Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 August 2025

Vulnerabilities

Attackers exploit link-wrapping services to steal Microsoft 365 logins

BleepingComputer - 02 August 2025 11:24

A threat actor has been abusing link wrapping services from reputed technology companies to mask malicious links leading to Microsoft 365 phishing pages that collect login credentials. [...]

AI-powered Cursor IDE vulnerable to prompt-injection attacks

BleepingComputer - 01 August 2025 10:00

A vulnerability that researchers call CurXecute is present in almost all versions of the AI-powered code editor Cursor, and can be exploited to execute remote code with developer privileges. [...]

Hackers Regularly Exploit Vulnerabilities Before Public Disclosure, Study Finds

Infosecurity Magazine - 01 August 2025 11:15

Spikes in attacker activity precede the disclosure of vulnerabilities 80% of the time, according to a new GreyNoise report

Threat actors and malware

Akira Ransomware targets SonicWall VPNs in likely zero-day attacks

Security Affairs - 03 August 2025 14:22

Akira ransomware targets fully patched SonicWall VPNs in suspected zero-day attacks, with multiple intrusions seen in late July 2025.

China Presses Nvidia Over Alleged Backdoors in H20 Chips Amid Tech Tensions

Security Affairs - 02 August 2025 22:38

China questioned Nvidia over suspected backdoors in its H20 chips, adding to rising tensions in the tech fight between the U.S. and Beijing. China's internet watchdog has summoned Nvidia over concerns that its H20 AI chips may contain hidden backdoors.

Attackers Use Fake OAuth Apps with Tycoon Kit to Breach Microsoft 365 Accounts

The Hacker News - 01 August 2025 19:32

Scottish Cyber Coordination Centre

Cybersecurity researchers have detailed a new cluster of activity where threat actors are impersonating enterprises with fake Microsoft OAuth applications to facilitate credential harvesting as part of account takeover attacks.

Storm-2603 Deploys DNS-Controlled Backdoor in Warlock and LockBit Ransomware Attacks

The Hacker News - 01 August 2025 15:14

The threat actor linked to the exploitation of the recently disclosed security flaws in Microsoft SharePoint Server is using a bespoke command-and-control (C2) framework called AK47 C2 (also spelled ak47c2) in its operations.

Lazarus Group rises again, this time with malware-laden fake FOSS

The Register - 04 August 2025 01:01

China says US spies exploited Microsoft Exchange zero-day to steal military info

The Register - 01 August 2025 19:45

Spy vs. spy China has accused US intelligence agencies of exploiting a Microsoft Exchange zero-day exploit to steal defense-related data and take over more than 50 devices belonging to a “major Chinese military enterprise” for nearly a year.

UK related

54% of Organizations in UK and Ireland Lack Cloud Cost Visibility

Security Magazine - 01 August 2025 13:00

A majority of organizations (54%) do not have complete visibility into cloud spends.

Hackers, secret cables and security fears: The explosive fight over the UK’s new Chinese embassy

BBC News - 04 August 2025 00:15

It will be the biggest embassy in Europe, if approved. But its opponents fear it brings with it certain risks and dangers

UK Leads the Way with £15m AI Alignment Project

Infosecurity Magazine - 01 August 2025 09:30

The UK’s AI Security Institute has announced a new AI misalignment research program