Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

6th March 2024

Vulnerabilities

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Current Activity - March 5 2024

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-21237 Android Pixel Information Disclosure Vulnerability CVE-2021-36380 Sunhillo SureLine OS Command Injection Vulnerablity These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Apple fixes two new iOS zero-days exploited in attacks on iPhones

BleepingComputer.com - March 5 2024

Apple released emergency security updates to fix two iOS zero-day vulnerabilities that were exploited in attacks on iPhones. [...]

New Kimsuky attacks involve ConnectWise ScreenConnect bugs

SC Magazine US - March 5 2024

z0Miner Exploits Korean Web Servers to Attack WebLogic Server

ASEC Blog - AhnLab English - March 6 2024

AhnLab SEcurity intelligence Center (ASEC) has found numerous cases of threat actors attacking vulnerable Korean servers. This post introduces one of the recent case in which the threat actor 'z0Miner' attacked Korean WebLogic servers. z0Miner was first introduced by Tencent Security, a Chinese Internet service provider. hxxps://s[.]tencent[.]com/research/report/1170.html (This link is only available in Chinese.)

Malware and threat actors

Cybercriminals Using Novel DNS Hijacking Technique for Investment Scams

MalwareTips.com - March 5 2024

TLP CLEAR: Disclosure is not limited

A new DNS threat actor dubbed Savvy Seahorse is leveraging sophisticated techniques to entice targets into fake investment platforms and steal funds.

"Savvy Seahorse is a DNS threat actor who convinces victims to create accounts on fake investment platforms, make deposits to a... Click to expand...
Read more

Fast-Growing RA Ransomware Group Goes Global

Dark Reading - March 5 2024

The rapidly evolving threat group uses high-impact tactics that include manipulating group policy to deploy payloads across environments.

Unveiling Earth Kapre aka RedCurl's Cyberespionage Tactics With Trend Micro MDR, Threat Intelligence

Trend Micro Research News Perspectives - March 6 2024

This blog entry will examine Trend Micro MDR team's investigation that successfully uncovered the intrusion sets employed by Earth Kapre in a recent incident, as well as how the team leveraged threat intelligence to attribute the extracted evidence to the cyberespionage threat group.

Tax Season Phishing Surge: Cyber Exploits with AsyncRAT

Security Boulevard - RSS - March 5 2024

Rise of AsyncRAT: Navigating Tax-Themed Cyber Threats and WinRAR Vulnerabilities In the last few days, we have seen a rise of cyber attacks conducted by AsyncRAT focusing on 'TAX attacks context.' AsyncRAT is a Remote Access Trojan that attackers use to...

BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare

Krebs on Security - March 6 2024

There are indications that U.S. healthcare giant Change Healthcare has made a $22 million extortion payment to the infamous BlackCat ransomware group (a.k.a. "ALPHV") as the company struggles to bring services back online amid a cyberattack that has disrupted prescription drug services nationwide for weeks. However, the cybercriminal who claims to have given BlackCat access to Change's network says the crime gang cheated them out of their share of the ransom, and that they still have the sensitive data Change reportedly paid the group to destroy.