



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

25 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
FatalRAT Phishing Attacks Target APAC Industries Using Chinese Cloud Services	2
PoC Exploit for Ivanti Endpoint Manager Vulnerabilities Released (CVE-2024-13159)	2
US CISA Adds Adobe ColdFusion and Oracle Agile PLM Flaws to Its Known Exploited Vulnerabilities Catalog	2
Botnet Targets Basic Auth in Microsoft 365 Password Spray Attacks	2
New Malware Campaign Uses Cracked Software to Spread Lumma and ACR Stealer.....	3
Exploits for Unpatched Parallels Desktop Flaw Give Root on Macs	3

Articles

FatalRAT Phishing Attacks Target APAC Industries Using Chinese Cloud Services

Various industrial organizations in the Asia-Pacific (APAC) region have been targeted as part of phishing attacks designed to deliver a known malware called FatalRAT. The threat was orchestrated by attackers using legitimate Chinese cloud content delivery network (CDN) myqcloud and the Youdao Cloud Notes service as part of their attack infrastructure. The attackers employed a sophisticated multi-stage payload delivery framework to ensure evasion of detection. The activity has singled out government agencies and industrial organizations, particularly manufacturing, construction, information technology, telecommunications, healthcare, power and energy, and large-scale logistics and transportation, in Taiwan, Malaysia, China, Japan, Thailand, South Korea, Singapore, the Philippines, Vietnam, and Hong Kong.

<https://thehackernews.com/2025/02/fatalrat-phishing-attacks-target-apac.html>

PoC Exploit for Ivanti Endpoint Manager Vulnerabilities Released (CVE-2024-13159)

A proof-of-concept (PoC) exploit for four critical Ivanti Endpoint Manager vulnerabilities has been released by Horizon3.ai researchers. The vulnerabilities – CVE-2024-10811, CVE-2024-13161, CVE-2024-13160 and CVE-2024-13159 – are all path traversal flaws that could be exploited by remote, unauthenticated attackers to leverage Ivanti EPM machine account credentials for relay attacks and, ultimately, to compromise the Ivanti EPM server. If you haven't already upgraded to one of the fixed versions – EPM 2024 January-2025 Security Update or EPM 2022 SU6 January-2025 Security Update – you should do so now.

<https://www.helpnetsecurity.com/2025/02/24/poc-exploit-for-ivanti-endpoint-manager-vulnerabilities-released-cve-2024-13159/>

US CISA Adds Adobe ColdFusion and Oracle Agile PLM Flaws to Its Known Exploited Vulnerabilities Catalog

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SonicWall SonicOS and Palo Alto PAN-OS vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog. CVE-2017-3066 (CVSS score of 9.8) is a Java deserialization vulnerability in the Apache BlazeDS library in Adobe ColdFusion 2016 Update 3 and earlier, ColdFusion 11 update 11 and earlier, ColdFusion 10 Update 22 and earlier. An attacker can exploit the vulnerability to achieve arbitrary code execution. CVE-2024-20953 (CVSS score of 8.8) is a Deserialization Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Export). The flaw affects supported version 9.3.6. A low-privileged attacker with network access via HTTP to compromise Oracle Agile PLM could exploit this vulnerability to takeover Oracle Agile PLM.

<https://securityaffairs.com/174613/security/u-s-cisa-adds-adobe-coldfusion-and-oracle-agile-plm-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

Botnet Targets Basic Auth in Microsoft 365 Password Spray Attacks

A massive botnet of over 130,000 compromised devices is conducting password-spray attacks against Microsoft 365 (M365) accounts worldwide, targeting basic authentication to evade multi-factor authentication.

According to a report by SecurityScorecard, the attackers are leveraging credentials stolen by infostealer malware to target the accounts at a large scale. The attacks rely on non-interactive sign-ins using Basic Authentication (Basic Auth) to bypass Multi-Factor Authentication (MFA) protections and gain unauthorized access without triggering security alerts.

<https://www.bleepingcomputer.com/news/security/botnet-targets-basic-auth-in-microsoft-365-password-spray-attacks/>

New Malware Campaign Uses Cracked Software to Spread Lumma and ACR Stealer

Cybersecurity researchers are warning of a new campaign that leverages cracked versions of software as a lure to distribute information stealers like Lumma and ACR Stealer. A notable aspect of the stealer malware is the use of a technique called dead drop resolver to extract the actual command-and-control (C2) server. This includes relying on legitimate services like Steam, Telegram's Telegraph, Google Forms, and Google Slides. Threat actors enter the actual C2 domain in Base64 encoding on a specific page. The malware accesses this page, parses the string, and obtains the actual C2 domain address to perform malicious behaviors.

<https://thehackernews.com/2025/02/new-malware-campaign-uses-cracked.html>

Exploits for Unpatched Parallels Desktop Flaw Give Root on Macs

Two different exploits for an unpatched Parallels Desktop privilege elevation vulnerability have been publicly disclosed, allowing users to gain root access on impacted Mac devices. Parallels Desktop is a virtualization software that allows Mac users to run Windows, Linux, and other operating systems alongside macOS. It is very popular among developers, businesses, and casual users who need Windows applications on their Macs without rebooting.

<https://www.bleepingcomputer.com/news/security/exploits-for-unpatched-parallels-desktop-flaw-give-root-on-macs/>