable plugins allows attackers to tailor its functionality to their needs. This RAT is also found to be using COVID-19 to distribute itself by using email subjects such as "Covid-19 Urgent Precaution Measures."



Follow   

Share 

IOCs

Type	IOC	Comment
Sha256	ca93f60e6d39a91381b26c1dd4d81b7e352aa3712a965a15f0d5eddb565a4730	Dropped Binary
Sha256	89b2324756b04df27036c59d7aaaeef384c5bfc98ec7141ce01a1309129cdf9f	Iso Attachment
Sha256	4b523168b86eafe41acf65834c1287677e15fd04f77fea3d0b662183ecee8fd0	Email

MITRE ATT&CK™ MATRIX

Technique ID	Technique	Technique details
T1193	Initial Access	Spear phishing Attachment
T1053	Execution	Scheduled Task
T1060	Persistence	Registry Run Keys / Startup Folder
T1143	Defense Evasion	Hidden Window
T1036	Defense Evasion	Masquerading
T1497	Defense Evasion	Virtualization/Sandbox Evasion
T1012	Discovery	Query Registry
T1124	Discovery	System Time Discovery
T1065	Command and Control	Uncommonly Used Port

---

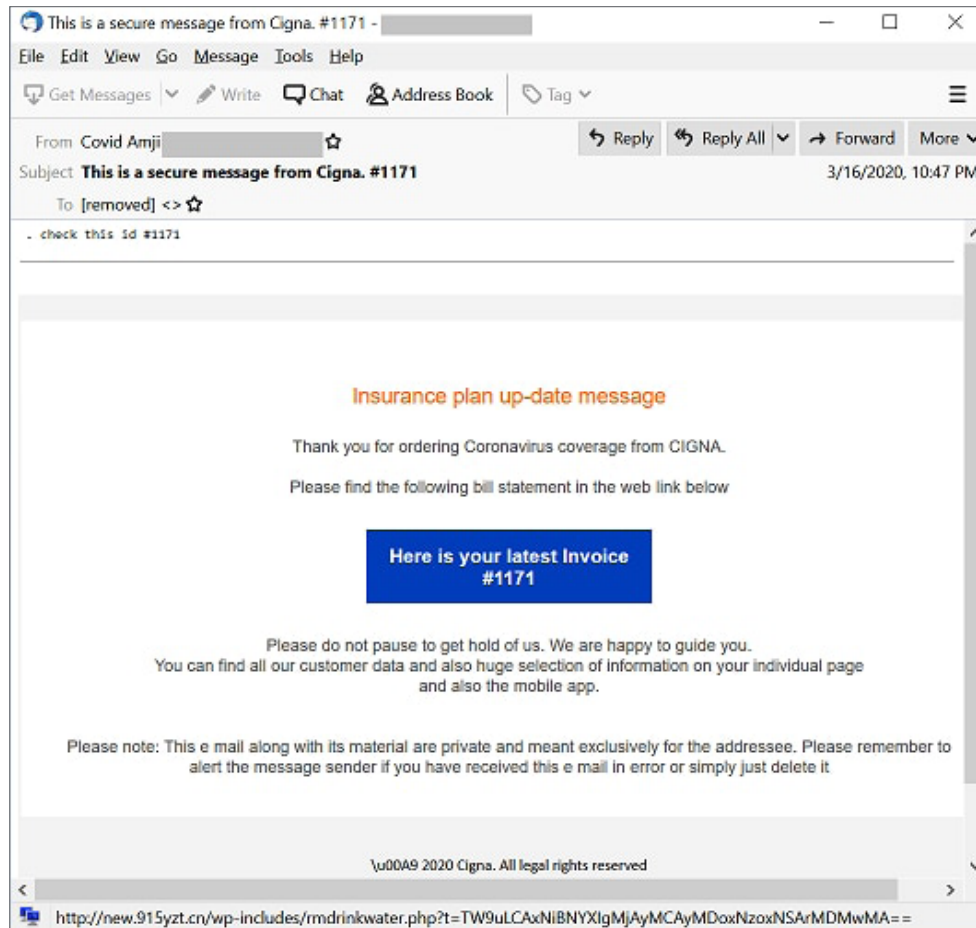
Follow   

Share 

### Hancitor Trojan

Hancitor trojan has also used COVID-19 themes to spread itself by posing as an email from an insurance company. The email contains a link to download a fake invoice which downloads a VBS file.

On executing the VBS, the Hancitor dll temp\_ adobe\_123452643.txt is created in the %AppData/Local/Temp folder. The DLL is executed using the Regsvr32.exe and then begins to communicate with its C&C.



Follow



Share



IOCs

Type	IOC	Comment
Sha256	2f87dd075fc12c2b6b15a1eb5ca209ba056bb6aa2feaf3518163192a17a7a3	Downloaded Binary
Sha256	0caef2718bc7130314b7f08559beba53ccf00e5ee5aba49523fb83e1d6a2a347	Downloaded Binary
Sha256	375d196227d62a95f82cf9c20657449ebea1b512d4cb19cdf9eb8f102dd9fa	Downloaded Binary
Sha256	0b8800734669aa7dbc6e67f93e268d827b5e67d4f30e33734169ddc93a026	Downloaded Binary
Sha256	9c40426f157a4b684047a428428f882618d07dc5154cf1bf89da5875a00d69c	Email

MITRE ATT&CK™ MATRIX

Technique ID	Technique	Technique details
T1192	Initial Access	Spear phishing Link
T1064	Execution	Scripting
T1117	Execution	Regsvr32
T1071	Command and Control	Standard Application layer Protocol

---

Follow   

---

Share 

## Ransomware

Ransomware campaigns made headlines across a variety of sectors in 2019. Ransomware-as-a-Service attackers trained their sights on municipal, healthcare, financial, and corporate targets. McAfee ATR researchers observed and analyzed significant ransomware campaigns such as [Sodinokibi \(aka REvil\)](#) that preceded COVID-19 making its way around the globe.

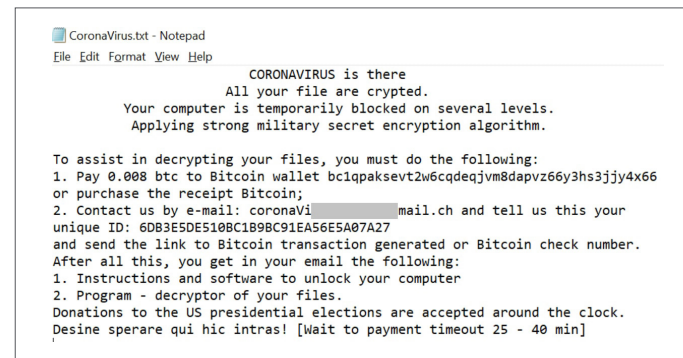
Security engineers, IT, and analysts were already challenged to protect and respond to ransomware threats before the need for a remote workforce raised the challenge to new heights. How do you ensure an equivalent level of adaptable malware protection on or off the corporate network?

As remote workers and IT engineers increasingly use Remote Desktop Protocol (RDP) to access internal resources, attackers are finding more weaknesses to exploit. These vulnerabilities include exploiting authentication or security controls and even resorting to buying RDP passwords in the underground markets. Exploiting these weaknesses can give an attacker admin access and an easy path to install ransomware or other types of malware, then find their way around the corporate network.

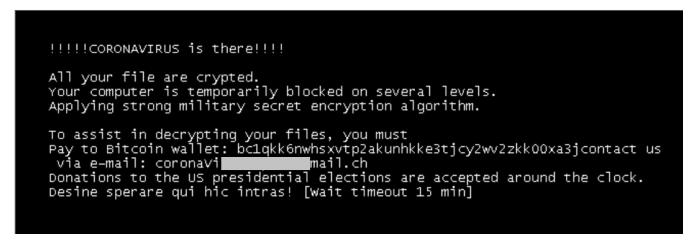
## Ransomware-GVZ

Ransomware-GVZ, a Coronavirus-themed ransomware campaign, emerged in March. Ransomware-GVZ displays a “ransom note” message demanding payment in return for decrypting their systems and the precious personal and corporate data they contain. Upon execution,

Ransomware-GVZ deletes shadow copies with vssadmin and proceed to encrypt all non-pe file types. Once a folder has been totally encrypted, the ransom note file below is created:



Ransomware-GVZ also created a lock screen component displaying the following message when a reboot is attempted:



Follow



Share



IOCs

Type	IOC	Comment
Sha256	3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3	Binary

MITRE ATT&CK™ MATRIX

Technique ID	Tactic	Technique details
T1486	Impact	Data Encrypted for Impact
T1083	Discovery	File and Directory Discovery
T1490	Impact	Inhibit System Recovery

Follow



Share



## Spams and Scams

### Mobile Threats

In March 2020 alone, McAfee Labs identified several malicious Android applications abusing keywords connected to the pandemic. The apps range from ransomware samples to spy-agents that spy on the victim's device. For example, while statically analyzing an app called "Corona Safety Mask," we observed that the amount of permissions was suspicious:



- Full Internet access that allows the app to create network sockets
- Read contact data from the victim's device
- Send SMS messages

When the user downloads the app, it can order a facemask from the following site: "*coronasafetymask.tk*." The SMS send permission is abused to send the scam to the victim's contact list.

Although attribution will clearly be a key concern it is not the primary focus of our research, however, APT groups appear to be incorporating the COVID-19 theme into their campaigns. For example, spreading documents that discuss the pandemic and are weaponized with malicious macro-code to download malware to the victim's system.

### Bogus SBA Loan Emails

Beginning in late March, a phishing campaign used emails claiming to originate from the U.S. Government Small Business Administration (SBA). These emails appeared to offer small businesses information and guidance on how to apply for SBA loans. In fact, they were a mechanism for infecting unsuspecting small business owners with the information-stealing **Remcos Remote Access Tool (RAT)**.

### Scam COVID-19 Tests

In March, cybercriminals distributed phishing emails appearing to originate from organizations offering COVID-19 testing. Users were prompted to open an attached document, which would then download the information stealing **Trickbot malware**.

### Scam COVID-19 Precautionary Measures

April saw the emergence of phishing email campaigns using subject lines such as "COVID-19 Urgent Precaution Measures" to distribute the **NanoCore Remote Access Tool (RAT)** for exfiltration of valuable information.

---

Follow



Share





### Underground Marketplaces

We have seen many examples of major events being abused by people whose interest is only financial gain and current global events are no exception. We conducted a short survey on some underground markets and Telegram channels offering protective masks and more. Two examples are shown below:

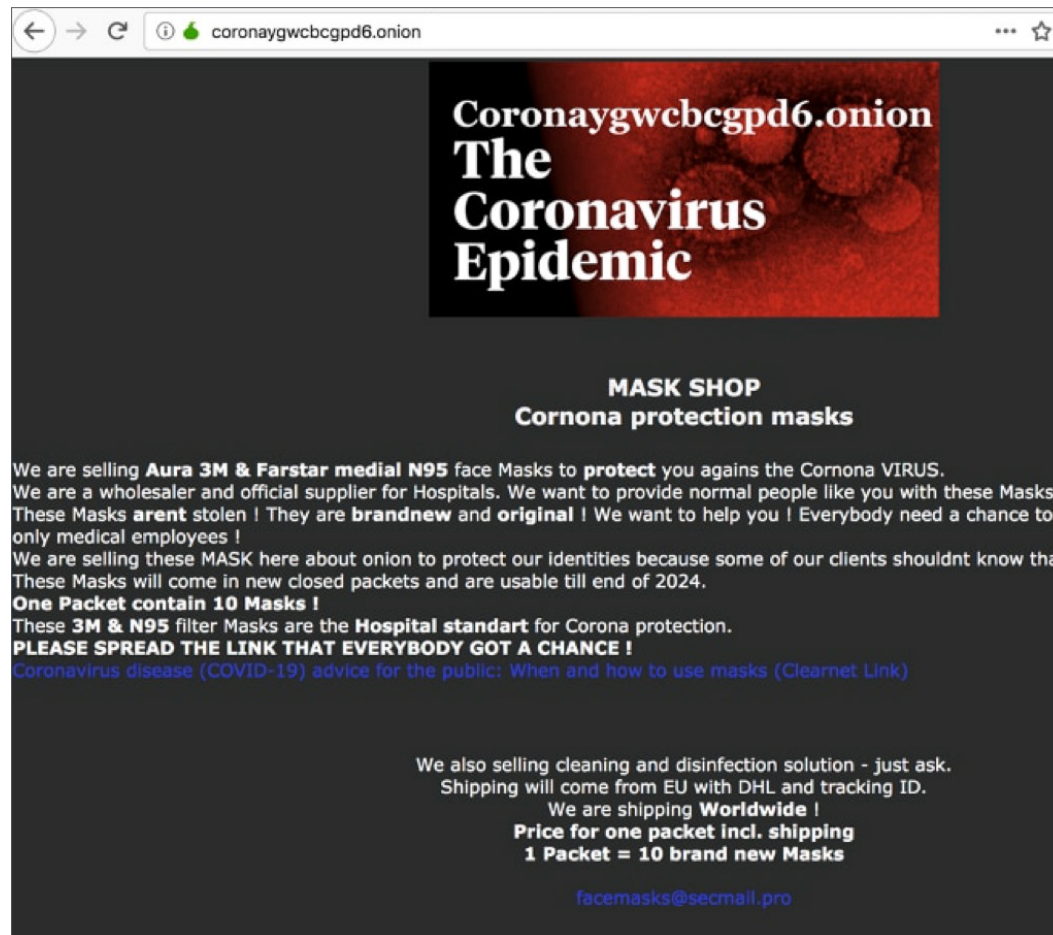


Figure 9. Onion-site offering masks

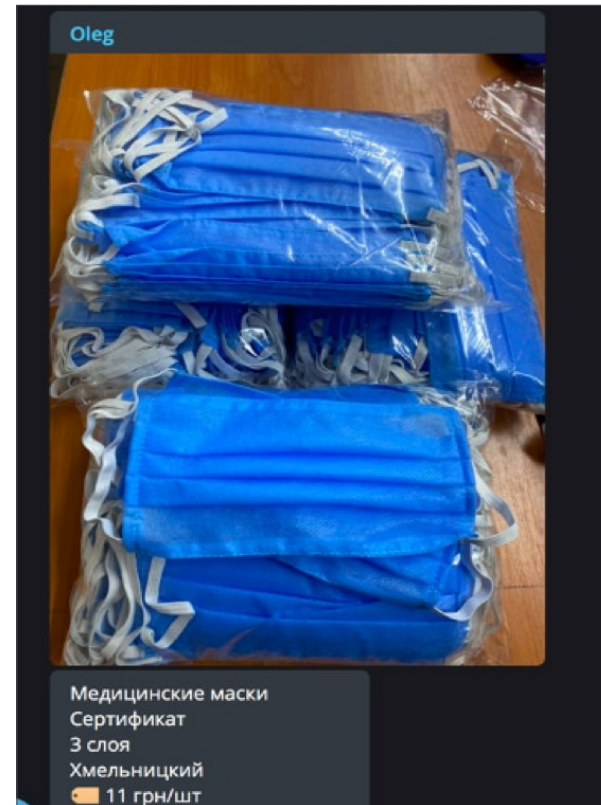


Figure 10. Telegram channel with multiple sellers of masks

Follow   

Share 

### Fake Johns Hopkins Infection Map

In April, cybercriminals used phishing emails to promote a fake website featuring a global Coronavirus infection map appearing to provide data from Johns Hopkins CSSE. Unfortunately, those same emails were used to infect inquisitive users with a strain of information stealing **Azorult malware**.



Figure 11. Fake Johns Hopkins Infection Map

### Bogus Insurance Invoices

In mid-April, cybercriminals used COVID-19-themed emails from a bogus insurance company to infect users' systems with fake invoice attachments carrying the Hancitor malware.

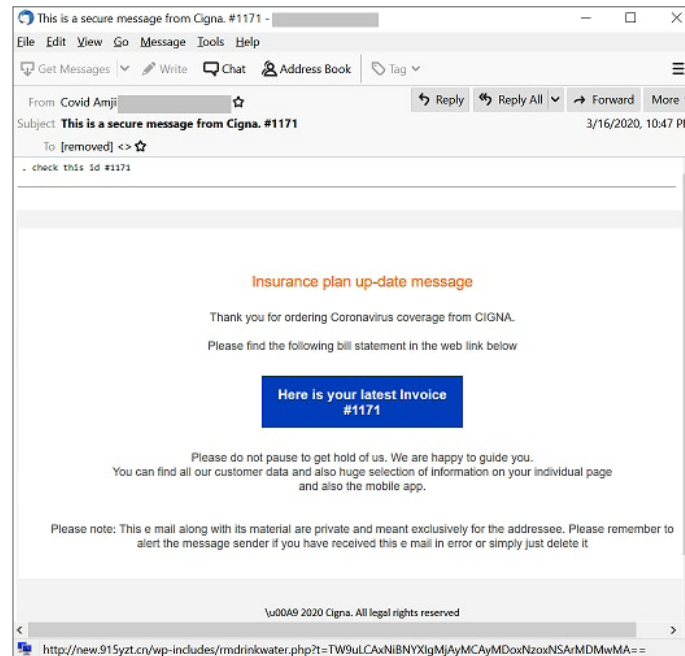


Figure 12. Fake insurance invoice

Follow



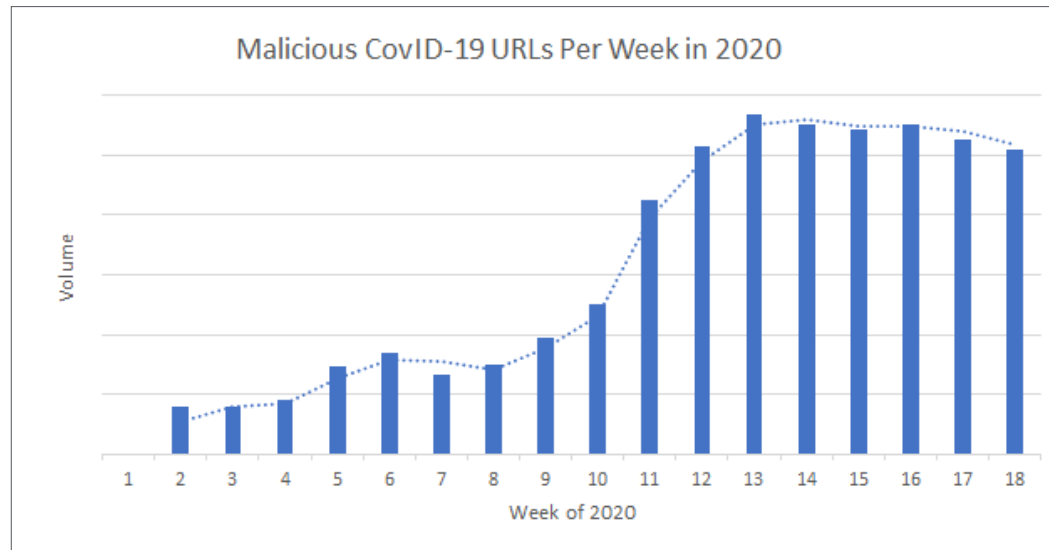
Share



### URL Scams

McAfee has detected thousands of COVID-19-themed spam emails and websites scamming victims seeking to purchase medical supplies such as testing kits, face masks, and other protective gear. Over the first 13 weeks of the pandemic, McAfee saw the number of bogus websites increase from 1,600 to more than 39,000 in just a few weeks.

We have observed the number of Malicious URLs with references to COVID-19 and Coronavirus spike in the last few weeks. The numbers increased from 1,600 a few weeks ago to over 39,000 in week 13. This highlights the importance of being vigilant when clicking on links and accessing websites as the number of malicious sites is increasing exponentially.



Follow



Share



Here are examples of malicious websites we have. False advertising is a common practice during such pandemics. At the time of this writing, there aren't any quick testing kits available. Also testing is initiated by health care providers and therefore it is important to educate yourself and others around you to not buy into scams.

The following is an example of a fake website which offers coronavirus testing services:



Face masks have been in high demand and in many places have run out. Additionally, there has been a shortage of masks even with the health care community. At times of panic and shortage, it is common for spammers to send out links to fake sites claiming to have medical supplies equipment. Here is a screenshot of fake online shop selling face masks:



Follow



Share



**COVID-19**


 [rucorgza@caravanholidays.cz](mailto:rucorgza@caravanholidays.cz)  
To 

Hi, neighbor.  
Tests confirmed that I was sick with a coronavirus.  
Doctors said that in the week I will leave the world.  
My parents will be left without my support.  
And at this time you will live enjoying.  
I think this is unfair, and I suggest you pay me.  
What I am sitting at home and don't try to infect your home.  
Life or money.  
Hurry up! Every hour, I hate you more and more.


My bitcoin address (BTC Wallet) 18P3S6DuNUpW2WLozsrrW6rRd6xh24Rc7N

CPM STRATEGIES FOR CORONAVIRUS (COVID-19)


All | Advertising | Donate | Emergency Prep Kit | Gift Cards | Gloves | Hand Sanitizer | Prevention Masks






20 Value Pack - 3M N95 8210 Prevention Masks  
\$40.00



3M Particulate Respirator 8210V, N95 Single Prevention Coronavirus Adult Mask  
\$5.00



3M N95 Single Prevention Coronavirus Adult Mask  
\$5.00



Read about an example of one McAfee researcher is giving back by [3D printing masks and shields](#).

Follow



Share



IOCs

Below is a partial list of IOCs we have observed in the field which have taken advantage of the Covid-19 outbreak. The IOCs in this section are a subset of those

detected by McAfee's solutions. We have broader coverage provided by our GTI Cloud, gateway, ATP and other products in our portfolio.

Type	Value
SHA256	2ec4d4c384fe93bbe24f9a6e2451ba7f9c179ff8d18494c35ed1e92fe129e7fa
SHA256	7e52f7a7645ea5495196d482f7630e5b3cd277576d0faf1447d130224f937b05
SHA256	69724a9bd8033bd16647bc9aea41d5fe9fb7f7a83c5d6fbfb439d21b7b9f53f6
SHA256	f92fecc6e4656652d66d1e63f29de8bfc09ea6537cf2c4dd01579dc909ba0113
SHA256	a5ab358d5ab14b81df2d37aedf52716b5020ab45da472dedc8b8330d129d70bf
SHA256	8028f988c145b98ddd4663d3b5ec00435327026a8533924f7b8320c32737acf4
SHA256	aab93bf5bb0e89a96f93a5340808a7fa2cebf4756bd45d4ff5d1e6c8bdccf75d
SHA256	2e93fe77fafd705e6ca2f61f24e24a224af2490e0a3640ed53a17ea4bf993ec8
SHA256	f850f746f1a5f52d3de1cbbc510b578899fc8f9db17df7b30e1f9967beb0cf71
SHA256	dd78b0ecc659c4a8baf4ea81e676b1175f609f8a7bba7b2d09b69d1843c182cb
SHA256	e352c07b12ef694b97a4a8dbef754fc38e9a528d581b9c37eabe43f384a8a519
SHA256	e82d49c11057f5c222a440f05daf9a53e860455dc01b141e072de525c2c74fb3
SHA256	8bcd1fbc8cee1058ccb5510df49b268dbfce541cfc4c83e135b41e7dd150e8d

See the full list on [the blog](#).

---

Follow   

---

Share 

## Recommendations

Cybercriminals will always seek to create ever more sophisticated and opportunistic attacks. Remote work paradigms create new opportunities and require new defense mechanisms and practices. This week's report illustrates the importance of maintaining strong cybersecurity defenses regardless of whether employees are in traditional office or home-office environments. We must formulate the right combination of technology and education to make that happen.

Organizations need to defend against cyber-threats at home with data protection solutions capable of preventing intellectual property and other forms of sensitive data from being stolen. McAfee is focused on helping address these challenges with its Unified Cloud Edge and CASB solutions that are inherently focused on protecting both mobile and traditional devices from threats and data theft. Additionally, modern endpoint and EDR capabilities are capable of detecting a wide range of threats that place the user and their organization at risk.

The future is uncertain, change and disruption are inevitable, and our adversaries are determined in their drive to exploit us at work, no matter where that may be. We must rise to the challenge of pushing technology forward, adapting, and developing stronger cyber defenses to ensure that the "future of work" is a secure one.

For more information on COVID-19 threats see these McAfee reports and blogs:

### [Cloud Adoption and Risk Report—Work from Home edition](#)

The recent work shift from on-site to home has dramatically changed how we live and work. Threat actors are following the trend by targeting cloud services.

### [ENS 10.7 rolls back the curtain on ransomware](#)

Attackers are taking advantage of the challenges of protecting the work-from-home force by exploring Remote Desktop Protocol (RDP) weaknesses to install ransomware and other types of malware.

### [Cybercriminals actively exploiting RDP to target remote orgs](#)

Enabling employees to work remotely on a global scale has increased the risks of exposing the RDP protocol and the associated misconfigurations to malware and other criminal activities.

### [COVID-19 threats now include Blood for Sale](#)

COVID-19 has revealed a multitude of vectors for sale on dark web forums.

In the meantime, we will continue to disseminate relevant threat information. To be kept up-to-date as we publish more content, stay connected to the [McAfee Labs Twitter feed](#).

---

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](http://www.mcafee.com)

1. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/>
2. <https://azure.microsoft.com/en-us/blog/update-2-on-microsoft-cloud-services-continuity/>
3. [https://www.researchgate.net/publication/308775653\\_The\\_Current\\_State\\_of\\_Cybercrime\\_in\\_Thailand\\_Legal\\_Technological\\_and\\_Economic\\_Barriers\\_to\\_Effective\\_Law\\_Enforcement](https://www.researchgate.net/publication/308775653_The_Current_State_of_Cybercrime_in_Thailand_Legal_Technological_and_Economic_Barriers_to_Effective_Law_Enforcement)
4. [https://www.researchgate.net/publication/308775653\\_The\\_Current\\_State\\_of\\_Cybercrime\\_in\\_Thailand\\_Legal\\_Technological\\_and\\_Economic\\_Barriers\\_to\\_Effective\\_Law\\_Enforcement](https://www.researchgate.net/publication/308775653_The_Current_State_of_Cybercrime_in_Thailand_Legal_Technological_and_Economic_Barriers_to_Effective_Law_Enforcement)

## 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>



2821 Mission College Blvd.  
Santa Clara, CA 95054  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2020 McAfee, LLC. 4517\_0720  
JULY 2020