



# Monthly Security Bulletin

J A N U A R Y / 2 4

Advanced Security  
Operations Center

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

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

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

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



## Why Advanced Security Operations Center (ASOC) by Telelink?

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

### LITE Plan

**425 EUR/mo**

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

**Get visibility on the cyber threats targeting your company!**

### PROFESSIONAL Plan

**1225 EUR/mo**

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

**Start to mitigate cyber threats and minimize the risk!**

### ADVANCED Plan

**2 575 EUR/mo**

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

**Complete visibility, deep analysis, and cyber threat mitigation!**

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

### What is inside:

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

## Table of Contents

1.	Hackers breach US govt agencies using Adobe ColdFusion exploit .....	4
2.	"Sierra:21" vulnerabilities impact critical infrastructure routers .....	6
3.	US senator: Govts spy on Apple, Google users via mobile notifications .....	10
4.	New SLAM attack steals sensitive data from AMD, future Intel CPUs .....	12
5.	AutoSpill attack steals credentials from Android password managers .....	14
6.	Toyota warns customers of data breach exposing personal, financial info .....	20
7.	50K WordPress sites exposed to RCE attacks by critical bug in backup plugin...	23
8.	Microsoft disrupts cybercrime gang behind 750 million fraudulent accounts....	25
9.	Ubiquiti users report having access to others' UniFi routers, cameras.....	27
10.	MongoDB says customer data was exposed in a cyberattack .....	30
11.	Terrapin attacks can downgrade security of OpenSSH connections .....	32
12.	Interpol operation arrests 3,500 cybercriminals, seizes \$300 million.....	35
13.	BlackCat Ransomware Raises Ante After FBI Disruption.....	37
14.	New phishing attack steals your Instagram backup codes to bypass 2FA .....	40
15.	Android malware Chameleon disables Fingerprint Unlock to steal PINs .....	43
16.	Lapsus\$ hacker behind GTA 6 leak gets indefinite hospital sentence .....	46
17.	Fake VPN Chrome extensions force-installed 1.5 million times.....	48
18.	Europol warns 443 online shops infected with credit card stealers .....	51
19.	Nissan Australia cyberattack claimed by Akira ransomware gang .....	53
20.	New Xamalicious Android malware installed 330k times on Google Play .....	55
21.	Malware abuses Google OAuth endpoint to 'revive' cookies, hijack accounts ...	59

## 1. Hackers breach US govt agencies using Adobe ColdFusion exploit



The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning about hackers actively exploiting a critical vulnerability in Adobe ColdFusion identified as CVE-2023-26360 to gain initial access to government servers.

The security issue allows executing arbitrary code on servers running Adobe ColdFusion 2018 Update 15 and older, and 2021 Update 5 and earlier. It was exploited as a zero day before Adobe fixed it in mid-March by releasing ColdFusion 2018 Update 16 and 2021 Update 6.

At the time, CISA published a notice about threat actors exploiting the flaw and urged federal organizations and state services to apply the available security updates.

In an alert today, America's Cyber Defense Agency warns that CVE-2023-26360 is still leveraged in attacks, showcasing incidents from June that impacted two federal agency systems.

*"In both incidents, Microsoft Defender for Endpoint (MDE) alerted of the potential exploitation of an Adobe ColdFusion vulnerability on public-facing web servers in the agency's pre-production environment" – CISA*

The agency notes that "both servers were running outdated versions of software which are vulnerable to various CVEs."

CISA says that the threat actors leveraged the vulnerability to drop malware using HTTP POST commands to the directory path associated with ColdFusion.

The first incident was recorded on June 26 and relied on the critical vulnerability to breach a server running Adobe ColdFusion v2016.0.0.3.



The attackers conducted process enumeration along with network checks and installed a web shell (config.jsp) that allowed them to insert code into a ColdFusion configuration file and extract credentials.

Their activities included deleting files used in the attack to hide their presence and creating files in the C:\IBM directory to facilitate malicious operations undetected.

File Name	Hash (SHA-1)	Description
eee.exe	b6818d2d5cbd902ce23461f24fc47e24937250e6	VirusTotal[3] flags this file as malicious. This was located in D:\\$RECYCLE.BIN.
edge.exe	75a8ceded496269e9877c2d55f6ce13551d93ff4	The dynamic-link library (DLL) file msedge.dll attempted to execute via edge.exe but received an error.  <b>Note:</b> This file is part of the official Microsoft Edge browser and is a cookie exporter.
fscan.exe	be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656	Analysis confirmed at least three subnets were scanned using fscan.exe, which was launched from the C:\IBM directory [T1046].
RC.exe	9126b8320d18a52b1315d5ada08e1c380d18806b	RCDLL.dll attempted to execute via RC.exe but received an error.  <b>Note:</b> This file is part of the official Windows operating system and is called Microsoft Resource Compiler.

#### *Tools the attacker used in the first attack (CISA)*

The second incident occurred on June 2 when the hackers exploited CVE-2023-26360 on a server running Adobe ColdFusion v2021.0.0.2.

In this case, the attackers gathered user account information before dropping a text file that decoded as a remote access trojan (d.jsp).

Next, they attempted to exfiltrate Registry files and security account manager (SAM) information. The attackers abused available security tools to access SYSVOL, a special directory present on every domain controller in a domain.

In both cases, the attacks were detected and blocked before the intruders were able to exfiltrate data or move laterally, and the compromised assets were removed from crucial networks within 24 hours.

CISA's analysis categorizes the attacks as reconnaissance efforts. However, it is unknown if the same threat actor is behind both intrusions.

To mitigate the risk, CISA recommends upgrading ColdFusion to the latest available version, applying network segmentation, setting up a firewall or WAF, and enforcing signed software execution policies.

Source: <https://www.bleepingcomputer.com/news/security/hackers-breach-us-govt-agencies-using-adobe-coldfusion-exploit/>

## 2. "Sierra:21" vulnerabilities impact critical infrastructure routers



A set of 21 newly discovered vulnerabilities impact Sierra OT/IoT routers and threaten critical infrastructure with remote code execution, unauthorized access, cross-site scripting, authentication bypass, and denial of service attacks.

The flaws discovered by Forescout Vedere Labs affect Sierra Wireless AirLink cellular routers and open-source components like TinyXML and OpenNDS (open Network Demarcation Service).

AirLink routers are highly regarded in the field of industrial and mission-critical applications due to high-performance 3G/4G/5G and WiFi and multi-network connectivity.

Various models are used in complex scenarios like passenger WiFi in transit systems, vehicle connectivity for emergency services, long-range gigabit connectivity to field operations, and various other performance-intensive tasks.

Forescout says Sierra routers are found in government systems, emergency services, energy, transportation, water and wastewater facilities, manufacturing units, and healthcare organizations.



*Sierra AirLink router applications (Forescout)*

## Flaws and impact

Forescout's researchers discovered 21 new vulnerabilities in Sierra AirLink cellular routers and the TinyXML and OpenNDS components, which are part of other products, too.

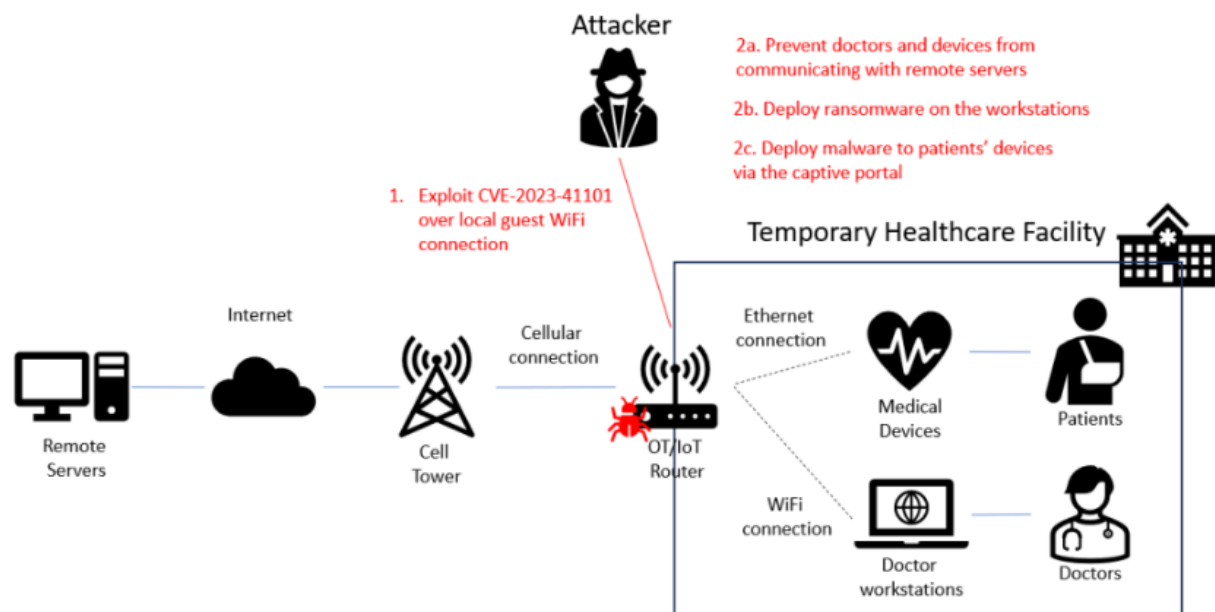
Only one of the security issues has been rated critical, eight of them received a high severity score, and a dozen present a medium risk.

The most noteworthy vulnerabilities are summarized below:

- **CVE-2023-41101** (Remote Code Execution in OpenNDS – critical severity score of 9.6)
- **CVE-2023-38316** (Remote Code Execution in OpenNDS – high severity score of 8.8)
- **CVE-2023-40463** (Unauthorized Access in ALEOS – high severity score of 8.1)
- **CVE-2023-40464** (Unauthorized Access in ALEOS – high severity score of 8.1)
- **CVE-2023-40461** (Cross Site Scripting in ACManager – high severity score of 8.1)
- **CVE-2023-40458** (Denial of Service in ACManager – high severity score of 7.5)
- **CVE-2023-40459** (Denial of Service in ACManager – high severity score of 7.5)
- **CVE-2023-40462** (Denial of Service in ACManager related to TinyXML – high severity score of 7.5)
- **CVE-2023-40460** (Cross Site Scripting in ACManager – high severity score of 7.1)



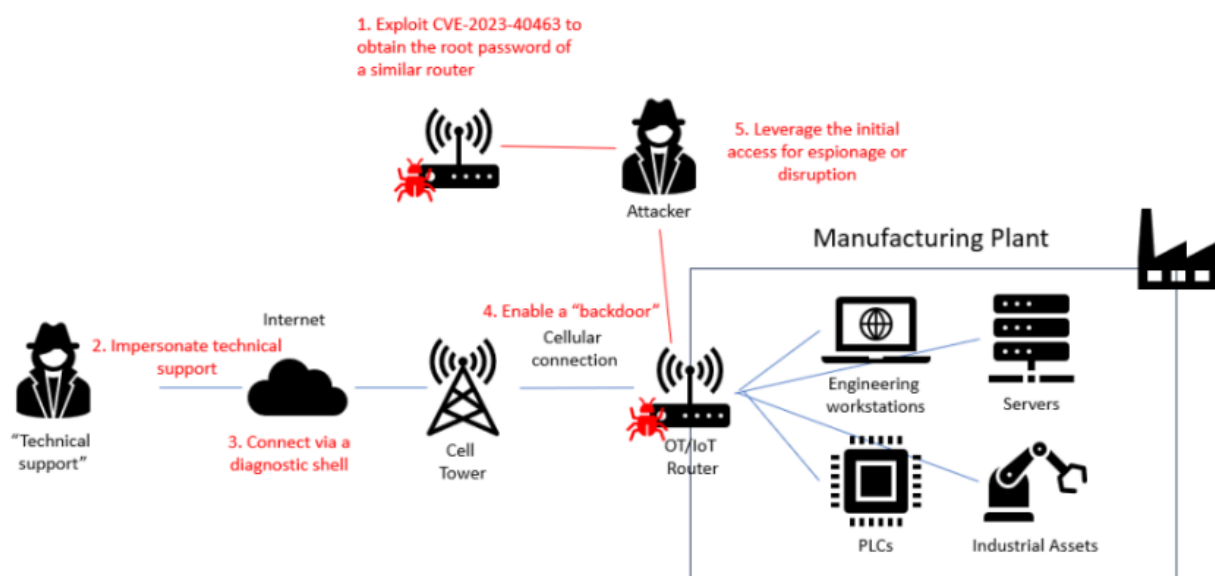
For at least five of the above flaws, attackers do not require authentication to exploit them. For several others affecting OpenNDS, authentication is likely not required, as common attack scenarios involve clients attempting to connect to a network or service.



Attack scenario on a healthcare provider (Forescout)

According to the researchers, an attacker could exploit some of the vulnerabilities "to take full control of an OT/IoT router in critical infrastructure." The compromise could lead to network disruption, enable espionage, or move laterally to more important assets, and malware deployment.

*"Apart from human attackers, these vulnerabilities can also be used by botnets for automatic propagation, communication with command-and-control servers, as well as performing DoS attacks," the researchers explain.*

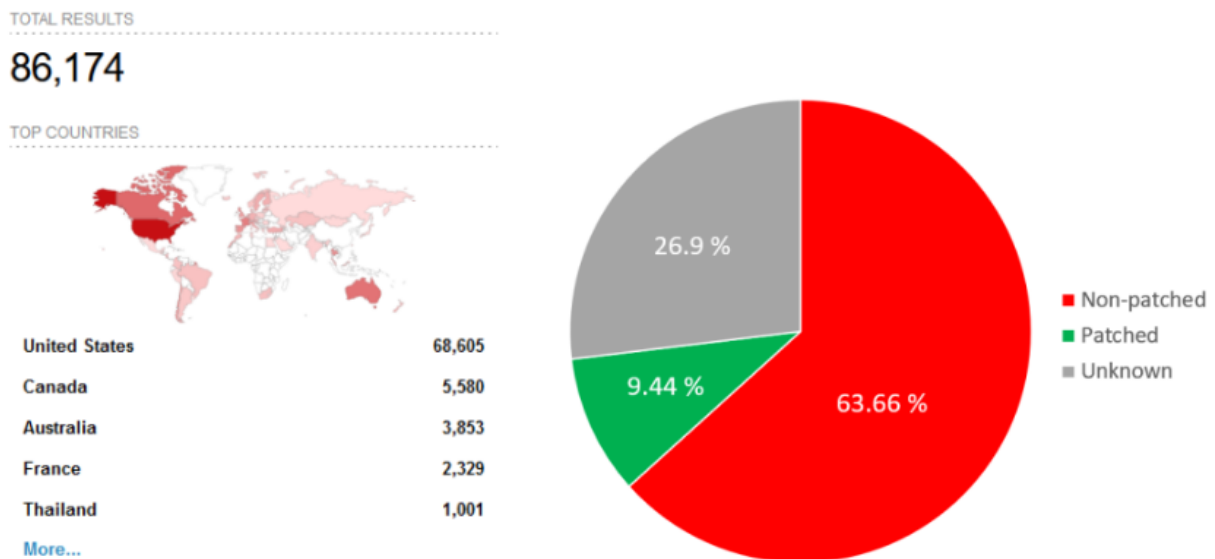


Attack scenario on an industrial setting (Forescout)

After running a scan on Shodan search engine for internet-connected devices, Forescout researchers found over 86,000 AirLink routers exposed online in critical organizations engaged in power distribution, vehicle tracking, waste management, and national health services.

About 80% of the exposed systems are in the United States, followed by Canada, Australia, France, and Thailand.

Of those, fewer than 8,600 have applied patches to vulnerabilities disclosed in 2019, and more than 22,000 are exposed to man-in-the-middle attacks due to using a default SSL certificate.



*Shodan scan results (Forescout)*

## Remediation advice

The recommended action for administrators is to upgrade to the ALEOS (AirLink Embedded Operating System) version 4.17.0, which addresses all flaws, or at least ALEOS 4.9.9, which contains all fixes except for those impacting OpenNDS captive portals that set a barrier between the public internet and a local area network.

The OpenNDS project has also released security updates for the vulnerabilities impacting the open-source project, with version 10.1.3.

Note that TinyXML is now abandonware, so there will be no fixes for the CVE-2023-40462 vulnerability that impacts the project.

Forescout also recommends taking the following additional actions for enhanced protection:

- Change default SSL certificates in Sierra Wireless routers and similar devices.
- Disable or restrict non-essential services like captive portals, Telnet, and SSH.
- Implement a web application firewall to protect OT/IoT routers from web vulnerabilities.
- Install an OT/IoT-aware IDS to monitor external and internal network traffic for security breaches.

Forescout has released a technical report that explains the vulnerabilities and the conditions that allow exploiting them.

According to the company, threat actors are increasingly targeting routers and network infrastructure environments, launching attacks with custom malware that use the devices for persistence and espionage purposes.

For cybercriminals, routers are usually a means to proxy malicious traffic or to increase the size of their botnet.

Source: <https://www.bleepingcomputer.com/news/security/sierra-21-vulnerabilities-impact-critical-infrastructure-routers>/<https://www.schneier.com/blog/archives/2022/12/sirius-xm-software-vulnerability.html>

### 3. US senator: Govts spy on Apple, Google users via mobile notifications



A U.S. senator revealed today that government agencies worldwide demand mobile push notification records from Apple and Google users to spy on their customers.

These revelations come after U.S. Senator Ron Wyden, who serves on the Senate Intelligence Committee, sent a letter to the Department of Justice warning that various governments around the world have been requesting push notification data from two major tech companies. The goal of these requests is likely to gain access to data required to link users with specific accounts or devices.

Wyden said that he received a tip about governments requesting this data in 2022, and his office has been investigating the matter over the past year.

Push notifications are smartphone alerts from mobile apps that go through intermediary gateways managed by the device vendor (through Google's Firebase Cloud Messaging and Apple's Push Notification Service).

App developers must use Apple's and Google's notification gateways, which provide the tech giants with insight into their customers' app usage patterns and make it easier for U.S. or international governments to monitor individuals of interest through data requests.

Data collection through this method helps link devices to Apple or Google accounts and may also allow access to unencrypted notification content, including text displayed on the receiving smartphone.

In his letter, Wyden also asked the DOJ to allow the two companies to share more details regarding this practice with their customers, seeing that this information is restricted from public release by the U.S. government.

*"Apple and Google should be permitted to be transparent about the legal demands they receive, particularly from foreign governments, just as the companies regularly notify users about other types of government demands for data," Wyden said.*

*"These companies should be permitted to generally reveal whether they have been compelled to facilitate this surveillance practice, to publish aggregate statistics about the number of demands they receive, and unless temporarily gagged by a court, to notify specific customers about demands for their data."*

## Apple and Google promise to share more info

In response to the letter, Apple said that this provides an opportunity to disclose further information to the public concerning how government entities use data related to such notifications for surveillance purposes.

*"In this case, the federal government prohibited us from sharing any information. Now that this method has become public we are updating our transparency reporting to detail these kinds of requests," Apple said in a statement shared with Reuters.*

A Google spokesperson added that the company shares "the Senator's commitment to keeping users informed about these requests."

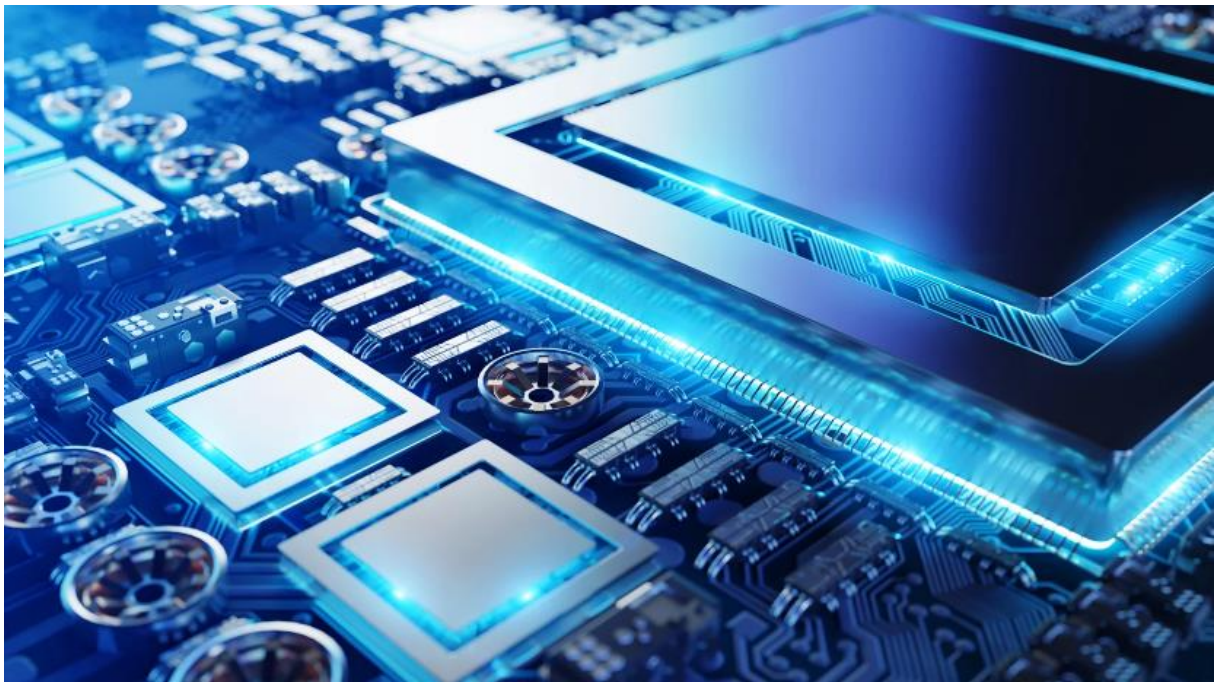
*"We were the first major company to publish a public transparency report sharing the number and types of government requests for user data we receive, including the requests referred to by Senator Wyden," BleepingComputer was told.*



An Apple spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today.

Source: <https://www.bleepingcomputer.com/news/security/us-senator-govts-spy-on-apple-google-users-via-mobile-notifications/>

#### 4. New SLAM attack steals sensitive data from AMD, future Intel CPUs



Academic researchers developed a new side-channel attack called SLAM that exploits hardware features designed to improve security in upcoming CPUs from Intel, AMD, and Arm to obtain the root password hash from the kernel memory.

SLAM is a transient execution attack that takes advantage of a memory feature that allows software to use untranslated address bits in 64-bit linear addresses for storing metadata.

CPU vendors implement this in different ways and have distinct terms for it. Intel calls it Linear Address Masking (LAM), AMD names it Upper Address Ignore (UAI), and Arm refers to the feature as Top Byte Ignore (TBI).

Short for Spectre based on LAM, the SLAM attack was discovered by researchers at Systems and Network Security Group (VUSec Group) at Vrije Universiteit Amsterdam, who demonstrated its validity by emulating the upcoming LAM feature from Intel on a last-generation Ubuntu system.

According to VUSec, SLAM impacts mainly future chips that meet specific criteria. The reasons for this include the lack of strong canonicity checks in future chip designs.



Additionally, while the advanced hardware features (e.g. LAM, UAI, and TBI) improve memory security and management, they also introduce exploitable micro-architectural race conditions.

## Leaking the root password hash

The attack leverages a new transient execution technique that focuses on exploiting a previously unexplored class of Spectre disclosure gadgets, specifically those involving pointer chasing.

Gadgets are instructions in software code that the attacker can manipulate to trigger speculative execution in a way that reveals sensitive information.

Although the results of speculative execution are discarded, the process leaves traces like altered cache states which attackers can observe to infer sensitive information such as data from other programs or even the operating system.

The SLAM attack targets "unmasked" gadgets that use secret data as a pointer, which the researchers report are common in software and can be exploited to leak arbitrary ASCII kernel data.

The researchers developed a scanner with which they found hundreds of exploitable gadgets on the Linux kernel. The following video demonstrates the attack that leaks the root password hash from the kernel.

In practical scenario, an attacker would need to execute on the target system code that interacts with the unmasked gadgets and then carefully measure the side effects using sophisticated algorithms to extract sensitive information such as passwords or encryption keys from the kernel memory.

The code and data for reproducing the SLAM attack are available on VUSec's GitHub repository. The researchers also published a technical paper explaining how the attack works.

VUSec notes that SLAM impacts the following processors:

- Existing AMD CPUs vulnerable to CVE-2020-12965
- Future Intel CPUs supporting LAM (both 4- and 5-level paging)
- Future AMD CPUs supporting UAI and 5-level paging
- Future Arm CPUs supporting TBI and 5-level paging

## Vendor response to SLAM

Responding to the researchers' disclosure, Arm published an advisory explaining that its systems already mitigate against Spectre v2 and Spectre-BHB and plan no further action in response to SLAM.

AMD also pointed to current Spectre v2 mitigations to address the SLAM attack described by the VUSec research group and did not provide any guidance or updates that would lower the risk.

Intel announced plans for providing software guidance before releasing future processors that support LAM, such as deploying the feature with the Linear Address Space Separation (LASS) security extension for preventing speculative address accesses across user/kernel mode.

Until further guidance becomes available, Linux engineers have created patches that disable LAM.

Source: <https://www.bleepingcomputer.com/news/security/new-slam-attack-steals-sensitive-data-from-amd-future-intel-cpus/>

## 5. AutoSpill attack steals credentials from Android password managers



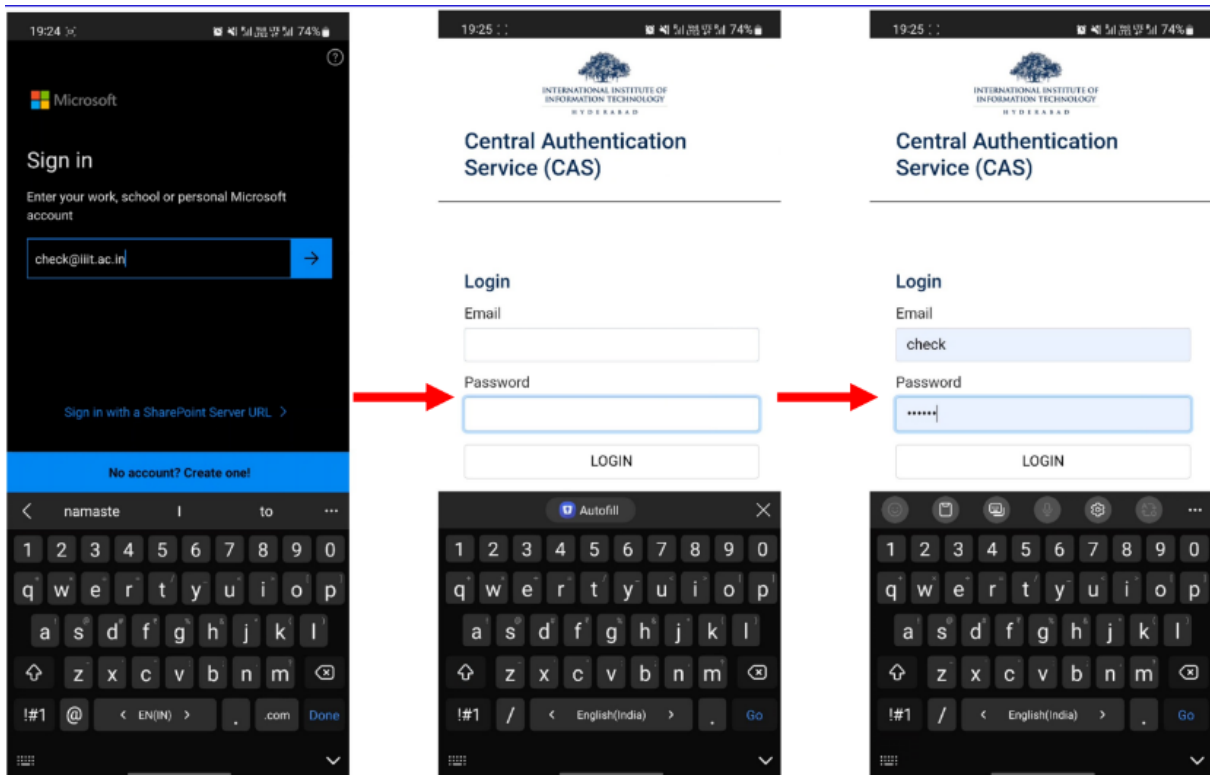
Security researchers developed a new attack, which they named AutoSpill, to steal account credentials on Android during the autofill operation.

In a presentation at the Black Hat Europe security conference, researchers from the International Institute of Information Technology (IIIT) at Hyderabad said that their tests showed that most password managers for Android are vulnerable to AutoSpill, even if there is no JavaScript injection.

### How AutoSpill works

Android apps often use WebView controls to render web content, such as login pages within the app, instead of redirecting the users to the main browser, which would be a more cumbersome experience on small-screen devices.

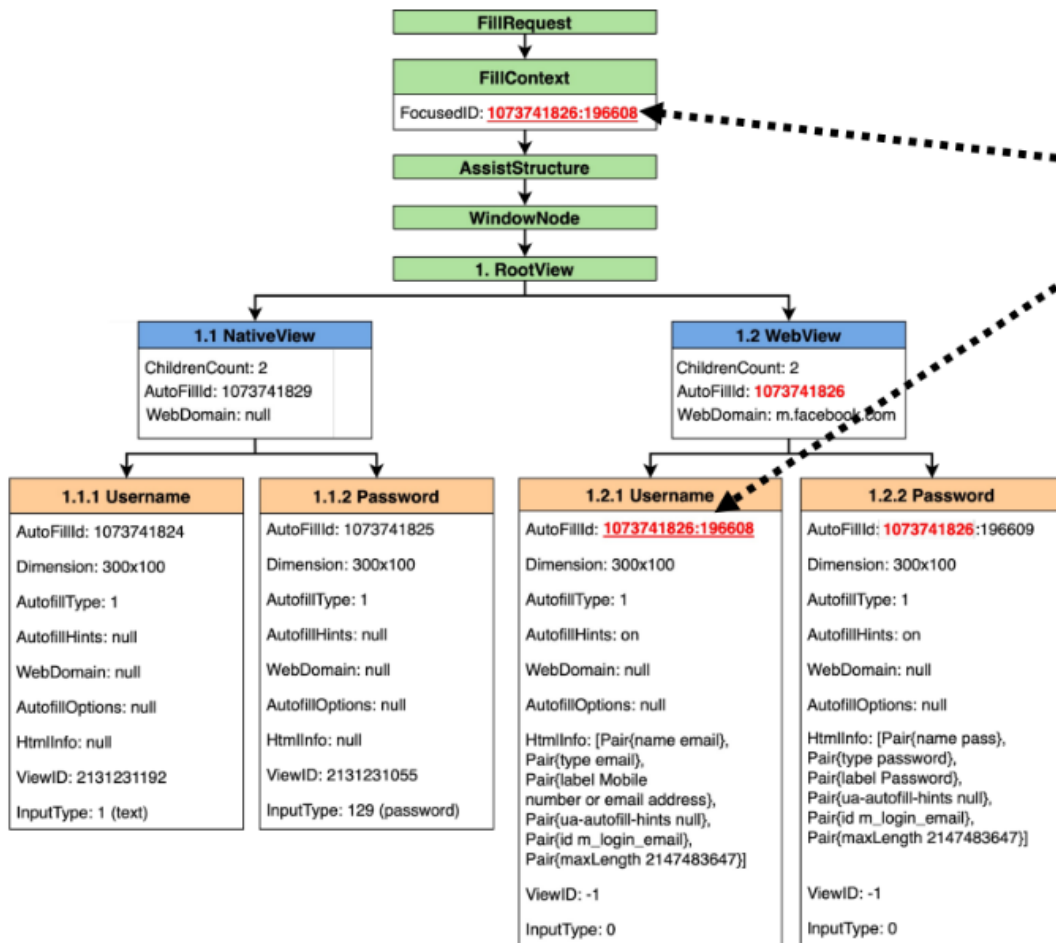
Password managers on Android use the platform's WebView framework to automatically type in a user's account credentials when an app loads the login page to services like Apple, Facebook, Microsoft, or Google.



*Logging in on a university portal using a Microsoft account*

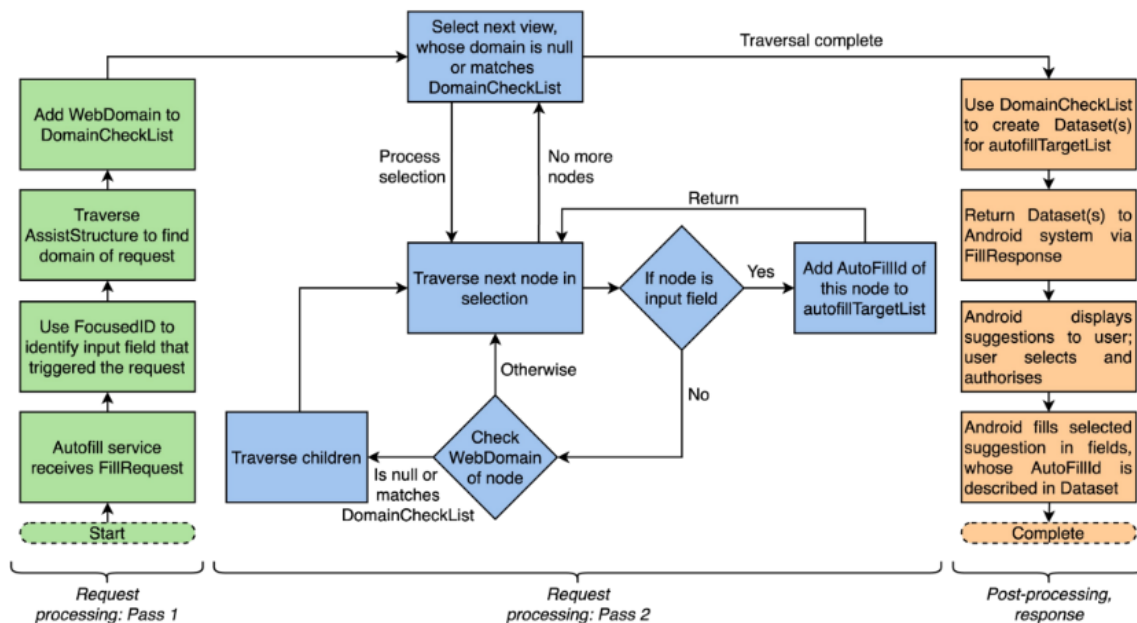
The researchers said that it is possible to exploit weaknesses in this process to capture the auto-filled credentials on the invoking app, even without JavaScript injection.

If JavaScript injections are enabled, the researchers say that all password managers on Android are vulnerable to the AutoSpill attack.



Internal structure of autofill management on Android

Specifically, the AutoSpill issue stems from Android's failure to enforce or to clearly define the responsibility for the secure handling of the auto-filled data, which can result in leaking it or being captured by the host app.



Process flow of the autofill service

In an attack scenario, a rogue app serving a login form could capture the user's credentials without leaving any indication of the compromise. Additional technical details about the AutoSpill attack are available in the researchers' slides from the Black Hat Europe presentation.

More details about the AutoSpill attack can be found in this document, which contains slides from the BlackHat presentation.

## Impact and fixing

The researchers tested AutoSpill against a selection of password managers on Android 10, 11, and 12 and found that 1Password 7.9.4, LastPass 5.11.0.9519, Enpass 6.8.2.666, Keeper 16.4.3.1048, and Keepass2Android 1.09c-r0 are susceptible to attacks due to using Android's autofill framework.

Google Smart Lock 13.30.8.26 and the DashLane 6.2221.3 followed a different technical approach for the autofill process. They did not leak sensitive data to the host app unless JavaScript injection was used.

PM	Native fields present in H <sub>A</sub>			
	2 Both username, password	1 Only username	1 Only password	1 Only none
Google Smart Lock	✓	✓	✓	✓
Dashlane	✓	✓	✓	✓
1Password	X	X	P	U
LastPass	U+P	U	P	U
Enpass	U+P	U	P	U
Keepass2Android	U+P	U	P	U
Keeper	U+P	U	P	U

*Test results: (U - username leaked), (P - password leaked), (X - not working), (✓ - safe from AutoSpill)*

The researchers disclosed their findings to impacted software vendors and Android's security team and shared their proposals for addressing the problem. Their report was acknowledged as valid, but no details about fixing plans were shared.

BleepingComputer has contacted multiple providers of password management products that are impacted by AutoSpill, as well as Google, asking about their plans to address the issue and we received the following comments so far:

*Many people have become accustomed to using autofill to quickly and easily enter their credentials. Through a malicious app installed on the user's device, a hacker could lead a user to unintentionally autofill their credentials. AutoSpill highlights this problem.*



*Keeping our customers' most important data safe is our utmost priority at 1Password. A fix for AutoSpill has been identified and is currently being worked on.*

*While the fix will further strengthen our security posture, 1Password's autofill function has been designed to require the user to take explicit action.*

*The update will provide additional protection by preventing native fields from being filled with credentials that are only intended for Android's WebView.*

*- Pedro Canahuati, CTO of **1Password***

*In 2022, we engaged with Dr. Gangwal via Bugcrowd, our bug bounty program partner. We analyzed the findings he submitted and found it to be a low-risk vulnerability due to the mechanisms required for it to be exploited.*

*What's important to note here is that this vulnerability requires the ability and opportunity to install a malicious app on the target device, which would indicate a complete compromise or the ability to execute code on the targeted device.*

*Prior to receiving Dr. Gangwal's findings, LastPass already had a mitigation in place via an in-product pop-up warning when the app detected an attempt to leverage the exploit. After analyzing the findings, we added more informative wording in the pop-up.*

*We confirmed this update with Dr. Gangwal but did not receive any acknowledgement of our update.*

*- **LastPass** spokesperson*

*On May 31, 2022, Keeper received a report from the researcher about a potential vulnerability. We requested a video from the researcher to demonstrate the reported issue. Based upon our analysis, we determined the researcher had first installed a malicious application and subsequently, accepted a prompt by Keeper to force the association of the malicious application to a Keeper password record.*

*Keeper has safeguards in place to protect users against automatically filling credentials into an untrusted application or a site that was not explicitly authorized by the user. On the Android platform, Keeper prompts the user when attempting to autofill credentials into an Android application or website. The user is asked to confirm the association of the application to the Keeper password record prior to filling any information. On June 29, we informed the researcher of this information and also recommended that he submit his report to Google since it is specifically related to the Android platform.*

*Generally, a malicious Android application would first need to be submitted to Google Play Store, reviewed by Google and subsequently, approved for publication to the Google Play Store. The user would then need to install the malicious application from Google Play and transact with the application. Alternatively, the user would need to override important security settings on their device in order to sideload a malicious application.*

*Keeper always recommends that individuals be cautious and vigilant about the applications they install and should only install published Android applications from trusted app stores such as the Google Play Store.*

*- Craig Lurey, CTO and co-founder of **Keeper Security***

*WebView is used in a variety of ways by Android developers, which include hosting login pages for their own services in their apps. This issue is related to how password managers leverage the autofill APIs when interacting with WebViews.*

*We recommend third-party password managers be sensitive as to where passwords are being inputted, and we have WebView best practices that we recommend all password managers implement. Android provides password managers with the required context to distinguish between native views and WebViews, as well as whether the WebView being loaded is not related to the hosting app.*

*For example, when using the Google Password Manager for autofill on Android, users are warned if they are entering a password for a domain Google determines may not be owned by the hosting app, and the password is only filled in on the proper field. Google implements server side protections for logins via WebView.*

*- **Google** spokesperson*

*Ankit Gangwal from the research team at the Indian Institutes of Information Technology reached out to us in June 2022 about the AutoSpill vulnerability in the Android Autofill framework. That vulnerability was subsequently patched in Enpass 6.8.3, released September 29, 2022.*

*- **Enpass** spokesperson*

Source: <https://www.bleepingcomputer.com/news/security/autospill-attack-steals-credentials-from-android-password-managers/>

## 6. Toyota warns customers of data breach exposing personal, financial info



Toyota Financial Services (TFS) is warning customers it suffered a data breach, stating that sensitive personal and financial data was exposed in the attack.

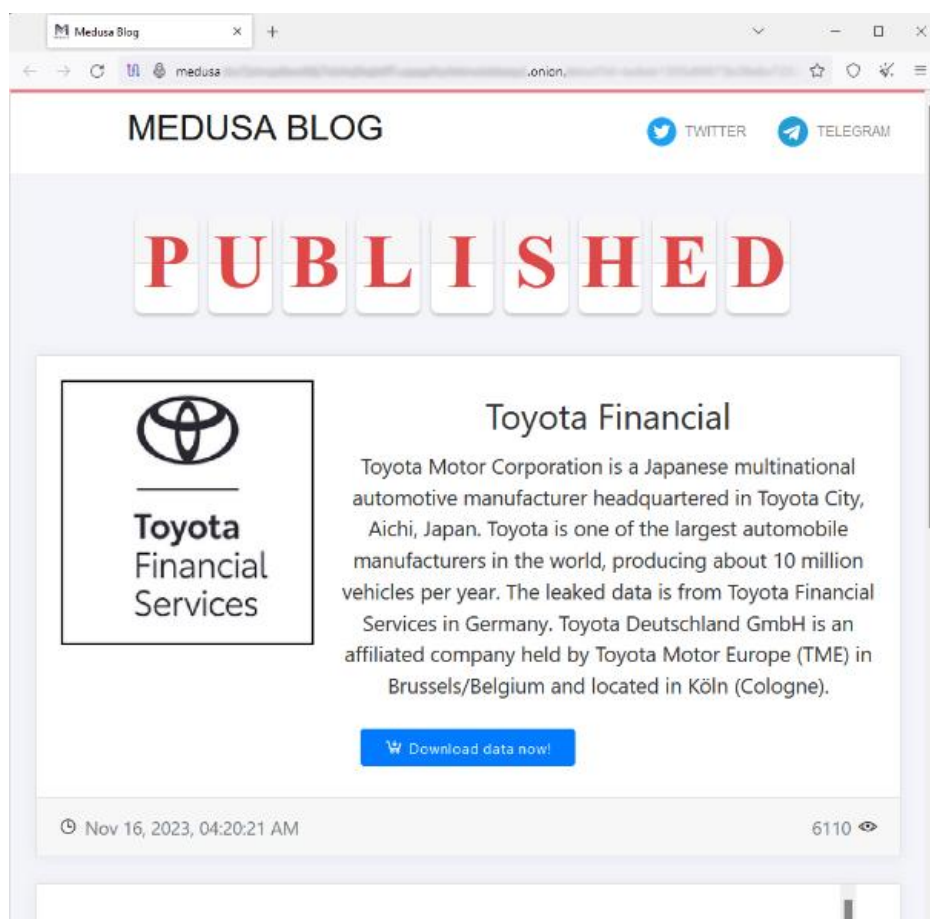
Toyota Financial Services, a subsidiary of Toyota Motor Corporation, is a global entity with a presence in 90% of the markets where Toyota sells its cars, providing auto financing to its customers.

Last month, the company confirmed that it detected unauthorized access on some of its systems in Europe and Africa, following a claim from Medusa ransomware about successfully compromising the Japanese automaker's division.

The threat actors demanded a payment of \$8,000,000 to delete the stolen data and gave Toyota 10 days to respond to their blackmail.

At the time, a Toyota spokesperson told BleepingComputer that the company had detected unauthorized access on some of its systems in Europe and Africa. The company took certain systems offline to contain the breach, which impacted customer services.

Presumably, Toyota has not negotiated a ransom payment with the cybercriminals, and currently, all data has been leaked on Medusa's extortion portal on the dark web.



*Stolen data available for download via Medusa's extortion portal (BleepingComputer)*

Earlier this month, Toyota Kreditbank GmbH in Germany was identified as one of the impacted divisions, admitting that hackers gained access to customers' personal data.

German news outlet Heise received a sample of the notices sent by Toyota to German customers, informing that the following data has been compromised:

- Full name
- Residence address
- Contract information
- Lease-purchase details
- IBAN (International Bank Account Number)

This type of data can be used in phishing, social engineering, scams, financial fraud, and even identity theft attempts.



*Notice sent to impacted customers (Heise)*

The notification verifies the above data as compromised based on the ongoing investigation. However, the internal investigation isn't complete yet, and there remains a possibility that attackers accessed additional information.

Toyota promises to promptly update affected customers should the internal investigation reveal further data exposure.

BleepingComputer has contacted Toyota for additional information, like the exact number of exposed customers, but we have not heard back by publication time.

Source: <https://www.bleepingcomputer.com/news/security/toyota-warns-customers-of-data-breach-exposing-personal-financial-info/>



## 7. 50K WordPress sites exposed to RCE attacks by critical bug in backup plugin



A critical severity vulnerability in a WordPress plugin with more than 90,000 installs can let attackers gain remote code execution to fully compromise vulnerable websites.

Known as Backup Migration, the plugin helps admins automate site backups to local storage or a Google Drive account.

The security bug (tracked as CVE-2023-6553 and rated with a 9.8/10 severity score) was discovered by a team of bug hunters known as Nex Team, who reported it to WordPress security firm Wordfence under a recently launched bug bounty program.

It impacts all plugin versions up to and including Backup Migration 1.3.6, and malicious actors can exploit it in low-complexity attacks without user interaction.

CVE-2023-6553 allows unauthenticated attackers to take over targeted websites by gaining remote code execution through PHP code injection via the `/includes/backup-heart.php` file.

"This is due to an attacker being able to control the values passed to an include, and subsequently leverage that to achieve remote code execution. This makes it possible for unauthenticated threat actors to easily execute code on the server," Wordfence said on Monday.

"By submitting a specially-crafted request, threat-actors can leverage this issue to include arbitrary, malicious PHP code and execute arbitrary commands on the underlying server in the security context of the WordPress instance."

In the `/includes/backup-heart.php` file used by the Backup Migration plugin, an attempt is made to incorporate `bypasser.php` from the `BMI_INCLUDES` directory (defined by merging `BMI_ROOT_DIR` with the `includes` string) at line 118.

However, `BMI_ROOT_DIR` is defined through the `content-dir` HTTP header found on line 62, thereby making `BMI_ROOT_DIR` subject to user control.

```
31 // Get fields from header
32 if (isFunctionEnabled('getallheaders')) {
33     $fields = getallheaders();
34 }
...
62 define('BMI_ROOT_DIR', $fields['content-dir']);
...
64 define('BMI_INCLUDES', BMI_ROOT_DIR . 'includes');
...
117 // Load bypasser
118 require_once BMI_INCLUDES . '/bypasser.php';
```

*Backup Migration vulnerable code (Wordfence)*

## Patch released within hours

Wordfence reported the critical security flaw to BackupBliss, the development team behind the Backup Migration plugin, on December 6, with the developers releasing a patch hours later.

However, despite the release of the patched Backup Migration 1.3.8 plugin version on the day of the report, almost 50,000 WordPress websites using a vulnerable version still have to be secured nearly one week later, as WordPress.org org download stats show.

Admins are strongly advised to secure their websites against potential CVE-2023-6553 attacks, given that this is a critical vulnerability that unauthenticated malicious actors can exploit remotely.

WordPress administrators are also being targeted by a phishing campaign attempting to trick them into installing malicious plugins using fake WordPress security advisories for a fictitious vulnerability tracked as CVE-2023-45124 as bait.

Last week, WordPress also fixed a Property Oriented Programming (POP) chain vulnerability that could allow attackers to gain arbitrary PHP code execution under certain conditions (when combined with some plugins in multisite installations).

Source: <https://www.bleepingcomputer.com/news/security/50k-wordpress-sites-exposed-to-rce-attacks-by-critical-bug-in-backup-plugin/>

## 8. Microsoft disrupts cybercrime gang behind 750 million fraudulent accounts



Microsoft's Digital Crimes Unit seized multiple domains used by a Vietnam-based cybercrime group (Storm-1152) that registered over 750 million fraudulent accounts and raked in millions of dollars by selling them online to other cybercriminals.

Storm-1152 is a major cybercrime-as-a-service provider and the number one seller of fraudulent Outlook accounts, as well as other illegal "products," including an automatic CAPTCHA-solving service to bypass Microsoft's CAPTCHA challenges and register more fraudulent Microsoft email accounts.

"Storm-1152 runs illicit websites and social media pages, selling fraudulent Microsoft accounts and tools to bypass identity verification software across well-known technology platforms. These services reduce the time and effort needed for criminals to conduct a host of criminal and abusive behaviors online," according to Amy Hogan-Burney, the General Manager of Microsoft's Digital Crimes Unit.

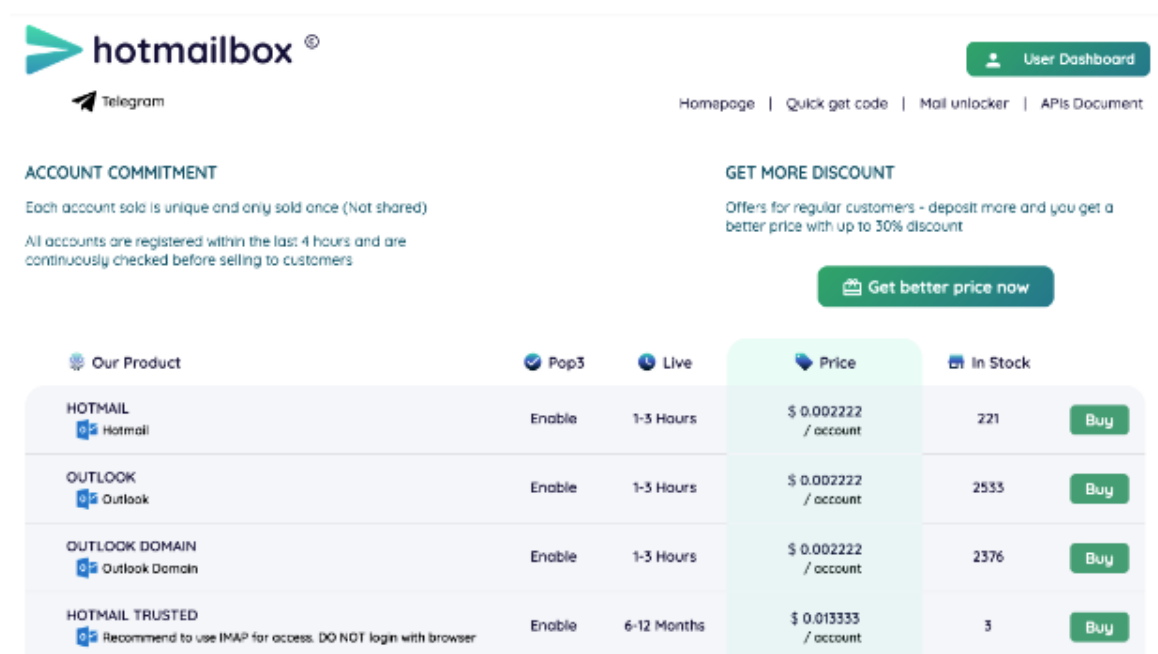
"Since at least 2021, the Defendants have been engaged in a scheme to obtain millions of Microsoft Outlook email accounts in the names of fictitious users based on a series of false representations, and then sell these fraudulent accounts to malicious actors for use in various types of cybercrime," according to the complaint.

According to Microsoft Threat Intelligence, numerous cybergroups involved in ransomware, data theft, and extortion have bought and used accounts provided by Storm-1152 in their attacks.

For instance, financially-motivated Storm-0252, Storm-0455, and Octo Tempest (aka Scattered Spider) cybercrime gangs used Storm-1152 fraudulent accounts to infiltrate organizations worldwide and deploy ransomware on their networks.

The resulting service disruptions resulted in damages estimated by Microsoft to be in the hundreds of millions of dollars.

"Upon information and belief, evidence gathered thus far by Microsoft's investigation in this case shows that Microsoft email accounts—which were fraudulently obtained by Defendants and sold to cybercriminals—have been used by organized cybercrime groups known to Microsoft as Storm-0252, Storm-0455, and Octo Tempest to engage in cybercrime activity, including email phishing scams, which are frequently used as a vehicle for spreading ransomware and other malware," the complaint adds.



Our Product	Pop3	Live	Price	In Stock	
<b>HOTMAIL</b> Hotmail	Enable	1-3 Hours	\$ 0.002222 / account	221	<a href="#">Buy</a>
<b>OUTLOOK</b> Outlook	Enable	1-3 Hours	\$ 0.002222 / account	2533	<a href="#">Buy</a>
<b>OUTLOOK DOMAIN</b> Outlook Domain	Enable	1-3 Hours	\$ 0.002222 / account	2376	<a href="#">Buy</a>
<b>HOTMAIL TRUSTED</b> Recommend to use IMAP for access. DO NOT login with browser	Enable	6-12 Months	\$ 0.013333 / account	3	<a href="#">Buy</a>

*Hotmailbox.me before seizure (BleepingComputer)*

On December 7, Microsoft seized Storm-1152's U.S.-based infrastructure and took down the following websites after obtaining a court order from the Southern District of New York:

- **Hotmailbox.me**, a website selling fraudulent Microsoft Outlook accounts
- **1stCAPTCHA, AnyCAPTCHA, and NoneCAPTCHA**, websites that facilitate the tooling, infrastructure, and selling of the CAPTCHA solving service to bypass the confirmation of use and account setup by a real person. These sites sold identity verification bypass tools for other technology platforms
- **The social media sites** actively used to market these services

The company also sued Duong Dinh Tu, Linh Van Nguyen (a/k/a Nguyen Van Linh), and Tai Van Nguyen for their purported involvement in hosting the cybercriminal operation on the seized domains.

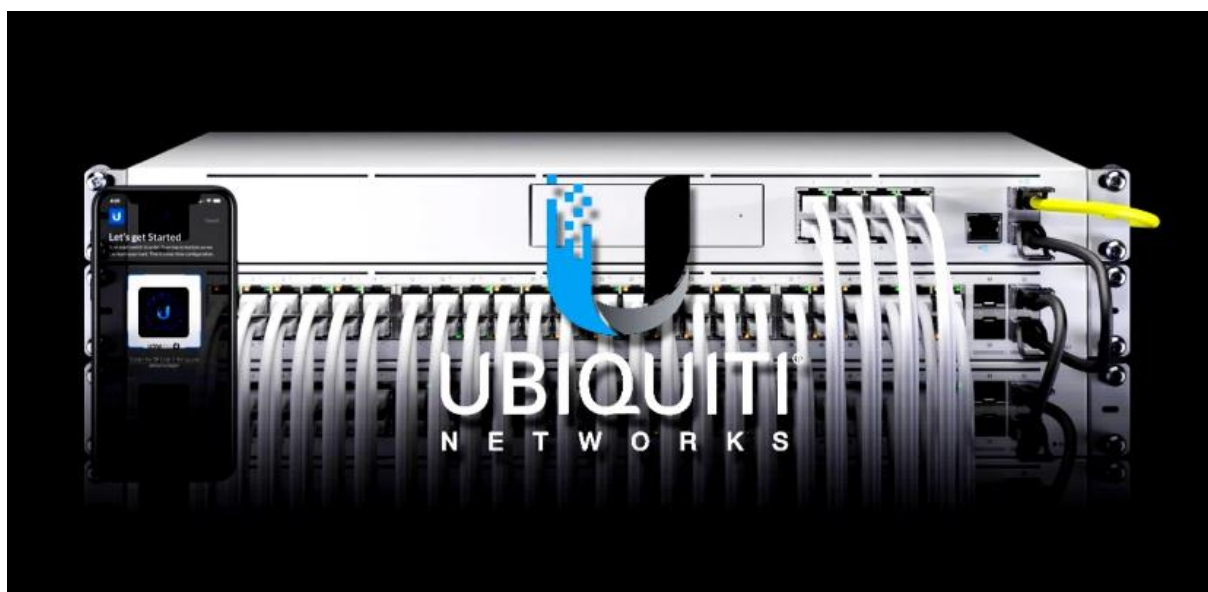


As further alleged in the complaint, the defendants managed and developed the code for the seized websites. They were also involved in publishing video guides on how to use the fraudulent Outlook accounts and offered chat support to 'customers' using their fraudulent services.

*"Today's action is a continuation of Microsoft's strategy of taking aim at the broader cybercriminal ecosystem and targeting the tools cybercriminals use to launch their attacks. It builds on our expansion of a legal method used successfully to disrupt malware and nation-state operations," Hogan-Burney said.*

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-disrupts-cybercrime-gang-behind-750-million-fraudulent-accounts/>

## 9. Ubiquiti users report having access to others' UniFi routers, cameras



*12/14/23 update with information from Ubiquiti added below.*

Since yesterday, users of Ubiquiti networking devices, ranging from routers to security cameras, have reported seeing other people's devices and notifications through the company's UniFi cloud services.

Ubiquiti is a popular networking device manufacturer offering a cloud-based UniFi platform where admins can manage all their devices from a single cloud portal.

The first report of these issues was from yesterday morning at around 8 AM ET when a Ubiquiti customer incorrectly received a notification through UniFi Protect from someone else's security camera.



*"I'm reaching out for some advice regarding a peculiar situation we encountered with UniFi Protect. Recently, my wife received a notification from UniFi Protect, which included an image from a security camera," reads a Reddit post.*

*"However, here's the twist - this camera doesn't belong to us."*



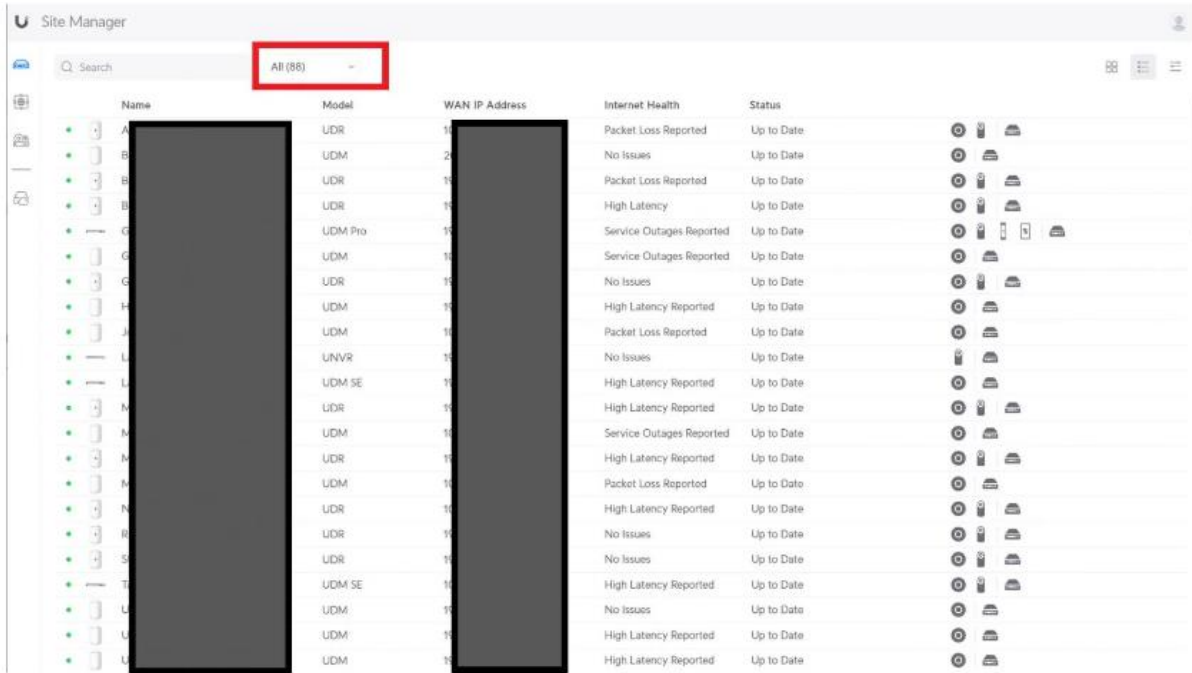
*UniFi Protect notification of another customer's camera*

*Source: Reddit*

To make matters worse, another Ubiquiti customer says that when they logged into the UniFi Site Manager portal to manage their devices, they saw 88 devices from another customer's account.

*"However this time I was presented with 88 consoles from another account. I had full access to these consoles, just as I would my own. This was only stopped when I forced a browser refresh, and I was presented again with my consoles," explains the UniFi customer.*

*"This is somewhat concerning, Has anyone else had this issue?"*



*Screenshot allegedly showing another customer's UniFi devices  
Source: Ubiquiti forums*

A similar experience occurred with others on Reddit who says they logged in and had access to someone else's UDM Pro and were able to manage the device and create additional WiFi networks.

In both situations, once the portal web page was refreshed, they were shown the devices usually associated with their accounts.

When BleepingComputer contacted Ubiquiti about these issues, we were told they are currently gathering information to assess what is causing the issues. Ubiquiti says that they will issue a statement after the review is complete.

Employees have already started gathering information on Reddit and the company's forums, reaching out to impacted customers to learn more about what happened.

*"This is not expected behavior. We reached out via Reddit Chat to gather more details and have our leads review immediately," reads a comment from an Ubiquiti representative on Reddit*

Some customers are skeptical that this is actually happening, saying that Ubiquiti should be given time to investigate the issue.

However, other customers are frustrated that Ubiquiti is not coming forth with a public statement or listing it as a potential issue on the company's network status page, considering that users are reporting that they can modify other's networking configurations.

### Caused by UniFi access misconfiguration

Ubiquiti has issued a statement saying that the bug allowing access to other customers' devices was caused by a misconfiguration in an upgrade to the UniFi cloud infrastructure.

The company says that 1,216 Ubiquiti accounts, which they call "Group 1," were associated with a separate group of 1,177 Ubiquiti accounts, known as "Group 2."

This misconfiguration allowed accounts in Group 2 to receive notifications meant for accounts in Group 1. It further allowed Group 2 accounts to see the devices of Group 1 customers when logged into the UniFi cloud management portal.

Ubiquiti says this issue occurred on December 13, between 6:47 AM and 3:45 PM UTC, and has since been fixed.

The company is still investigating the incident but believes that only twelve accounts were improperly accessed by other Ubiquiti customers. Account holders whose accounts were accessed by mistake will be notified via email.

Source: <https://www.bleepingcomputer.com/news/security/ubiquiti-users-report-having-access-to-others-unifi-routers-cameras/>

## 10. MongoDB says customer data was exposed in a cyberattack

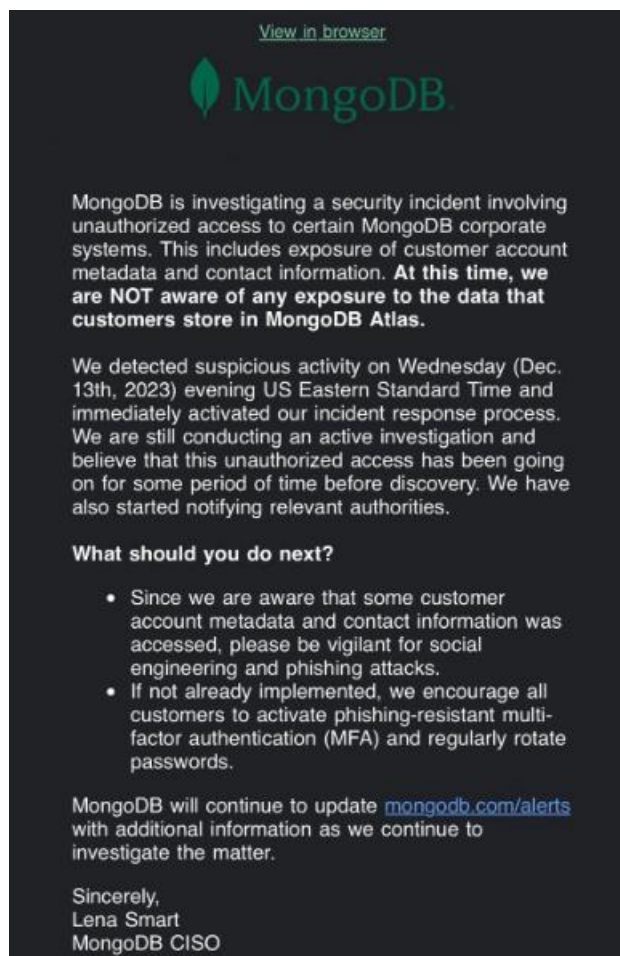


MongoDB is warning that its corporate systems were breached and that customer data was exposed in a cyberattack that was detected by the company earlier this week.

In emails sent to MongoDB customers from CISO Lena Smart, the company says they detected their systems were hacked on Wednesday evening (December 13th) and started investigating the incident.

*"MongoDB is investigating a security incident involving unauthorized access to certain MongoDB corporate systems," reads the email from MongoDB.*

*"This includes exposure of customer account metadata and contact information. At this time, we are NOT aware of any exposure to the data that customers store in MongoDB Atlas."*



**Notification sent to MongoDB customers**

**Source:** [vx-underground](#)

The company does not believe the hackers accessed any customer data stored in MongoDB Atlas. However, MongoDB says the threat actors had access to its systems for some time before they were discovered.

*"We are still conducting an active investigation and believe that this unauthorized access has been going on for some period of time before discovery," reads the security incident notification.*

Unfortunately, data theft usually occurs in breaches like this, where a threat actor has had persistent access for long periods.

As customer metadata was exposed, MongoDB recommends all customers enable multi-factor authentication on their accounts, rotate passwords, and be vigilant against potential targeted phishing and social engineering attacks.

In response to our questions about the breach, MongoDB says that they are still investigating the security incident and had nothing further to add.

The company says it will continue to post updates about the breach at the MongoDB Alerts web page, which they use to post updates about outages and other incidents.

*This is a developing story.*

*Update: Added response from MongoDB.*

Source: <https://www.bleepingcomputer.com/news/security/mongodb-says-customer-data-was-exposed-in-a-cyberattack>/<https://www.bleepingcomputer.com/news/security/worlds-largest-commercial-bank-icbc-confirms-ransomware-attack/>

## 11. Terrapin attacks can downgrade security of OpenSSH connections



Academic researchers developed a new attack called Terrapin that manipulates sequence numbers during the handshake process to break the SSH channel integrity when certain widely-used encryption modes are used.

This manipulation lets attackers remove or modify messages exchanged through the communication channel, which leads to downgrading the public key algorithms used for user authentication or disabling defenses against keystroke timing attacks in OpenSSH 9.5.



*"The Terrapin attack exploits weaknesses in the SSH transport layer protocol in combination with newer cryptographic algorithms and encryption modes introduced by OpenSSH over 10 years ago." - Ruhr University Bochum*

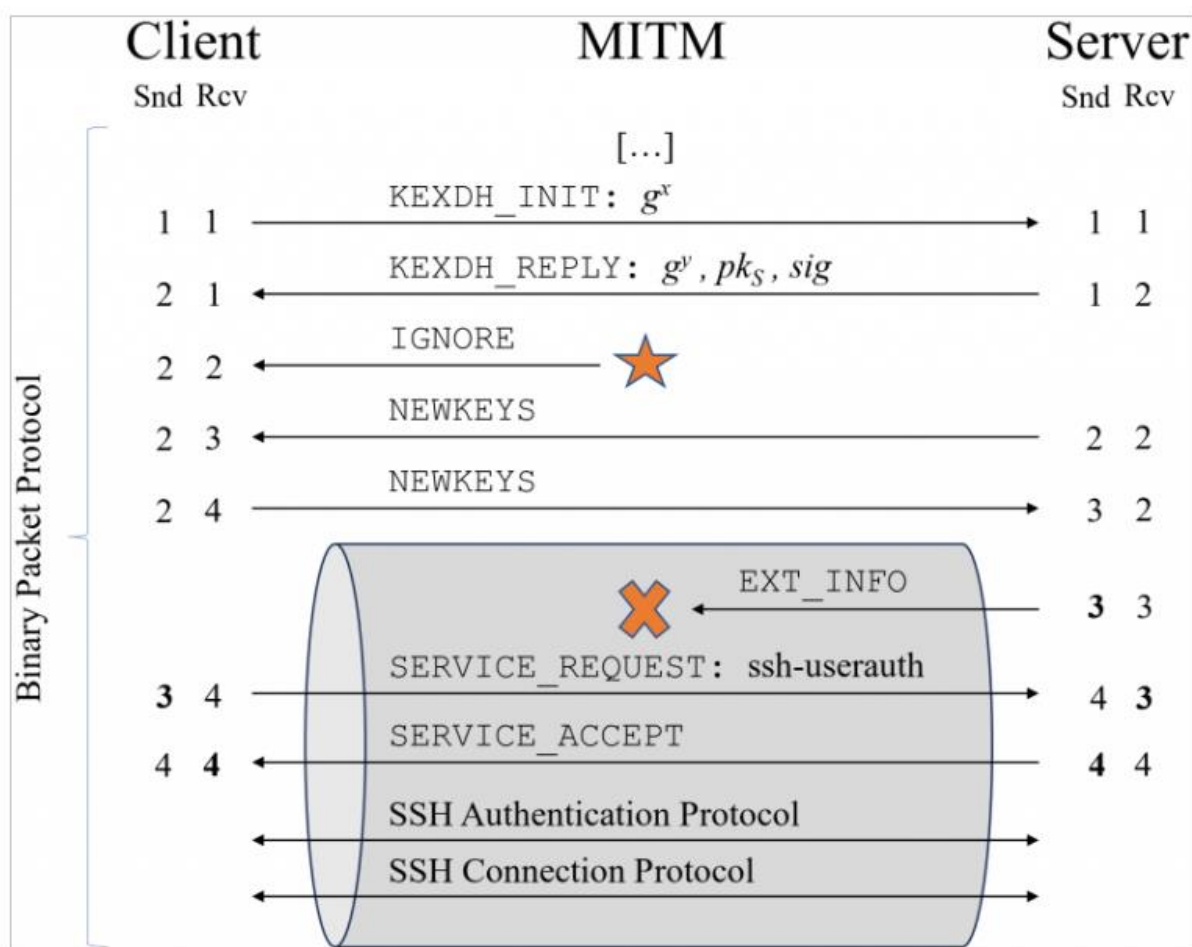
A Terrapin attack lowers the security of the established connection by truncating important negotiation messages without the client or server noticing it.

Researchers from the Ruhr University Bochum developed the Terrapin attack and also discovered exploitable implementation flaws in AsyncSSH.

The weaknesses and flaws associated with the attack are now identified as CVE-2023-48795, CVE-2023-46445 and CVE-2023-46446.

One thing to note about Terrapin is that the attackers need to be in an adversary-in-the-middle (MiTM) position at the network layer to intercept and modify the handshake exchange, and the connection must be secured by either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC.

The data in the messages exchanged after the completion of the handshake determines the severity of the attack's repercussions.



*Terrapin attack overview*

Despite the specific requirements for Terrapin, the extensive adoption of the mentioned encryption modes (scans show 77%) makes the attack feasible in a real-world scenario.

*"The Terrapin attack exploits weaknesses in the SSH transport layer protocol in combination with newer cryptographic algorithms and encryption modes introduced by OpenSSH over 10 years ago," say the researchers, adding that "these have been adopted by a wide range of SSH implementations, therefore affecting a majority of current implementations."*

Multiple vendors are gradually mitigating the security problem. One solution is to implement a strict key exchange that makes package injection during the handshake unattainable.

However, it will take a while for such an issue to be addressed universally and the researchers note that the strict key exchange countermeasure is only effective when implemented on both the client and the server.

The team has published a Terrapin vulnerability scanner on GitHub, which admins can use to determine if an SSH client or server is vulnerable to the attack.

*Terrapin is not a simple software bug that can be fixed with an update to a single library or component. Instead, clients and servers need to be updated to protect the connection against prefix truncation attacks. - Ruhr University Bochum*

Right now, the biggest mitigation factor for the attack is the MiTM requirement, which makes Terrapin a less severe threat. For this reason, patching CVE-2023-48795 may not be a priority in many cases.

More details about the Terrapin attack are available in the technical whitepaper released by the German researchers.

Source: <https://www.bleepingcomputer.com/news/security/terrapin-attacks-can-downgrade-security-of-openssh-connections>/<https://www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/>

## 12. Interpol operation arrests 3,500 cybercriminals, seizes \$300 million



An international law enforcement operation codenamed 'Operation HAECHI IV' has led to the arrest of 3,500 suspects of various lower-tier cybercrimes and seized \$300 million in illicit proceeds.

The South Korean authorities led HAECHI operations and worked with law enforcement agencies from 34 countries, including the United States, the United Kingdom, Japan, Hong Kong (China), and India.

The latest operation, which occurred between July and December 2023, targeted threat actors engaging in voice phishing, romance scams, online sextortion, investment fraud, money laundering associated with illegal online gambling, business email compromise, and e-commerce fraud.

In addition, Interpol's financial intelligence mechanism, I-GRIP, flagged and froze 82,112 bank accounts in 34 countries linked to various cybercrimes and fraudulent operations.

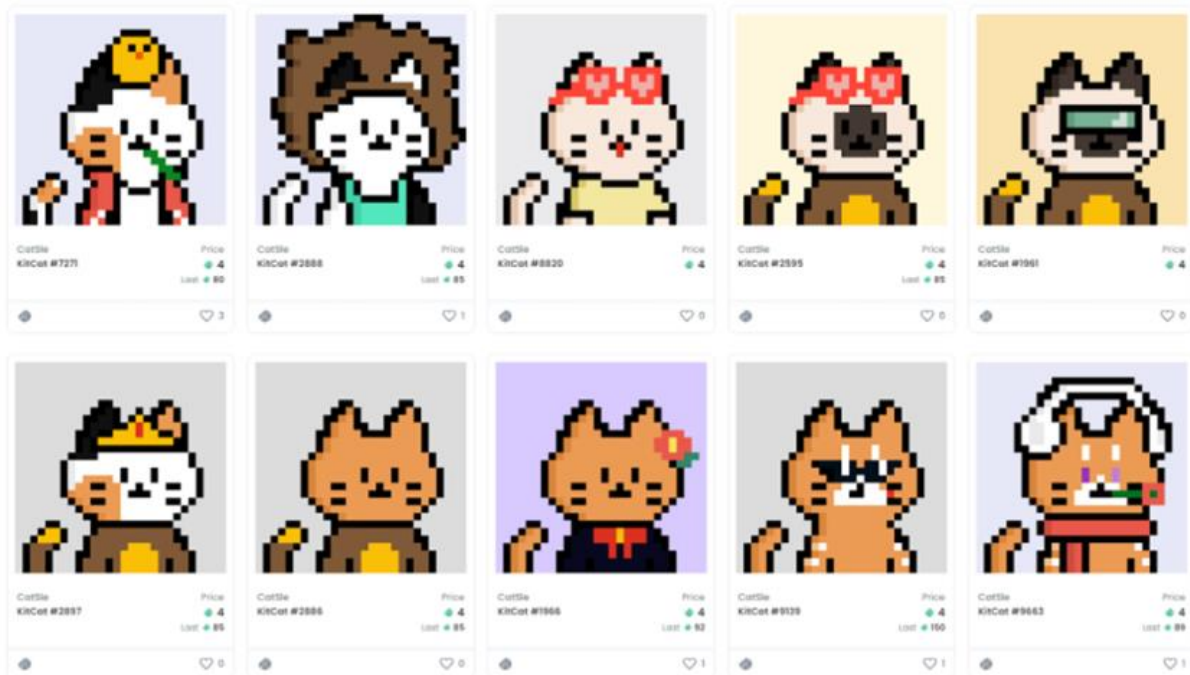
\$199 million of the seized amounts concern hard currency, and the remaining \$101 million corresponds to the value of 367 digital/virtual assets, such as NFTs (non-fungible tokens) linked to cybercrime.

*"The seizure of USD 300 million represents a staggering sum and clearly illustrates the incentive behind today's explosive growth of transnational organized crime," stated Interpol's Stephen Kavanagh.*

*"This vast accumulation of unlawful wealth is a serious threat to global security and weakens the economic stability of nations worldwide."*

A highlighted arrest that occurred during this operation concerns an online gambling criminal in Manila, whom the Korean police have been hunting for over two years.

A trend that emerged from HAECHI arrests concerns digital investment frauds and NFT investment platforms that operate for a short time before they "rug pull," which is to steal all investment money, delete official sites and social media handles, and disappear.



*NFTs linked to scam platforms  
Source: Interpol*

Another emerging scam tool is AI and deep fake tools to generate synthetic content that appears realistic to the targets or even the voice of a person close to them.

The UK authorities participating in HAECHI reported the disruption of several cases where fraudsters leveraged AI in impersonation scams, online sexual blackmail, and investment fraud.

Unfortunately, AI technology gives the edge to cybercriminals at this point in time, but Interpol continually refines its tactics to keep up with emerging trends and tackle the threats.

The HAECHI IV operation saw a 260% increase in arrests compared to HAECHI III, which occurred between June and November 2022.

Interpol and its partners arrested 975 suspects during that operation and froze \$130,000,000.

Source: <https://www.bleepingcomputer.com/news/security/interpol-operation-arrests-3-500-cybercriminals-seizes-300-million/>



### 13. BlackCat Ransomware Raises Ante After FBI Disruption

The **U.S. Federal Bureau of Investigation** (FBI) disclosed today that it infiltrated the world's second most prolific ransomware gang, a Russia-based criminal group known as **ALPHV** and **BlackCat**. The FBI said it seized the gang's darknet website, and released a decryption tool that hundreds of victim companies can use to recover systems. Meanwhile, BlackCat responded by briefly "unseizing" its darknet site with a message promising 90 percent commissions for affiliates who continue to work with the crime group, and open season on everything from hospitals to nuclear power plants.



*A slightly modified version of the FBI seizure notice on the BlackCat darknet site (Santa caps added).*

Whispers of a possible law enforcement action against BlackCat came in the first week of December, after the ransomware group's darknet site went offline and remained unavailable for roughly five days. BlackCat eventually managed to bring its site back online, blaming the outage on equipment malfunctions.

But earlier today, the BlackCat website was replaced with an FBI seizure notice, while federal prosecutors in Florida released a search warrant explaining how FBI agents were able to gain access to and disrupt the group's operations.

A statement on the operation from the **U.S. Department of Justice** says the FBI developed a decryption tool that allowed agency field offices and partners globally to offer more than 500 affected victims the ability to restore their systems.

"With a decryption tool provided by the FBI to hundreds of ransomware victims worldwide, businesses and schools were able to reopen, and health care and emergency services were able to come back online," **Deputy Attorney General Lisa O. Monaco** said. "We will



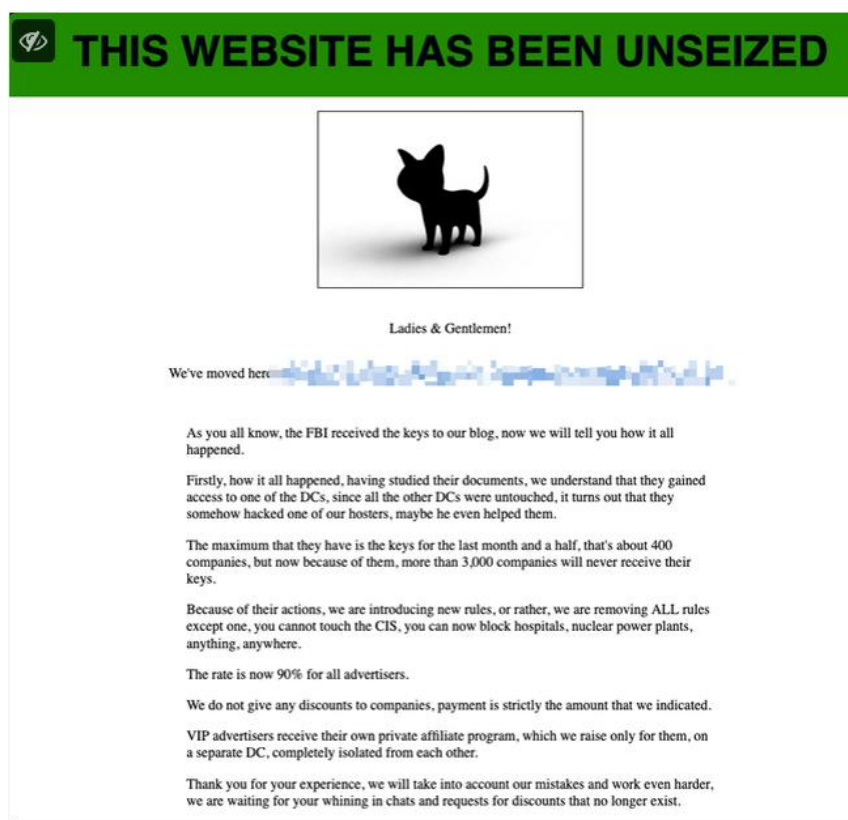
continue to prioritize disruptions and place victims at the center of our strategy to dismantle the ecosystem fueling cybercrime.”

The DOJ reports that since BlackCat’s formation roughly 18 months ago, the crime group has targeted the computer networks of more than 1,000 victim organizations. BlackCat attacks usually involve encryption and theft of data; if victims refuse to pay a ransom, the attackers typically publish the stolen data on a BlackCat-linked darknet site.

BlackCat formed by recruiting operators from several competing or disbanded ransomware organizations — including REvil, BlackMatter and DarkSide. The latter group was responsible for the Colonial Pipeline attack in May 2021 that caused nationwide fuel shortages and price spikes.

Like many other ransomware operations, BlackCat operates under the “ransomware-as-a-service” model, where teams of developers maintain and update the ransomware code, as well as all of its supporting infrastructure. Affiliates are incentivized to attack high-value targets because they generally reap 60-80 percent of any payouts, with the remainder going to the crooks running the ransomware operation.

BlackCat was able to briefly regain control over their darknet server today. Not long after the FBI’s seizure notice went live the homepage was “unseized” and retrofitted with a statement about the incident from the ransomware group’s perspective.



*The message that was briefly on the homepage of the BlackCat ransomware group this morning. Image: @GossiTheDog.*

BlackCat claimed that the FBI's operation only touched a portion of its operations, and that as a result of the FBI's actions an additional 3,000 victims will no longer have the option of receiving decryption keys. The group also said it was formally removing any restrictions or discouragement against targeting hospitals or other critical infrastructure.

*"Because of their actions, we are introducing new rules, or rather, we are removing ALL rules except one, you cannot touch the CIS [a common restriction against attacking organizations in Russia or the Commonwealth of Independent States]. You can now block hospitals, nuclear power plants, anything, anywhere."*

The crime group also said it was setting affiliate commissions at 90 percent, presumably to attract interest from potential affiliates who might otherwise be spooked by the FBI's recent infiltration. BlackCat also promised that all "advertisers" under this new scheme would manage their affiliate accounts from data centers that are completely isolated from each other.

BlackCat's darknet site currently displays the FBI seizure notice. But as BleepingComputer founder **Lawrence Abrams** explained on Mastodon, both the FBI and BlackCat have the private keys associated with the Tor hidden service URL for BlackCat's victim shaming and data leak site.

*"Whoever is the latest to publish the hidden service on Tor (in this case the BlackCat data leak site), will resume control over the URL," Abrams said.  
"Expect to see this type of back and forth over the next couple of days."*

The DOJ says anyone with information about BlackCat affiliates or their activities may be eligible for up to a \$10 million reward through the State Department's "Rewards for Justice" program, which accepts submissions through a Tor-based tip line (visiting the site is only possible using the Tor browser).

Source: <https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/>

## 14. New phishing attack steals your Instagram backup codes to bypass 2FA



A new phishing campaign pretending to be a 'copyright infringement' email attempts to steal the backup codes of Instagram users, allowing hackers to bypass the two-factor authentication configured on the account.

Two-factor authentication is a security feature that requires users to enter an additional form of verification when logging into the account. This verification is usually in the form of one-time passcodes sent via SMS text message, codes from an authentication app, or through hardware security keys.

Using 2FA helps protect your accounts if your credentials are stolen or purchased from a cybercrime marketplace, as the threat actor would need access to your mobile device or email to log into your protected account.

When configuring two-factor authentication on Instagram, the site will also provide eight-digit backup codes that can be used to regain access to accounts if you cannot verify your account using 2FA. This could happen for multiple reasons, such as switching your mobile number, losing your phone, and losing access to your email account.

However, backup codes come with some risk, as if a threat actor can steal those codes, they can hijack Instagram accounts using unrecognized devices simply by knowing the target's credentials, which can be stolen through phishing or found in unrelated data breaches.

Copyright infringement phishing messages claim the recipient has posted something that violates intellectual property protection laws, and hence, their account has been restricted.

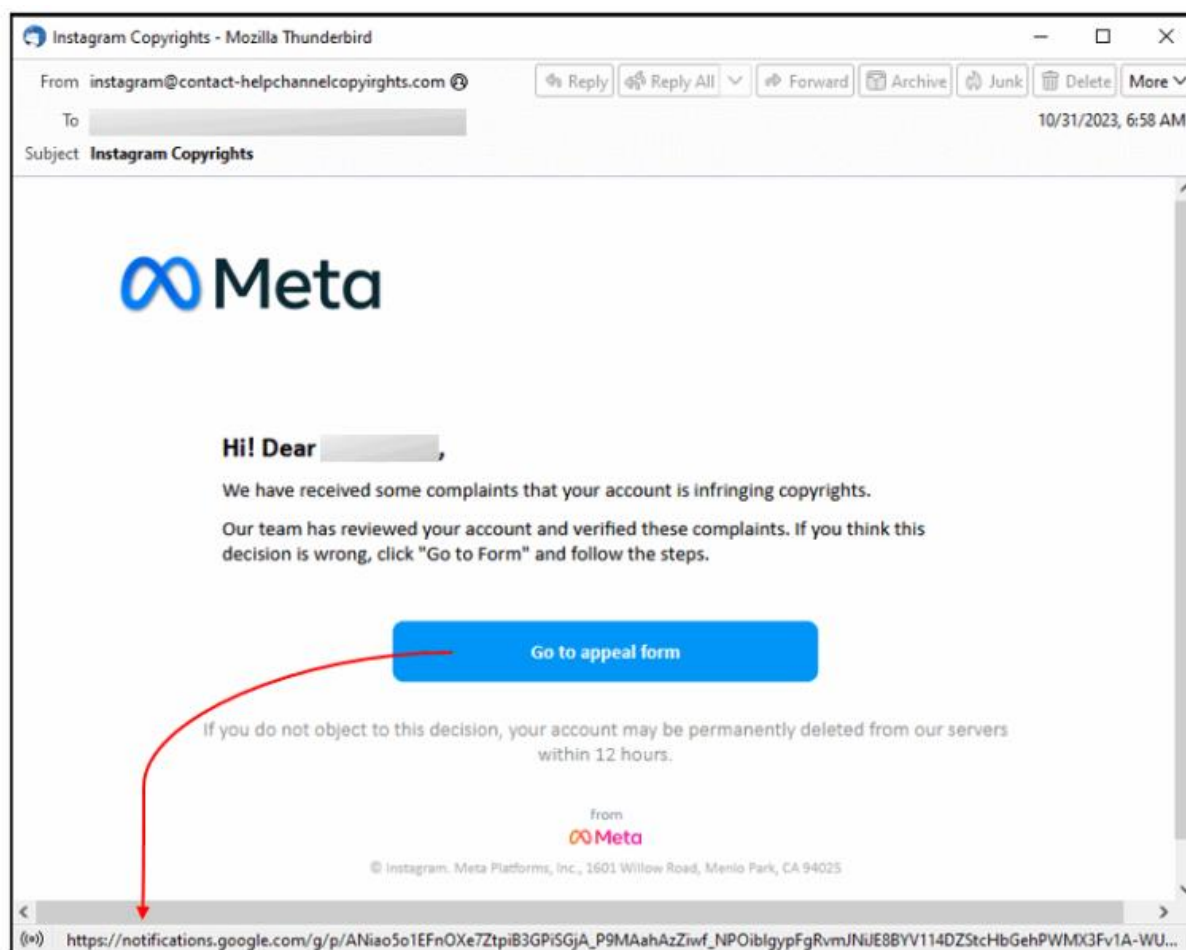
Recipients of these messages are urged to click a button to appeal the decision, which redirects them to phishing pages where they enter their account credentials and other details.

The same theme has been used several times, including against Facebook users, and has facilitated infection chains for the LockBit ransomware and the BazaLoader malware, among others.

## New Instagram phishing campaign

The latest variant of these attacks was spotted by Trustwave analysts, who report that the increasing adoption rate of 2FA protection pushes phishing actors to broaden their targeting scope.

The latest phishing emails impersonate Meta, Instagram's parent company, warning that Instagram users received copyright infringement complaints. The email then prompts the user to fill out an appeal form to resolve the issue.

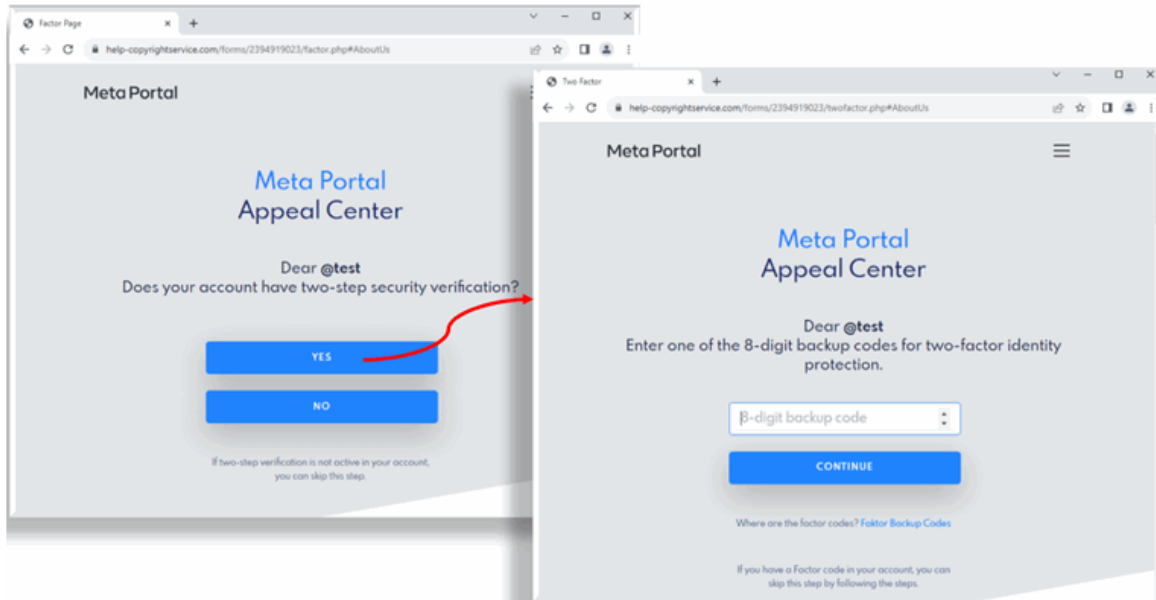


*Phishing email (Trustwave)*

Clicking the button takes the target to a phishing site impersonating Meta's actual violations portal, where the victim clicks a second button labeled "Go to Confirmation Form (Confirm My Account)."

The second button redirects to another phishing page designed to appear as Meta's "Appeal Center" portal, where the victims are requested to enter their username and password (twice).

After siphoning these details, the phishing site asks the target if their account is protected by 2FA and, upon confirmation, requests the 8-digit backup code.



*Phishing the account's backup codes (Trustwave)*

Despite the campaign being characterized by multiple signs of fraud, like the sender's address, the redirection page, and phishing page URLs, the convincing design and sense of urgency could still trick a significant percentage of targets into giving away their account credentials and backup codes.

Backup codes are meant to be kept private and stored securely. Account holders should treat them with the same level of secrecy as their passwords and refrain from entering them anywhere unless necessary for accessing their accounts.

If you still have access to your 2FA codes/keys, there's never a reason to enter your backup codes anywhere other than within the Instagram website or app.

Source: <https://www.bleepingcomputer.com/news/security/new-phishing-attack-steals-your-instagram-backup-codes-to-bypass-2fa/>



## 15. Android malware Chameleon disables Fingerprint Unlock to steal PINs



The Chameleon Android banking trojan has re-emerged with a new version that uses a tricky technique to take over devices — disable fingerprint and face unlock to steal device PINs.





It does this by using an HTML page trick to acquire access to the Accessibility service and a method to disrupt biometric operations to steal PINs and unlock the device at will.

Earlier versions of Chameleon spotted in April this year impersonated Australian government agencies, banks, and the CoinSpot cryptocurrency exchange, performing keylogging, overlay injection, cookie theft, and SMS theft on compromised devices.

Researchers at ThreatFabric, who have been following the malware, report that it is currently distributed via the Zombinder service, posing as Google Chrome.

Zombinder "glues" malware to legitimate Android apps so that victims can enjoy the full functionality of the app they intended to install, making it less likely to suspect that dangerous code is running in the background.

The platform claims its malicious bundles are undetectable in runtime, bypassing Google Protect alerts and evading any anti-virus products running on the infected device.

Icon / App name / Package name	Malware family	Malware variant	Malware types
 Chrome (Z72645c414ce232f45.Z35aad4dde2ff09b48) 2211c48a4ace970e0a9b3da75ac246bd9abaaaf4f0806ec32401589856ea2434	Chameleon	Chameleon.B	Banker
 Chrome (qWQCnKxHcb4762ce6c5c584085f9d70.qWQCnKxHcc4d1... c892786de2f7a8b6ccf6c48cdc6fb39234feb988ac9b9d1de3eccf8ee61ea147	Chameleon	Chameleon.B	Banker
 Chrome (cTfoGw1db1eada1946a0e4cae.cTfoGwba06e365976c568... a27170030cecd641d0ed2d7ede87b4d0c5b469d47a8cf611372376e0bd3344dd	Chameleon	Chameleon.B	Banker
 Chrome (FIdce47ff6d0098ccb8c97.FI30efa7256a963112de8d) 2d05a21d944038ef00837f0c89e8dad695f5d7daddd249c3f7884323931a6f84	Chameleon	Chameleon.B	Banker

*Chameleon-carrying APKs posing as Google Chrome (ThreatFabric)*

## New Chameleon features

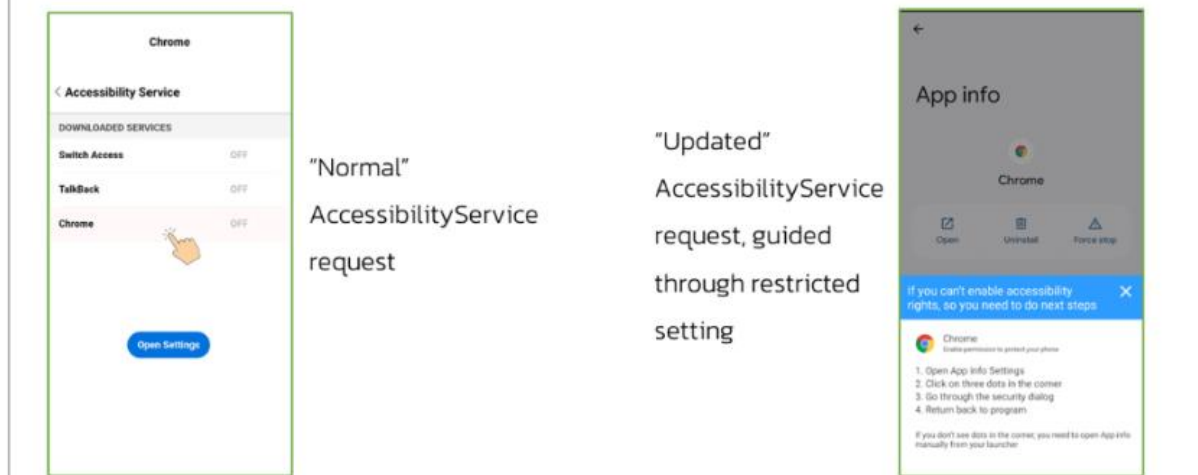
The first new feature seen in the latest Chameleon variant is the ability to display an HTML page on devices running Android 13 and later, prompting victims to give the app permission to use the Accessibility service.

Android 13 and later are protected by a security feature called "Restricted setting," which blocks the approval of dangerous permissions like Accessibility, which malware can leverage to steal on-screen content, grant itself additional permissions, and perform navigation gestures.

When Chameleon detects Android 13 or 14 upon launch, it loads an HTML page that guides the user through a manual process to enable Accessibility for the app, bypassing the system's protection.

## Android 13: HTML Prompt

Guides users through a detailed step-by-step process via an HTML page to enable AccessibilityService within Restricted Settings



*Chameleon's HTML page prompt (ThreatFabric)*

The second notable new feature is the ability to interrupt biometric operations on the device, like fingerprint and face unlock, by using the Accessibility service to force a fallback to PIN or password authentication.

The malware captures any PINs and passwords the victim enters to unlock their device and can later use them to unlock the device at will to perform malicious activities hidden from view.

```
public final void interruptBiometric(AccessibilityEvent accessibilityEvent0) {
    if (accessibilityEvent0.getPackageName() != null) {
        if (bCBFNOgmB2372b7065b5f58f8f9f.screenstatus != 1 && (KeyguardManager != null && (KeyguardManager.isKeyguardSecure())) {
            if (getInstance().findViewById<View>(getInstance().getRootInActiveWindow(), "lockPatternView") != null) {
                return;
            }
            if (getInstance().findViewById<View>(getInstance().getRootInActiveWindow(), "pinEntry") != null) {
                return;
            }
            if (getInstance().findViewById<View>(getInstance().getRootInActiveWindow(), "passwordEntry") != null) {
                return;
            }
        }
    }
}
```

*Java code snippet disrupting the biometric service on Android (ThreatFabric)*

Finally, ThreatFabric reports that Chameleon has added task scheduling through the AlarmManager API to manage the periods of activity and define the type of activity.

Depending on whether Accessibility is enabled or disabled, the malware adapts to launching overlay attacks or performing app usage data collection to decide on the best moment for injection.

*"These enhancements elevate the sophistication and adaptability of the new Chameleon variant, making it a more potent threat in the ever-evolving landscape of mobile banking trojans," warns ThreatFabric.*

To keep the Chameleon threat at bay, avoid sourcing APKs (Android package files) from unofficial sources, as this is the primary distribution method for the Zombinder service.

Additionally, ensure that Play Protect is enabled at all times, and run regular scans to ensure your device is clean of malware and adware.

Source: <https://www.bleepingcomputer.com/news/security/android-malware-chameleon-disables-fingerprint-unlock-to-steal-pins/>

## 16. Lapsus\$ hacker behind GTA 6 leak gets indefinite hospital sentence



Lapsus\$ cybercrime and extortion group member, Arion Kurtaj has been sentenced indefinitely in a 'secure hospital' by a UK judge.

Kurtaj who is 18 years of age and autistic is among the primary Lapsus\$ threat actors, and was involved in the leak of assets associated with the video game, Grand Theft Auto VI.

### Sentenced indefinitely in a 'secure hospital'

Arion Kurtaj, a member of the Lapsus\$ cybercrime group, was sentenced indefinitely in a "secure hospital" by a British judge, according to a BBC report.

Kurtaj, an Oxford resident, served as a key Lapsus\$ member who leaked clips from Rockstar Games' upcoming video game, Grand Theft Auto VI.

According to the judge, Kurtaj continued to be a "high risk" to the public given his abilities and desire to commit cybercrime.

As such, unless and until doctors clear him of no longer posing a danger, he shall remain at a secure hospital.

In addition to the hacker's involvement in cybercriminal activity, the court heard that the hacker had been violent while in custody leading to "dozens of reports of injury or property damage."

Because of his autism, healthcare professionals had deemed Kurtaj unfit to stand trial, deferring it to the jury to decide whether his alleged acts were committed with criminal intent.

The BBC reported that a mental health assessment conducted in conjunction with the sentencing hearing determined that Kurtaj remains highly motivated to "return to cyber-crime as soon as possible."

In the same trial spanning six weeks, another 17-year-old Lapsus\$ member (unnamed due to legal reasons), has been deemed guilty at Southwark Crown Court, London.

The unnamed minor collaborated with Kurtaj and other gang members to breach tech giants NVIDIA and telcos including BT/EE, before attempting to extort them for a \$4 million ransom that was not paid. The minor has been sentenced in a Youth Rehabilitation Order for 18 months with rigorous supervision in place, and a "ban on using VPNs online."

Previously, Kurtaj was "caught red handed" circumventing his bail conditions, state the prosecutors, when his hotel room TV was found with an Amazon Fire Stick that let him connect to cloud computing services with his smartphone, keyboard, and mouse. That's how he was able to conduct the GTA 6 leak, despite having his laptop confiscated.

Believed to be one of the leaders of the group, Arion Kurtaj was arrested twice in 2022, first in January and then again in March, in connection with Lapsus\$ hacking activity.

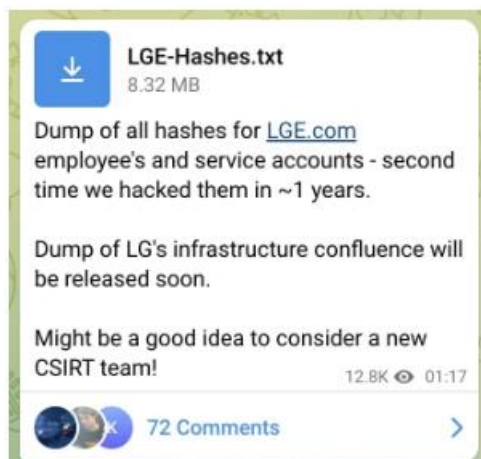
### **Lapsus\$: hacking high-profile names**

Although the Lapsus\$ gang purportedly comprises teenagers, it may be naïve to underestimate their abilities or the threat posed by the group to an organization's cyber infrastructure.

Lapsus\$ cybercrime gang has previously taken responsibility for high-profile cyberattacks—ranging from the one at Okta to Uber to fintech giant Revolut as well as the attack concerning Microsoft's internal Azure server through which the group allegedly leaked 37 GB of stolen source code for Bing, Cortana, and other Microsoft projects.

The group has also previously claimed to have breached LG Electronics (LGE) for a "second time" in a year.





*Lapsus\$ says it also breached LG Electronics (BleepingComputer)*

BleepingComputer had been unable to confirm the claim at the time and had reached out to LG.

Lapsus\$ has previously leaked gigabytes of proprietary data purportedly stolen from leading companies such as Samsung, NVIDIA, and Mercado Libre.

Data extortion groups like Lapsus\$ breach victims, but as opposed to encrypting confidential files like a ransomware operator would, these actors steal and hold on to victims' proprietary data, and publish it should their extortion demands not be met.

Source: <https://www.bleepingcomputer.com/news/security/lapsus-hacker-behind-gta-6-leak-gets-indefinite-hospital-sentence/>

## 17. Fake VPN Chrome extensions force-installed 1.5 million times



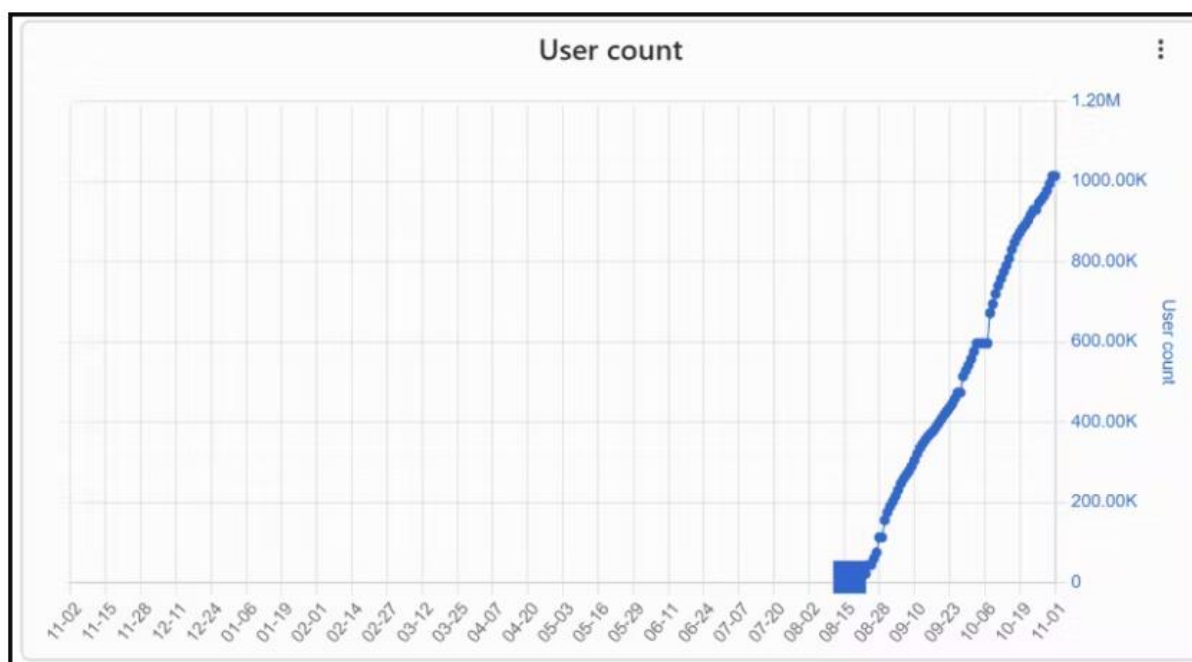
Three malicious Chrome extensions posing as VPN (Virtual Private Networks) infected were downloaded 1.5 million times, acting as browser hijackers, cashback hack tools, and data stealers.

According to ReasonLabs, which discovered the malicious extensions, they are spread via an installer hidden in pirated copies of popular video games like Grand Theft Auto, Assassins Creed, and The Sims 4, which are distributed from torrent sites.

ReasonLabs notified Google of its findings, and the tech giant removed the offending extensions from the Chrome Web Store, but only after those had amassed a total of 1.5 million downloads.

Specifically, the malicious extensions were netPlus (1 million installs), netSave, and netWin (500,000 installs).

Most infections are in Russia and countries like Ukraine, Kazakhstan, and Belarus, so the campaign appears to target Russian-speaking users.



*netPlus infections over time (ReasonLabs)*

## Planting fake VPN extensions

ReasonLabs discovered over a thousand distinct torrent files that deliver the malicious installer file, which is an electron app measuring between 60MB and 100MB in size.

The installation of the VPN extensions is automatic and forced, taking place on the registry level, and does not involve the user or require any action on the victim's side.

Eventually, the installer checks for antivirus products on the infected machine, then drops netSave on Google Chrome and netPlus on Microsoft Edge, covering either use case.

```
function t() {
  this.list = [{
    id: "a1",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\AVAST Software\\Avast",
    detected: !1
  }, {
    id: "a2",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Avg",
    detected: !1
  }, {
    id: "a3",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Avira\\SoftwareUpdater",
    detected: !1
  }, {
    id: "a4",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\360TotalSecurity\\DriverUpdater",
    detected: !1
  }, {
    id: "a5",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Doctor Web\\Bases",
    detected: !1
  }, {
    id: "a6",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Panda Security",
    detected: !1
  }, {
    id: "a7",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Microsoft\\Windows Defender",
    detected: !1
  }, {
    id: "a8",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\IObit\\IObit Malware Fighter",
    detected: !1
  }, {
    id: "a9",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\McAfee\\MCL0GS",
    detected: !1
  }, {
    id: "a10",
    directory: process.env.USERPROFILE + "\\AppData\\Local\\Kaspersky Lab\\AVP20.0",
    detected: !1
  }
];
}
```

#### **AV check** (ReasonLabs)

The malicious extensions use a realistic VPN user interface with some functionality and a paid subscription option to create a sense of authenticity.

Code analysis shows that the extension also has access to "tabs," "storage," "proxy," "webRequest," "webRequestBlocking," "declarativeNetRequest," "scripting," "alarms," "cookies," "activeTab," "management," and "offscreen."

ReasonLabs points out that the abuse of the 'offscreen' permission enables the malware to run scripts through the Offscreen API and stealthily interact with the web page's current DOM (Document Object Model).

This extensive access to the DOM enables the extensions to steal sensitive user data, perform browsing hijacks, manipulate web requests, and even disable other extensions installed on the browser.

Another function of the extension is to disable other cashback and coupon extensions to eliminate competition on the infected device and redirect profits to the attackers.

ReasonLabs reports the malware targets over 100 cashback extensions, including Avast SafePrice, AVG SafePrice, Honey: Automatic Coupons & Rewards, LetyShops, Megabonus, AliRadar Shopping Assistant, Yandex.Market Adviser, ChinaHelper, and Backlit.

The extensions' communication with the C2 (command and control) servers involves data exchange concerning instructions and commands, IDing the victim, exfiltrating sensitive data, and more.

This report highlights the massive security issues around web browser extensions, many of which are highly obfuscated to make it harder to determine what behavior they exhibit.

For this reason, you should routinely check the extensions installed in your browser and check for new reviews in the Chrome Web Store to see if others are reporting malicious behavior.

Source: <https://www.bleepingcomputer.com/news/security/fake-vpn-chrome-extensions-force-installed-15-million-times/https://www.bleepingcomputer.com/news/security/mysql-servers-targeted-by-ddostf-ddos-as-a-service-botnet/>

## 18. Europol warns 443 online shops infected with credit card stealers



Europol has notified over 400 websites that their online shops have been hacked with malicious scripts that steal debit and credit cards from customers making purchases.

Skimmers are small snippets of JavaScript code added to checkout pages or loaded from a remote resource to evade detection. They are designed to intercept and steal payment card numbers, expiration dates, verification numbers, names, and shipping addresses and then upload the information to the attackers' servers.

Threat actors use the stolen data to perform unauthorized transactions, such as online purchases, or resell them to other cybercriminals on dark web marketplaces.

These attacks can go undetected for weeks or even several months, and depending on the popularity of the breached e-commerce platforms, cybercriminals can collect large numbers of payment card details.

Coordinated by Europol and spearheaded by Greece, a two-month international operation involving law enforcement from 17 countries and private entities such as Group-IB and Sansec identified skimmer infections on 443 websites.

*"With the support of national Computer Security Incident Response Teams (CSIRT), the two-month action has enabled Europol and its partners to notify 443 online merchants that their customers' credit card or payment card data had been compromised," explained Europol.*

Additional details shared by Group-IB reveal that the operation unearthed 23 distinct families of JavaScript sniffers, including ATMZOW, health\_check, FirstKiss, FakeGA, AngryBeaver, Inter, and R3nin.

The above families are known for elusive behavior, such as abusing Google Tag Manager to update their malicious code snippets and mimicking Google Analytics code to dodge detection during website code inspections.

For more information on the threat of digital skimming, online merchants are recommended to consult this guide from Europol.

This action comes at a critical moment as online shopping activity spikes during the holiday season.

Using digital payment methods or one-time private cards can help minimize the likelihood of having payment card details stolen.

It is also advisable to scrutinize credit card statements for unauthorized charges, which can help alert if a card has been compromised.

Source: <https://www.bleepingcomputer.com/news/security/europol-warns-443-online-shops-infected-with-credit-card-stealers>/<https://www.bleepingcomputer.com/news/security/darkgate-and-pikabot-malware-emerge-as-qakbots-successors/>



## 19. Nissan Australia cyberattack claimed by Akira ransomware gang



Today, the Akira ransomware gang claimed that it breached the network of Nissan Australia, the Australian division of Japanese car maker Nissan.

In a new entry added to the operation's data leak blog on December 22, Akira says that its operators allegedly stole around 100GB of documents from the automaker's systems.

The attackers have threatened to leak sensitive business and client data online, as ransom negotiations with Nissan failed after the company either refused to engage or pay the ransom.

*"They seem not to be very interested in the data, so we will upload it for you within a few days," the ransomware group says. "You will find docs with personal information of their employees in the archives and much other interested stuff like NDAs, projects, information about clients and partners etc."*

Akira surfaced in March 2023 and drew attention after quickly amassing a large number of victims from various industry sectors.

In June 2023, Akira ransomware operators started deploying a Linux variant of their encryptor designed to target VMware ESXi virtual machines widely used in enterprise environments.

According to negotiations seen by BleepingComputer, the ransomware group is asking for ransom payments from \$200,000 to millions of dollars, depending on the breached organization's size.

While another ransomware strain named Akira was released five years ago, in 2017, the two operations are unlikely to be related.

```
[ AKIRA ]
2023-12-22 | Nissan Australia | We've obtained 100 GB of data of Nissan Australia. They seem not
| | | to be very interested in the data, so we will upload it for you
| | | within a few days. You will find docs with personal information o
| | | f their employees in the archives and much other interested stuff
| | | like NDAs, projects, information about clients and partners etc.
| | | By the way, there is a notice on their website regarding investi
| | | gation about possible personal information leakage, so we will co
| | | nfirm that with the data uploading.
```

*Akira Nissan data leak entry (BleepingComputer)*

## Nissan still working to restore systems

While the company has yet to attribute a cyberattack disclosed on December 5, it did add a new update to its website today confirming that attackers have breached some of its systems in Australia and New Zealand.

Nissan says it's still investigating the incident's impact and whether personal information has been accessed. It's also working on restoring systems affected in the attack (a process that started on December 5, after the incident was disclosed).

*"We cannot yet confirm the extent of the cyber incident. We are working with our global incident response team and cybersecurity experts to investigate the incident as a matter of urgency," Nissan said.*

*"Some dealer systems will be impacted however, your local Nissan Dealership is operating. Please speak directly to your local Nissan dealer to assist with all vehicle and servicing queries."*

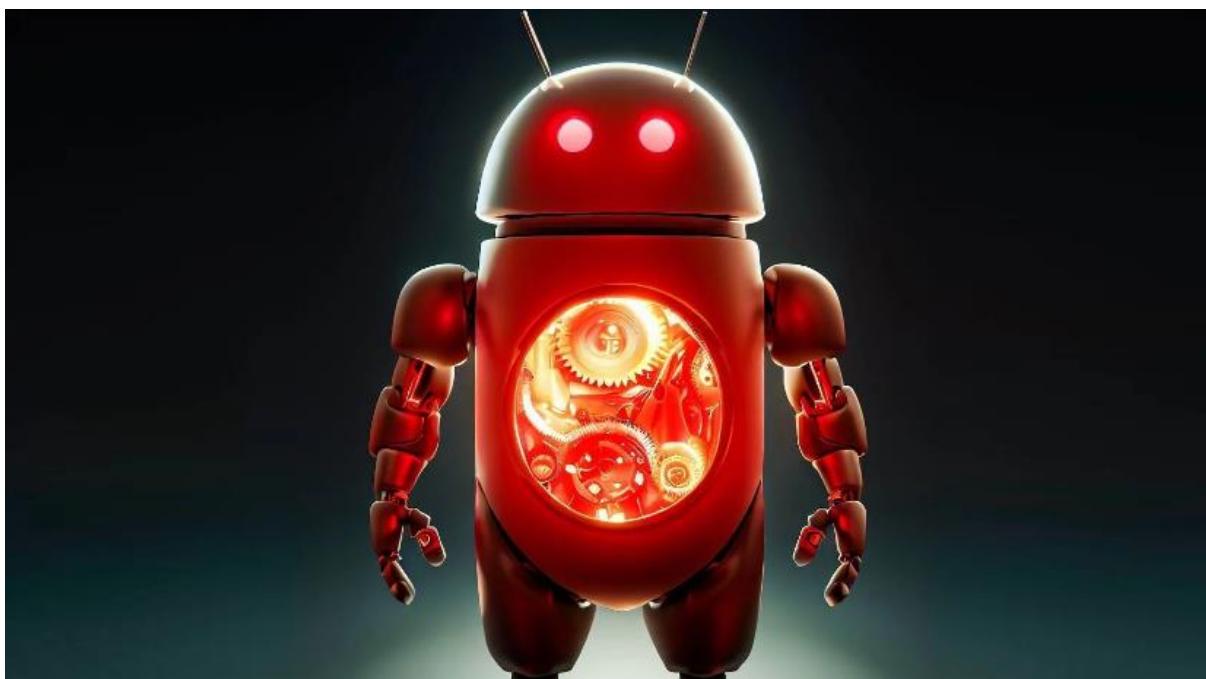
After detecting the breach, Nissan notified the Australian and the New Zealand Cyber Security Centres and relevant privacy regulators and law enforcement bodies.

Likely because of the risk that some data stored on the compromised systems was either accessed or stolen, Nissan also warned customers to "be vigilant for any unusual or suspicious online activity."

Nissan has yet to reply to a request for comment and additional information on the cyber incident from BleepingComputer.

Source: <https://www.bleepingcomputer.com/news/security/nissan-australia-cyberattack-claimed-by-akira-ransomware-gang/>

## 20. New Xamalicious Android malware installed 330k times on Google Play



A previously unknown Android backdoor named 'Xamalicious' has infected approximately 338,300 devices via malicious apps on Google Play, Android's official app store.

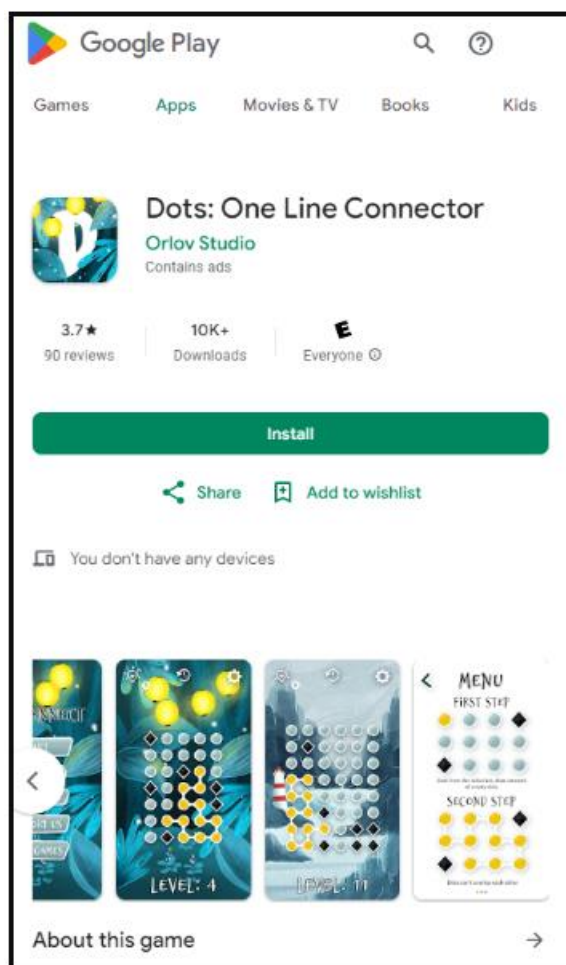
McAfee, a member of the App Defense Alliance, discovered 14 infected apps on Google Play, with three having 100,000 installs each.

Even though the apps have since been removed from Google Play, users who installed them since mid-2020 might still carry active Xamalicious infections on their phones, requiring manual scans and cleanup.

The most popular of the Xamalicious apps are the following:

- **Essential Horoscope for Android** – 100,000 installs
- **3D Skin Editor for PE Minecraft** – 100,000 installs
- **Logo Maker Pro** – 100,000 installs
- **Auto Click Repeater** – 10,000 installs
- **Count Easy Calorie Calculator** – 10,000 installs
- **Dots: One Line Connector** – 10,000 installs
- **Sound Volume Extender** – 5,000 installs

Also, a separate set of 12 malicious apps carrying the Xamalicious threat, for which download stats aren't available, are distributed on unofficial third-party app stores, infecting users via downloadable APK (Android package) files.



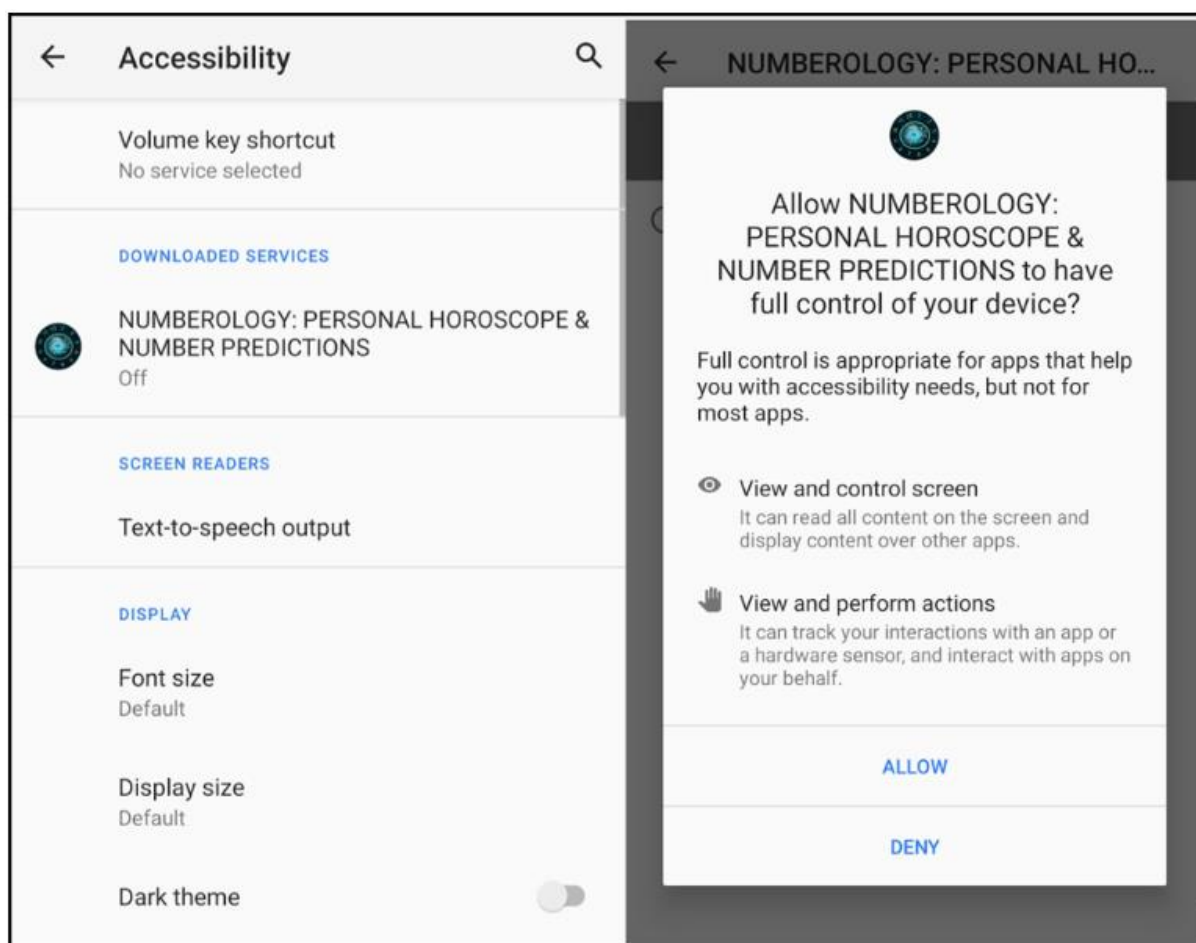
*Xamalicious game app on Google Play*  
Source: McAfee

According to McAfee's telemetry data, most infections were installed on devices in the United States, Germany, Spain, the U.K., Australia, Brazil, Mexico, and Argentina.

## The Xamalicious Android backdoor

Xamalicious is a .NET-based Android backdoor embedded (in the form of 'Core.dll' and 'GoogleService.dll') within apps developed using the open-source Xamarin framework, making the analysis of its code more challenging.

Upon installation, it requests access to the Accessibility Service, enabling it to perform privileged actions like navigation gestures, hide on-screen elements, and grant additional permissions to itself.

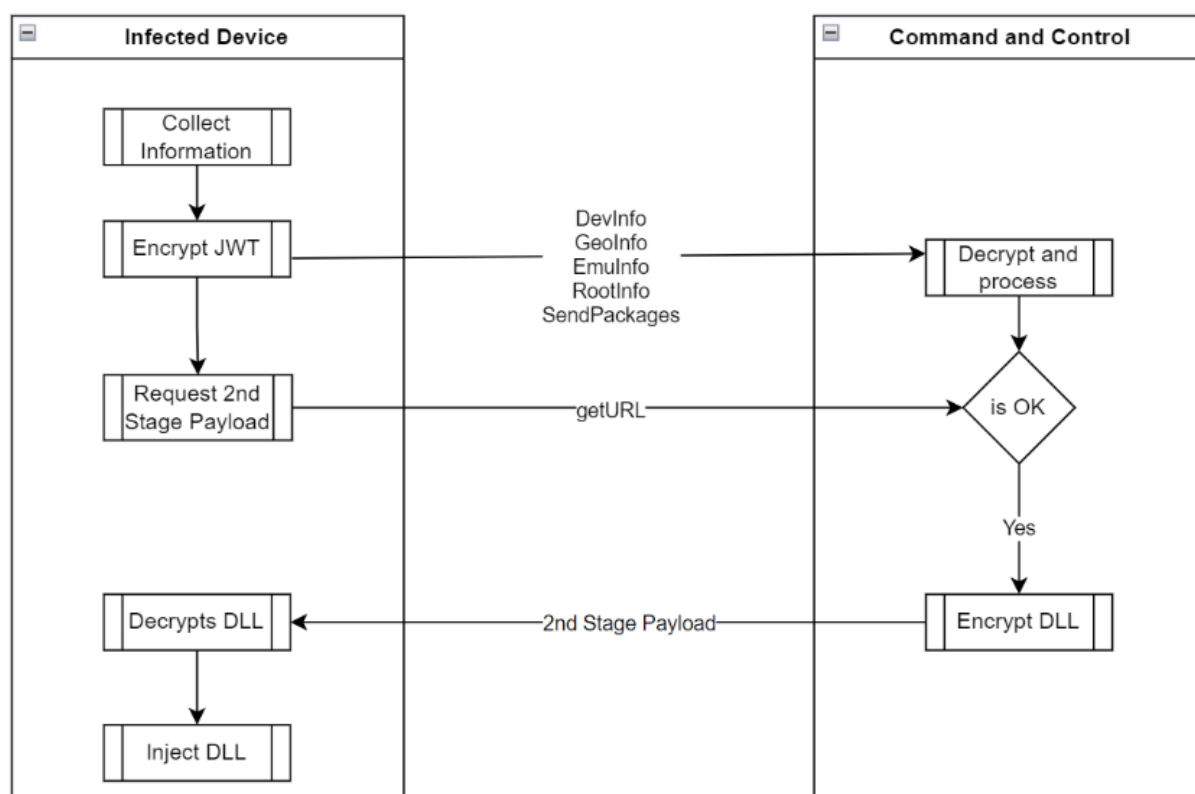


*Tricking users into approving Accessibility permission*

*Source: McAfee*

After installation, it communicates with the C2 (command and control) server to fetch the second-stage DLL payload ('cache.bin') if specific geographical, network, device configuration, and root status prerequisites are met.





*Data exchange with the C2 server*

*Source: McAfee*

The malware is capable of executing the following commands:

- **DevInfo:** Gathers device and hardware information, including Android ID, brand, CPU, model, OS version, language, developer options status, SIM details, and firmware.
- **GeoInfo:** Determines the device's geographic location using its IP address, collecting ISP name, organization, services, and a fraud score to detect non-genuine users.
- **EmulInfo:** Lists adbProperties to ascertain if the client is a real device or an emulator, checking CPU, memory, sensors, USB configuration, and ADB status.
- **RootInfo:** Identifies if the device is rooted using various methods and provides the rooting status.
- **Packages:** Lists all system and third-party apps installed on the device using system commands.
- **Accessibility:** Reports the status of accessibility services permissions.
- **GetURL:** Requests the second-stage payload from the C2 server by providing the Android ID and receives the status and potentially an encrypted assembly DLL.

McAfee has also found links between Xamalicious and an ad-fraud app called 'Cash Magnet,' which automatically clicks ads and installs adware on the victim's device to generate revenue for its operators.

Therefore, it's possible that Xamalicious also performs ad fraud on infected devices, diminishing processor performance and network bandwidth.

Although Google Play isn't immune to malware uploads, initiatives like the App Defense Alliance aim to detect and remove novel threats that appear on the app store, which isn't the case on unofficial and poorly moderated platforms.

Android users should avoid downloading apps from third-party sources, limit themselves to essential apps, thoroughly read user reviews before installation, and conduct a comprehensive background check on the app's developer/publisher to limit malware infections on their mobile devices.

Source: <https://www.bleepingcomputer.com/news/security/new-xamalicious-android-malware-installed-330k-times-on-google-play/>

## 21. Malware abuses Google OAuth endpoint to 'revive' cookies, hijack accounts



Multiple information-stealing malware families are abusing an undocumented Google OAuth endpoint named "MultiLogin" to restore expired authentication cookies and log into users' accounts, even if an account's password was reset.

Session cookies are a special type of browser cookie that contains authentication information, allowing a person to automatically log in to websites and services without entering their credentials.

These types of cookies are meant to have a limited lifespan, so they cannot be used indefinitely by threat actors to log into accounts if they are stolen.

In late November 2023, BleepingComputer reported on two information-stealers, namely Lumma and Rhadamanthys, who claimed they could restore expired Google authentication cookies stolen in attacks.

These cookies would allow the cybercriminals to gain unauthorized access to Google accounts even after the legitimate owners have logged out, reset their passwords, or their session has expired.

BleepingComputer has contacted Google multiple times over a month with questions about these claims and how they plan to mitigate the issue, but we never received a response.

## Exploiting Google OAuth endpoint

A report published today by CloudSEK researchers sheds more light on how this zero-day exploit works and paints a dire picture regarding the scale of its exploitation.

The exploit was first revealed by a threat actor named PRISMA on October 20, 2023, who posted on Telegram that they discovered a way to restore expired Google authentication cookies.

After reverse engineering the exploit, CloudSEK discovered it uses an undocumented Google OAuth endpoint named "MultiLogin," which is intended for synchronizing accounts across different Google services by accepting a vector of account IDs and auth-login tokens.

*"This request is used to set chrome accounts in browser in the Google authentication cookies for several google websites (e.g. youtube)," explains a description of the API endpoint in the Google Chrome source code.*

*"This request is part of Gaia Auth API, and is triggered whenever accounts in cookies are not consistent with accounts in browser," a variable in the source code further explains.*

CloudSEK says that information-stealing malware abusing this endpoint extracts tokens and account IDs of Chrome profiles logged into a Google account. This stolen information contains two crucial pieces of data: service (GAIA ID) and encrypted\_token.

The encrypted tokens are decrypted using an encryption stored in Chrome's 'Local State' file. This same encryption key is also used to decrypt saved passwords in the browser.

Using the stolen token:GAIA pairs with the MultiLogin endpoint, the threat actors can regenerate expired Google Service cookies and maintain persistent access on compromised accounts.

```

random rand = new Random();
foreach (string file in Directory.GetFiles(dirPath, "tokens.txt" SearchOption.AllDirectories))
{
    string[] tokens = File.ReadAllLines(file);
    foreach (string token in tokens)
    {
        bool flag = token == "";
        if (!flag)
        {
            HttpRequest req = new HttpRequest();
            req.IgnoreProtocolErrors = true;
            req.AddHeader("Accept", "/*/*");
            req.AddHeader("User-Agent", "com.google.Drive/6.0.230903 iSL/3.4 iPhone/15.7.4 hw/iPhone9_4 (gzip)");
            req.AddHeader("Authorization", "MultiBearer " + token);
            req.AddHeader("Accept-Language", "en-US,en;q=0.9");
            req.AddHeader("Content-Type", "application/x-www-form-urlencoded");
            try
            {
                string resp = req.Post("https://accounts.google.com/oauth/multilogin", new StringContent
                ("source=com.google.Drive"));
            }
        }
    }
}

```

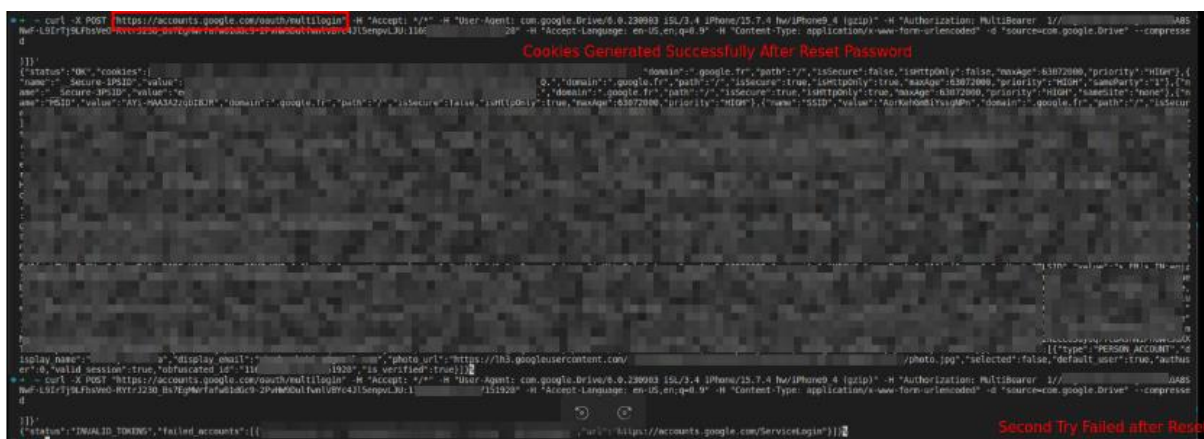
Folder with all Token:GAIA Id Pairs

Endpoint which is exploited

*Using token:GAIA pairs read from a text file to generate requests to MultiLogin*

*Source: CloudSEK*

In a discussion with CloudSek researcher Pavan Karthick, BleepingComputer was told they reverse-engineered the exploit and were able to use it to regenerate expired Google authentication cookies, as shown below.



Curl command and output showing successful cookie regeneration after a password reset.

*Successful cookie regeneration following password reset*

*Source: CloudSEK*

However, Karthick explained that the authentication cookie can only be regenerated once if a user resets their Google password. Otherwise, it can be regenerated multiple times, providing persistent access to the account.

## Malware devs rush to add exploit

Lumma stealer first adopted the exploit on November 14, whose developers applied blackboxing techniques such as encrypting the token:GAIA pair with private keys to hide the mechanism from competitors and prevent the replication of the feature.

Still, others were able to copy the feature or incorporate PRISMA's exploit into their stealers, with Rhadamanthys being the first to follow on November 17.

Since then, numerous other information stealers have adopted the exploit, including Stealc on December 1, Medusa on December 11, RisePro on December 12, and Whitesnake on December 26.

So, at least six info-stealers currently claim the ability to regenerate Google cookies using this API endpoint.

Threat intelligence firm Hudson Rock has also published the following video on YouTube, where a cybercriminal demonstrates how the cookie restoration exploit works.

A subsequent release by Lumma updated the exploit to counteract Google's mitigations, suggesting that the tech giant knows about the actively exploited zero-day flaw.

Specifically, Lumma turned to using SOCKS proxies to evade Google's abuse detection measures and implemented encrypted communication between the malware and the MultiLogin endpoint.

However, since Google hasn't confirmed the abuse of the MultiLogin endpoint, the status of the exploitation and its mitigation efforts remain unclear at this time.

Source: <https://www.bleepingcomputer.com/news/security/malware-abuses-google-oauth-endpoint-to-revive-cookies-hijack-accounts/>



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