



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

12 Feb 25

## Cyber Threat Roundup

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

### Contents

Articles .....	2
Microsoft Patches 'Wormable' Windows Flaw and File-Deleting Zero-Day .....	2
Cisco Says Ransomware Group's Leak Related to Old Hack.....	2
Fortinet Discloses Second Firewall Auth Bypass Patched in January .....	2
Russian Cybercrime Network Targeted for Sanctions Across US, UK and Australia .....	3
Russian Military Hackers Deploy Malicious Windows Activators in Ukraine .....	3

## Articles

### Microsoft Patches ‘Wormable’ Windows Flaw and File-Deleting Zero-Day

The Microsoft Patch Tuesday machine hummed loudly this month with the rollout of urgent fixes for a pair of already-exploited zero-days in its flagship Windows platform. Redmond's security response team patched at least 55 documented software defects in Windows OS and applications, and flagged a privilege escalation bug in Windows Storage, along with a code execution issue in the Windows Ancillary Function Driver for WinSock for immediate attention due to active exploitation. The Windows Storage Elevation of Privilege bug, tagged as CVE-2025-21391, lets attackers delete targeted files on a system, potentially causing major disruption and service outages. The company also urged Windows administrators to prioritize CVE-2025-21418 as a matter of urgency, warning that the Windows Ancillary Function Driver for WinSock contains a nasty flaw that provides SYSTEM privileges to a successful attacker. Microsoft slapped critical-severity ratings on three bulletins and noted that two other issues have already been publicly discussed. Security experts are also calling attention to CVE-2025-21376 which covers a remote code execution bug in the Windows Lightweight Directory Access Protocol (LDAP).

<https://www.securityweek.com/microsoft-patches-wormable-windows-flaw-and-file-deleting-zero-day/>

### Cisco Says Ransomware Group's Leak Related to Old Hack

Cisco says that the information recently posted on a ransomware group's Tor-based leak site refers to data stolen in a cyberattack three years ago. The data, a list of credentials apparently exfiltrated from Cisco's systems, appeared over the weekend on a new data leak site operated by the Kraken ransomware group. Cisco detailed the cyberattack in August 2022, after a ransomware group named Yanluowang added the tech giant to its leak site, claiming the theft of gigabytes of information. The incident was attributed to UNC2447, a Russia-linked threat actor known for using FiveHands and HelloKitty ransomware, to the infamous Lapsus\$ hacking gang, which dispersed in late 2022 after two British members were arrested and convicted, and to Yanluowang. Over the weekend, part of that data, namely a list of usernames, identifiers, and password hashes, was posted on Kraken's leak site, which features a total of six posts at this time.

<https://www.securityweek.com/cisco-says-ransomware-groups-leak-related-to-old-hack/>

### Fortinet Discloses Second Firewall Auth Bypass Patched in January

After publishing our story, Fortinet has informed us that the new CVE-2025-24472 flaw added to FG-IR-24-535 today is not a zero-day and was already fixed in January. Furthermore, even though today's updated advisory indicates that both flaws were exploited in attacks and even includes a workaround for the new CSF proxy requests exploitation pathway, Fortinet says that only CVE-2024-55591 was exploited. Fortinet told BleepingComputer that if a customer previously upgraded based on the guidance in FG-IR-24-535 / CVE-2024-55591, then they are already protected against the newly disclosed vulnerability. Successful exploitation of this authentication bypass vulnerability (CVE-2025-24472) allows remote attackers to gain super-admin privileges by making maliciously crafted CSF proxy requests. The security flaw impacts FortiOS 7.0.0 through 7.0.16, FortiProxy 7.0.0 through 7.0.19, and FortiProxy 7.2.0 through 7.2.12. Fortinet fixed it in FortiOS 7.0.17 or above and FortiProxy 7.0.20/7.2.13 or above.

<https://www.bleepingcomputer.com/news/security/fortinet-discloses-second-firewall-auth-bypass-patched-in-january/>

### **Russian Cybercrime Network Targeted for Sanctions Across US, UK and Australia**

The U.S., U.K. and Australia on Tuesday sanctioned a Russian web-hosting services provider and two Russian men who administer the service in support of Russian ransomware syndicate LockBit. The Treasury Department's Office of Foreign Assets Control and its U.K. and Australian counterparts sanctioned Zservers, a Russia-based bulletproof hosting services provider — which is a web-hosting service that ignores or evades law enforcement requests — and two Russian nationals serving as Zservers operators. Treasury alleges that Zservers provided LockBit access to specialized servers designed to resist law enforcement actions. LockBit ransomware attacks have extracted more than \$120 million from thousands of victims around the world. LockBit has operated since 2019, and is the most deployed ransomware variant across the world and continues to be prolific, according to the U.S. Cybersecurity and Infrastructure Security Agency.

<https://www.securityweek.com/russian-cybercrime-network-targeted-for-sanctions-across-us-uk-and-australia/>

### **Russian Military Hackers Deploy Malicious Windows Activators in Ukraine**

The Sandworm Russian military cyber-espionage group is targeting Windows users in Ukraine with trojanized Microsoft Key Management Service (KMS) activators and fake Windows updates. These attacks likely started in late 2023 and have now been linked by EclecticIQ threat analysts with Sandworm hackers based on overlapping infrastructure, consistent Tactics, Techniques and Procedures (TTPs), and frequently used ProtonMail accounts to register domains used in the attacks. The attackers also used a BACKORDER loader to deploy DarkCrystal RAT (DcRAT) malware (used in previous Sandworm attacks) and debug symbols referencing a Russian-language build environment, further reinforcing the researchers' confidence that Russian military hackers were involved. The attacks' end goal is to collect sensitive information from infected computers and send it to attacker-controlled servers. The malware steals keystrokes, browser cookies, browser history, saved credentials, FTP credentials, system information, and screenshots. Sandworm's use of malicious Windows activators was likely prompted by the vast attack surface opened by the heavy use of pirated software in Ukraine, which also plagues the country's government sector.

<https://www.bleepingcomputer.com/news/security/russian-military-hackers-deploy-malicious-windows-activators-in-ukraine/>