Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

11 January 2023

Vulnerabilities

Ivanti customers urged to patch vulnerabilities allegedly exploited by Chinese state hackers

Record by Recorded Future - January 10 2024

The Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday urged customers of IT company Ivanti to patch two vulnerabilities that are being actively exploited.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Current Activity - January 10 2024

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-21887 Ivanti Connect Secure and Policy Secure Command Injection Vulnerability CVE-2023-46805 Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability.

Data compromise, NTLM relay attacks likely with Kyocera Device Manager bug

SC Magazine US - January 10 2024

Kyocera Device Manager instances impacted by the already patched path traversal vulnerability, tracked as CVE-2023-50916, could be targeted by threat actors to facilitate further malicious activity, including unauthorized account access and data exfiltration, reports The Hacker News.

Ransomware

Crooks pose as researchers to retarget ransomware victims

SC Magazine US - January 10 2024

Threat actors masquerading as cybersecurity researchers are approaching victims of the Royal and Akira ransomware gangs, offering to delete files the groups have stolen – for a price. It’s unclear whether the fraudulent offers of help – described as a follow-on extortion campaign – are being made by the same criminals responsible for the initial ransomware attacks.

Hackers are targeting exposed MS SQL servers with Mimic ransomware

Help Net Security - News - January 10 2024

Hackers are brute-forcing exposed MS SQL database servers to deliver Mimic ransomware, Securonix researchers are warning. About Mimic ransomware Mimic ransomware was first spotted in the wild in June 2022 and analyzed by Trend Micro researchers in January 2023.

Malware and threat actors

Pikabot Malware Surfaces As Qakbot Replacement for Black Basta Attacks

Dark Reading - January 10 2024

A threat actor associated with Black Basta ransomware attacks has been wielding a new loader similar to the notoriously hard-to-kill Qakbot, in a widespread phishing campaign aimed at gaining entry to organization networks for further malicious activity. Tracked as Water Curupira by Trend Micro, the actor is best known for conducting dangerous campaigns to drop backdoors such as Cobalt Strike that ultimately lead to Black Basta ransomware attacks, researchers said in a post published Jan. 9.

Yet another Mirai-based botnet is spreading an illicit cryptominer

Record by Recorded Future - January 10 2024

A well-designed operation is using a version of the infamous Mirai malware to secretly distribute cryptocurrency mining software, researchers said Wednesday.

Pikabot Malware Spreading Through Phishing Campaigns

KnowBe4 - Blog - RSS - January 10 2024

Researchers at Trend Micro warn that a threat actor known as “Water Curupira” is distributing the Pikabot malware loader via widespread phishing campaigns.