Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 July 2026

Vulnerabilities

UK and partners expose Russian state-supported actors for new 'zero-click' phishing campaign targeting Western organisations

NCSC - 23 July 2026 13:00

GCHQ's National Cyber Security Centre and international partners issue warning as 'LAUNDRY BEAR' cyber threat group exposed for targeted phishing campaign.

New RefluXFS Linux flaw lets attackers gain root privileges

BleepingComputer - 23 July 2026 08:40

A nine-year-old race condition vulnerability in the Linux kernel's XFS filesystem, tracked as CVE-2026-64600, allows local attackers to overwrite protected files and gain root privileges.

Check Point patches actively exploited SmartConsole authentication bypass flaw

Security Affairs - 23 July 2026 09:33

Check Point has released security updates to fix multiple vulnerabilities, including CVE-2026-16232 (CVSS score of 9.3), a critical authentication bypass flaw affecting Security Management and Multi-Domain Management (MDSM).

Threat actors and malware

New Dolphin X Stealer Employs AI Profiling to Prioritize Targets

Infosecurity Magazine - 23 July 2026 11:19

Dolphin X is a new infostealer that uses AI to sort and rank victims, giving cybercriminals a faster way to identify lucrative targets.

Chaos ransomware deploys browser-based msaRAT to evade network detection

Security Affairs - 23 July 2026 19:26

Cisco Talos disclosed msaRAT, a Rust-based remote access trojan attributed to the Chaos ransomware group that routes its entire command-and-control channel through the victim's own Chrome or Edge browser.

Fake Claude app promoted by Bing ads pushes SectopRAT malware

BleepingComputer - 23 July 2026 16:48

A malvertising campaign on the Bing search service is pushing a fake Claude desktop app installer hosted on a legitimate Claude.ai domain to deliver the SectopRAT malware.

Scottish Cyber Coordination Centre

Hackers abuse Notepad++ plugins to stealthily install malware

BleepingComputer - 23 July 2026 13:32

Ukraine's CERT has uncovered attacks distributing an archive containing the legitimate Notepad++ application and a malicious utility called LunchPoke disguised as a plugin to establish persistence.