Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

01 May 2025

Vulnerabilities

SonicWall: SMA100 VPN vulnerabilities now exploited in attacks

BleepingComputer - 30 April 2025 14:23

Cybersecurity company SonicWall has warned customers that several vulnerabilities impacting its Secure Mobile Access (SMA) appliances are now being actively exploited in attacks.

Chrome 136, Firefox 138 Patch High-Severity Vulnerabilities

SecurityWeek - 30 April 2025 08:53

Chrome 136 and Firefox 138 were released in the stable channel with patches for multiple high-severity vulnerabilities.

Threat actors and malware

Chinese Hackers Abuse IPv6 SLAAC for AitM Attacks via Spellbinder Lateral Movement Tool

The Hacker News - 30 April 2025 17:35

A China-aligned advanced persistent threat (APT) group called TheWizards has been linked to a lateral movement tool called Spellbinder that can facilitate adversary-in-the-middle (AitM) attacks.

FBI shares massive list of 42,000 LabHost phishing domains

BleepingComputer - 30 April 2025 13:01

The FBI has shared 42,000 phishing domains tied to the LabHost cybercrime platform, one of the largest global phishing-as-a-service (PhaaS) platforms that was dismantled in April 2024.

RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control

The Hacker News - 30 April 2025 16:45

Cybersecurity researchers have revealed that RansomHub’s online infrastructure has “inexplicably” gone offline as of April 1, 2025, prompting concerns among affiliates of the ransomware-as-a-service (RaaS) operation.

Nebulous Mantis Targets NATO-Linked Entities with Multi-Stage Malware Attacks

The Hacker News - 30 April 2025 16:50

Cybersecurity researchers have shed light on a Russian-speaking cyber espionage group called Nebulous Mantis that has deployed a remote access trojan called RomCom RAT since mid-2022. RomCom "employs advanced evasion techniques, including living-off-the-land (LOTL) tactics and encrypted command and control (C2) communications, while continuously evolving its infrastructure.

UK incidents

UK Retailer Co-op Confirms Hack, Reports "Small Impact" to Its Systems

Infosecurity Magazine - 30 April 2025 14:30

After reports of an internal letter informing staff that the company has been forced to shut down parts of its IT systems, the Co-operative Group (Co-op) confirmed that it has recently experienced "attempts to gain unauthorised access to some systems".