Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

27 February 2025

Vulnerabilities

Hackers Exploited Krpano Framework Flaw to Inject Spam Ads on 350+ Websites

The Hacker News - 26 February 2025 23:49

A cross-site scripting (XSS) vulnerability in a virtual tour framework has been weaponized by malicious actors to inject malicious scripts across hundreds of websites with the goal of manipulating search results and fueling a spam ads campaign at scale.

Threat actors and malware

New Linux Malware ‘Auto-Color’ Grants Hackers Full Remote Access to Compromised Systems

The Hacker News - 26 February 2025 17:34

Universities and government organizations in North America and Asia have been targeted by a previously undocumented Linux malware called Auto-Color between November and December 2024, according to new findings from Palo Alto Networks Unit 42.

New Anubis Ransomware Could Pose Major Threat to Organizations

SecurityWeek - 26 February 2025 17:04

Threat Intelligence firm Kela warns of a new ransomware group called Anubis operating as a RaaS service with an extensive array of options for affiliates.

New Ghostwriter campaign targets Ukrainian Government and opposition activists in Belarus

Security Affairs - 26 February 2025 23:05

A Ghostwriter campaign using a new variant of PicassoLoader targets opposition activists in Belarus, and Ukrainian military and government organizations.

New LightSpy spyware variant comes with enhanced data collection features targeting social media platforms

Security Affairs - 26 February 2025 10:46

Cybersecurity researchers at Hunt.io have found an updated version of the LightSpy spyware that supports an expanded set of data collection features to target social media platforms like Facebook and Instagram.

EncryptHub breaches 618 orgs to deploy infostealers, ransomware

BleepingComputer - 26 February 2025 11:31

A threat actor tracked as ‘EncryptHub,’ aka Larva-208, has been targeting organizations worldwide with spear-phishing and social engineering attacks to gain access to corporate networks.

UK related

Southern Water says Black Basta ransomware attack cost £4.5M in expenses

BleepingComputer - 26 February 2025 19:50

United Kingdom water supplier Southern Water has disclosed that it incurred costs of £4.5 million ($5.7M) due to a cyberattack it suffered in February 2024.