



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

14 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets.....	2
Hacker Leaks Account Data of 12 Million Zacks Investment Users	2
Hackers Use CAPTCHA Trick on Webflow CDN PDFs to Bypass Security Scanners	2
PostgreSQL Flaw Exploited as Zero-day in BeyondTrust Breach.....	3
Chinese Hackers Breach More US Telecoms via Unpatched Cisco Routers.....	3

Articles

The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets

Resecurity identified an increase in malicious cyber activity targeting UAV and counter-UAV (C-UAV/C-UAS) technologies. That was especially notable during active periods of local conflicts, including the escalation of the Russia-Ukraine war and the Israel-Hamas confrontation. The trend of malicious targeting in the drone manufacturing segment increased during Q3-Q4 2024 and continued into Q1 2025. Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become integral to modern military operations, particularly for intelligence, surveillance, and reconnaissance (ISR) missions. As their use has expanded, so has the focus on counter-UAV (C-UAV) technologies designed to detect and neutralize these aerial threats. Cybercriminal groups, mercenaries and foreign nation-state actors express a significant interest in these technologies. Resecurity observed an increased interest in specialists involved in science and technology (S&T) and drone engineering by foreign actors, which enables them to pivot from cyber to traditional industrial espionage.

<https://securityaffairs.com/174199/intelligence/the-rise-of-cyber-espionage-uav-and-c-uav-technologies-as-targets.html>

Hacker Leaks Account Data of 12 Million Zacks Investment Users

Zacks Investment Research (Zacks) last year reportedly suffered another data breach that exposed sensitive information related to roughly 12 million accounts. Zacks is an American investment research company that provides its customers data-driven insights through a proprietary stock performance assessment tool called 'Zacks Rank', to help with making informed financial decisions. In late January, a threat actor published data samples on a hacker forum, claiming a breach at Zacks in June 2024 that exposed data of millions of customers. The published data, available to forum members in exchange for a small cryptocurrency amount, contains full names, usernames, email addresses, physical addresses, and phone numbers. It should be noted that there is also the possibility of threat actors scraping the information from other services and compiling a database with user information associated with Zacks.

<https://www.bleepingcomputer.com/news/security/hacker-leaks-account-data-of-12-million-zacks-investment-users/>

Hackers Use CAPTCHA Trick on Webflow CDN PDFs to Bypass Security Scanners

A widespread phishing campaign has been observed leveraging bogus PDF documents hosted on the Webflow content delivery network (CDN) with an aim to steal credit card information and commit financial fraud. The activity, ongoing since the second half of 2024, entails users looking for book titles, documents, and charts on search engines like Google to redirect users to PDF files hosted on Webflow CDN. These PDF files come embedded with an image that mimics a CAPTCHA challenge, causing users who click on it to be taken to a phishing page that, this time, hosts a real Cloudflare Turnstile CAPTCHA. In doing so, the attackers aim to lend the process a veneer of legitimacy, fooling victims into thinking that they had interacted with a security check, while also evading detection by static scanners. The development comes as SlashNext detailed a new phishing kit named Astaroth (not to be confused with a banking malware of the same name) that's advertised on Telegram and cybercrime marketplaces for \$2,000 in exchange for six-months of updates and bypass techniques.

<https://thehackernews.com/2025/02/hackers-use-captcha-trick-on-webflow.html>

PostgreSQL Flaw Exploited as Zero-day in BeyondTrust Breach

Rapid7's vulnerability research team says attackers exploited a PostgreSQL security flaw as a zero-day to breach the network of privileged access management company BeyondTrust in December. BeyondTrust revealed that attackers breached its systems and 17 Remote Support SaaS instances in early December using two zero-day bugs (CVE-2024-12356 and CVE-2024-12686) and a stolen API key. Less than one month later, in early January, the U.S. Treasury Department disclosed that its network was breached by threat actors who used a stolen Remote Support SaaS API key to compromise its BeyondTrust instance. Since then, the Treasury breach has been linked to Chinese state-backed hackers tracked as Silk Typhoon, a cyber-espionage group involved in reconnaissance and data theft attacks that became widely known after hacking an estimated 68,500 servers in early 2021 using Microsoft Exchange Server ProxyLogon zero-days.

<https://www.bleepingcomputer.com/news/security/postgresql-flaw-exploited-as-zero-day-in-beyondtrust-breach/>

Chinese Hackers Breach More US Telecoms via Unpatched Cisco Routers

China's Salt Typhoon hackers are still actively targeting telecoms worldwide and have breached more U.S. telecommunications providers via unpatched Cisco IOS XE network devices. Recorded Future's Insikt Group threat research division states that the Chinese hacking group (tracked Salt Typhoon and RedMike) has exploited the CVE-2023-20198 privilege escalation and CVE-2023-20273 Web UI command injection vulnerabilities. These ongoing attacks have already resulted in network breaches at multiple telecommunications providers, including a U.S. internet service provider (ISP), a U.S.-based affiliate of a U.K. telecommunications provider, a South African telecom provider, an Italian ISP, and a large Thailand telecommunications provider. These breaches are part of a broader campaign confirmed by the FBI and CISA in October. In these attacks, the Chinese state hackers breached multiple U.S. telecom carriers (including AT&T, Verizon, Lumen, Charter Communications, Consolidated Communications, and Windstream) and telecom companies in dozens of other countries.

<https://www.bleepingcomputer.com/news/security/chinese-hackers-breach-more-us-telecoms-via-unpatched-cisco-routers/>