Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

25 June 2025

Threat actors and malware

APT28 Uses Signal Chat to Deploy BEARDSHELL Malware and COVENANT in Ukraine

The Hacker News - 24 June 2025 15:36

The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of a new cyber attack campaign by the Russia-linked APT28 (aka UAC-0001) threat actors using Signal chat messages to deliver two previously undocumented malware families dubbedd BEARDSHELL and COVENANT.

New FileFix attack weaponizes Windows File Explorer for stealthy commands

BleepingComputer - 24 June 2025 12:00

A cybersecurity researcher has developed FileFix, a variant of the ClickFix social engineering attack that tricks users into executing malicious commands via the File Explorer address bar in Windows.

Chinese APT Hacking Routers to Build Espionage Infrastructure

SecurityWeek - 24 June 2025 10:50

A Chinese APT has been infecting SOHO routers with the ShortLeash backdoor to build stealthy espionage infrastructure.

Hackers Target Over 70 Microsoft Exchange Servers to Steal Credentials via Keyloggers

The Hacker News - 24 June 2025 19:56

Unidentified threat actors have been observed targeting publicly exposed Microsoft Exchange servers to inject malicious code into the login pages that harvest their credentials.