Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 May 2025

Vulnerabilities

Critical Flaw Allows Remote Hacking of AutomationDirect Industrial Gateway

SecurityWeek - 21 May 2025 16:37

More than 100 AutomationDirect MB-Gateway devices may be vulnerable to attacks from the internet due to CVE-2025-36535.

Critical Samlify SSO flaw lets attackers log in as admin

BleepingComputer - 21 May 2025 19:11

A critical Samlify authentication bypass vulnerability has been discovered that allows attackers to impersonate admin users by injecting unsigned malicious assertions into legitimately signed SAML responses.

A critical flaw in OpenPGP.js lets attackers spoof message signatures

Security Affairs - 21 May 2025 09:46

A critical vulnerability, tracked as CVE-2025-47934, in OpenPGP.js allowed spoofing of message signature verification. OpenPGP.js is an open-source JavaScript library that implements the OpenPGP standard for email and data encryption.

Ivanti EPMM Exploitation Tied to Previous Zero-Day Attacks

darkreading - 21 May 2025 22:24

Wiz researchers found an opportunistic threat actor has been targeting vulnerable edge devices, including Ivanti VPNs and Palo Alto firewalls.

GitLab, Atlassian Patch High-Severity Vulnerabilities

SecurityWeek - 22 May 2025 06:05

GitLab and Atlassian have released patches for over a dozen vulnerabilities in their products, including high-severity bugs.

Threat actors and malware

Threat Actors Target U.S. Critical Infrastructure with LummaC2 Malware

CISA Advisories -

CISA and the Federal Bureau of Investigation released a joint Cybersecurity Advisory on LummaC2 Malware Targeting U.S. Critical Infrastructure Sectors. This advisory details the TTP's, and IOCs linked to threat actors deploying LummaC2 malware.

Scottish Cyber Coordination Centre

Cybercriminals Mimic Kling AI to Distribute Infostealer Malware

Infosecurity Magazine - 21 May 2025 16:45

A new malware campaign disguised as Kling AI used fake Facebook ads and counterfeit websites to distribute an infostealer

PureRAT Malware Spikes 4x in 2025, Deploying PureLogs to Target Russian Firms

The Hacker News - 21 May 2025 19:40

Russian organizations have become the target of a phishing campaign that distributes malware called PureRAT, according to new findings from Kaspersky.

3AM ransomware uses spoofed IT calls, email bombing to breach networks

BleepingComputer - 21 May 2025 14:27

A 3AM ransomware affiliate is conducting highly targeted attacks using email bombing and spoofed IT support calls to socially engineer employees into giving credentials for remote access to corporate systems.

Russian Hackers Exploit Email and VPN Vulnerabilities to Spy on Ukraine Aid Logistics

The Hacker News - 22 May 2025 00:36

Russian cyber threat actors have been attributed to a state-sponsored campaign targeting Western logistics entities and technology companies since 2022. The activity has been assessed to be orchestrated by APT28 (aka BlueDelta, Fancy Bear, or Forest Blizzard).

DragonForce targets rivals in a play for dominance

Threat Research – Sophos News - 21 May 2025 14:00

Not content with attacking retailers, this aggressive group is fighting a turf war with other ransomware operators

UK incidents

M&S warns of £300M dent in profits from cyberattack

The Register - 21 May 2025 10:19

Marks & Spencer says the disruption related to its ongoing cyberattack is likely to knock around £300 million ($402 million) off its operating profits for the next financial year.