



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

28 May 25

## Cyber Threat Roundup

*A collection of recent open-source items of interest to the Defense Industrial Base*

### Contents

|   |   |
|---|---|
| Articles .....  | 2 |
| Over 70 Malicious npm and VS Code Packages Found Stealing Data and Crypto.....                | 2 |
| Fake Zenmap. WinMRT sites target IT staff with Bumblebee malware.....                         | 2 |
| Hackers Use Fake VPN and Browser NSIS Installers to Deliver Winos 4.0 Malware .....           | 2 |
| ViciousTrap Uses Cisco Flaw to Build Global Honeypot from 5,300 Compromised Devices .....     | 2 |
| TikTok videos now push infostealer malware in ClickFix attacks .....                          | 2 |
| CISA Warns of Suspected Broader SaaS Attacks Exploiting App Secrets and Cloud Misconfigs..... | 3 |
| Russian Threat Actor TAG-110 Goes Phishing in Tajikistan.....                                 | 3 |

## Articles

### Over 70 Malicious npm and VS Code Packages Found Stealing Data and Crypto

As many as 60 malicious npm packages have been discovered in the package registry with malicious functionality to harvest hostnames, IP addresses, DNS servers, and user directories to a Discord-controlled endpoint. The packages, published under three different accounts, come with an install-time script that's triggered during npm install, Socket security researcher Kirill Boychenko said in a report published last week. The libraries have been collectively downloaded over 3,000 times.

<https://thehackernews.com/2025/05/over-70-malicious-npm-and-vs-code.html>

### Fake Zenmap. WinMRT sites target IT staff with Bumblebee malware

The Bumblebee malware SEO poisoning campaign uncovered earlier this week impersonating RVTools is using more typosquatting domains mimicking other popular open-source projects to infect devices used by IT staff. Both of these tools are commonly used by IT staff to diagnose or analyze network traffic, requiring administrative privileges for some of the features to work. This makes users of these tools prime targets for threat actors looking to breach corporate networks and spread laterally to other devices.

<https://www.bleepingcomputer.com/news/security/bumblebee-malware-distributed-via-zenmap-winmrt-seo-poisoning/>

### Hackers Use Fake VPN and Browser NSIS Installers to Deliver Winos 4.0 Malware

Cybersecurity researchers disclosed a malware campaign that uses fake software installers masquerading as popular tools like LetsVPN and QQ Browser to deliver the Winos 4.0 framework. The campaign, first detected by Rapid7 in February 2025, involves the use of a multi-stage, memory-resident loader called Catena. "Catena uses embedded shellcode and configuration switching logic to stage payloads like Winos 4.0 entirely in memory, evading traditional antivirus tools," security researchers Anna Širokova and Ivan Feigl said. "Once installed, it quietly connects to attacker-controlled servers – mostly hosted in Hong Kong – to receive follow-up instructions or additional malware."

<https://thehackernews.com/2025/05/hackers-use-fake-vpn-and-browser-nsis.html>

### ViciousTrap Uses Cisco Flaw to Build Global Honeypot from 5,300 Compromised Devices

Cybersecurity researchers disclosed that a threat actor codenamed ViciousTrap compromised nearly 5,300 unique network edge devices across 84 countries and turned them into a honeypot-like network. The threat actor has been observed exploiting a critical security flaw impacting Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers (CVE-2023-20118) to corral them into a set of honeypots en masse. A majority of the infections are located in Macau, with 850 compromised devices.

<https://thehackernews.com/2025/05/vicioustrap-uses-cisco-flaw-to-build.html>

### TikTok videos now push infostealer malware in ClickFix attacks

Cybercriminals are using TikTok videos to trick users into infecting themselves with Vidar and StealC information-stealing malware in ClickFix attacks. As Trend Micro recently discovered, the threat actors behind this TikTok social

engineering campaign are using videos likely generated using AI that ask viewers to run commands claiming to activate Windows and Microsoft Office, as well as premium features in various legitimate software like CapCut and Spotify. "This attack uses videos (possibly AI-generated) to instruct users to execute PowerShell commands, which are disguised as software activation steps. TikTok's algorithmic reach increases the likelihood of widespread exposure, with one video reaching more than half a million views," Trend Micro said.

<https://www.bleepingcomputer.com/news/security/tiktok-videos-now-push-infostealer-malware-in-clickfix-attacks/>

### **CISA Warns of Suspected Broader SaaS Attacks Exploiting App Secrets and Cloud Misconfigs**

On Thursday, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) revealed that Commvault is monitoring cyber threat activity targeting applications hosted in their Microsoft Azure cloud environment. "Threat actors may have accessed client secrets for Commvault's (Metallic) Microsoft 365 (M365) backup software-as-a-service (SaaS) solution, hosted in Azure," the agency said. The advisory comes weeks after Commvault revealed that Microsoft notified the company in February 2025 of unauthorized activity by a nation-state threat actor within its Azure environment.

<https://thehackernews.com/2025/05/cisa-warns-of-suspected-broader-saas.html>

### **Russian Threat Actor TAG-110 Goes Phishing in Tajikistan**

Recorded Future's Insikt Group published research detailing a Russia-aligned threat actor tracked as TAG-110 conducting espionage against government, educational, and research-related entities in Tajikistan. Ukrainian cyber agency CERT-UA said with medium confidence that TAG-110's activities overlap with UAC-0063 (a cyber espionage group that targets Central Asian nations) and has been linked to APT28 — the high-profile Russian nation-state group otherwise tracked as Fancy Bear. TAG-110 has been tracked for a few years now, with overlapping group UAC-0063 tracked since 2021. Since 2023, Recorded Future said, TAG-110 has been observed deploying an HTML application (HTA) file-based malware payload, known as HATVIBE. The campaign detailed today concerns about unrelated phishing activity tracked between January and February.

<https://www.darkreading.com/threat-intelligence/russian-threat-actor-tag-110-phishing-tajikistan>