Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

22 July 2025

Vulnerabilities

ExpressVPN bug leaked user IPs in Remote Desktop sessions

BleepingComputer - 21 July 2025 13:06

ExpressVPN has fixed a flaw in its Windows client that caused Remote Desktop Protocol (RDP) traffic to bypass the virtual private network (VPN) tunnel, exposing the users' real IP addresses. [...]

Microsoft issues emergency patches for SharePoint zero-days exploited in "ToolShell" attacks

Security Affairs - 21 July 2025 12:14

Microsoft patched an exploited SharePoint flaw (CVE-2025-53770) and disclosed a new one, warning of ongoing attacks on on-prem servers. Microsoft released emergency SharePoint updates for two zero-day flaws, tracked as CVE-2025-53770 and CVE-2025-53771, exploited since July 18 in attacks dubbed "ToolShell."

Hackers Exploiting Microsoft Flaw to Attack Governments, Businesses

Security Boulevard - 21 July 2025 14:42

Hackers are exploiting a significant Microsoft vulnerability chain that allows them gain control of on-premises SharePoint servers, steal cryptographic keys, and access Windows applications like Outlook, Teams, and OneDrive. It also gives them persistence in the systems even after reboots and updates.

Exploited CrushFTP Zero-Day Provides Admin Access to Servers

SecurityWeek - 21 July 2025 08:34

Hackers are exploiting a zero-day vulnerability in CrushFTP to gain administrative privileges on vulnerable servers via HTTPS.

Threat actors and malware

MuddyWater deploys new DCHSpy variants amid Iran-Israel conflict

Security Affairs - 21 July 2025 19:39

Iran-linked APT MuddyWater is deploying new DCHSpy spyware variants to target Android users amid the ongoing conflict with Israel. Lookout researchers observed Iran-linked APT MuddyWater (aka SeedWorm, TEMP.Zagros, and Static Kitten) is deploying a new version of the DCHSpy Android spyware in the context of the Israel-Iran conflict.

China-Linked Hackers Launch Targeted Espionage Campaign on African IT Infrastructure

The Hacker News - 21 July 2025 22:57

The China-linked cyber espionage group tracked as APT41 has been attributed to a new campaign targeting government IT services in the African region."The attackers used hardcoded names of internal services, IP addresses, and proxy servers embedded within their malware," Kaspersky researchers Denis Kulik and Daniil Pogorelov said.

PoisonSeed Hackers Bypass FIDO Keys Using QR Phishing and Cross-Device Sign-In Abuse

The Hacker News - 21 July 2025 12:43

Cybersecurity researchers have disclosed a novel attack technique that allows threat actors to downgrade Fast IDentity Online (FIDO) key protections by deceiving users into approving authentication requests from spoofed company login portals.

3,500 Websites Hijacked to Secretly Mine Crypto Using Stealth JavaScript and WebSocket Tactics

The Hacker News - 21 July 2025 09:30

A new attack campaign has compromised more than 3,500 websites worldwide with JavaScript cryptocurrency miners, marking the return of browser-based cryptojacking attacks once popularized by the likes of CoinHive.

Europol Sting Leaves Russian Cybercrime's 'NoName057(16)' Group Fractured

darkreading - 21 July 2025 19:27

National authorities have issued seven arrest warrants in total relating to the cybercrime collective known as NoName057(16), which recruits followers to carry out DDoS attacks on perceived enemies of Russia.

UK related

OpenAI and UK sign deal to use AI in public services

BBC News - 22 July 2025 04:25

The US tech firm behind ChatGPT say it will work with the UK government to "deliver prosperity for all".