

Daily Threat Bulletin

24 April 2025

Vulnerabilities

[ASUS releases fix for AMI bug that lets hackers brick servers](#)

BleepingComputer - 23 April 2025 11:50

ASUS has released security updates to address CVE-2024-54085, a maximum severity flaw that could allow attackers to hijack and potentially brick servers.

Threat actors and malware

[Iran-Linked Hackers Target Israel with MURKYTOUR Malware via Fake Job Campaign](#)

The Hacker News - 23 April 2025 19:38

The Iran-nexus threat actor known as UNC2428 has been observed delivering a backdoor known as MURKYTOUR as part of a job-themed social engineering campaign aimed at Israel in October 2024. Google-owned Mandiant described UNC2428 as a threat actor aligned with Iran that engages in cyber espionage-related operations.

[Russian Hackers Exploit Microsoft OAuth to Target Ukraine Allies via Signal and WhatsApp](#)

The Hacker News - 23 April 2025 17:19

Multiple suspected Russia-linked threat actors are “aggressively” targeting individuals and organizations with ties to Ukraine and human rights with an aim to gain unauthorized access to Microsoft 365 accounts since early March 2025.

[Ransomware groups test new business models to hit more victims, increase profits](#)

The Record from Recorded Future News - 23 April 2025 16:37

The operators behind the DragonForce and Anubis ransomware-as-a-service schemes are launching new business models to attract affiliates, according to research published Wednesday.

UK incidents

[British retailer giant Marks & Spencer \(M&S\) is managing a cyber incident](#)

Security Affairs - 23 April 2025 10:08

Marks and Spencer Group plc (M&S) announced it has been managing a cyber incident in recent days with the help of external cyber security experts.