Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

6 February 2024

Vulnerabilities

Experts warn of a surge of attacks targeting Ivanti SSRF flaw

Security Affairs - February 5 2024

The Ivanti SSRF vulnerability tracked as CVE-2024-21893 is actively exploited in attacks in the wild by multiple threat actors. The Ivanti Server-Side Request Forgery (SSRF) vulnerability, identified as CVE-2024-21893, is currently being actively exploited in real-world attacks by various threat actors.

Latest Critical Vulnerabilities in Juniper Secure Analytics and Mastodon: CVE-2023-37920, CVE-2021-4048, CVE-2024-23832

SOCRadar - February 5 2024

The latest serious issues demanding attention include severe vulnerabilities found in Juniper Networks' Secure Analytics and the decentralized social network "Mastodon". Of critical concern is the vulnerability in Mastodon, along with two vulnerabilities highlighted in the Juniper Secure Analytics advisory, each with CVSS scores exceeding 9.0.

Ransomware

US Department of Defense Contractor Targeted by Donut Ransomware

The Cyber Express - February 5 2024

The Donut ransomware group has expanded its victim list to include a prominent US Department of Defense contractor. The group, known for its malicious activities, posted a chilling message related to the DOD Contractor cyberattack on the dark web.

Group-IB Assists INTERPOL Operation Synergia vs. Ransomware in 50+ Countries

Cyber Security Asean - February 6 2024

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, took part in a global INTERPOL-led law enforcement operation named Synergia, aimed at combating the surge of phishing, banking malware, and ransomware

attacks in more than 50 countries. As part of the global operation, the Group-IB team identified more than 500 IP addresses hosting phishing resources and over 1,900 IP addresses associated with ransomware, Trojans, and banking malware operations.

Malware and threat actors

Pegasus Spyware Targets Jordanian Civil Society in Wide-Ranging Attacks
Dark Reading - February 5 2024

As the Middle East nation enforces strict cybercrime laws, citizens face crackdowns on free speech with nearly three dozen journalists and lawyers targeted with the NSO Group's spyware.

Fresh 'Mispadu Stealer' Variant Emerges
Dark Reading - February 5 2024

Latest iteration of the malware appears aimed at targets in Mexico.