Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 November 2025

Vulnerabilities

Fortinet warns of new FortiWeb zero-day exploited in attacks

BleepingComputer - 18 November 2025 15:01

Today, Fortinet released security updates to patch a new FortiWeb zero-day vulnerability that threat actors are actively exploiting in attacks.

Google fixed the seventh Chrome zero-day in 2025

Security Affairs - 18 November 2025 09:59

Google released Chrome security updates to address two flaws, including a high-severity V8 type confusion bug tracked as CVE-2025-13223 that has been actively exploited in the wild.

Threat actors and malware

Cloudflare Outage Not Caused by Cyberattack

SecurityWeek - 18 November 2025 19:09

Major online services such as ChatGPT, X, and Shopify were disrupted in a global Cloudflare outage on Nov. 18th, as well as transit and city services.

Microsoft Mitigates Record 15.72 Tbps DDoS Attack Driven by AISURU Botnet

The Hacker News - 18 November 2025 14:47

Microsoft on Monday disclosed that it automatically detected and neutralized a distributed denial-of-service (DDoS) attack targeting a single endpoint in Australia that measured 15.72 terabits per second (Tbps) and nearly 3.64 billion packets per second (pps).

Sneaky 2FA Phishing Kit Adds BitB Pop-ups Designed to Mimic the Browser Address Bar

The Hacker News - 19 November 2025 01:01

The malware authors associated with a Phishing-as-a-Service (PhaaS) kit known as Sneaky 2FA have incorporated Browser-in-the-Browser (BitB) functionality into their arsenal, underscoring the continued evolution of such offerings and further making it easier for less-skilled threat actors to mount attacks at scale.

Scottish Cyber Coordination Centre

The Tycoon 2FA Phishing Platform and the Collapse of Legacy MFA

BleepingComputer - 18 November 2025 11:01

Tycoon 2FA enables turnkey real-time MFA relays behind 64,000+ attacks this year, proving legacy MFA collapses the moment a phishing kit targets it.

Iranian Hackers Use DEEPROOT and TWOSTROKE Malware in Aerospace and Defense Attacks

The Hacker News - 18 November 2025 19:24

Suspected espionage-driven threat actors from Iran have been observed deploying backdoors like TWOSTROKE and DEEPROOT as part of continued attacks aimed at aerospace, aviation, and defense industries in the Middle East.