



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

18 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
Cybercriminals Shift Focus to Social Media as Attacks Reach Historic Highs	2
FreSSH Bugs Undiscovered for Years Threaten OpenSSH Security	2
Xerox VersaLink C7025 Multifunction Printer Flaws May Expose Windows Active Directory Credentials to Attackers.....	2
Russian State Hackers Target Organizations with Device Code Phishing.....	2

Articles

Cybercriminals Shift Focus to Social Media as Attacks Reach Historic Highs

The risk of encountering a threat climbed to 27.7% in Q4, with social engineering attacks accounting for 86% of all blocked threats. This underscores the increasingly sophisticated psychological tactics cybercriminals are using to deceive victims. Phishing attacks surged by 14% in Q4 2024, with cybercriminals exploiting website-building platforms like Wix to create convincing fake sites and spoofing brands like Apple iCloud through fraudulent invoice scams. Malvertising also remained a dominant attack vector, accounting for 41% of all blocked threats in the quarter, fueling scams and malware distribution.

<https://www.helpnetsecurity.com/2025/02/18/cybercriminals-social-media-attacks/>

FreSSH Bugs Undiscovered for Years Threaten OpenSSH Security

Vulnerabilities in OpenSSH allow miscreants to perform machine-in-the-middle (MitM) attacks on the OpenSSH client and pre-authentication denial-of-service (DoS) attacks. Patches for CVE-2025-26465 and CVE-2025-26466 were released this morning. Although their respective severity scores (6.8 and 5.9) don't necessarily scream "patch me right away" – it certainly doesn't seem as bad as last year's regreSSHion issue – they're both likely to raise some degree of concern given the tool's prominence. If an attacker exploits the MitM vulnerability, they could intercept or manipulate data transferred over what users expect to be a secure, encrypted channel. The DoS vulnerability (CVE-2025-26466) affects both the OpenSSH client and server, and could lead to prolonged outages preventing admins from performing maintenance on key servers, Abbasi added. It's caused by an asymmetric resource consumption of both memory and CPU.

https://www.theregister.com/2025/02/18/openssh_vulnerabilities_mitm_dos/

Xerox VersaLink C7025 Multifunction Printer Flaws May Expose Windows Active Directory Credentials to Attackers

Rapid7 researchers discovered vulnerabilities in Xerox Versalink C7025 Multifunction printers (MFPs) that could allow attackers to capture authentication credentials via pass-back attacks via LDAP and SMB/FTP services. The vulnerabilities impact Xerox Versalink MFPs and Firmware Version: 57.69.91 and earlier. "If a malicious actor can successfully leverage these issues, it would allow them to capture credentials for Windows Active Directory," concludes the report. "This means they could then move laterally within an organization's environment and compromise other critical Windows servers and file systems." Organizations using Xerox VersaLink C7025 Multifunction printers should update to the latest firmware. If patching isn't possible, they should set a strong admin password, avoid using high-privilege Windows accounts for LDAP or SMB, and disable unauthenticated remote access.

<https://securityaffairs.com/174342/hacking/xerox-versalink-c7025-multifunction-printer-flaws.html>

Russian State Hackers Target Organizations with Device Code Phishing

A Russia-linked threat actor tracked as Storm-2372 has been targeting government and private organizations in a global campaign employing device code phishing for account compromise, Microsoft reports. As part of a device code phishing attack, the threat actor asks the targeted service to generate a device code and convinces the victim to enter that code on a legitimate sign-in page. The targeted service then generates an access token that the attacker can recover and abuse to access the target's accounts and data. The threat actor can use the tokens to

access email and cloud storage services that the victim has permissions to, without a password, and to move laterally. “Storm-2372 likely targeted potential victims using third-party messaging services including WhatsApp, Signal, and Microsoft Teams, falsely posing as a prominent person relevant to the target to develop rapport before sending subsequent invitations to online events or meetings via phishing emails,” Microsoft notes.

<https://www.securityweek.com/russian-state-hackers-target-organizations-with-device-code-phishing/>