# BRAINTRACE

## THREAT ADVISORY REPORT

**APRIL 15, 2021**

braintrace™
INTELLIGENT CYBERSECURITY

braintrace™
INTELLIGENT CYBERSECURITY

## TABLE OF CONTENTS

## BACKGROUND

This report was created to update our clients on up-and-coming vulnerabilities and exploits that our security experts have discovered. Our team works diligently on researching threats and vulnerabilities to provide you with a safer network. If you have any questions, do not hesitate to contact us.

## VULNERABILITIES PATCHED IN NETTLE'S SIGNATURE VERIFICATION

Nettle is a low-level cryptographic library written in C that is used in several contexts regarding application interfaces. Nettle can be directly from a program written in C or employed through an object-oriented wrapper to accommodate other languages and applications.

### Affected Systems

- Systems with Nettle Versions before 3.7.2 in use

### Vulnerability Overview

A vulnerability in Nettle versions before 3.7.2 involves several of Nettle's functions used for signature verification cause the ECC (Elliptic Curve Cryptography) point multiply function to be called with values that are out of range, providing incorrect results. These functions include ECDSA, EDDSA, DSA, and GOST.

A malicious party could force an invalid signature to achieve validation or assertion failure resulting in the ruin of a system's CIA (confidentiality, integrity, and availability).

### Recommendation

Patch older versions of Nettle.

### Reference

https://bugzilla.redhat.com/show_bug.cgi?id=1942533

## APPLE MAIL ZERO-CLICK VULNERABILITY

A recent discovery of a zero-click vulnerability in Apple's macOS Mail could lead to a cyber-attacker executing arbitrary code inside the mail program's sandbox. According to Mikko Kenttälä, CEO of SensorFu, this could lead to a range of attacks, from information disclosure, credential changes and theft, and worm-like activity.

### Affected Systems

- macOS Mail

### Vulnerability Overview

The issue was recently patched in macOS 10.14.6, 10.13.6, and 10.15.5. That said, the issue has to do with Apple Mail uncompressing files that another user of the program has compressed. It is possible to

exploit a configuration problem with how ZIP files are processed. In some cases, this leads to data not being removed from a temporary directory. This could allow attackers to pivot and move further within the environment.

### Recommendation

Apple has already provided patches for this issue. As such, it is recommended to verify your systems and apps are up to date.

### Reference

https://threatpost.com/apple-mail-zero-click-security-vulnerability/165238/

## FAKE NETFLIX APP CALLED FLIXONLINE LURING ANDROID USERS THROUGH WHATSAPP MESSAGES

Researchers from Check Point have reported to Google about the new Android malware using Netflix as bait and spreading by auto-reply mechanism to received WhatsApp messages. Google removed this application named FlixOnline from Google Play, but the methodology used is expected to be used again in future cyber-attacks.

A new wormable malware functioning as a malicious credential and data harvester is spreading among Android devices via WhatsUp messages. It is disguised as an application named "FlixOnline" with a promising advertisement strategy of "2 Months of Netflix Premium Free Anywhere in the World for 60 Days". However, it begins harvesting your data and credentials when downloaded to your phone. It monitors WhatsUp notifications and replies back using the message received from the command-and-control (C2) center.

The malicious application stayed on Google Play for two months and spread around 500 victims. Even though this is not a high number, nobody knows whether or to what extent this malware has spread among the victims. Google took down the application after being informed by Check Point, which discovered this malware.

The official Android App store is known to have hosted some other malicious apps before. For example, nine malicious applications used for financial data harvesting purposes from android phones were detected in March 2021.

### Affected Systems

- Android Phones

### Vulnerability Overview

FlixOnline lured the victims with the tagline of "2 Months of Netflix Premium Free at no cost For REASON OF QUARANTINE (CORONA VIRUS)* Get 2 Months of Netflix Premium Free anywhere in the world for 60 days. Get it now HERE [malicious domain redacted]." which utilized two different social engineering factors: free services and the current pandemic. FlixOnline then requested the following three permissions after being installed on the victim's device:

- Overlay permission: Used for creating fake login screens for credential harvesting,
- Battery Optimization Ignore permission: preventing the malicious software from being shut down at long idle time ranges,
- Notification permission: Providing the right to retrieve and automatically dismiss or reply to the notification messages.

### Indicators of Compromise

**SHA256:** 1d09743692 7f85b1ab9bf69913071abd0845bfcf1afa186112e91e1ca22e32df

**SHA 1:** bec2c0448558729c1edf4e45ab76b6a3ee6e42b7

**Domain:** netflixwatch.site

### Recommendation

According to the researchers from Check Point, end-users should be highly cautious about the attached files and downloading links received through WhatsUp or other messaging apps, even if they come from trusted friends or messaging groups. If you detect this malicious app in your android, you should remove the application from your phone as soon as possible and change all your credentials.

### Reference

https://threatpost.com/netflix-app-google-play-malware-whatsapp/165288/

## CHARMING KITTEN APT GROUP TARGETING MEDICAL RESEARCHERS

Late last year, we wrote about an APT group based out of Iran called Charming Kitten. Recently, security researchers indicated the kitten had claws. The group appears to be part of a campaign called Bad Blood due to a history of geopolitical tensions involved therein.

### Affected Systems

- All Systems

### Vulnerability Overview

A group of researchers from Proofpoint recently posted about a campaign being conducted by the group in question. The group, which is suspected to be based in Iran, targets medical researchers to steal authentication credentials. The group is alleged to be aligned with various parts of Iran's military.

This recent campaign appears to be part of a slight departure from the group's previous activities. In this case, the group seemed to be sending phishing emails posed as being from a prominent physicist from Israel. Utilizing social engineering techniques, the group piques the target's interest and has them click on a link. This leads to a website spoofing Microsoft's OneDrive service. Opening it leads to the landing page where the victim is intended to enter their credentials. Once the victim's credentials are entered, they are forwarded to a benign site with a document titled "Nuclear weapons at a glance: Israel."

### Recommendation

As most APT campaigns utilize social engineering techniques, such as phishing or whaling, it is imperative that training be conducted on these matters to obtain their directives. Further, email filtering and monitoring are good supplemental defenses against these forms of attacks.

### Reference

https://threatpost.com/charming-kitten-pounces-on-researchers/165129/

## GIGASET ANDROID UPDATE SERVER HACKED TO INSTALL MALWARE ON USERS' DEVICES

Gigaset has revealed a malware infection that was discovered in some of its Android devices. This infection comes from a compromise of a server belonging to an external updated service provider. This malware took the shape of different unwanted apps that were automatically downloaded and installed thru a pre-installed system update app.

### Affected Systems

- This impacts older smartphone models GS100, GS160, GS170, GS180, GS270 (plus), and GS370 (plus) series.

### Vulnerability Overview

The infections of the multiple devices have begun around March 27th of this year, and steps to alert the service provider of the issue prevent further infections on April 7th. There are multiple apps that that were installed on the devices that were mentioned in the affected systems section. The apps installed on the devices include GEM, Smart, Xiaoan, asenf, Tayase, com.yhn4621.ujm0317, com.wagd.smarter, and com.wagd.xiaoan. Gigaset has urged users to check for signs of any infections by going to their Settings app and Manually uninstall the apps in question, in addition to the Recommendation below.

### Recommendation

It is recommended that systems have the most updated anti-malware and antivirus protection running on their systems. It has also been suggested that users have the devices connected to the internet while connected to the charging cable. From there, the device will automatically be released after 8 hours of the malware.

### Reference

https://thehackernews.com/2021/04/gigaset-android-update-server-hacked-to.html

## 'MORE_EGGS' MALWARE TARGETS PROFESSIONALS WITH LINKEDIN JOB OFFERS

More_eggs is malware written in JScript, which is used in campaigns that offer fake jobs. Hackers are targeting different US companies. All of them shared one thing in common. They all had some type of online shopping portal. Malicious actors usually contact the victim through LinkedIn messaging service. Hackers will generate follow-up emails that will contain job offers and malicious links with a fake website. Once a victim clicks on the link, it will receive more_eggs backdoor. More_eggs uses Windows processes which makes it hard to detect with antiviruses. Researchers still have not discovered who is behind this campaign, but they say that these activities were noticed earlier with Evilnum, FIN6, and Cobalt Group.

### Affected Systems

- LinkedIn

### Vulnerability Overview

Once the recipient of the malicious email clicks on the infected file or link, it is allowing backdoor Trojan inside their system. This backdoor is enabling remote access over the victim's device. Once they are in, they can sell backdoor as MaaS to the other hackers on Dark Web or use its privilege to install different ransomware and steal data. Indicators of compromise were taken from https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/.

### Indicators of Compromise

**Domain:**

- interrafcu[.]com
- usstaffing[.]services
- usastaffing[.]services
- usstaffing[.]services
- jobhyper[.]com
- api[.]cloudservers[.]kz
- mail[.]rediffmail[.]kz
- secure[.]cloudserv[.]ink
- metric[.]onlinefonts[.]kz
- news[.]bradpitt[.]kz

**SHA256:**

- edb39c4eb28cf526f1e606365cdef009cb9aa8ba99feb448db615326bf495042
- d39cb07e97fd91e75c51f75ccef1a8d7ce8ec8c951943501f981ce98d6319e01
- 2bca33c8be6483aec5cbb29d18c5f626a86205fca92191468b8b1032d38aebea
- 2470ac1632546ecf5c9c9d93c6dc088253ba682ba9cf19ae6984b6cee3f8e2b5
- 73defd8066549e5b09c509064bc5bd29e77eca2c18d114c0bcf3dfa1cefe6939
- b3537701e054823836da9c532560d30f01e38e549fb813206afd699ecde8a97c
- 28497c50d65c9f1d0233fc193a43014497fadddb1af8e7f5dbc6eefb3d4ede02
- 80716c2a49739850d8ccd1c035ea4bcc2da39527693c71b800c99ed2ea2c430f
- 37831e465728a913acab317b65c4474b8e6a4570e78c39c8b8c9b956e5d6db25
- d9a245f1fb502606c226c364aa1090f25916e68f5ff24ef75be87ad6a2e6dcc9

- 78a87d540c1758c6b4dcabb7b825ea3a186ef61e7439045ece3ce3205c7e85a2

**Hostname:**

- mail[.]rediffmail[.]kz
- onlinemail[.]kz
- api[.]cloudservers[.]kz
- secure[.]cloudserv[.]ink
- tonsandmillions[.]com
- contactlistsagregator[.]com

**IP Address:**

- 185[.]204[.]2[.]182
- 185[.]162[.]128[.]70
- 185[.]243[.]115[.]50
- 192[.]99[.]20[.]90
- 192[.]187[.]103[.]42
- 37[.]1[.]221[.]212.

### Recommendation

It is recommended to scan for reported indicators of compromise. Education about phishing emails and malicious attachments can mitigate future malicious attacks. It is essential to patch vulnerabilities regularly. If possible, conduct penetration testing.

### Patch URL

https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/

### Reference

https://thehackernews.com/2021/04/hackers-targeting-professionals-with.html

## SONICWALL EMAIL SECURITY VULNERABLE TO MALICIOUS HTTP REQUESTS

SonicWall Email Security is an on-premise protection solution against inbound and outbound email threats. A critical vulnerability has been discovered that allows malicious parties to create administrative accounts by sending malicious HTTP requests to the remote device.

### Affected Systems

- SonicWall Email Security Versions 10.0.9.x and earlier.

### Vulnerability Overview

The vulnerability stems from an unidentified block of code in the HTTP request handler component. The needed input to achieve privilege escalation is also unknown at this time. However, it is known that the attack can be initiated remotely and only requires a single successful authentication for exploitation.

### Recommendation

SonicWall has not released an update, and there are no known countermeasures. It has been suggested to replace the affected products in the meantime.

### Reference

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007

## CONTI RANSOMWARE: EVASIVE BY NATURE AND HOW IT WORKS.

There have been many ransomware attacks in the news today. The most recent comes from a relatively new yet very evasive form named "Conti." Conti is assumed to be the successor of Ryuk with strategic differences. Conti's unique features include updates faster and can quickly encrypt a system with its auto-spreading functionality. They now also threaten to leak the exfiltrated data to get the victims to pay the ransom. This means of the attack shows that no organization, including retail, manufacturing, construction, and the public sector, is protected from these attacks.

### Affected Systems

- Microsoft, Linux, and Apple products

### Vulnerability Overview

The most recent attack from this group of ransomware has been against the Broward County School Systems, with a demand for $40 million to release encrypted data. Conti ransomware is so different compared to the other versions out there already. One of the main differences is that Conti is designed to be activated by hackers who have already compromised a computer system. This can include attacks launched via malicious email attachments or download. This means that the attackers can sit inside the system gathering all the information they need so when the attack begins, they know exactly where to hit in the shortest amount of time. They are also known to exploit vulnerabilities, covered by CVE-2018-13379 and CVE-2018-13374, in the FortiGate firewall version 5.6.3 build. This ransomware is usually delivered at the end of a series of Cobalt Strike and Meterpreter payloads that use reflective DLL injection techniques to push the malware into memory. The reflective loaders delivering the payload into memory do not write the ransomware binary to the infected computer's file system. This way, Conti eliminates the problem the other groups have in that there is no artifact left afterward for analysts to study.

### Recommendation

It is recommended that systems have the most updated anti-malware and antivirus protection running on their systems and have current backups of the systems. It is also recommended that users avoid clicking on unknown or suspicious links within their emails.

### Reference

https://www.bankinfosecurity.com/how-conti-ransomware-works-a-15763

## REVIL RANSOMWARE NOW CHANGES PASSWORD TO AUTO-LOGIN IN SAFE MODE

We have heard about the ransomware called REvil in numerous other articles and headlines. They are headlining again with a recent change that has been made to the ransomware. Back in March, it was reported that there was a Windows safe encryption mode added to the REvil/Sodinokibi ransomware. At the time of the report, it required someone to manually log in to Windows safe mode before encrypting. By the end of March, things have evolved for this ransomware.

### Affected Systems

- Windows

### Vulnerability Overview

A sample of this new version of REvil ransomware was found at the end of March, showing the updated logging in features. The feature refines the Safe Mode encryption by changing the logged-in user's password and configuring the Windows system to automatically login upon reboot. When the -smode is used, the ransomware changes the user's password to "DTrump4ever" (minus the quotes) via a script.

It is not sure that the group will continue to use the same password for the past two days. REvil is continuing, like other groups, to evolve and has stated they will perform DDoS attacks on victims and email partners regarding the stolen data if the ransom continues to not be paid.

### Recommendation

It is recommended that systems have the most updated anti-malware and antivirus protection running on their systems. All systems should have the most updated and patched operating systems running. It is also recommended that users avoid clicking on unknown or suspicious links within their emails. There should also be current/updated backup files stored in case of an attack.

### Reference

https://www.bleepingcomputer.com/news/security/revil-ransomware-now-changes-password-to-auto-login-in-safe-mode/

## NEW VULNERABILITY TARGETS POPULAR WINDOWS TIME SYNCH SOFTWARE

Security researchers have recently uncovered a remote code execution (RCE) vulnerability within the popular software Greyware Domain Time II. This Windows time-keeping tool can be used to ensure accurate time across an entire network via GPS and servers, making it both useful and widespread. Attackers were witnessed utilizing a 'Man-in-the-Middle' technique to hijack the internal process and virtually remain hidden within many essential business services. Greyware is used by corporations ranging from Insurance, Government, Finance, and more.

### Affected Systems

- Windows-Greyware Domain Time II

### Vulnerability Overview

Methods used in this vulnerability focus on tricking an internal user into downloading and executing the attacker-controlled payload by posing as legitimate updates. Additional knowledge has shown that it also performs in a man-on-the-side (MotS) context, thus preventing the hacker(s) from changing any exchanged data between servers. However, there is evidence that they may create their responses and 'race' local traffic to attempt to open a specific URL and initiate the man-in-the-middle (MITM) session. Due to the capability that the attacker may install malware or create backdoors(in addition to the info gained via internal access already possessed), the trend can be increasingly dangerous to corporate settings.

### Recommendation

Mitigating this type of behavior can be difficult from the levels of network-wide correlation that are required. However, implementing proper time sync procedures and good security practices can be manageable instead of impossible to prevent.

### Reference

https://www.scmagazine.com/home/security-news/bug-allows-attackers-to-hijack-windows-time-sync-software-used-to-track-security-incidents/?web_view=true

## RISING TIDE IN FIRMWARE CYBERATTACKS

A new report from Microsoft presents evidence for the rising tide of firmware cyber-attacks. More than 80 percent of the organizations that participated in a Microsoft survey have been attacked at least one firmware-related cyber-attack in 2019 and 2020. Moreover, according to NIST, the number of firmware attacks has increased by around 500% since 2017. The major underlying causes of firmware attacks for being one of the favorites of cybercriminals are:

- It exists just below the operating systems where sensitive data like credentials of cryptographic keys are stored in memory,
- It is out of the monitorization scope of cybersecurity teams,
- It is not visible to antivirus software.

### Affected Systems

- Firmware

### Vulnerability Overview

Organizations are not sensitive enough to firmware cyber-attacks. 82% of the decision-makers participating in the MS survey stated that they did not have enough security work sources since they were too busy with vulnerability management, patching, updating, and upgrading the software and hardware.

### Recommendation

Microsoft notes that to protect your organization from kernel-level attacks, you should prevent attackers from damaging the OS's kernel memory or read it at runtime by providing hardware-based security features such as kernel data protection or memory encryption. The company released a UEFI scanner in Microsoft's Defender ATP to check malware's existence in the firmware file system. Moreover, the Redmond Giant also began using the "Secured-Core" feature in Windows 10 PCs to prevent malware modify or damage the code in motherboards for booting the computer.

### Reference

https://threatpost.com/enterprises-firmware-cyberattacks/165174/
https://www.zdnet.com/article/microsoft-firmware-attacks-are-on-the-rise-and-you-arent-worrying-about-them-enough/

## UNPATCHED VULNERABILITY FOUND IN CISCO ROUTER MANAGEMENT INTERFACE

Cisco Small Business routers' web-based management interface contains a vulnerability that could permit a remote and unauthenticated malicious actor to use arbitrary code execution attacks on affected routers.

### Affected Systems

Cisco Small Business RV Series Routers:

- RV110W Wireless-N VPN Firewall
- RV130 VPN Router
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

### Vulnerability Overview

This vulnerability stems from improperly implemented validation of input supplied by users of the web management interface. The malicious actor could send crafted HTTP requests containing arbitrary executable code capable of acting as the root user to interact with the underlying router operating system.

### Recommendation

Until Cisco releases a patch, go to the web management interface -> Basic Settings -> Remote Management -> Uncheck the remote management box.

### Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm

## CRING RANSOMWARE SEEN TARGETING UNPATCHED FORTINET VPNS

Though this is not a brand-new vulnerability, researchers have spotted Cringe Ransomware targeting Fortinet VPN Servers that do not have CVE-2018-13379 patched. This ransomware gang is known to have attacked many companies in the industrial sector. Swiss researchers in January 2021 first observed this gang. Once this group gains initial access by exploiting the network's vulnerability, they can deploy custom mimikatz files. These mimikatz programs harvest the admins' credentials so that the attackers can deliver the payloads to other target servers with cobalt or PowerShell.

### Affected Systems

- Fortinet VPN Servers

### Vulnerability Overview

CVE-2018-13379 is a vulnerability that involves a failure to limit pathname access to an important folder. Another term to describe the issue is unauthenticated "path traversal." Problems with the web portal allow malicious actors to steal files with customized HTTP requests.

### Recommendation

Update Fortinet VPN Servers as soon as possible.

### Patch URL

https://docs.fortinet.com/document/forticlient/6.4.0/administration-guide/991309/upgrading-forticlient

### Reference

https://www.bleepingcomputer.com/news/security/new-cring-ransomware-hits-unpatched-fortinet-vpn-devices/

## RAGNAROK RANSOMWARE ATTACKS BOGGI MILANO MENSWEAR

A Luxury Italian clothing brand, Boggi Milano, has confirmed being attacked by Ragnarok Ransomware and leaked 40 gigabytes worth of data, including Human resources files and salary information.

### Affected Systems

- Boggi Milano's internal file
- Microsoft Windows operating systems

### Vulnerability Overview

Ransomware attacks are the new digital robbery for swiping business data and demand a ransom from victims to restore access to the information upon payments to get a decryption key.

Bloomberg confirmed the breach when provided access to Boggi Milano's sensitive data. TechNadu also reported using KELA, a monitoring use for the dark web, investigated Boggi Milano's payroll files, invoice PDFs, vouchers, tax documents, and more leaked by Ragnarok ransomware.

Nobody has said how much the ransom was to decrypt Boggi Milano's files. Boggi Milano's official website is still running, and the brand mentioned working with authorities on this issue. Although the company's operation's impact appears minimal, the stolen of 40 gigabytes of data, including employees and customers, could become a significant issue with a substantial number of fines.

### Recommendation

Practice good cyber hygiene: Secure endpoints, two-factor authentication, backup planning strategy, and implement employee security training.

### Reference

https://threatpost.com/ragnarok-ransomware-boggi-milano-menswear/165161/

## CRITICAL ZOOM RCE VULNERABILITY

This year's Pwn2Own contest, hosted by the Zero Day Initiative, led to several new zero-day vulnerabilities being discovered. A new remote code execution (RCE) zero-day in Microsoft Zoom Chat was especially noteworthy of the contest's vulnerabilities. While Microsoft is working on getting this patched, technical details and proof-of-concept PoC exploits have not been made public due to the critical severity.

### Affected Systems

- Microsoft Zoom Chat up to version date 04/09/2021

### Vulnerability Overview

Few details are available on the vulnerability at this time. We know that the attacker needs to be in the same organization or in the victim's contact list to exploit the vulnerability. If these criteria are met, further input from the victim is not required for a successful attack. Thus, it is advised to be cautious and only accepts external contact invitations from trusted parties.

### Recommendation

Apply vendor-provided patches when they become made available.

### Reference

https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/04/zoom-zero-day-discovery-makes-calls-safer-hackers-200000-richer/

## TECH SUPPORT SCAM

A new tech support scam was noticed first time in March. Researchers from Vade Secure published that they have seen a spike in the number of these emails reaches over 200,000 per day. The scammers will try to impersonate companies like Norton LifeLock, Microsoft, and McAfee. They would target victims with emails that would require payments for billing subscriptions in amounts from $350 to $399. Scammers are giving victims the option to cancel the subscription in emails. The requirement for cancellation is to dial customer service on the provided number in the email.

### Affected Systems

- All systems

### Vulnerability Overview

When the victim calls this number, they will be asked which antivirus protection they are using. Victims are manipulated into clicking on the fake 1800support.weebly[.]com site. This is a fake BestBuy Geek Squad website. The scammer will then provide instructions to the victim, step by step, on how to install AnyDesk remote access software on their device. This will allow scammers to take complete control over their computer. Further instruction manipulated people into typing their personal information in the Notepad by suggesting that this information will be used to complete the refund of their money.

### Recommendation

We recommend staying up to date with current scamming trends. It is essential to know that you should not be calling the number provided in the email when they require some type of payment. The best practice is to google the company mentioned and contact the number provided on their official web page.

### Reference

https://www.bleepingcomputer.com/news/security/tech-support-scammers-lure-victims-with-fake-antivirus-billing-emails/
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

## CRITICAL AUTHENTICATION BYPASS BUG FOUND IN SECURITY PRODUCT INSIDE VMWARE DATA CENTER

A new critical authentication vulnerability discovered in VMware Carbon Black Cloud Workload product could be exploited and circumvent authentication and take control of the systems. It is tracked as CVE-2021-21982 and affects all product versions before 1.0.1. Carbon Black Cloud Workload is a VMware security product data center that protects crucial servers and workloads hosted on vSphere.

### Affected Systems

- VMware Carbon Black Cloud Workload appliance.

### Vulnerability Overview

The authentication bypass vulnerability in the VMware Carbon Black Cloud workload appliance allows a bad actor who has network access to enter the VMware Carbon Black Could Workload appliance's administrative interface and gain a valid authentication token. After exploiting the systems, the attacker could view and change administrative configuration settings.

VMware also disclosed two other bugs in the vRealize Operations Manager solution that a bad actor could exploit through network accessing the API and execute Server-Side Request Forgery (SSRF) to steal admin credentials, CVE-2021-21975, and execute files to arbitrary locations on the underlying photon operating system, CVE-2021-21983).

### Recommendation

No mitigations were known other than patching any affected systems as soon as it is practical.

### Reference

https://thehackernews.com/2021/04/critical-auth-bypass-bug-found-in.html

## GITHUB ACTIONS EXPLOITED TO MINE CRYPTOCURRENCY

Threat actors are actively attacking GitHub repositories that use GitHub actions to mine cryptocurrency on GitHub servers. Repositories use GitHub Actions to set up CI/CD automated, periodic tasks. These attacks use GitHub Actions code to fork repositories and to create a Pull Request. There also appear to be copycat attacks targeting GitHub Actions. GitHub has released a statement stating that they are currently investigating these attacks.

### Affected Systems

- GitHub

### Vulnerability Overview

The threat actors add malicious code to a legitimate forked repository with GitHub Actions enabled and create a Pull Request from the legitimate repository to merge the code. The malicious code downloads and executes a misnamed crypto miner named npm[.]exe hosted on Git Lab. The attack does not require the maintainer from the original repository to get approved for the malicious code's Pull Request. This triggers GitHub's systems to execute the malicious code on their servers, leading to the crypto miner's loading and execution with the threat actor's crypto wallet address as an argument.

### Recommendation

It is recommended to maintain strong security practices when using GitHub.

### Reference

https://www.bleepingcomputer.com/news/security/github-actions-being-actively-abused-to-mine-cryptocurrency-on-github-servers/

## ANDROID APP STORE APKPURE TROJANS

The Google Play Store and Apple IOS store is an online suite that provides apps vetted by Google and Apple to be downloaded by consumers. It is usually recommended to download apps for your mobile device from these sources, but there are other online sources that you can download apps for your mobile devices. APKPure is an open-source platform that allows android users to download direct files for their Android devices. Recently, hackers have been trying to distribute malware through various apps available through APKPure.

### Affected Systems

- Users that have APKPure version 3.17.18

### Vulnerability Overview

Researchers have shared that APKPure client version 3.17.18 has been possibly affected by hackers and has an SDK advertisement that tricks users into downloading a malicious application embedded with a trojan dropper. The researchers have noted that the SDK was from an unverified source.

Research has stated that the type of Trojan depends on what Android version is installed on the device. Android versions 6 or 7 could be affected with the xHelper Trojan, and Android 8 or higher would install modules for the Triada Trojan, leading to more malware.

### Recommendation

Do not download apps from unofficial sources and update to the latest version of the APKPure app, 3.17.19

### Reference

https://www.kaspersky.com/blog/infected-apkpure/39273/

## THE HAVE I BEEN PWNED PROJECT

The Have I Been Pwned Project collects and analyzes the sensitive information compiled from "data breaches" where cybercriminals may have captured your personal information. A website named haveibeenpwned.com has been established to provide service to the public. Victims, including 553 million Facebook users of the last week's data breach, have the chance to learn about the compromises of their accounts. It is possible to check for your mobile number or email addresses and know if they are involved in any data breaches. Please keep in mind that your data, including highly critical personal information such as first and last names, phone number, gender, occupation, city, country, and marital status, maybe on sale in the darknet market like the other 533 million Facebook accounts as reported by Alon Gal from Under the Breach on Jan. 14, 2021.

### Affected Systems

- All Online Accounts

### Vulnerability Overview

What happens if threat actors know your mobile phone number?

Step 1: In addition to unsolicited calls, the hackers will have a chance to see your social media accounts like Instagram, Twitter, Facebook, and LinkedIn, which rely on that compromised phone number for password resets.

Step 2: A SIM-swapping attack is carried out by tricking or bribing the employees at the mobile phone stores for transferring ownership of the victim's phone number to a mobile device controlled by the criminals.

Step 3: The passwords of any victim accounts linked to that mobile phone number are reset, and MFA-related one-time tokens are captured.

### Recommendation

Remove your phone numbers from your online accounts if possible, and do not opt for SMS or phone calls for MFA (multi-factor authentication purposes). Use unique, complex, and strong passwords for all your online accounts together with the most robust authentication applications like Google Authenticator, which produces one-time tokens, or you may prefer to use even more secure solutions such as physical security keys.

Further, do not let your phone number be present as a backup in your email accounts and online accounts. If it is required while setting up your account, you can remove it later. Finally, check if your phone number and email account have been breached and if so, take all measures to protect yourself.

### Reference

https://krebsonsecurity.com/2021/04/are-you-one-of-the-533m-people-who-got-facebooked/
https://haveibeenpwned.com/About

## MARIADB SYSTEM VARIABLE VULNERABILITY

When surfing the internet, an account can be created on a visited site, and that organization will usually save that account information. Websites will usually have some type of database structure established to hold this information, and a popular database vendor is MariaDB. MariaDB is open-sourced software, and it provides a relational database that allows information to be stored and accessed by related content. And the vulnerability discovered could allow an attacker to perform a remote execution attack.

### Affected Systems

- MariaDB versions 10.2, 10.3, 10.4, and 10.5

### Vulnerability Overview

Two system variables within the software could be modified and taken advantage of and lead an attacker to execute operating system commands after successfully modifying the variables. The wsrep_provider and wsrep_notify_cmd variables can be modified by a superuser at run time within the

database to allow them to be writable, leading to an untrusted search path eval injection, which allows an attacker to execute arbitrary code.

### Recommendation

Upgrade to the latest version MariaDB.

### Reference

https://nvd.nist.gov/vuln/detail/CVE-2021-27928#vulnCurrentDescriptionTitle