Scottish Cyber Coordination Centre

Daily threat bulletin

23 July 2024

Vulnerabilities

EvilVideo, a Telegram Android zero-day allowed sending malicious APKs disguised as videos

Security Affairs - 22 July 2024 22:53

EvilVideo is a zero-day in the Telegram App for Android that allowed attackers to send malicious APK payloads disguised as videos. ESET researchers discovered a zero-day exploit named EvilVideo that targets the Telegram app for Android.

Windows users targeted with zero-day attacks via Internet Explorer

Security Magazine - 23 July 2024 01:00

Windows users are being targeted with zero-day attacks. Security leaders are sharing their insights.

Threat actors and malware

PINEAPPLE and FLUXROOT Hacker Groups Abuse Google Cloud for Credential Phishing

The Hacker News - 22 July 2024 18:56

A Latin America (LATAM)-based financially motivated actor codenamed FLUXROOT has been observed leveraging Google Cloud serverless projects to orchestrate credential phishing activity, highlighting the abuse of the cloud computing model for malicious purposes.

Kaspersky Is an Unacceptable Risk Threatening the Nation's Cyber Defense

darkreading - 22 July 2024 15:00

As geopolitical tensions rise, foreign software presents a grave supply chain risk and an ideal attack vector for nation-state adversaries.

Experts Uncover Chinese Cybercrime Network Behind Gambling and Human Trafficking

The Hacker News - 22 July 2024 19:35

The relationship between various TDSs and DNS associated with Vigorish Viper and the final landing experience for the userA Chinese organized crime syndicate with links to money laundering and human trafficking across Southeast Asia has been using an advanced "technology suite" that runs the whole cybercrime supply chain spectrum to spearhead its operations.