



telelink  
business  
services

# Monthly Security Bulletin

A P R I L / 2 5



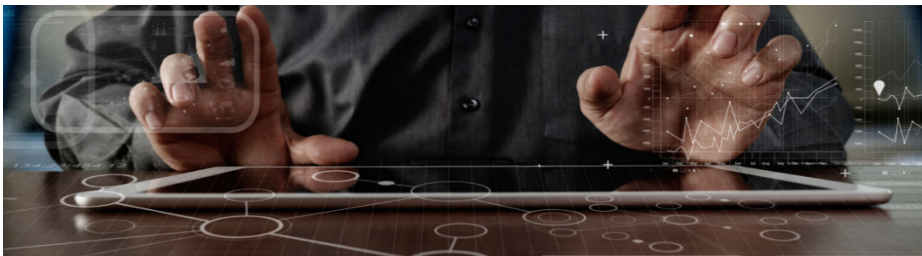
Advanced Security  
Operations Center

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

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

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

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



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

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

### LITE Plan

**425 EUR/mo**

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

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

### PROFESSIONAL Plan

**1225 EUR/mo**

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

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

### ADVANCED Plan

**2 575 EUR/mo**

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

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

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

### What is inside:

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

## Table of Contents

1.	Nearly 12,000 API keys and passwords found in AI training dataset .....	4
2.	Silk Typhoon hackers now target IT supply chains to breach networks .....	5
3.	Open-source tool 'Rayhunter' helps users detect Stingray attacks .....	7
4.	Ransomware gang encrypted network from a webcam to bypass EDR .....	8
5.	Critical PHP RCE vulnerability mass exploited in new attacks .....	10
6.	Silk Typhoon Hackers Indicted.....	11
7.	Cisco IOS XR vulnerability lets attackers crash BGP on routers .....	12
8.	ClickFix: How to Infect Your PC in Three Easy Steps .....	13
9.	New Akira ransomware decryptor cracks encryptions keys using GPUs .....	16
10.	Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts .....	18
11.	Critical RCE flaw in Apache Tomcat actively exploited in attacks .....	20
12.	New Windows zero-day exploited by 11 state hacking groups since 2017 .....	21
13.	New Arcane infostealer infects YouTube, Discord users via game cheats.....	24
14.	HellCat hackers go on a worldwide Jira hacking spree .....	27
15.	Critical GitHub Attack.....	29
16.	Critical Cisco Smart Licensing Utility flaws now exploited in attacks .....	29
17.	Veeam RCE bug lets domain users hack backup servers, patch now .....	30
18.	Microsoft Trusted Signing service abused to code-sign malware .....	31
19.	More Countries are Demanding Backdoors to Encrypted Apps .....	36
20.	Critical flaw in Next.js lets hackers bypass authorization .....	36
21.	New VanHelsing ransomware targets Windows, ARM, ESXi systems.....	37
22.	Report on Paragon Spyware .....	40
23.	AI Data Poisoning.....	41
24.	RedCurl cyberspies create ransomware to encrypt Hyper-V servers .....	42
25.	Oracle customers confirm data stolen in alleged cloud breach is valid.....	44
26.	Mozilla warns Windows users of critical Firefox sandbox escape flaw .....	45
27.	New Ubuntu Linux security bypasses require manual mitigations .....	46
28.	Microsoft's killing script used to avoid Microsoft Account in Windows 11 .....	48



## 1. Nearly 12,000 API keys and passwords found in AI training dataset

Close to 12,000 valid secrets that include API keys and passwords have been found in the Common Crawl dataset used for training multiple artificial intelligence models.

The Common Crawl non-profit organization maintains a massive open-source repository of petabytes of web data collected since 2008 and is free for anyone to use.

Because of the large dataset, many artificial intelligence projects may rely, at least in part, on the digital archive for training large language models (LLMs), including ones from OpenAI, DeepSeek, Google, Meta, Anthropic, and Stability.

### AWS root keys and MailChimp API keys

Researchers at Truffle Security - the company behind the TruffleHog open-source scanner for sensitive data, found valid secrets after checking 400 terabytes of data from 2.67 billion web pages in the Common Crawl December 2024 archive.

They discovered 11,908 secrets that authenticate successfully, which developers hardcoded, indicating the potential of LLMs being trained on insecure code.

It should be noted that LLM training data is not used in raw form and goes through a pre-processing stage that involves cleaning and filtering out unnecessary content like irrelevant data, duplicate, harmful, or sensitive information.

Despite such efforts, it is difficult to remove confidential data, and the process offers no guarantee for stripping such a large dataset of all personally identifiable information (PII), financial data, medical records, and other sensitive content.

After analyzing the scanned data, Truffle Security found valid API keys for Amazon Web Services (AWS), MailChimp, and WalkScore services.

```
<form id="signup" action="/index.php" method="get">
  <input type="text" name="email" id="email" class="input-newsletter"/>
  <input type="hidden" name="_mailchimp_key" id="_mailchimp_key" value="be8[REDACTED]-us8"/>
  <input type="hidden" name="_mailchimp_list" id="_mailchimp_list" value="d[REDACTED]"/>
  <input type="submit" src="" name="submit" value="" class="btn submit-newsletter" alt="Submit" />
  <input type="text" style="display: none" value="https://[REDACTED].org/wp-content/themes
  <div class="clear"></div>
  <label for="email" id="address-label">
    <span id="response">
      </span>
    </label>
  </form>
```

*AWS root key in front-end HTML  
source: Truffle Security*

Overall, TruffleHog identified 219 distinct secret types in the Common Crawl dataset, the most common being MailChimp API keys.

*"Nearly 1,500 unique Mailchimp API keys were hard coded in front-end HTML and JavaScript" - Truffle Security*

The researchers explain that the developers' mistake was to hardcode them into HTML forms and JavaScript snippets and did not use server-side environment variables.

```
<form id="signup" action="/index.php" method="get">
  <input type="text" name="email" id="email" class="input-newsletter"/>
  <input type="hidden" name="mailchimp_key" id="mailchimp_key" value="be8[REDACTED]-us8"/>
  <input type="hidden" name="mailchimp_list" id="mailchimp_list" value="dt[REDACTED]"/>
  <input type="submit" src="" name="submit" value="" class="btn submit-newsletter" alt="Submit" />
  <input type="text" style="display: none" value="https://[REDACTED].org/wp-content/themes/
  <div class="clear"></div>
  <label for="email" id="address-label">
    <span id="response">
      </span>
    </label>
  </form>
```

MailChimp API key leaked in front-end HTML  
source: Truffle Security

An attacker could use these keys for malicious activity such as phishing campaigns and brand impersonation. Furthermore, leaking such secrets could lead to data exfiltration.

Another highlight in the report is the high reuse rate of the discovered secrets, saying that 63% were present on multiple pages. One of them though, a WalkScore API key, “appeared 57,029 times across 1,871 subdomains.”

The researchers also found one webpage with 17 unique Slack webhooks, which should be kept secret because they allow apps to post messages into Slack.

*“Keep it secret, keep it safe. Your webhook URL contains a secret. Don't share it online, including via public version control repositories,” Slack warns.*

Following the research, Truffle Security contacted impacted vendors and worked with them to revoke their users' keys. “We successfully helped those organizations collectively rotate/revoke several thousand keys,” the researchers say.

Even if an artificial intelligence model uses older archives than the dataset the researchers scanned, Truffle Security's findings serve as a warning that insecure coding practices could influence the behavior of the LLM.

Source: <https://www.bleepingcomputer.com/news/security/nearly-12-000-api-keys-and-passwords-found-in-ai-training-dataset/>

## 2. Silk Typhoon hackers now target IT supply chains to breach networks

Microsoft warns that Chinese cyber-espionage threat group 'Silk Typhoon' has shifted its tactics, now targeting remote management tools and cloud services in supply chain attacks that give them access to downstream customers.

The tech giant has confirmed breaches across multiple industries, including government, IT services, healthcare, defense, education, NGOs, and energy.

"They [Silk Typhoon] exploit unpatched applications that allow them to elevate their access in targeted organizations and conduct further malicious activities," reads Microsoft's report.

"After successfully compromising a victim, Silk Typhoon uses the stolen keys and credentials to infiltrate customer networks where they can then abuse a variety of deployed applications, including Microsoft services and others, to achieve their espionage objectives."

## Silk Typhoon storms IT supply chains

Silk Typhoon is a Chinese state-sponsored espionage group known for hacking the U.S. Office of Foreign Assets Control (OFAC) office in early December 2024 and stealing data from the Committee on Foreign Investment in the United States (CFIUS).

Microsoft reports that Silk Typhoon switched tactics around that period, abusing stolen API keys and compromised credentials for IT providers, identity management, privileged access management, and RMM solutions, which are then used to access downstream customer networks and data.

Microsoft says the attackers scan GitHub repositories and other public resources to locate leaked authentication keys or credentials and then use them to breach environments. The threat actors are also known for using password spray attacks to gain access to valid credentials.

Previously, the threat actors were primarily leveraging zero-day and n-day flaws in public-facing edge devices to gain initial access, plant web shells, and then move laterally via compromised VPNs and RDPs.

Switching from organization-level breaches to MSP-level hacks allows the attackers to move within cloud environments, stealing Active Directory sync credentials (AADConnect), and abusing OAuth applications for a much stealthier attack.

The threat actors no longer rely on malware and web shells, with Silk Typhoon now exploiting cloud apps to steal data and then clear logs, leaving only a minimal trace behind.

According to Microsoft's observations, Silk Typhoon continues to exploit vulnerabilities alongside its new tactics, sometimes as zero days, for initial access.

Most recently, the threat group was observed exploiting a critical Ivanti Pulse Connect VPN privilege escalation flaw (CVE-2025-0282) as a zero-day to breach corporate networks.

Earlier, in 2024, Silk Typhoon exploited CVE-2024-3400, a command injection vulnerability in Palo Alto Networks GlobalProtect, and CVE-2023-3519, a remote code execution flaw in Citrix NetScaler ADC and NetScaler Gateway.

Microsoft says the threat actors have created a "CovertNetwork" consisting of compromised Cyberoam appliances, Zyxel routers, and QNAP devices, which are used to launch attacks and obfuscate malicious activities.

Microsoft has listed updated indicators of compromise and detection rules that reflect Silk Typhoon's latest shift in tactics at the bottom of its report, and defenders are recommended to add the available information to their security tools to detect and block any attacks timely.

Source: <https://www.bleepingcomputer.com/news/security/silk-typhoon-hackers-now-target-it-supply-chains-to-breach-networks/>

### 3. Open-source tool 'Rayhunter' helps users detect Stingray attacks

The Electronic Frontier Foundation (EFF) has released a free, open-source tool named Rayhunter that is designed to detect cell-site simulators (CSS), also known as IMSI catchers or Stingrays.

Stingray devices mimic legitimate cell towers to trick phones into connecting, allowing them to capture sensitive data, accurately geolocate users, and potentially intercept communications.

With the release of the Rayhunter, EFF seeks to give users the power to detect these instances, allowing them to protect themselves and also help draw a clearer picture of the exact deployment scale of Stingrays.

#### How Rayhunter works

Rayhunter is an open-source tool designed to detect Stingrays by capturing control traffic (signaling data) between the mobile hotspot and the cell tower it is connected to, but without monitoring user activity.

"Rayhunter works by intercepting, storing, and analyzing the control traffic (but not user traffic, such as web requests) between the mobile hotspot Rayhunter runs on and the cell tower to which it's connected," reads EFF's announcement.

"Rayhunter analyzes the traffic in real-time and looks for suspicious events, which could include unusual requests like the base station (cell tower) trying to downgrade your connection to 2G which is vulnerable to further attacks, or the base station requesting your IMSI under suspicious circumstances."

Compared to other Stingray detection methods that require rooted Android phones and expensive software-defined radios, Rayhunter runs on a \$20 Orbic RC400L mobile hotspot device (portable 4G LTE router).

EFF chose this hardware for its testing of Rayhunter due to its affordability, widespread availability (Amazon, eBay), and portability, but notes that their software may work well on other Linux/Qualcomm devices too.



*Rayhunter running on an Orbic RC400L*

*Source: EFF*

When Rayhunter detects suspicious network traffic, Orbic's default green/blue screen turns red, informing users of a potential Stingray attack.

The users may then access and download the PCAP logs kept on the device to get more information about the incident or use them to support forensic investigations.

For more instructions on how to install and use Rayhunter, check out EFF's GitHub repository.

The EFF includes a legal disclaimer noting that the software is likely not illegal to use in the United States. However, before attempting to use this project, it is advisable to check with a lawyer to determine if it's legal to use in your country.

BleepingComputer has not tested Rayhunter and cannot guarantee its safety or effectiveness, so use it at your own risk.

Source: <https://www.bleepingcomputer.com/news/security/open-source-tool-rayhunter-helps-users-detect-stingray-attacks/>

#### **4. Ransomware gang encrypted network from a webcam to bypass EDR**

The Akira ransomware gang was spotted using an unsecured webcam to launch encryption attacks on a victim's network, effectively circumventing Endpoint Detection and Response (EDR), which was blocking the encryptor in Windows.

Cybersecurity firm S-RM team discovered the unusual attack method during a recent incident response at one of their clients.

Notably, Akira only pivoted to the webcam after attempting to deploy encryptors on Windows, which were blocked by the victim's EDR solution.

## Akira's unorthodox attack chain

The threat actors initially gained access to the corporate network via an exposed remote access solution at the targeted company, likely by leveraging stolen credentials or brute-forcing the password.

After gaining access, they deployed AnyDesk, a legitimate remote access tool, and stole the company's data for use as part of the double extortion attack.

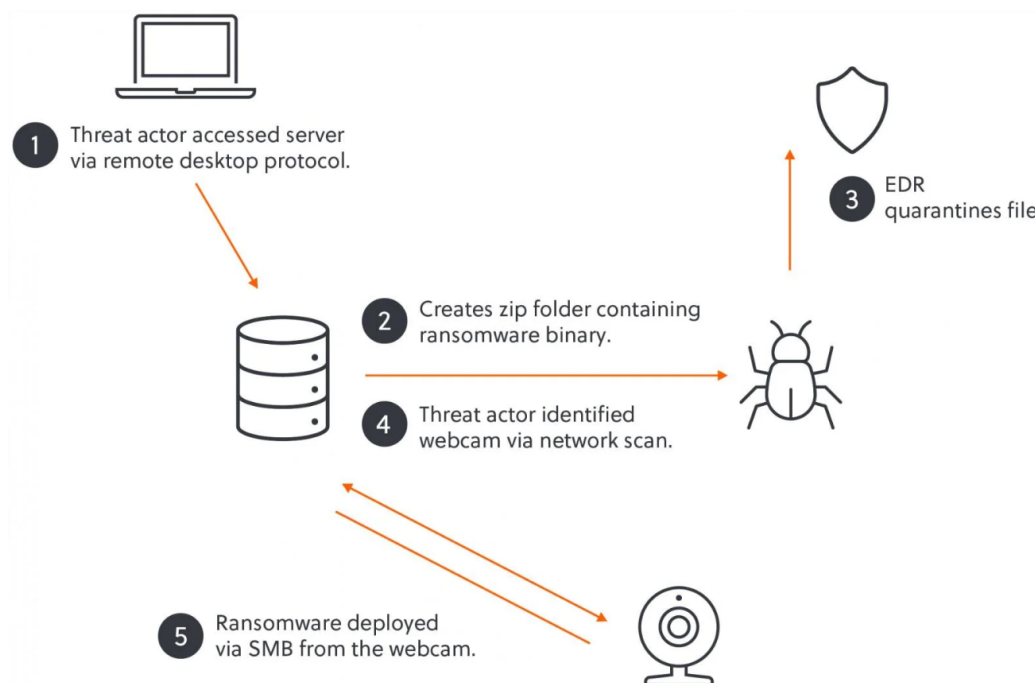
Next, Akira used Remote Desktop Protocol (RDP) to move laterally and expand their presence to as many systems as possible before deploying the ransomware payload.

Eventually, the threat actors dropped a password-protected ZIP file (win.zip) containing the ransomware payload (win.exe), but the victim's EDR tool detected and quarantined it, essentially blocking the attack.

After this failure, Akira explored alternative attack pathways, scanning the network for other devices that could be used to encrypt the files and finding a webcam and fingerprint scanner.

S-RM explains that the attackers opted for the webcam because it was vulnerable to remote shell access and unauthorized video feed viewing.

Furthermore, it ran on a Linux-based operating system compatible with Akira's Linux encryptor. It also did not have an EDR agent, making it an optimal device to remotely encrypt files on network shares.



Overview of Akira's attack steps  
Source: S-RM

S-RM confirmed to BleepingComputer that the threat actors utilized the webcam's Linux operating system to mount Windows SMB network shares of the company's other devices. They then launched the Linux encryptor on the webcam and used it to encrypt the network shares over SMB, effectively circumventing the EDR software on the network.



"As the device was not being monitored, the victim organisation's security team were unaware of the increase in malicious Server Message Block (SMB) traffic from the webcam to the impacted server, which otherwise may have alerted them," explains S-RM.

"Akira was subsequently able to encrypt files across the victim's network."

S-RM told BleepingComputer that there were patches available for the webcam flaws, meaning that the attack, or at least this vector, was avoidable.

The case shows that EDR protection isn't an all-encompassing security solution, and organizations shouldn't rely on it alone to protect against attacks.

Furthermore, IoT devices are not as closely monitored and maintained as computers but still pose a significant risk.

Due to this, these types of devices should be isolated from the more sensitive networks, like production servers and workstations.

Of equal importance, all devices, even IoT devices, should have their firmware updated regularly to patch known flaws that could be exploited in attacks.

*Source: <https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypted-network-from-a-webcam-to-bypass-edr/>*

## 5. Critical PHP RCE vulnerability mass exploited in new attacks

Threat intelligence company GreyNoise warns that a critical PHP remote code execution vulnerability that impacts Windows systems is now under mass exploitation.

Tracked as CVE-2024-4577, this PHP-CGI argument injection flaw was patched in June 2024 and affects Windows PHP installations with PHP running in CGI mode. Successful exploitation enables unauthenticated attackers to execute arbitrary code and leads to complete system compromise following successful exploitation.

A day after PHP maintainers released CVE-2024-4577 patches on June 7, 2024, WatchTower Labs released proof-of-concept (PoC) exploit code, and the Shadowserver Foundation reported observing exploitation attempts.

GreyNoise's warning comes after Cisco Talos revealed earlier that an unknown attacker had exploited the same PHP vulnerability to target Japanese organizations since at least early January 2025.

While Talos observed the attackers attempting to steal credentials, it believes their goals extend beyond just credential harvesting, based on post-exploitation activities, which include establishing persistence, elevating privileges to SYSTEM level, deployment of adversarial tools and frameworks, and usage of "TaoWu" Cobalt Strike kit plugins.

### New attacks expand to targets worldwide

However, as GreyNoise reported, the threat actors behind this malicious activity cast a much wider net by targeting vulnerable devices globally, with significant increases observed in the United States, Singapore, Japan, and other countries since January 2025.

In January alone, its worldwide network of honeypots known as Global Observation Grid (GOG) spotted 1,089 unique IP addresses attempting to exploit this PHP security flaw.

"While initial reports focused on attacks in Japan, GreyNoise data confirms that exploitation is far more widespread [...] More than 43% of IPs targeting CVE-2024-4577 in the past 30 days are from Germany and China," the threat intelligence firm said, warning that at least 79 exploits are available online.

"In February, GreyNoise detected a coordinated spike in exploitation attempts against networks in multiple countries, suggesting additional automated scanning for vulnerable targets."

Previously, CVE-2024-4577 was exploited by unknown attackers who backdoored a university's Windows systems in Taiwan with newly discovered malware dubbed Msupedge.

The TellYouThePass ransomware gang also started exploiting the vulnerability to deploy webshells and encrypt victims' systems less than 48 hours after patches were released in June 2024.

Source: <https://www.bleepingcomputer.com/news/security/critical-php-rce-vulnerability-mass-exploited-in-new-attacks/>

## 6. Silk Typhoon Hackers Indicted

Lots of interesting details in the story:

The US Department of Justice on Wednesday announced the indictment of 12 Chinese individuals accused of more than a decade of hacker intrusions around the world, including eight staffers for the contractor i-Soon, two officials at China's Ministry of Public Security who allegedly worked with them, and two other alleged hackers who are said to be part of the Chinese hacker group APT27, or Silk Typhoon, which prosecutors say was involved in the US Treasury breach late last year.

[...]

According to prosecutors, the group as a whole has targeted US state and federal agencies, foreign ministries of countries across Asia, Chinese dissidents, US-based media outlets that have criticized the Chinese government, and most recently the US Treasury, which was breached between September and December of last year. An internal Treasury report obtained by Bloomberg News found that hackers had penetrated at least 400 of the agency's PCs and stole more than 3,000 files in that intrusion.

The indictments highlight how, in some cases, the hackers operated with a surprising degree of autonomy, even choosing targets on their own before selling stolen information to Chinese government clients. The indictment against Yin Kecheng, who was previously sanctioned by the Treasury Department in January for his involvement in the Treasury breach, quotes from his communications with a colleague in which he notes his personal preference for hacking American targets and how he's seeking to 'break into a big target,' which he hoped would allow him to make enough money to buy a car.

Source: <https://www.schneier.com/blog/archives/2025/03/silk-typhoon-hackers-indicted.html>



## 7. Cisco IOS XR vulnerability lets attackers crash BGP on routers

Cisco has patched a denial of service (DoS) vulnerability that lets attackers crash the Border Gateway Protocol (BGP) process on IOS XR routers with a single BGP update message.

IOS XR runs on the company's carrier-grade, Network Convergence System (NCS), and Carrier Routing System (CRS) series of routers, such as the ASR 9000, NCS 5500, and 8000 series.

This high-severity flaw (tracked as CVE-2025-20115) was found in the confederation implementation for the Border Gateway Protocol (BGP), and it only affects Cisco IOS XR devices if BGP confederation is configured.

Successful exploitation allows unauthenticated attackers to take down vulnerable devices remotely in low-complexity attacks by causing memory corruption via buffer overflow, leading to a BGP process restart.

"This vulnerability is due to a memory corruption that occurs when a BGP update is created with an AS\_CONFED\_SEQUENCE attribute that has 255 autonomous system numbers (AS numbers)," the company explains in a security advisory issued this week.

"An attacker could exploit this vulnerability by sending a crafted BGP update message, or the network could be designed in such a manner that the AS\_CONFED\_SEQUENCE attribute grows to 255 AS numbers or more."

To exploit the CVE-2025-20115 vulnerability, "the network must be designed in such a manner that the AS\_CONFED\_SEQUENCE attribute grows to 255 AS numbers or more," or the attackers must have control of a BGP confederation speaker within the same autonomous system as the targeted device(s).

Cisco IOS XR Software Release	First Fixed Release
7.11 and earlier	Migrate to a fixed release.
24.1 and earlier	Migrate to a fixed release.
24.2	24.2.21 (future release)
24.3	24.3.1
24.4	Not affected.

Those who can't immediately apply the security patches released earlier this week are advised to restrict the BGP AS\_CONFED\_SEQUENCE attribute to 254 or fewer AS numbers to limit potential attacks' impact.

"While this workaround has been deployed and was proven successful in a test environment, customers should determine the applicability and effectiveness in their own environment and under their own use conditions," Cisco said.

The company's Product Security Incident Response Team (PSIRT) found no evidence that this vulnerability has been exploited in the wild, but Cisco says a write-up published in September on APNIC's blog provides additional CVE-2025-20115 technical details.

Earlier this month, Cisco warned customers of a vulnerability in Webex for BroadWorks that can let unauthenticated attackers access credentials remotely.

The same week, CISA tagged a remote command execution security flaw impacting Cisco RV016, RV042, RV042G, RV082, RV320, and RV325 VPN routers as actively exploited in attacks and ordered U.S. federal agencies to secure any vulnerable devices by March 23.

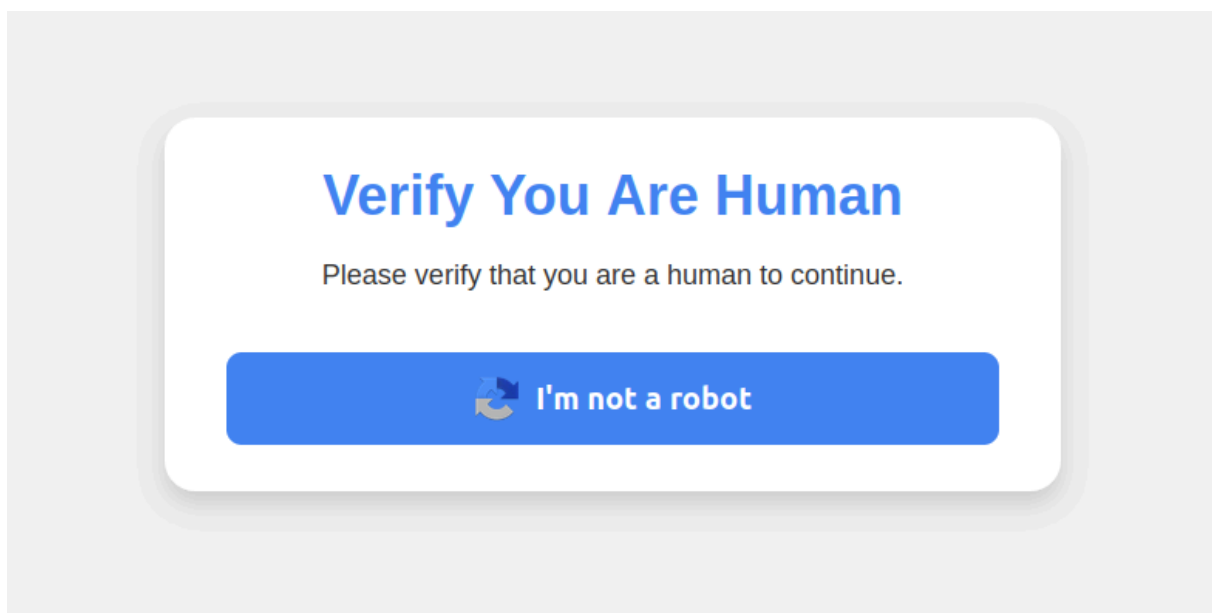
"Cisco continues to strongly recommend that customers upgrade their hardware to Meraki or Cisco 1000 Series Integrated Services Routers to remediate these vulnerabilities," the company urged in an advisory updated days after CISA's order was issued.

Source: <https://www.bleepingcomputer.com/news/security/cisco-vulnerability-lets-attackers-crash-bgp-on-ios-xr-routers/>

## 8. ClickFix: How to Infect Your PC in Three Easy Steps

A clever malware deployment scheme first spotted in targeted attacks last year has now gone mainstream. In this scam, dubbed "**ClickFix**," the visitor to a hacked or malicious website is asked to distinguish themselves from bots by pressing a combination of keyboard keys that causes **Microsoft Windows** to download password-stealing malware.

ClickFix attacks mimic the "Verify You are a Human" tests that many websites use to separate real visitors from content-scraping bots. This particular scam usually starts with a website popup that looks something like this:



This malware attack pretends to be a CAPTCHA intended to separate humans from bots.

Clicking the "I'm not a robot" button generates a pop-up message asking the user to take three sequential steps to prove their humanity.

## Verification Steps

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

Executing this series of keypresses prompts Windows to download password-stealing malware.

Step 1 involves simultaneously pressing the keyboard key with the Windows icon and the letter "R," which opens a Windows "Run" prompt that will execute any specified program that is already installed on the system.

Step 2 asks the user to press the "CTRL" key and the letter "V" at the same time, which pastes malicious code from the site's virtual clipboard.

Step 3 — pressing the "Enter" key — causes Windows to download and launch malicious code through "**mshta.exe**," a Windows program designed to run Microsoft HTML application files.

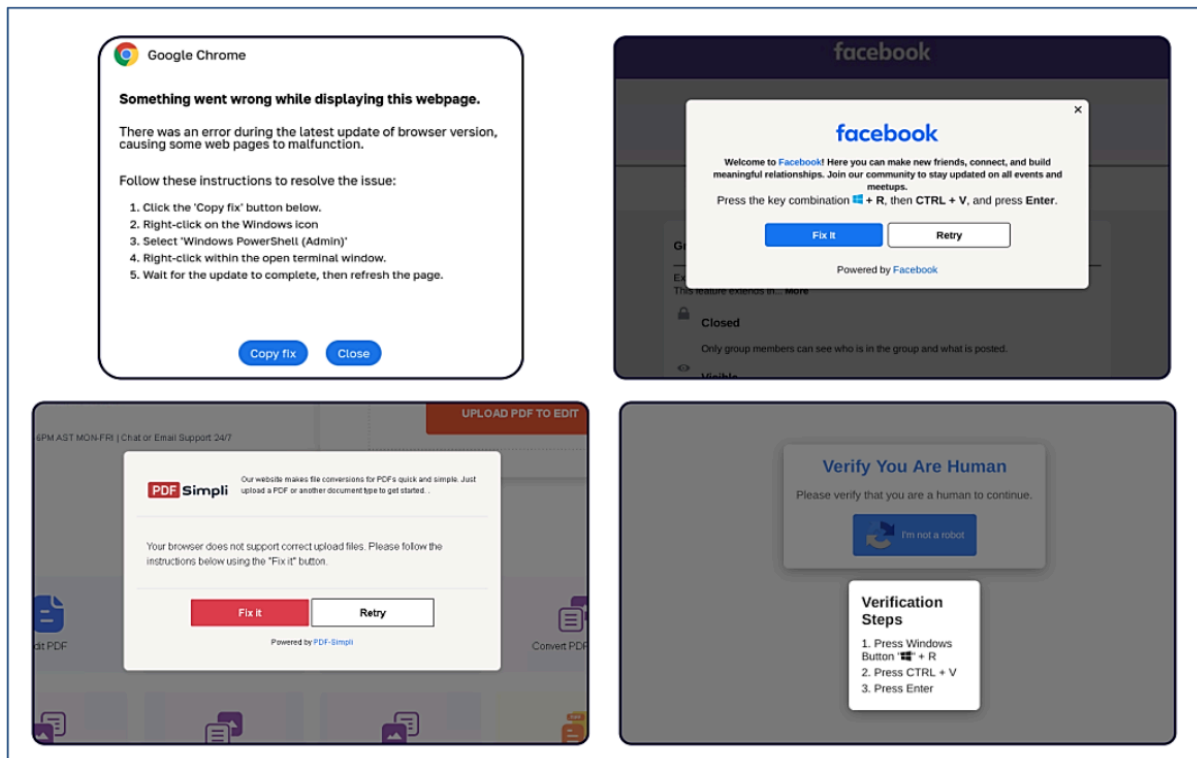
"This campaign delivers multiple families of commodity malware, including XWorm, Lumma stealer, VenomRAT, AsyncRAT, Danabot, and NetSupport RAT," **Microsoft** wrote in a blog post on Thursday. "Depending on the specific payload, the specific code launched through mshta.exe varies. Some samples have downloaded PowerShell, JavaScript, and portable executable (PE) content."

According to Microsoft, hospitality workers are being tricked into downloading credential-stealing malware by cybercriminals impersonating **Booking.com**. The company said attackers have been sending malicious emails impersonating Booking.com, often referencing negative guest reviews, requests from prospective guests, or online promotion opportunities — all in a bid to convince people to step through one of these ClickFix attacks.

In November 2024, KrebsOnSecurity reported that hundreds of hotels that use booking.com had been subject to targeted phishing attacks. Some of those lures worked, and allowed thieves to gain control over booking.com accounts. From there, they sent out phishing messages asking for financial information from people who'd just booked travel through the company's app.

Earlier this month, the security firm **Arctic Wolf** warned about ClickFix attacks targeting people working in the healthcare sector. The company said those attacks leveraged malicious code stitched into the widely used physical therapy video site HEP2go that redirected visitors to a ClickFix prompt.

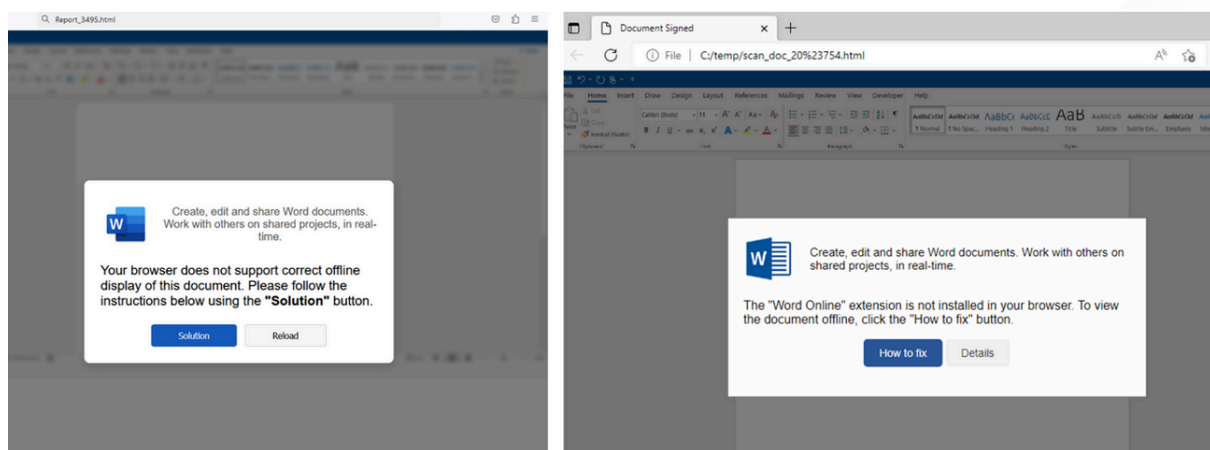
An alert (PDF) released in October 2024 by the **U.S. Department of Health and Human Services** warned that the ClickFix attack can take many forms, including fake **Google Chrome** error pages and popups that spoof **Facebook**.



ClickFix tactic used by malicious websites impersonating Google Chrome, Facebook, PDFSimpli, and reCAPTCHA. Source: Sekoia.

The ClickFix attack — and its reliance on mshta.exe — is reminiscent of phishing techniques employed for years that hid exploits inside **Microsoft Office macros**. Malicious macros became such a common malware threat that Microsoft was forced to start blocking macros by default in Office documents that try to download content from the web.

Alas, the email security vendor **Proofpoint** has documented plenty of ClickFix attacks via phishing emails that include HTML attachments spoofing Microsoft Office files. When opened, the attachment displays an image of Microsoft Word document with a pop-up error message directing users to click the “Solution” or “How to Fix” button.



HTML files containing ClickFix instructions. Examples for attachments named “Report\_” (on the left) and “scan\_doc\_” (on the right). Image: Proofpoint.

Organizations that wish to do so can take advantage of Microsoft Group Policy restrictions to prevent Windows from executing the “run” command when users hit the Windows key and the “R” key simultaneously.

Source: <https://krebsonsecurity.com/2025/03/clickfix-how-to-infect-your-pc-in-three-easy-steps/>

## 9. New Akira ransomware decryptor cracks encryptions keys using GPUs

Security researcher Yohanes Nugroho has released a decryptor for the Linux variant of Akira ransomware, which utilizes GPU power to retrieve the decryption key and unlock files for free.

Nugroho developed the decryptor after being asked for help from a friend, deeming the encrypted system solvable within a week, based on how Akira generates encryption keys using timestamps.

The project ended up taking three weeks due to unforeseen complexities, and the researcher spent \$1,200 on GPU resources to crack the encryption key, but eventually, he succeeded.

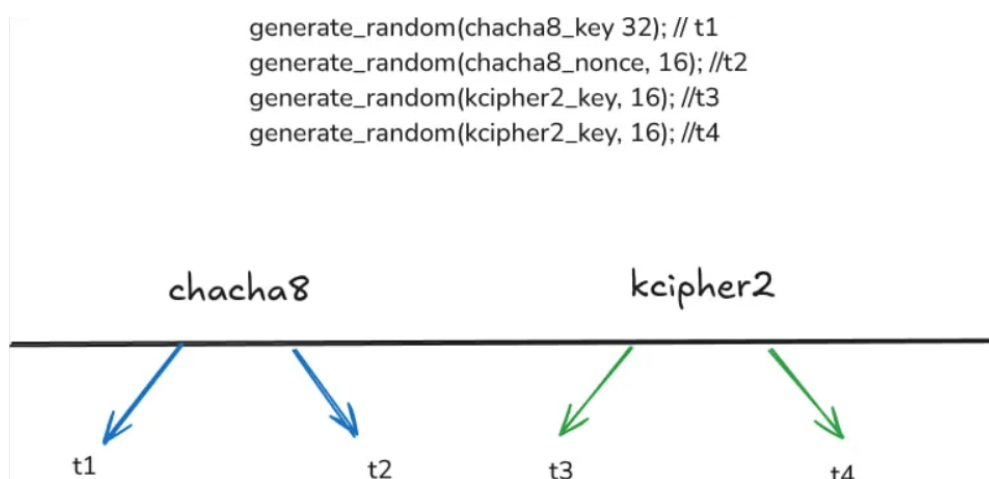
### Using GPUs to brute force keys

Nugroho's decryptor does not work like a traditional decryption tool where users supply a key to unlock their files.

Instead, it brute-forces encryption keys (unique for each file) by exploiting the fact that the Akira encryptor generates its encryption keys based on the current time (in nanoseconds) as a seed.

An encryption seed is data used with cryptographic functions to generate strong, unpredictable encryption keys. Since the seed influences the key generation, keeping it secret is critical to prevent attackers from recreating encryption or decryption keys through brute force or other cryptographic attacks.

Akira ransomware dynamically generates unique encryption keys for each file using four different timestamp seeds with nanosecond precision and hashes through 1,500 rounds of SHA-256.

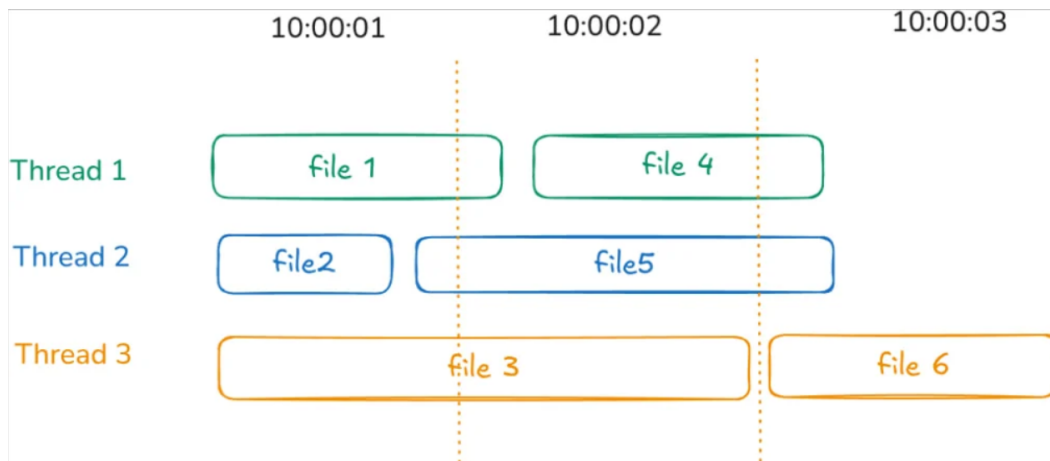


*Four timestamps used for generating keys  
Source: tinyhack.com*

These keys are encrypted with RSA-4096 and appended at the end of each encrypted file, so decrypting them without the private key is hard.

The level of timing precision in the timestamps creates over a billion possible values per second, making it difficult to brute force the keys.

Also, Nugroho says that Akira ransomware on Linux encrypts multiple files simultaneously using multi-threading, making it hard to determine the timestamp used and adding further complexity.



*CPU threads handling file encryption at different times  
Source: tinyhack.com*

The researcher narrowed down the possible timestamps to brute-force by looking at log files shared by his friend. This allowed him to see when the ransomware was executed, the file metadata to estimate the encryption completion times, and produce encryption benchmarks on different hardware to create predictable profiles.

Initial attempts using an RTX 3060 were far too slow, with a ceiling of only 60 million encryption tests per second. Upgrading to an RTX 3090 didn't help much either.

Eventually, the researcher turned to using RunPod & Vast.ai cloud GPU services that offered enough power at the right price to confirm the effectiveness of his tool.

Specifically, he used sixteen RTX 4090 GPUs to brute-force the decryption key in roughly 10 hours. However, depending on the amount of encrypted files that need recovery, the process may take a couple of days.

The researcher noted in his write-up that GPU experts could still optimize his code, so performance can likely be improved.

Nugroho has made the decryptor available on GitHub, with instructions on how to recover Akira-encrypted files.

As always, when attempting to decrypt files, make a backup of the original encrypted files, as there's a possibility that files can be corrupted if the wrong decryption key is used.

BleepingComputer has not tested the tool and cannot guarantee its safety or effectiveness, so use it at your own risk.

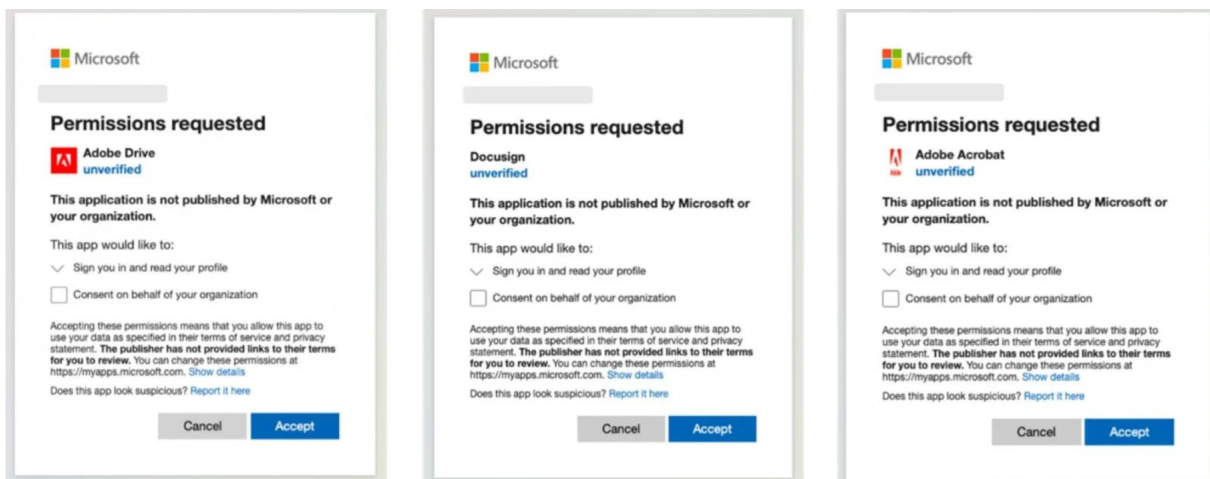
Source: <https://www.bleepingcomputer.com/news/security/gpu-powered-akira-ransomware-decryptor-released-on-github/>

## 10. Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts

Cybercriminals are promoting malicious Microsoft OAuth apps that masquerade as Adobe and DocuSign apps to deliver malware and steal Microsoft 365 accounts credentials.

The campaigns were discovered by Proofpoint researchers, who characterized them as "highly targeted" in a thread on X.

The malicious OAuth apps in this campaign are impersonating Adobe Drive, Adobe Drive X, Adobe Acrobat, and DocuSign.



*Malicious OAuth apps  
Source: Proofpoint*

These apps request access to less sensitive permissions such as 'profile', 'email', and 'openid,' to avoid detection and suspicion.

If those permissions are granted, the attacker is given access to:

- **profile** – Full name, User ID, Profile picture, Username
- **email** – primary email address (no inbox access)
- **openid** – allows confirmation of user's identity and retrieval of Microsoft account details

Proofpoint told BleepingComputer that the phishing campaigns were sent from charities or small companies using compromised email accounts, likely Office 365 accounts.

The emails targeted multiple US and European industries, including government, healthcare, supply chain, and retail. Some of the emails seen by the cybersecurity firm use RFPs and contract lures to trick recipients into opening the links.

While the privileges from accepting the Microsoft OAuth app only provided limited data to the attackers, the information could still be used for more targeted attacks.

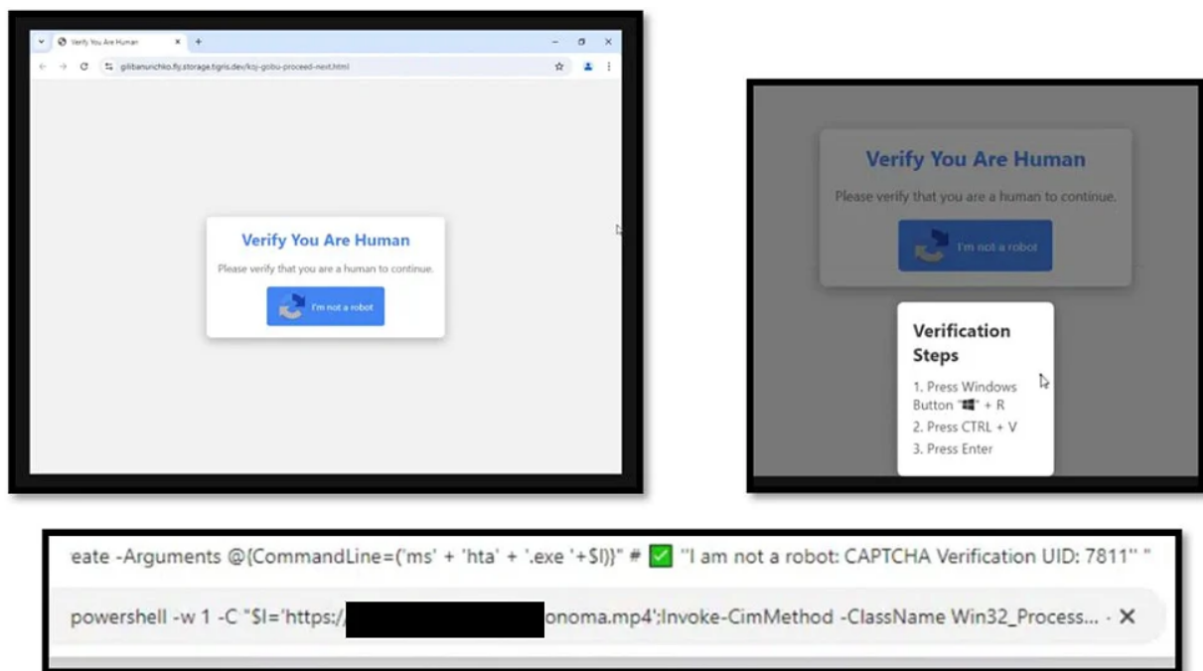


Furthermore, once permission is given to the OAuth app, it redirects users to landing pages that display phishing forms to Microsoft 365 credentials or distributed malware.

"The victims went through multiple redirections and stages after authorizing O365 OAuth app, until presented with the malware or the phishing page behind," Proofpoint told BleepingComputer.

"In some cases, the victims were redirected to an "O365 login" page (hosted on malicious domain). In less than a minute after the authorization, Proofpoint detected suspicious login activity to the account."

Proofpoint said that they could not determine the malware being distributed, but the attackers utilized the ClickFix social engineering attack, which has become very popular over the past year.



*ClickFix landing page used in the malicious OAuth campaign  
Source: Proofpoint*

The attacks are similar to those reported years ago, indicating that OAuth apps remain an effective way to hijack Microsoft 365 accounts without stealing credentials.

Users are advised to be cautious with OAuth app permission requests and always verify their source and legitimacy before approving them.

To check existing approvals, go to 'My Apps' (myapplications.microsoft.com) → 'Manage your apps' → and revoke any unrecognized apps on that screen.

Microsoft 365 administrators can also limit users' permission to consent to third-party OAuth app requests entirely through 'Enterprise Applications' → 'Consent and Permissions' → set 'Users can consent to apps' to 'No.'

Source: <https://www.bleepingcomputer.com/news/security/malicious-adobe-docuSign-oauth-apps-target-microsoft-365-accounts/>



## 11. Critical RCE flaw in Apache Tomcat actively exploited in attacks

A critical remote code execution (RCE) vulnerability in Apache Tomcat tracked as CVE-2025-24813 is actively exploited in the wild, enabling attackers to take over servers with a simple PUT request.

Hackers are reportedly leveraging proof-of-concept (PoC) exploits that were published on GitHub just 30 hours after the flaw was disclosed last week.

The malicious activity was confirmed by Wallarm security researchers, who warned that traditional security tools fail to detect it as PUT requests appear normal and the malicious content is obfuscated using base64 encoding.

Specifically, the attacker sends a PUT request containing a base64-encoded serialized Java payload saved to Tomcat's session storage.

The attacker then sends a GET request with a JSESSIONID cookie pointing to the uploaded session file, forcing Tomcat to deserialize and execute the malicious Java code, granting complete control to the attacker.

The attack does not require authentication and is caused by Tomcat accepting partial PUT requests and its default session persistence.

"This attack is dead simple to execute and requires no authentication," [explains Wallarm](#).

"The only requirement is that Tomcat is using file-based session storage, which is common in many deployments. Worse, base64 encoding allows the exploit to bypass most traditional security filters, making detection challenging."

### The Tomcat RCE

The CVE-2025-24813 remote code execution vulnerability flaw was first disclosed by Apache on March 10, 2025, impacting Apache Tomcat 11.0.0-M1 to 11.0.2, 10.1.0-M1 to 10.1.34, and 9.0.0.M1 to 9.0.98.

The security bulletin warned users that, under certain conditions, an attacker could view or inject arbitrary content on security-sensitive files.

The conditions were the following:

- Writes enabled for the default servlet (readonly= "false") — (Disabled by default)
- Support for partial PUT is enabled (Enabled by default.)
- Security-sensitive uploads occur in a sub-directory of a public upload directory.
- The attacker knows the names of security-sensitive files being uploaded.
- These security-sensitive files are being uploaded using partial PUT.

Apache recommended that all users upgrade to Tomcat versions 11.0.3+, 10.1.35+, or 9.0.99+, which are patched against CVE-2025-24813.

Tomcat users may also mitigate the problem by reverting to the default servlet configuration (readonly= "true"), turning off partial PUT support, and avoiding storing security-sensitive files in a subdirectory of public upload paths.

Wallarm warns that the bigger issue highlighted in this case isn't the exploitation activity itself but the potential for more RCE vulnerabilities arising from the partial PUT handling in Tomcat.

"Attackers will soon start shifting their tactics, uploading malicious JSP files, modifying configurations, and planting backdoors outside session storage. This is just the first wave," cautioned Wallarm.

Source: <https://www.bleepingcomputer.com/news/security/critical-rce-flaw-in-apache-tomcat-actively-exploited-in-attacks/>

## 12. New Windows zero-day exploited by 11 state hacking groups since 2017

At least 11 state-backed hacking groups from North Korea, Iran, Russia, and China have been exploiting a new Windows vulnerability in data theft and cyber espionage zero-day attacks since 2017.

However, as security researchers Peter Girnus and Aliakbar Zahravi with Trend Micro's Zero Day Initiative (ZDI) reported today, Microsoft tagged it as "not meeting the bar servicing" in late September and said it wouldn't release security updates to address it.

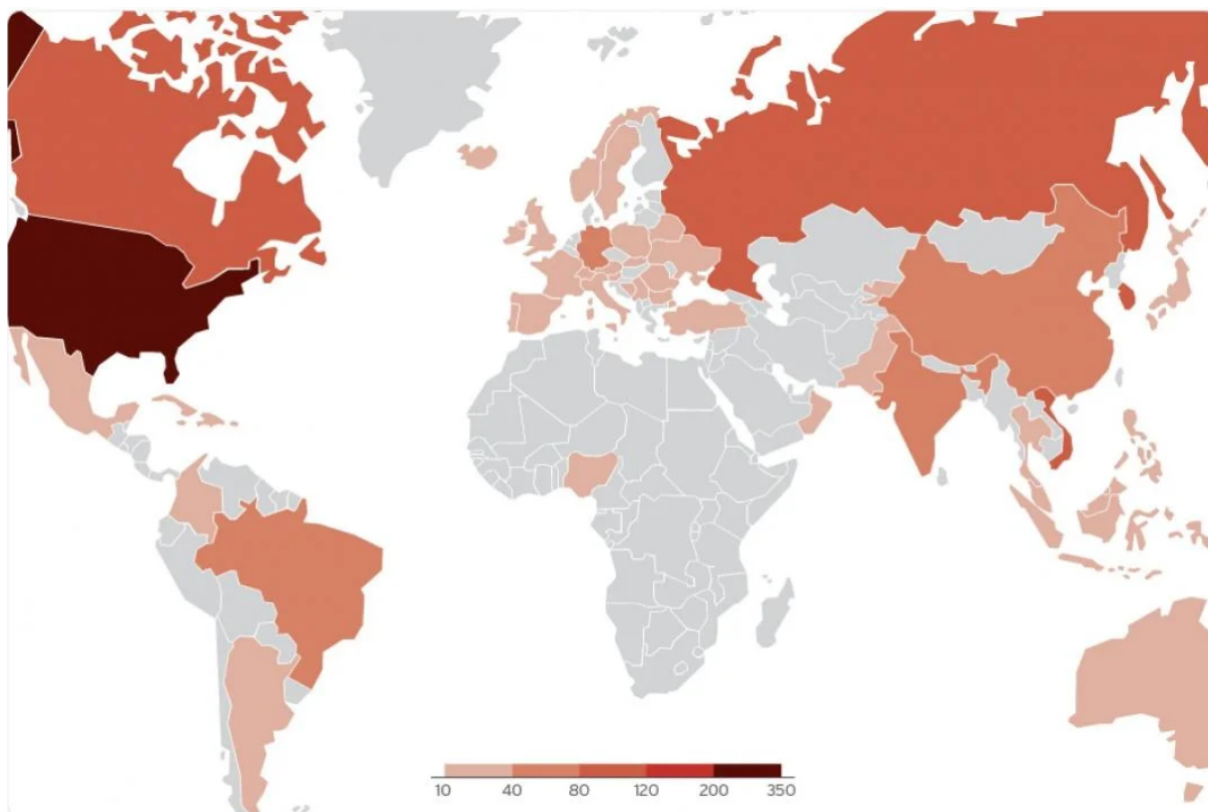
"We discovered nearly a thousand Shell Link (.lnk) samples that exploit ZDI-CAN-25373; however, it is probable that the total number of exploitation attempts are much higher," they said. "Subsequently, we submitted a proof-of-concept exploit through Trend ZDI's bug bounty program to Microsoft, who declined to address this vulnerability with a security patch."

A Microsoft spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today.

While Microsoft has yet to assign a CVE-ID to this vulnerability, Trend Micro is tracking it internally as ZDI-CAN-25373 and said it enables attackers to execute arbitrary code on affected Windows systems.

As the researchers found while investigating in-the-wild ZDI-CAN-25373 exploitation, the security flaw has been exploited in widespread attacks by many state-sponsored threat groups and cybercrime gangs, including Evil Corp, APT43 (Kimsuky), Bitter, APT37, Mustang Panda, SideWinder, RedHotel, Konni, and others.

Although the campaigns have targeted victims worldwide, they've been primarily focused on North America, South America, Europe, East Asia, and Australia. Out of all the attacks analyzed, nearly 70% were linked to espionage and information theft, while financial gain was the focus of only 20%.



*Map of countries targeted in ZDI-CAN-25373 attacks (Trend Micro)*

"Diverse malware payloads and loaders like Ursnif, Gh0st RAT, and Trickbot have been tracked in these campaigns, with malware-as-a-service (MaaS) platforms complicating the threat landscape," Trend Micro added.

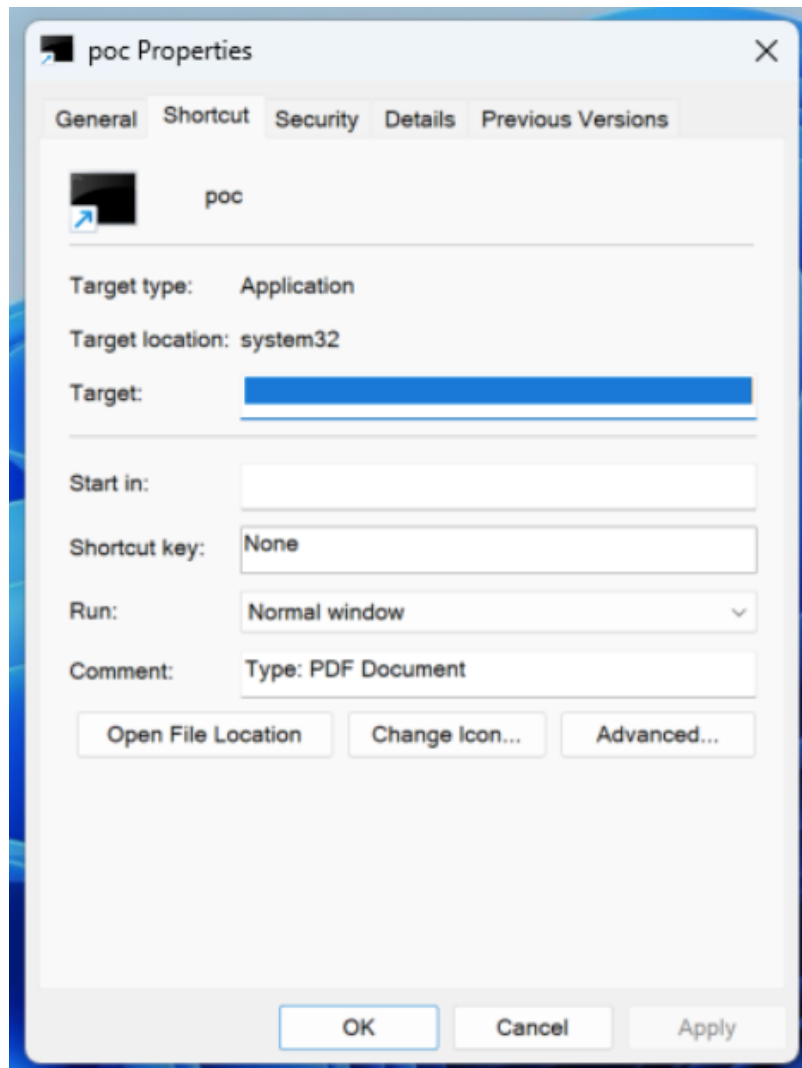
## The ZDI-CAN-25373 Windows zero-day

This heavily exploited Windows vulnerability (tracked as ZDI-CAN-25373) is caused by a User Interface (UI) Misrepresentation of Critical Information (CWE-451) weakness, which allows attackers to exploit how Windows displays shortcut (.lnk) files to evade detection and execute code on vulnerable devices without the user's knowledge.

Threat actors exploit ZDI-CAN-25373 by hiding malicious command-line arguments within .LNK shortcut files using padded whitespaces added to the `COMMAND_LINE_ARGUMENTS` structure.

The researchers say these whitespaces can be in the form of hex codes for Space (\x20), Horizontal Tab (\x09), Linefeed (\x0A), Vertical Tab (\x0B), Form Feed (\x0C), and Carriage Return (\x0D) that can be used as padding.

If a Windows user inspects such a .lnk file, the malicious arguments are not displayed in the Windows user interface because of the added whitespaces. As a result, the command line arguments added by the attackers remain hidden from the user's view.



*Malicious arguments not showing in the Target field (Trend Micro)*

"User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file," a Trend Micro advisory issued today explains.

"Crafted data in an .LNK file can cause hazardous content in the file to be invisible to a user who inspects the file via the Windows-provided user interface. An attacker can leverage this vulnerability to execute code in the context of the current user."

This vulnerability is similar to another flaw tracked as CVE-2024-43461 that enabled threat actors to use 26 encoded braille whitespace characters (%E2%A0%80) to camouflage HTA files that can download malicious payloads as PDFs. CVE-2024-43461 was found by Peter Girus, a Senior Threat Researcher at Trend Micro's Zero Day, and patched by Microsoft during the September 2024 Patch Tuesday.

The Void Banshee APT hacking group exploited CVE-2024-43461 in zero-day attacks to deploy information-stealing malware in campaigns against organizations across North America, Europe, and Southeast Asia.

*Update March 18, 13:46 EDT:* A Microsoft spokesperson sent the following statement after publishing time, saying the company is considering to address the flaw in the future:

*We appreciate the work of ZDI in submitting this report under a coordinated vulnerability disclosure. Microsoft Defender has detections in place to detect and block this threat activity, and the Smart App Control provides an extra layer of protection by blocking malicious files from the Internet. As a security best practice, we encourage customers to exercise caution when downloading files from unknown sources as indicated in security warnings, which have been designed to recognize and warn users about potentially harmful files. While the UI experience described in the report does not meet the bar for immediate servicing under our severity classification guidelines, we will consider addressing it in a future feature release.*

Source: <https://www.bleepingcomputer.com/news/security/new-windows-zero-day-exploited-by-11-state-hacking-groups-since-2017/>

### 13. New Arcane infostealer infects YouTube, Discord users via game cheats

A newly discovered information-stealing malware called Arcane is stealing extensive user data, including VPN account credentials, gaming clients, messaging apps, and information stored in web browsers.

According to Kaspersky, the malware has no links or code that overlaps with the Arcane Stealer V, which has been circulating on the dark web for years.

The Arcane malware campaign started in November 2024, having gone through several evolutionary steps, including primary payload replacements.

All conversations and public posts by its operators are in Russian, with Kaspersky's telemetry showing that most Arcane infections are in Russia, Belarus, and Kazakhstan.

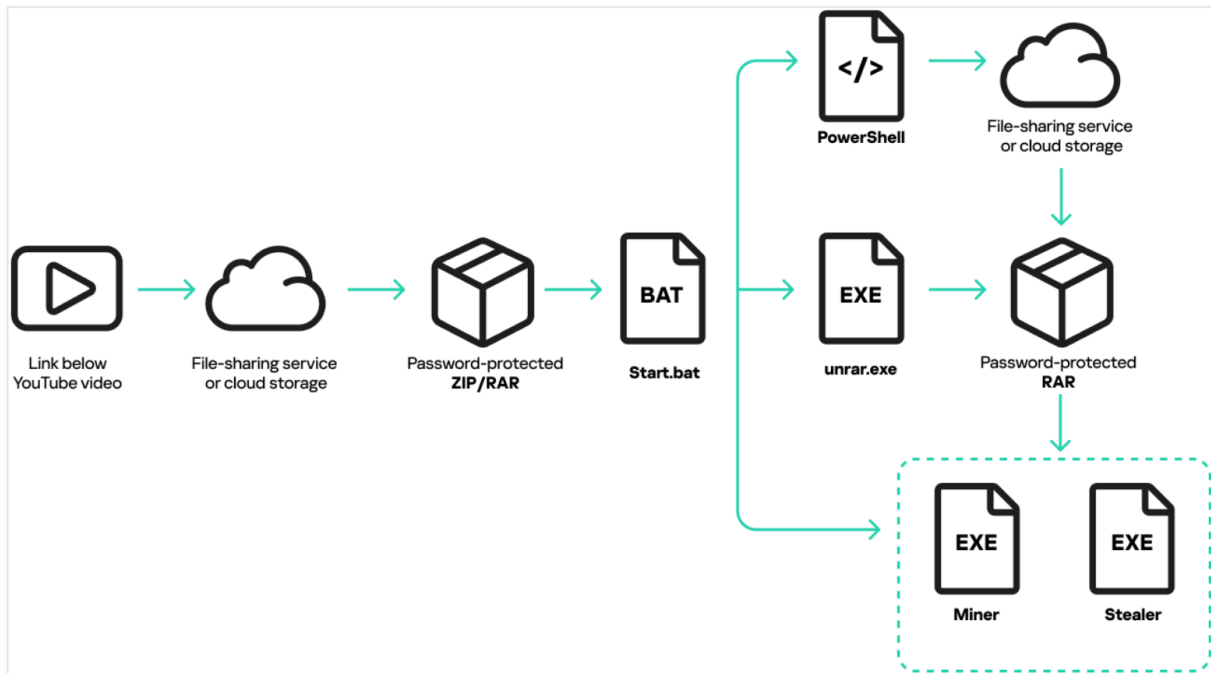
This is particularly notable, as most threat actors based in Russia typically avoid targeting users within the country and other CIS nations to prevent conflicts with local authorities.

#### Arcane stealer infection chain

The campaign distributing Arcane Stealer relies on YouTube videos promoting game cheats and cracks, tricking users into following a link to download a password-protected archive.

These files contained a heavily obfuscated 'start.bat' script that fetched a second password-protected archive with malicious executables.

The downloaded files add an exclusion to Windows Defender's SmartScreen filter for all drive root folders or turn it off completely through Windows Registry modifications.

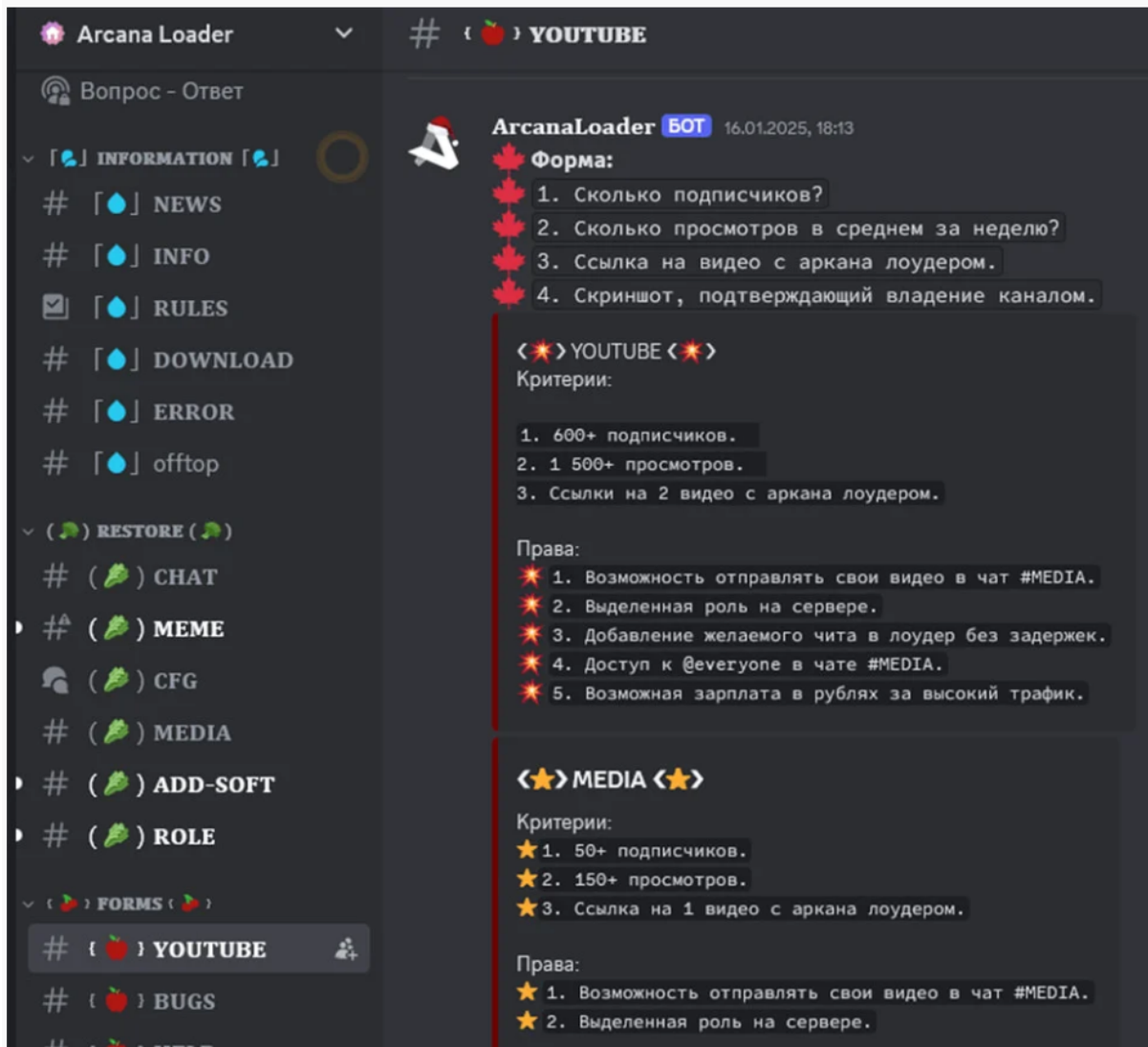


*Infection chain diagram*  
*Source: Kaspersky*

Previously, the attacks used another stealer malware family called VGS, a rebranded version of the Phemedrone trojan, but they switched to Arcane in November 2024.

Kaspersky also found recent changes in the distribution method, including the use of a fake software downloader, supposedly for popular game cracks and cheats, named ArcanaLoader.

ArcanaLoader has been heavily promoted on YouTube and Discord, with the operators even inviting content creators to promote it on their blogs/videos for a fee.



Attempting to recruit YouTube creators on Discord  
Source: Kaspersky

## Stealing a ton of data

Kaspersky comments that Arcane's broad data theft makes it stand out in the populous infostealer space.

First, it profiles the infected system, stealing hardware and software details such as OS version, CPU and GPU details, installed antivirus, and browsers.

The current version of the malware targets account data, settings, and configuration files from the following apps:

- **VPN clients:** OpenVPN, Mullvad, NordVPN, IPVanish, Surfshark, Proton, hidemy.name, PIA, CyberGhost, ExpressVPN
- **Network tools:** ngrok, Playit, Cyberduck, FileZilla, DynDNS
- **Messagers:** ICQ, Tox, Skype, Pidgin, Signal, Element, Discord, Telegram, Jabber, Viber
- **Email clients:** Outlook
- **Gaming clients:** Riot Client, Epic, Steam, Ubisoft Connect (ex-Uplay), Roblox, Battle.net, various Minecraft clients



- **Cryptocurrency wallets:** Zcash, Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, Atomic, Guarda, Coinomi
- **Web browsers:** Saved logins, passwords, and cookies (for Gmail, Google Drive, Google Photos, Steam, YouTube, Twitter, Roblox) from Chromium-based browsers.

Arcane also captures screenshots that can reveal sensitive information about what you are doing on the computer and retrieves saved Wi-Fi network passwords.

Even though Arcane currently has specific targeting, its operators could expand it to cover additional countries or themes.

Becoming infected with an infostealer is devastating, leading to financial fraud, extortion, and future attacks. Cleaning up after these attacks is a massive time sink as you need to change the passwords on every website and application you use and ensure they are not compromised.

Therefore, users should always keep in mind the risks of downloading unsigned pirate and cheat tools. The risk from these tools is too high, and they should be avoided entirely.

Source: <https://www.bleepingcomputer.com/news/security/new-arcane-infostealer-infests-youtube-discord-users-via-game-cheats/>

## 14. HellCat hackers go on a worldwide Jira hacking spree

Swiss global solutions provider Ascom has confirmed a cyberattack on its IT infrastructure as a hacker group known as Hellcat targets Jira servers worldwide using compromised credentials.

The company announced in a press release that hackers on Sunday breached its technical ticketing system and is currently investigating the incident.

Ascom is a telecommunications company with subsidiaries in 18 countries focusing on wireless on-site communications.

HellCat hacking group claimed the attack and told BleepingComputer that they stole about 44GB of data that may impact all of the company's divisions.

Ascom says that the hackers compromised its technical ticketing system, the incident had no impact on the company's business operations, and that customers and partners do not need to take any preventive action.

*"Investigations against such criminal offenses were initiated immediately and are ongoing. Ascom is working closely with the relevant authorities" - Ascom*

Rey, a member of the HellCat hacking group, told BleepingComputer that they stole from Ascom source code for multiple products, details about various projects, invoices, confidential documents, and issues from the ticketing system.

The Swiss company did not provide technical details about the breach but targeting the Jira ticketing system has become a common attack method for the HellCat hackers.



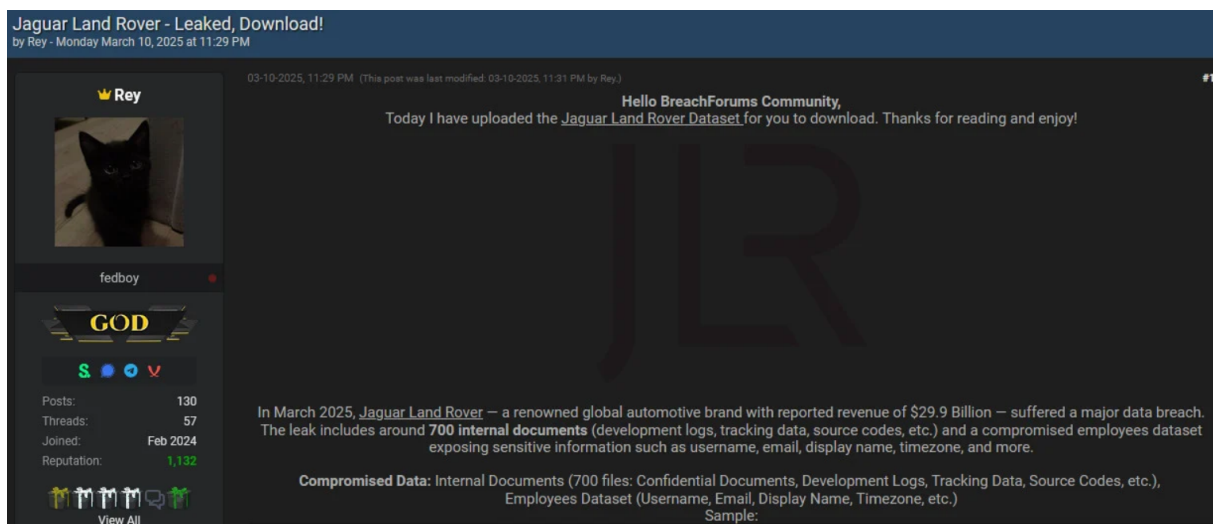
## HellCat on a Jira hacking spree

Jira is a project management and issue-tracking platform commonly used by software developers and IT teams to track and manage projects. The platform often contains sensitive data, such as source code, authentication keys, IT plans, customer information, and internal discussions related to these projects.

Previous incidents claimed by HellCat and confirmed by the targeted companies count Schneider Electric, Telefónica, and Orange Group, and in all three instances the hackers breached their way in through Jira servers.

Recently, the same hackers also took responsibility for an attack on the British multinational car maker Jaguar Land Rover (JLR) and stole and leaked about 700 internal documents.

As the threat actor describes it, the leak includes “development logs, tracking data, source codes” and an employee’s data that exposed “sensitive information such as username, email, display name, timezone, and more.”



*HellCat ransomware claims Jaguar Land Rover breach*

Alon Gal, co-founder and CTO at threat intelligence company Hudson Rock, says the JLR breach follows a pattern specific to HellCat hackers.

*“At the heart of this latest incident lies a technique that has become HELLCAT’s signature: exploiting Jira credentials harvested from compromised employees that were infected by Infostealers” - Alon Gal*

The researcher said that the JLR incident was possible by using the credentials of an LG Electronics employee with third-party credentials to JLR’s Jira server.

Gal highlights that the compromised credentials were not fresh and had been exposed for several years but remained valid all this time, allowing hackers to take advantage.

HellCat’s activity didn’t stop at these breaches as the threat actor announced today that they compromised the Jira system of Affinitiv, a marketing company that provides data analytics a platform for OEMs and dealerships in the automotive industry.

The threat actor confirmed to BleepingComputer that they breached Affinitiv through a Jira system and disclosed publicly that they stole a database with a little over 470,000 “unique emails” and more than 780,000 records.

When contacted by BleepingComputer about the alleged attack, Affinitiv said that they had begun an investigation.

To prove the breach, hackers published two screenshots with names, email addresses, postal addresses, and dealership names.

Alon Gal is warning that Jira “has become a prime target for attackers due to its centrality in enterprise workflows and the wealth of data it houses” and this type of access can be used to “move laterally, escalate privileges, and extract sensitive information.”

As credentials collected by infostealers are easy to find and given that some of them remain unchanged for years as companies fail to include them in a regular rotation process, such attacks will likely become more frequent.

Source: <https://www.bleepingcomputer.com/news/security/hellcat-hackers-go-on-a-worldwide-jira-hacking-spree/>

## 15. Critical GitHub Attack

This is serious:

A sophisticated cascading supply chain attack has compromised multiple GitHub Actions, exposing critical CI/CD secrets across tens of thousands of repositories. The attack, which originally targeted the widely used “tj-actions/changed-files” utility, is now believed to have originated from an earlier breach of the “reviewdog/action-setup@v1” GitHub Action, according to a report.

[...]

CISA confirmed the vulnerability has been patched in version 46.0.1.

Given that the utility is used by more than 23,000 GitHub repositories, the scale of potential impact has raised significant alarm throughout the developer community.

Source: <https://www.schneier.com/blog/archives/2025/03/critical-github-attack.html>

## 16. Critical Cisco Smart Licensing Utility flaws now exploited in attacks

Attackers have started targeting Cisco Smart Licensing Utility (CSLU) instances unpatched against a vulnerability exposing a built-in backdoor admin account.

The CSLU Windows application allows admins to manage licenses and linked products on-premises without connecting them to Cisco's cloud-based Smart Software Manager solution.

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

The company also addressed a second critical CSLU information disclosure vulnerability (CVE-2024-20440) that unauthenticated attackers can use to access log files containing sensitive data (including API credentials) by sending crafted HTTP requests to vulnerable devices.

These two vulnerabilities only impact systems running vulnerable Cisco Smart Licensing Utility releases and are only exploitable if the user starts the CSLU app—which isn't designed to run in the background by default.

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

## Targeted in attacks

SANS Technology Institute's Dean of Research Johannes Ullrich reported that threat actors are now chaining the two security flaws in exploitation attempts targeting CSLU instances exposed on the Internet.

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

While the end goal of these attacks is not known, the threat actor behind them is also trying to exploit other security vulnerabilities, including what looks like an information disclosure flaw with a public proof-of-concept exploit (CVE-2024-0305) impacting Guangzhou Yingke Electronic DVRs.

Cisco's security advisory for CVE-2024-20439 and CVE-2024-20440 still says that its Product Security Incident Response Team (PSIRT) has found no evidence that threat actors exploit the two security flaws in attacks.

CVE-2024-20439 isn't the first backdoor account Cisco removed from its products in recent years, with previous hardcoded credentials found in the company's Digital Network Architecture (DNA) Center, IOS XE, Wide Area Application Services (WAAS), and Emergency Responder software.

Source: <https://www.bleepingcomputer.com/news/security/critical-cisco-smart-licensing-utility-flaws-now-exploited-in-attacks/>

## 17. Veeam RCE bug lets domain users hack backup servers, patch now

Veeam has patched a critical remote code execution vulnerability tracked as CVE-2025-23120 in its Backup & Replication software that impacts domain-joined installations.

The flaw was disclosed yesterday and affects Veeam Backup & Replication version 12.3.0.310 and all earlier version 12 builds. The company fixed it in version 12.3.1 (build 12.3.1.1139), which was released yesterday.

According to a technical writeup by watchTower Labs, who discovered the bug, CVE-2025-23120 is a deserialization vulnerability in the Veeam.Backup.EsxManager.xmlFrameworkDs and Veeam.Backup.Core.BackupSummary .NET classes.

A deserialization flaw is when an application improperly processes serialized data, allowing attackers to inject malicious objects, or gadgets, that can execute harmful code.

Last year, while fixing a previous deserialization RCE flaw discovered by researcher Florian Hauser. To fix the flaw, Veeam introduced a blacklist of known classes or objects that could be exploited.

However, watchTower was able to find a different gadget chain that was not blacklisted to achieve remote code execution.

"Anyway, you've probably guessed where this is going today - it seems Veeam, despite being a ransomware gang's favourite play toy - didn't learn after the lesson given by Frycos in previous research published. You guessed it - they fixed the deserialization issues by adding entries to their deserialization blacklist."

The good news is that the flaw only impacts Veeam Backup & Replication installations that are joined to a domain. The bad news is that any domain user can exploit this vulnerability, making it easily exploitable in those configurations.

Unfortunately, many companies have joined their Veeam server to a Windows domain, ignoring the company's long-standing best practices.

Ransomware gangs have told BleepingComputer in the past that Veeam Backup & Replication servers are always targets, as it allows them an easy way to steal data and block restoration efforts by deleting backups.

This flaw would make Veeam installs even more valuable due to the ease with which threat actors can breach the servers.

While there are no reports of this flaw being exploited in the wild, watchTower has shared enough technical details that it would not be surprising to see a proof-of-concept (PoC) released soon.

Those companies using Veeam Backup & Replication should make it a priority to upgrade to 12.3.1 as soon as possible.

Furthermore, given ransomware gangs' interest in this application, it is strongly advised to review Veeam's best practices and disconnect the server from your domain.

Source: <https://www.bleepingcomputer.com/news/security/veeam-rce-bug-lets-domain-users-hack-backup-servers-patch-now/>

## 18. Microsoft Trusted Signing service abused to code-sign malware

Cybercriminals are abusing Microsoft's Trusted Signing platform to code-sign malware executables with short-lived three-day certificates.

Threat actors have long sought after code-signing certificates as they can be used to sign malware to appear like they are from a legitimate company.


Signed malware also has the advantage of potentially bypassing security filters that would normally block unsigned executables, or at least treat them with less suspicion.


The holy grail for threat actors is to obtain Extended Validation (EV) code-signing certificates, as they automatically gain increased trust from many cybersecurity programs due to the more rigorous verification process. Even more important, EV certificates are believed to gain a reputation boost in SmartScreen, helping to bypass alerts that would normally be displayed for unknown files.


However, EV code-signing certificates can be difficult to obtain, requiring them to be stolen from other companies or for threat actors to set up fake businesses and spend thousands of dollars to purchase one. Furthermore, once the certificate is used in a malware campaign, it is usually revoked, making it unusable for future attacks.

## Abusing Microsoft Trusted Signing service

Recently, cybersecurity researchers have seen threat actors utilizing the Microsoft Trusted Signing service to sign their malware with short-lived, three-day code-signing certificates.



**MalwareHunterTeam**   
 @malwrhunterteam · [Follow](#)



"InLine" signed "AddInProcess64.exe" sample:  
 f1eaf2e1269594edcf61f2e77d6ca25fc3947cff8508b34744  
 27521e67d6a5a

If remember right, this the first time I see a malware sample that was signed with a cert having "Microsoft ID Verified CS EOC CA 01" as issuer. And only valid 3 days? 🤔

**Signature Verification**

🟢 Signed file, valid signature

**File Version Information**

Original Name	AddInProcess64.exe
Internal Name	AddInProcess64.exe
File Version	1.0.0.0
Date signed	2025-03-08 16:03:00 UTC

**Signers**

— InLine

Name	InLine
Status	Valid
Issuer	Microsoft ID Verified CS EOC CA 01
Valid From	01:11 PM 03/08/2025
Valid To	01:11 PM 03/11/2025
Valid Usage	1.3.6.1.4.1.311.97.1.0, Code Signing, 1.3.6.1.4.1.311.97.65.1660658.716263006.411740162.823580325
Algorithm	sha384RSA
Thumbprint	91C71CD1B81D99B0B51D1EC542A4FB278B8F42E2
Serial Number	33 00 02 01 B5 D7 23 72 EE 41 6F 0D 8F 00 00 00 02 01 B5

+ Microsoft ID Verified CS EOC CA 01

+ Microsoft ID Verified Code Signing PCA 2021


+ Microsoft Identity Verification Root Certificate Authority 2020




**Counter Signers**

+ Microsoft Public RSA Time Stamping Authority

+ Microsoft Public RSA Timestamping CA 2020

+ Microsoft Identity Verification Root Certificate Authority 2020

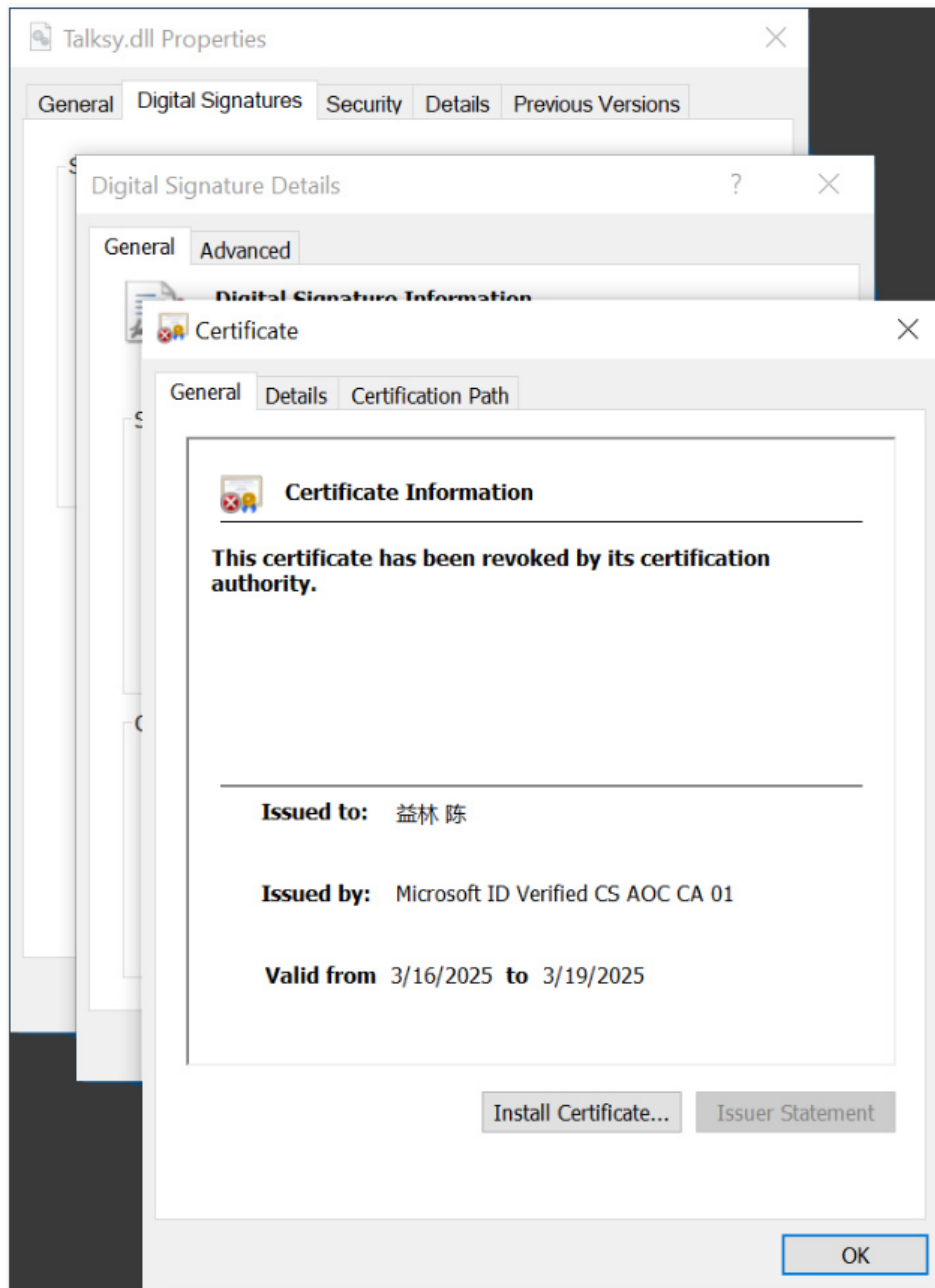
5:33 PM · Mar 8, 2025 

 **26**
 **Reply**
 **Copy link**

[Read 4 replies](#)

These malware samples are signed by "Microsoft ID Verified CS EOC CA 01" and the certificate is only valid for three days. While the certificate expires three days after being issued, it is important to note that executables signed with it will still be considered valid until the issuer revokes the certificate.

Since then other researchers and BleepingComputer have found numerous other samples used in ongoing malware campaigns, including those used in a Crazy Evil Trafffers crypto-theft campaign [VirusTotal] and Lumma Stealer [VirusTotal] campaigns.



*Signed DLL from Crazy Evil traffers campaign  
Source: BleepingComputer*

The Microsoft Trusted Signing service launched in 2024 and is a cloud-based service that allows developers to easily have their programs signed by Microsoft.

"Trusted Signing is a complete code signing service with an intuitive experience for developers and IT professionals, backed by a Microsoft managed certification authority," reads a Microsoft announcement for the service.

"The service supports both public and private trust signing scenarios and includes a timestamping service."

The platform has a \$9.99 monthly subscription service designed to make it easy for developers to sign their executables, while also offering additional security.



This increased security is accomplished by using short-lived certificates that can easily be revoked in the event of abuse and by never issuing the certificates directly to the developers, preventing them from being stolen in the event of a breach.

Microsoft also says certificates issued through the Trusted Signing service provide a similar SmartScreen reputation boost to executables signed by its service.

"A Trusted Signing signature ensures that your application is trusted by providing base reputation on smart screen, user mode trust on Windows, and integrity check signature validation compliant," reads an FAQ on the Trusted Signing site.

To protect against abuse, Microsoft is currently only allowing certificates to be issued under a company name if they have been in business for three years.

However, individuals can sign up and get approved more easily if they are okay with the certificates being issued under their name.

## A simpler path

A cybersecurity researcher and developer known as 'Squiblydoo,' who has been tracking malware campaigns abusing certificates for years, told BleepingComputer that they believe threat actors are switching to Microsoft's service out of convenience.

"I think there are a few reasons for the change. For a long time, using EV certificates has been the standard, but Microsoft has announced changes to EV certificates," Squiblydoo told BleepingComputer.

"However, the changes to EV certificates really aren't clear to anyone: not certificate providers, not attackers. However, due to these potential changes and lack of clarity, just having a code-signing certificate may be adequate for attacker needs."

"In this regard, the verification process for Microsoft's certificates is substantially easier than the verification process for EV certificates: due to the ambiguity over EV certificates, it makes sense to use the Microsoft certificates."

BleepingComputer contacted Microsoft about the abuse and was told that the company uses threat intelligence monitoring to find and revoke certificates as they are found.

"We use active threat intelligence monitoring to constantly look for any misuse or abuse of our signing service," Microsoft told BleepingComputer.

"When we detect threats we immediately mitigate with actions such as broad certificate revocation and account suspension. The malware samples you shared are detected by our antimalware products and we have already taken action to revoke the certificates and prevent further account abuse."

Source: <https://www.bleepingcomputer.com/news/security/microsoft-trusted-signing-service-abused-to-code-sign-malware/>



## 19. More Countries are Demanding Backdoors to Encrypted Apps

Last month, I wrote about the UK forcing Apple to break its Advanced Data Protection encryption in iCloud. More recently, both Sweden and France are contemplating mandating backdoors. Both initiatives are attempting to scare people into supporting backdoors, which are—of course—are terrible idea.

Also: “A Feminist Argument Against Weakening Encryption.”

Source: <https://www.schneier.com/blog/archives/2025/03/more-countries-are-demanding-backdoors-to-encrypted-apps.html>

## 20. Critical flaw in Next.js lets hackers bypass authorization

A critical severity vulnerability has been discovered in the Next.js open-source web development framework, potentially allowing attackers to bypass authorization checks.

The flaw, tracked as CVE-2025-29927, enables attackers to send requests that reach destination paths without going through critical security checks.

Next.js is a popular React framework with more than 9 million weekly downloads on npm. It is used for building full-stack web apps and includes middleware components for authentication and authorization.

Front-end and full-stack developers use it to build web apps with React. Some of the more notable companies using it for their sites/apps are TikTok, Twitch, Hulu, Netflix, Uber, and Nike.

### Authorization bypass

In Next.js, middleware components run before a request hits an application routing system and serve purposes like authentication, authorization, logging, error handling, redirecting users, applying geo-blocking or rate limits.

To prevent infinite loops where middleware re-triggers itself, Next.js uses a header called 'x-middleware-subrequest' that dictates if middleware functions should be applied or not.

The header is retrieved by the 'runMiddleware' function responsible for processing incoming requests. If it detects the 'x-middleware-subrequest' header, with a specific value, the entire middleware execution chain is bypassed and the request is forwarded to its destination.

An attacker can manually send a request that includes the header with a correct value and thus bypass protection mechanisms.

According to researchers Allam Rachid and Allam Yasser (inzo\_), who discovered the vulnerability and published a technical write-up, "the header and its value act as a universal key allowing rules to be overridden."

The vulnerability impacts all Next.js versions before 15.2.3, 14.2.25, 13.5.9. and 12.3.5. Users are recommended to upgrade to newer revisions as soon as possible, since technical details for exploiting the security issue are public.

Next.js' security bulletin clarifies that CVE-2025-29927 impacts only self-hosted versions that use 'next start' with 'output: standalone'. Next.js apps hosted on Vercel and Netlify, or deployed as static exports, are not affected.

Also affected are environments where middleware is used for authorization or security checks and there is no validation later in the application.

If patching is not possible at the time, the recommendation is to block external user requests that include the 'x-middleware-subrequest header'.

Source: <https://www.bleepingcomputer.com/news/security/critical-flaw-in-nextjs-lets-hackers-bypass-authorization/>

## 21. New VanHelsing ransomware targets Windows, ARM, ESXi systems

A new multi-platform ransomware-as-a-service (RaaS) operation named VanHelsing has emerged, targeting Windows, Linux, BSD, ARM, and ESXi systems.

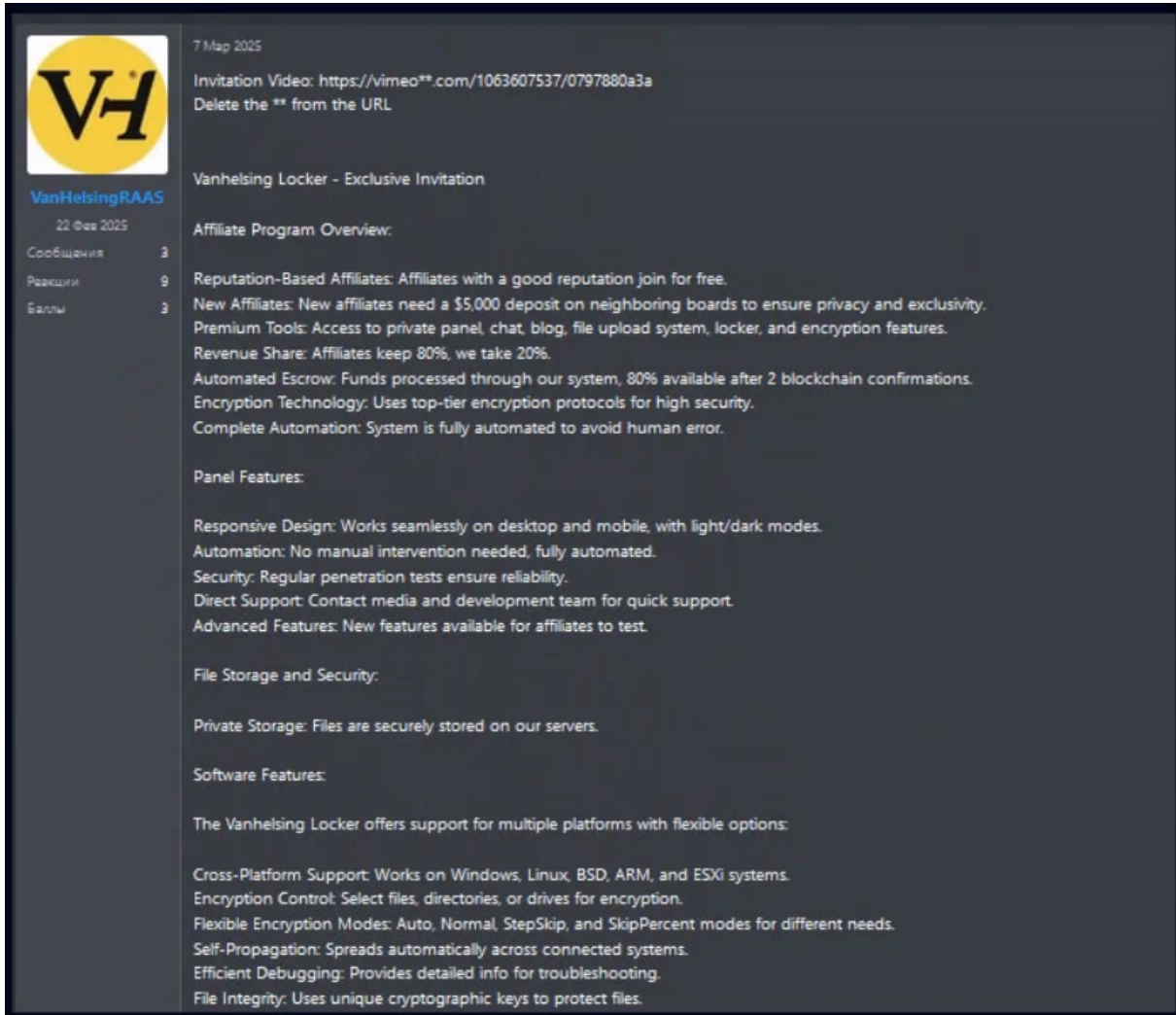
VanHelsing was first promoted on underground cybercrime platforms on March 7, offering experienced affiliates a free pass to join while mandating a deposit of \$5,000 from less experienced threat actors.

The new ransomware operation was first documented by CYFIRMA late last week, while Check Point Research performed a more in-depth analysis published yesterday.

### Inside VanHelsing

Check Point's analysts report that VanHelsing is a Russian cybercrime project that forbids targeting systems in CIS (Commonwealth of Independent States) countries.

Affiliates are allowed to keep 80% of the ransom payments while the operators take a 20% cut. The payments are handled via an automated escrow system that employs two blockchain confirmations for security.



7 Mar 2025

Invitation Video: <https://vimeo.com/1063607537/0797880a3a>  
Delete the \*\* from the URL

VanHelsing Locker - Exclusive Invitation

Affiliate Program Overview:

- Reputation-Based Affiliates: Affiliates with a good reputation join for free.
- New Affiliates: New affiliates need a \$5,000 deposit on neighboring boards to ensure privacy and exclusivity.
- Premium Tools: Access to private panel, chat, blog, file upload system, locker, and encryption features.
- Revenue Share: Affiliates keep 80%, we take 20%.
- Automated Escrow: Funds processed through our system, 80% available after 2 blockchain confirmations.
- Encryption Technology: Uses top-tier encryption protocols for high security.
- Complete Automation: System is fully automated to avoid human error.

Panel Features:

- Responsive Design: Works seamlessly on desktop and mobile, with light/dark modes.
- Automation: No manual intervention needed, fully automated.
- Security: Regular penetration tests ensure reliability.
- Direct Support: Contact media and development team for quick support.
- Advanced Features: New features available for affiliates to test.

File Storage and Security:

- Private Storage: Files are securely stored on our servers.

Software Features:

The VanHelsing Locker offers support for multiple platforms with flexible options:

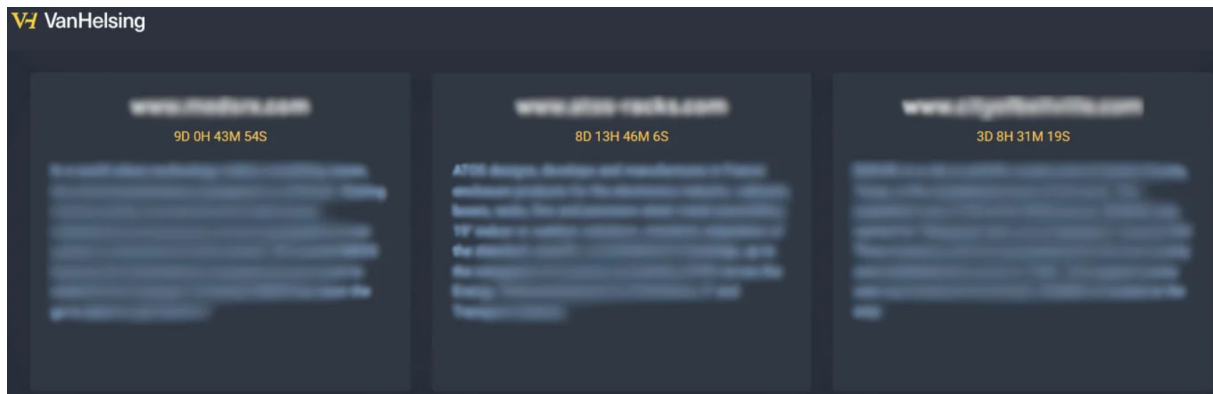
- Cross-Platform Support: Works on Windows, Linux, BSD, ARM, and ESXi systems.
- Encryption Control: Select files, directories, or drives for encryption.
- Flexible Encryption Modes: Auto, Normal, StepSkip, and SkipPercent modes for different needs.
- Self-Propagation: Spreads automatically across connected systems.
- Efficient Debugging: Provides detailed info for troubleshooting.
- File Integrity: Uses unique cryptographic keys to protect files.

*VanHelsing advertisement inviting affiliates to join  
Source: Check Point*

Accepted affiliates gain access to a panel with full operational automation, while there's also direct support from the development team.

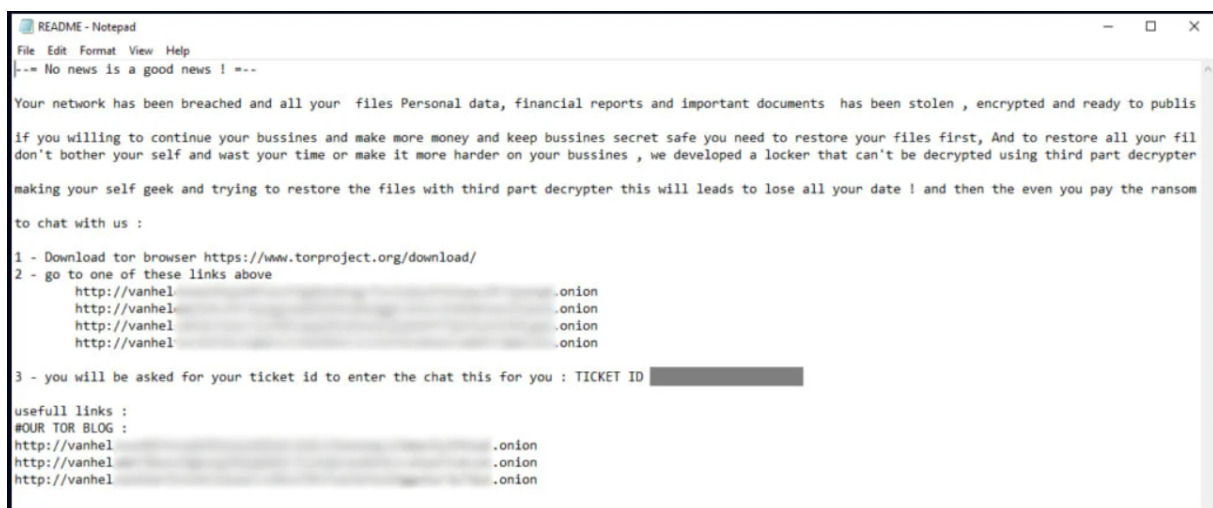
Files stolen from the victims' networks are stored directly on the VanHelsing operation's servers, while the core team claims that they perform regular penetration tests to ensure top-notch security and system reliability.

Currently, the VanHelsing extortion portal on the dark web lists three victims, two in the U.S. and one in France. One of the victims is a city in Texas, while the other two are technology companies.



*The VanHelsing extortion page  
Source: BleepingComputer*

The ransomware operators threaten to leak the stolen files in the coming days if their financial demands aren't met. According to Check Point's investigation, that's a \$500,000 ransom payment.



*The VanHelsing ransom note  
Source: Check Point*

## Stealth mode

The VanHelsing ransomware is written in C++, and evidence suggests that it was deployed in the wild for the first time on March 16.

VanHelsing uses the ChaCha20 algorithm for file encryption, generating a 32-byte (256-bit) symmetric key and a 12-byte nonce for each file.

These values are then encrypted using an embedded Curve25519 public key, and the resulting encrypted key/nonce pair is stored in the encrypted file.

VanHelsing partially encrypts files larger than 1GB in size, but runs the full process on smaller files.

The malware supports rich CLI customization to tailor attacks per victim, such as targeting specific drives and folders, restricting the scope of encryption, spreading via SMB, skipping shadow copies deletion, and enabling two-phase stealth mode.

In normal encryption mode, VanHelsing enumerates files and folders, encrypts the file contents, and renames the resulting file appending the '.vanhelsing' extension.

In stealth mode, the ransomware decouples encryption from file renaming, which is less likely to trigger alarms because file I/O patterns mimic normal system behavior.

```
int __thiscall silent_encryption_40BA50(LPCWSTR *ExistingFileName)
{
    DWORD LastError; // eax
    WCHAR NewFileName[6240]; // [esp+8h] [ebp-4838h] BYREF
    WCHAR v5[3002]; // [esp+30C8h] [ebp-1778h] BYREF

    if ( flag_silent_564DB0 == TRUE )
    {
        formatString_40B0A0((char *)NewFileName, 0x1860, (const char *)L"%s.vanhelsing", *ExistingFileName);
        wprintfW(v5, L"[*] File %s LOCKED SUCCESSFULLY\n", NewFileName);
        if ( flag_verbose_564DB4 == 1 )
            printf_4011D0((char *)L"%s\n", v5);
        if ( !MoveFileExW(*ExistingFileName, NewFileName, 3u) )
        {
            LastError = GetLastError();
            wprintfW(v5, L"[*] Failed to change file name, error id: %d \n", LastError);
            if ( flag_verbose_564DB4 == TRUE )
                printf_4011D0((char *)L"%s\n", v5);
        }
    }
    return 1;
}
```

*Stealth encryption function*

*Source: Check Point*

Even if security tools react at the start of the renaming phase, on the second pass, the entire targeted dataset will have been already encrypted.

While VanHelsing appears advanced and quickly evolving, Check Point noticed a few flaws that reveal code immaturity.

These include mismatches in the file extension, errors in the exclusion list logic that may trigger double encryption passes, and several unimplemented command-line flags.

Despite the presence of errors, VanHelsing remains a worrying rising threat that appears that could start gaining traction soon.

Source: <https://www.bleepingcomputer.com/news/security/new-vanhelsing-ransomware-targets-windows-arm-esxi-systems/>

## 22. Report on Paragon Spyware

Zyxel Citizen Lab has a new report on Paragon's spyware:

### Key Findings:

- **Introducing Paragon Solutions.** Paragon Solutions was founded in Israel in 2019 and sells spyware called Graphite. The company differentiates itself by claiming it has safeguards to prevent the kinds of spyware abuses that NSO Group and other vendors are notorious for.
- **Infrastructure Analysis of Paragon Spyware.** Based on a tip from a collaborator, we mapped out server infrastructure that we attribute to Paragon's Graphite spyware

tool. We identified a subset of suspected Paragon deployments, including in Australia, Canada, Cyprus, Denmark, Israel, and Singapore.

- **Identifying a Possible Canadian Paragon Customer.** Our investigation surfaced potential links between Paragon Solutions and the Canadian Ontario Provincial Police, and found evidence of a growing ecosystem of spyware capability among Ontario-based police services.
- **Helping WhatsApp Catch a Zero-Click.** We shared our analysis of Paragon’s infrastructure with Meta, who told us that the details were pivotal to their ongoing investigation into Paragon. WhatsApp discovered and mitigated an active Paragon zero-click exploit, and later notified over 90 individuals who it believed were targeted, including civil society members in Italy.
- **Android Forensic Analysis: Italian Cluster.** We forensically analyzed multiple Android phones belonging to Paragon targets in Italy (an acknowledged Paragon user) who were notified by WhatsApp. We found clear indications that spyware had been loaded into WhatsApp, as well as other apps on their devices.
- **A Related Case of iPhone Spyware in Italy.** We analyzed the iPhone of an individual who worked closely with confirmed Android Paragon targets. This person received an Apple threat notification in November 2024, but no WhatsApp notification. Our analysis showed an attempt to infect the device with novel spyware in June 2024. We shared details with Apple, who confirmed they had patched the attack in iOS 18.
- **Other Surveillance Tech Deployed Against The Same Italian Cluster.** We also note 2024 warnings sent by Meta to several individuals in the same organizational cluster, including a Paragon victim, suggesting the need for further scrutiny into other surveillance technology deployed against these individuals.

Source: <https://www.schneier.com/blog/archives/2025/03/ai-data-poisoning.html>

## 23. AI Data Poisoning

Cloudflare has a new feature—available to free users as well—that uses AI to generate random pages to feed to AI web crawlers:

Instead of simply blocking bots, Cloudflare’s new system lures them into a “maze” of realistic-looking but irrelevant pages, wasting the crawler’s computing resources. The approach is a notable shift from the standard block-and-defend strategy used by most website protection services. Cloudflare says blocking bots sometimes backfires because it alerts the crawler’s operators that they’ve been detected.

“When we detect unauthorized crawling, rather than blocking the request, we will link to a series of AI-generated pages that are convincing enough to entice a crawler to traverse them,” writes Cloudflare. “But while real looking, this content is not actually the content of the site we are protecting, so the crawler wastes time and resources.”

The company says the content served to bots is deliberately irrelevant to the website being crawled, but it is carefully sourced or generated using real scientific facts—such as neutral



information about biology, physics, or mathematics—to avoid spreading misinformation (whether this approach effectively prevents misinformation, however, remains unproven).

It's basically an AI-generated honeypot. And AI scraping is a growing problem:

The scale of AI crawling on the web appears substantial, according to Cloudflare's data that lines up with anecdotal reports we've heard from sources. The company says that AI crawlers generate more than 50 billion requests to their network daily, amounting to nearly 1 percent of all web traffic they process. Many of these crawlers collect website data to train large language models without permission from site owners....

Presumably the crawlers will now have to up both their scraping stealth and their ability to filter out AI-generated content like this. Which means the honeypots will have to get better at detecting scrapers and more stealthy in their fake content. This arms race is likely to go back and forth, wasting a lot of energy in the process.

Source: <https://www.schneier.com/blog/archives/2025/03/ai-data-poisoning.html>

## 24. RedCurl cyberspies create ransomware to encrypt Hyper-V servers

A threat actor named 'RedCurl,' known for stealthy corporate espionage operations since 2018, is now using a ransomware encryptor designed to target Hyper-V virtual machines.

Previously, RedCurl was spotted by Group-IB targeting corporate entities worldwide, later expanding its operations and increasing the victim count.

However, as Bitdefender Labs researchers report, the threat actors have started deploying ransomware on compromised networks.

"We've seen RedCurl stick to their usual playbook in most cases, continuing with data exfiltration over longer periods of time," reads the Bitdefender report.

"However, one case stood out. They broke their routine and deployed ransomware for the first time."

As the enterprise increasingly moves to virtual machines to host their servers, ransomware gangs have followed the trend, creating encryptors that specifically target virtualization platforms.

While most ransomware operations focus on targeting VMware ESXi servers, RedCurl's new "QWCrypt" ransomware specifically targets virtual machines hosted on Hyper-V.

### QWCrypt attacks

The attacks observed by Bitdefender start with phishing emails with ".IMG" attachments disguised as CVs. IMG files are disk image files that are automatically mounted by Windows under a new drive letter when they are double-clicked.

The IMG files contain a screensaver file vulnerable to DLL sideloading using a legitimate Adobe executable, which downloads a payload and sets persistence via a scheduled task.



RedCurl leverages "living-off-the-land" tools to maintain stealth on Windows systems, uses a custom wmiexec variant to spread laterally in the network without triggering security tools, and uses the tool 'Chisel' for tunneling/RDP access.

To turn off defenses before the ransomware deployment, the attackers use encrypted 7z archives and a multi-stage PowerShell process.

Unlike many Windows ransomware encryptors, QWCrypt supports numerous command-line arguments that control how the encryptor will target Hyper-V virtual machines to customize attacks.

```
--excludeVM string  Exclude VMs (csv list)
--hv                Encrypt HyperV VMs
--kill              Kill VM process
--turnoff           TurnOff HyperV VMs (default true)
```

In attacks seen by Bitdefender, RedCurl utilized the --excludeVM argument to avoid encrypting virtual machines that acted as network gateways to avoid disruption.

When encrypting files, the researchers say that QWCrypt ('rbcw.exe') uses the XChaCha20-Poly1305 encryption algorithm and appends either the .locked\$ or .randombits\$ extension to encrypted files.

The encryptor also offers the option to use intermittent encryption (block skipping) or selective file encryption based on size for increased speed.

The ransom note created by QWCrypt is named "!!!how\_to\_unlock\_randombits\_files.txt\$" and contains a mixture of text from LockBit, HardBit, and Mimic ransom notes.

The absence of a dedicated leak site for double extortion raises questions on whether RedCurl is using ransomware as a false flag or for true extortion attacks.

## Money, disruption, or diversion?

Bitdefender outlines two main hypotheses for why RedCurl now includes ransomware in its operations.

The first is that RedCurl operates as a mercenary group offering services to third parties, which results in a mix of espionage operations and financially motivated attacks.

In some situations, the ransomware could be a distraction to cover for data theft, or a fallback to monetize access when a client fails to pay for their primary services (data collection).

The second theory is that RedCurl does engage in ransomware operations for enrichment, but opts to do so silently, preferring private negotiations over public ransom demands and data leaks.

"The RedCurl group's recent deployment of ransomware marks a significant evolution in their tactics," concludes Bitdefender.

"This departure from their established modus operandi raises critical questions about their motivations and operational objectives."

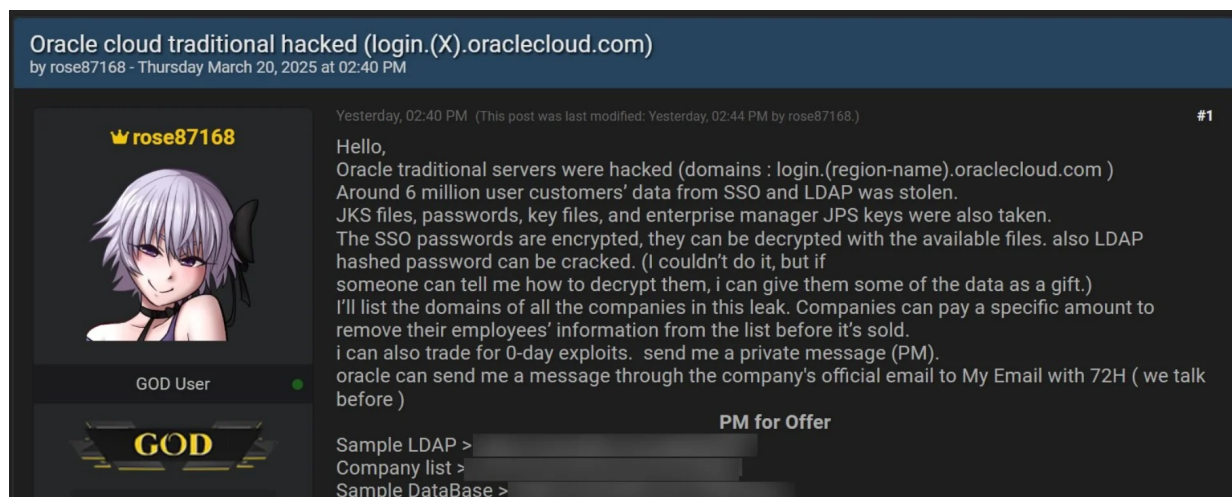
Source: <https://www.bleepingcomputer.com/news/security/redcurl-cyberspies-create-ransomware-to-encrypt-hyper-v-servers/>

## 25. Oracle customers confirm data stolen in alleged cloud breach is valid

Despite Oracle denying a breach of its Oracle Cloud federated SSO login servers and the theft of account data for 6 million people, BleepingComputer has confirmed with multiple companies that associated data samples shared by the threat actor are valid.

Last week, a person named 'rose87168' claimed to have breached Oracle Cloud servers and began selling the alleged authentication data and encrypted passwords of 6 million users. The threat actor also said that stolen SSO and LDAP passwords could be decrypted using the info in the stolen files and offered to share some of the data with anyone who could help recover them.

The threat actor released multiple text files consisting of a database, LDAP data, and a list of 140,621 domains for companies and government agencies that were allegedly impacted by the breach. It should be noted that some of the company domains look like tests, and there are multiple domains per company.



*Threat actor selling allegedly stolen Oracle Cloud data  
Source: BleepingComputer*

In addition to the data, rose87168 shared an Archive.org URL with BleepingComputer for a text file hosted on the "login.us2.oraclecloud.com" server that contained their email address. This file indicates that the threat actor could create files on Oracle's server, indicating an actual breach.

However, Oracle has denied that it suffered a breach of Oracle Cloud and has refused to respond to any further questions about the incident.

"There has been no breach of Oracle Cloud. The published credentials are not for the Oracle Cloud. No Oracle Cloud customers experienced a breach or lost any data," the company told BleepingComputer last Friday.

This denial, however, contradicts findings from BleepingComputer, which received additional samples of the leaked data from the threat actor and contacted the associated companies.

Representatives from these companies, all who agreed to confirm the data under the promise of anonymity, confirmed the authenticity of the information. The companies stated that the associated LDAP display names, email addresses, given names, and other identifying information were all correct and belonged to them.

The threat actor also shared emails with BleepingComputer, claiming to be part of an exchange between them and Oracle.

One email shows the threat actor contacting Oracle's security email (secalert\_us@oracle.com) to report that they hacked the servers.

"I've dug into your cloud dashboard infrastructure and found a massive vulnerability that has handed me full access to info on 6 million users," reads the email seen by BleepingComputer.

Another email thread shared with BleepingComputer shows an exchange between the threat actor and someone using a ProtonMail email address who claims to be from Oracle. BleepingComputer has redacted the email address of this other person as we could not verify their identity or the veracity of the email thread.

In this email exchange, the threat actor says someone from Oracle using a @proton.me email address told them that "We received your emails. Let's use this email for all communications from now on. Let me know when you get this."

Cybersecurity firm Cloudsek has also found an Archive.org URL showing that the "login.us2.oraclecloud.com" server was running Oracle Fusion Middleware 11g as of February 17, 2025. Oracle has since taken this server offline after news of the alleged breach was reported.

This version of the software was impacted by a vulnerability tracked as CVE-2021-35587 that allowed unauthenticated attackers to compromise Oracle Access Manager. The threat actor claimed that this vulnerability was used in the alleged breach of Oracle's servers.

BleepingComputer has emailed Oracle numerous times about this information but has not received any response.

Source: <https://www.bleepingcomputer.com/news/security/oracle-customers-confirm-data-stolen-in-alleged-cloud-breach-is-valid/>

## 26. Mozilla warns Windows users of critical Firefox sandbox escape flaw

Mozilla has released Firefox 136.0.4 to patch a critical security vulnerability that can let attackers escape the web browser's sandbox on Windows systems.

Tracked as CVE-2025-2857, this flaw is described as an "incorrect handle could lead to sandbox escapes" and was reported by Mozilla developer Andrew McCreight.

The vulnerability impacts the latest Firefox standard and extended support releases (ESR) designed for organizations that require extended support for mass deployments. Mozilla fixed the security flaw in Firefox 136.0.4 and Firefox ESR versions 115.21.1 and 128.8.1.

While Mozilla didn't share technical details regarding CVE-2025-2857, it said the vulnerability is similar to a Chrome zero-day exploited in attacks and patched by Google earlier this week.

"Following the sandbox escape in CVE-2025-2783, various Firefox developers identified a similar pattern in our IPC code. Attackers were able to confuse the parent process into leaking handles into unprivileged [sic] child processes leading to a sandbox escape," Mozilla said in a Thursday advisory.

"The original vulnerability was being exploited in the wild. This only affects Firefox on Windows. Other operating systems are unaffected."

## Chrome zero-day exploited to target Russia

Kaspersky's Boris Larin and Igor Kuznetsov, who discovered and reported CVE-2025-2783 to Google, said on Tuesday that the zero-day was exploited in the wild to bypass Chrome sandbox protections and infect targets with sophisticated malware.

They spotted CVE-2025-2783 exploits deployed in a cyber-espionage campaign dubbed Operation ForumTroll, targeting Russian government organizations and journalists at unnamed Russian media outlets.

"The vulnerability CVE-2025-2783 really left us scratching our heads, as, without doing anything obviously malicious or forbidden, it allowed the attackers to bypass Google Chrome's sandbox protection as if it didn't even exist," they said.

"The malicious emails contained invitations supposedly from the organizers of a scientific and expert forum, 'Primakov Readings,' targeting media outlets, educational institutions and government organizations in Russia."

In October, Mozilla also patched a zero-day vulnerability (CVE-2024-9680) in Firefox's animation timeline feature exploited by the Russian-based RomCom cybercrime group that let the attackers gain code execution in the web browser's sandbox.

The flaw was chained with a Windows privilege escalation zero-day (CVE-2024-49039) that allowed the Russian hackers to execute code outside the Firefox sandbox. Their victims were tricked into visiting an attacker-controlled website that downloaded and executed the RomCom backdoor on their systems.

Months earlier, it fixed two Firefox zero-day vulnerabilities one day after they were exploited at the Pwn2Own Vancouver 2024 hacking competition.

Source: <https://www.bleepingcomputer.com/news/security/mozilla-warns-windows-users-of-critical-firefox-sandbox-escape-flaw/>

## 27. New Ubuntu Linux security bypasses require manual mitigations

Three security bypasses have been discovered in Ubuntu Linux's unprivileged user namespace restrictions, which could enable a local attacker to exploit vulnerabilities in kernel components.

The issues allow local unprivileged users to create user namespaces with full administrative capabilities and impact Ubuntu versions 23.10, where unprivileged user namespaces restrictions are enabled, and 24.04 which has them active by default.

Linux user namespaces allow users to act as root inside an isolated sandbox (namespace) without having the same privileges on the host.

Ubuntu added AppArmor-based restrictions in version 23.10 and enabled them by default in 24.04 to limit the risk of namespace misuse.

Researchers at cloud security and compliance company Qualys found that these restrictions can be bypassed in three different ways.

“Qualys TRU uncovered three distinct bypasses of these namespace restrictions, each enabling local attackers to create user namespaces with full administrative capabilities,” the researchers say.

*“These bypasses facilitate exploiting vulnerabilities in kernel components requiring powerful administrative privileges within a confined environment” - Qualys*

The researchers note that these bypasses are dangerous when combined with kernel-related vulnerabilities, and they are not enough to obtain complete control of the system.

Qualys provides technical details for the three bypass methods, which are summarized as follows:

- **Bypass via aa-exec:** Users can exploit the *aa-exec* tool, which allows running programs under specific AppArmor profiles. Some of these profiles - like *trinity*, *chrome*, or *flatpak* - are configured to allow creating user namespaces with full capabilities. By using the *unshare* command through *aa-exec* under one of these permissive profiles, an unprivileged user can bypass the namespace restrictions and increase privileges within a namespace.
- **Bypass via busybox:** The busybox shell, installed by default on both Ubuntu Server and Desktop, is associated with an AppArmor profile that also permits unrestricted user namespace creation. An attacker can launch a shell via busybox and use it to execute *unshare*, successfully creating a user namespace with full administrative capabilities.
- **Bypass via LD\_PRELOAD:** This technique leverages the dynamic linker’s LD\_PRELOAD environment variable to inject a custom shared library into a trusted process. By injecting a shell into a program like Nautilus - which has a permissive AppArmor profile - an attacker can launch a privileged namespace from within that process, bypassing the intended restrictions.

Qualys notified the Ubuntu security team of their findings on January 15 and agreed to a coordinated release. However, the busybox bypass was discovered independently by vulnerability researcher Roddux, who published the details on March 21.

## Canonical’s response and mitigations

Canonical, the organization behind Ubuntu Linux, has acknowledged Qualys’ findings and confirmed to BleepingComputer that they are developing improvements to the AppArmor protections.

A spokesperson told us that they are not treating these findings as vulnerabilities per se but as limitations of a defense-in-depth mechanism. Hence, protections will be released according to standard release schedules and not as urgent security fixes.

In a bulletin published on the official discussion forum (Ubuntu Discourse), the company shared the following hardening steps that administrators should consider:

- Enable `kernel.apparmor_restrict_unprivileged_unconfined=1` to block *aa-exec* abuse. (not enabled by default)
- Disable broad AppArmor profiles for busybox and Nautilus, which allow namespace creation.
- Optionally apply a stricter bwrap AppArmor profile for applications like Nautilus that rely on user namespaces.
- Use *aa-status* to identify and disable other risky profiles.

Source: <https://www.bleepingcomputer.com/news/security/new-ubuntu-linux-security-bypasses-require-manual-mitigations/>

## 28. Microsoft's killing script used to avoid Microsoft Account in Windows 11

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

This change was introduced in the latest Windows 11 Insider Dev preview build, which means it will likely be coming to production builds.

"We're removing the bypassnro.cmd script from the build to enhance security and user experience of Windows 11," reads the Windows 11 Insider Preview Build 26200.5516 release notes.

"This change ensures that all users exit setup with internet connectivity and a Microsoft Account."

Since the release of Windows 11, Microsoft has made it hard to use the operating system with a local account, instead forcing users to log in with a Microsoft Account.

Microsoft says this is done to make using the company's ecosystem of cloud-based features and services easier, such as using your account to store BitLocker recovery keys.

"When a user signs in with a Microsoft account, the device is connected to cloud services," explains Microsoft.

"The user can share many of their settings, preferences, and apps across devices."

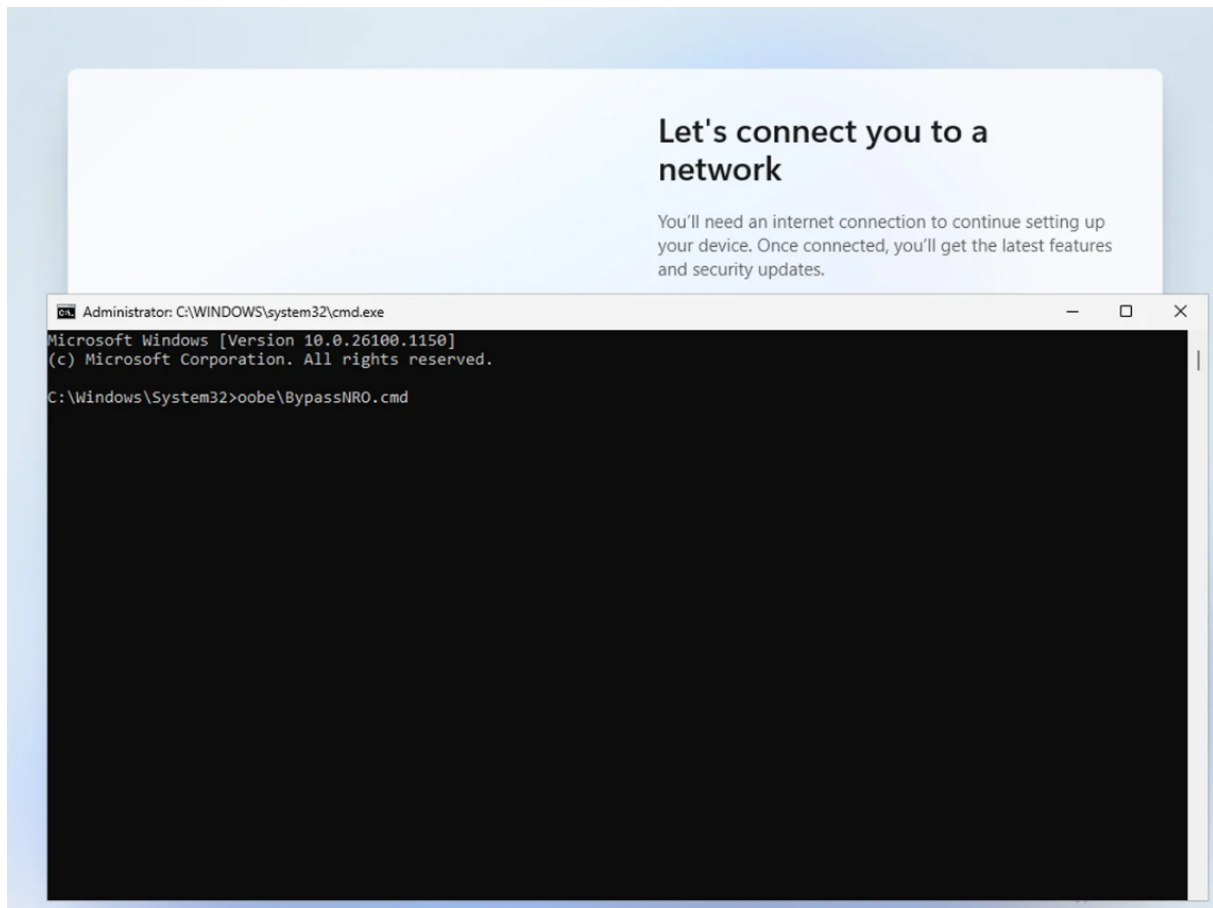
However, many users do not want to use a Microsoft Account, thinking it reduces their privacy and allows Microsoft to monitor their activities.

A popular method to bypass a Microsoft Account during setup is to use a script named 'C:\windows\system32\oobe\BypassNRO.cmd.' When run during Windows 11 setup, it creates a Registry value that removes the requirement to connect to the Internet during setup, which allows you to set up the operating system with a local account instead.

The script can be run during setup by pressing **Shift+F10** at the "Let's connect you to a network" screen to open a Windows command prompt.

In the command prompt window, type `c:\windows\system32\oobe\BypassNRO.cmd` to run the script and reboot your computer.





*Running the BypassNRO.cmd script  
Source: BleepingComputer*

On reboot, the Windows 11 setup will run again, and when you get to the networking screen, you will now have the option to skip-networking and set up a local account.

While Microsoft is now removing this script, they have not yet removed the BypassNRO Registry value. This means you can manually enter the following commands to achieve the same functionality as the now-removed script.

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE /v BypassNRO /t REG_DWORD /d 1 /f  
shutdown /r /t 0
```

If you feel comfortable modifying the Windows Registry, you can manually create the BypassNRO manually using Regedit, which can be launched from the Shift+F10 command prompt.

Unfortunately, it would not be surprising to see Microsoft remove the functionality of this Registry value in the future, making this technique no longer work.

Source: <https://www.bleepingcomputer.com/news/microsoft/microsofts-killing-script-used-to-avoid-microsoft-account-in-windows-11/>



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

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

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

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