Scottish Cyber Coordination Centre

Daily Threat Bulletin

06 March 2025

Vulnerabilities

Android zero-day vulnerabilities actively abused. Update as soon as you can

Malwarebytes - 05 March 2025 13:03

Android's March 2025 security update includes two zero-days which are under active exploitation in targeted attacks.

Chrome 134, Firefox 136 Patch High-Severity Vulnerabilities

SecurityWeek - 05 March 2025 12:06

Chrome 134 and Firefox 136 are rolling out across desktop and mobile with patches for multiple high-severity vulnerabilities.

Threat actors and malware

Open-source tool 'Rayhunter' helps users detect Stingray attacks

BleepingComputer - 05 March 2025 16:36

The Electronic Frontier Foundation (EFF) has released a free, open-source tool named Rayhunter that is designed to detect cell-site simulators (CSS), also known as IMSI catchers or Stingrays.

BadBox malware disrupted on 500K infected Android devices

BleepingComputer - 05 March 2025 12:44

The BadBox Android malware botnet has been disrupted again by removing 24 malicious apps from Google Play and sinkholing communications for half a million infected devices.

China-Linked Silk Typhoon Expands Cyber Attacks to IT Supply Chains for Initial Access

The Hacker News - 05 March 2025 22:14

The China-linked threat actor behind the zero-day exploitation of security flaws in Microsoft Exchange servers in January 2021 has shifted its tactics to target the information technology (IT) supply chain as a means to obtain initial access to corporate networks.

'Crafty Camel' APT Targets Aviation, OT With Polygot Files

darkreading - 05 March 2025 20:41

The Iran-linked nation-state group made its debut with a stealthy, sophisticated, and laser-focused cyber-espionage attack on targets in UAE.

Black Basta Pivots to Cactus Ransomware Group

darkreading - 05 March 2025 15:00

The future of the formerly fearsome cybercriminal group remains uncertain as key members have moved to a new affiliation, in fresh attacks that use novel persistence malware BackConnect.

UK related

Apple drags UK government to court over ‘backdoor’ order

The Register - 05 March 2025 15:38

Apple has reportedly filed a legal complaint with the UK’s Investigatory Powers Tribunal (IPT) contesting the British government’s order that it must forcibly break the encryption of iCloud data.