Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

19 June 2025

Vulnerabilities

CISA warns of attackers exploiting Linux flaw with PoC exploit

BleepingComputer - 18 June 2025 10:54

CISA has warned U.S. federal agencies about attackers targeting a high-severity vulnerability in the Linux kernel's OverlayFS subsystem that allows them to gain root privileges. [...]

Critical Vulnerability Patched in Citrix NetScaler

SecurityWeek - 18 June 2025 14:02

Citrix has released patches for critical- and high-severity vulnerabilities in NetScaler and Secure Access Client and Workspace for Windows.The post Critical Vulnerability Patched in Citrix NetScaler appeared first on SecurityWeek.

Chrome 137 Update Patches High-Severity Vulnerabilities

SecurityWeek - 18 June 2025 10:43

Google has released a Chrome 137 update to resolve two memory bugs in the browser's V8 and Profiler components.The post Chrome 137 Update Patches High-Severity Vulnerabilities appeared first on SecurityWeek.

Threat actors and malware

Pro-Israel hackers hit Iran's Nobitex exchange, burn $90M in crypto

BleepingComputer - 18 June 2025 18:56

The pro-Israel "Predatory Sparrow" hacking group claims to have stolen over $90 million in cryptocurrency from Nobitex, Iran's largest crypto exchange, and burned the funds in a politically motivated cyberattack. [...]

North Korean hackers deepfake execs in Zoom call to spread Mac malware

BleepingComputer - 18 June 2025 17:37

North Korean advanced persistent threat (APT) 'BlueNoroff' (aka 'Sapphire Sleet' or 'TA444') are using deepfake company executives during fake Zoom calls to trick employees into installing custom malware on their computers. [...]

ChainLink Phishing: How Trusted Domains Become Threat Vectors

BleepingComputer - 18 June 2025 11:02

Phishing has evolved—and trust is the new attack vector. ChainLink Phishing uses real platforms like Google Drive & Dropbox to sneak past filters and steal credentials in the browser. Watch Keep Aware's on-demand webinar to see how these attacks work—and how to stop them. […]

New Malware Campaign Uses Cloudflare Tunnels to Deliver RATs via Phishing Chains

The Hacker News - 18 June 2025 22:11

A new campaign is making use of Cloudflare Tunnel subdomains to host malicious payloads and deliver them via malicious attachments embedded in phishing emails.The ongoing campaign has been codenamed SERPENTINE#CLOUD by Securonix.It leverages "the Cloudflare Tunnel infrastructure and Python-based loaders to deliver memory-injected payloads through a chain of shortcut files and obfuscated

Russian Hackers Bypass Gmail MFA With App-Specific Password Ruse

SecurityWeek - 18 June 2025 19:55

Russian hackers posed as US State Department staff and convinced targets to generate and give up Google app-specific passwords.The post Russian Hackers Bypass Gmail MFA With App-Specific Password Ruse appeared first on SecurityWeek.

UK related

Iran-Israel War Triggers a Maelstrom in Cyberspace

darkreading - 19 June 2025 07:00

As Iran closes its cyberspace to the outside world, hacktivists are picking sides, while attacks against Israel surge and spread across the region.

UK Government Publishes Plan to Boost Cyber Sector Growth

Infosecurity Magazine - 18 June 2025 12:00

The new Cyber Growth Action Plan aims to support the UK's cyber industry, including the development of innovative new technologies and startups

Takeover of British Russia expert's email accounts used novel phishing tactic

The Record from Recorded Future News - 18 June 2025 19:28