Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

18 March 2024

Vulnerabilities

'GhostRace' Speculative Execution Attack Impacts All CPU, OS Vendors

Dark Reading - March 15 2024

Researchers at IBM and VU Amsterdam have developed a new attack that exploits speculative execution mechanisms in modern computer processors to bypass checks in operating systems against what are known as race conditions. The attack leverages a vulnerability (CVE-2024-2193) that the researchers found affecting Intel, AMD, ARM, and IBM processors.

Hackers exploit Aiohttp bug to find vulnerable networks

BleepingComputer.com - March 16 2024

The ransomware actor 'ShadowSyndicate' was observed scanning for servers vulnerable to CVE-2024-23334, a directory traversal vulnerability in the aiohttp Python library.

Malware and threat actors

APT28 Hacker Group Targeting Europe, Americas, Asia in Widespread Phishing Scheme

The Hacker News - March 18 2024

The Russia-linked threat actor known as APT28 has been linked to multiple ongoing phishing campaigns that employ lure documents imitating government and non-governmental organizations (NGOs) in Europe, the South Caucasus, Central Asia, and North and South America.

Threat actors leaked 70,000,000+ records allegedly stolen from AT&amp;T

Security Affairs - March 17 2024

Researchers at vx-underground first noticed that more than 70,000,000 records from AT&T were leaked on the Breached hacking forum.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

&ldquo;gitgub&rdquo; malware campaign targets Github users with RisePro info-stealer

Security Affairs - March 17 2024

Cybersecurity researchers discovered multiple GitHub repositories hosting cracked software that are used to drop the RisePro info-stealer. G-Data researchers found at least 13 such Github repositories hosting cracked software designed to deliver the RisePro info-stealer.

StopCrypt: Most widely distributed ransomware evolves to evade detection

MalwareTips.com - March 16 2024

A new variant of StopCrypt ransomware (aka STOP) was spotted in the wild, employing a multi-stage execution process that involves shellcodes to evade security tools.

Inside the Rabbit Hole: BunnyLoader 3.0 Unveiled

Unit 42 – Palo Alto Networks Blog - March 15 2024

We analyze recent samples of BunnyLoader 3.0 to illuminate this malware’s evolved and upscaled capabilities, including its new downloadable module system. The post Inside the Rabbit Hole: BunnyLoader 3.0 Unveiled appeared first on Unit 42.

Nation State Hackers Deploying AI

Red Sky Alliance - X-Industry - RSS - March 15 2024

Cyber security is undergoing a massive transformation, with Artificial intelligence (AI) at the forefront of this change, posing both a threat and an opportunity. AI can potentially empower organizations to defeat cyberattacks at machine speed and drive innovation and efficiency in threat detection, hunting, and incident response.