Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

26 February 2024

Vulnerabilities

Analysis of Nood RAT Used in Attacks Against Linux (Gh0st RAT&rsquo;s Variant)

ASEC Blog - AhnLab English - February 26 2024

AhnLab SEcurity intelligence Center (ASEC) recently discovered that Nood RAT is being used in malware attacks. Nood RAT is a variant of Gh0st RAT that works in Linux. Although the number of Gh0st RAT for Linux is fewer compared to Gh0st RAT for Windows, the cases of Gh0st RAT for Linux are continuously being collected.

SEO Poisoning to Domain Control: The Gootloader Saga Continues

The DFIR Report - Blog - February 26 2024

Key Takeaways More information about Gootloader can be found in the following reports: The DFIR Report, GootloaderSites, Mandiant, Red Canary, & Kroll.

Russian Ministry Software Backdoored with North Korean KONNI Malware

HackRead - February 24 2024

Russian Ministry Software Backdoored with North Korean KONNI Malware

Exclusive: Cyberattack on Change Healthcare was an exploit of the ConnectWise flaw

SC Magazine US - February 23 2024

Security experts have warned for the past couple of days that the two flaws recently uncovered in ConnectWise’s ScreenConnect app could become the major cybersecurity story of 2024 – and that the healthcare and critical infrastructure sectors were especially vulnerable.

Vital Basic - DarkMe

Red Sky Alliance - X-Industry - RSS - February 23 2024

A newly disclosed security flaw in the Microsoft Defender SmartScreen has been exploited as a zero-day by an advanced persistent threat actor called Water Hydra (aka DarkCasino) targeting financial market traders.

Updated: Top Cyber Actions for Securing Water Systems

CISA Current Activity - February 23 2024

TLP CLEAR: Disclosure is not limited

Today, CISA, the Environmental Protection Agency (EPA), and the Federal Bureau of Investigation (FBI) updated the joint fact sheet Top Cyber Actions for Securing Water Systems.

Malware and threat actors

LockBit ransomware returns, restores servers after police disruption

Bleeping Computer - February 25 2024

The LockBit gang is relaunching its ransomware operation on a new infrastructure less than a week after law enforcement hacked their servers, and is threatening to focus more of their attacks on the government sector.