Scottish Cyber Coordination Centre

Daily threat bulletin

31 July 2024

Vulnerabilities

CISA warns of VMware ESXi bug exploited in ransomware attacks

BleepingComputer - 30 July 2024 16:54

CISA has ordered U.S. Federal Civilian Executive Branch (FCEB) agencies to secure their servers against a VMware ESXi authentication bypass vulnerability exploited in ransomware attacks. [...]

DigiCert mass-revoking TLS certificates due to domain validation bug

BleepingComputer - 30 July 2024 12:02

DigiCert is warning that it will be mass-revoking SSL/TLS certificates due to a bug in how the company verified if a customer owned or operated a domain and requires impacted customers to reissue certificates within 24 hours. [...]

Threat actors and malware

Massive SMS stealer campaign infects Android devices in 113 countries

BleepingComputer - 30 July 2024 18:29

A malicious campaign targeting Android devices worldwide utilizes thousands of Telegram bots to infect devices with SMS-stealing malware and steal one-time 2FA passwords (OTPs) for over 600 services. [...]

Dark Angels ransomware receives record-breaking $75 million ransom

BleepingComputer - 30 July 2024 17:22

A Fortune 50 company paid a record-breaking $75 million ransom payment to the Dark Angels ransomware gang, according to a report by Zscaler ThreatLabz. [...]

Black Basta ransomware switches to more evasive custom malware

BleepingComputer - 30 July 2024 15:55

The Black Basta ransomware gang has shown resilience and an ability to adapt to a constantly shifting space, using new custom tools and tactics to evade detection and spread throughout a network. [...]

Google Chrome adds app-bound encryption to block infostealer malware

BleepingComputer - 30 July 2024 14:03

Scottish Cyber Coordination Centre

Google Chrome has added app-bound encryption for better cookie protection on Windows systems and improved defenses against information-stealing malware attacks. [...]

A crafty phishing campaign targets Microsoft OneDrive users

Security Affairs - 30 July 2024 09:20

Researchers detected a sophisticated phishing campaign targeting Microsoft OneDrive users to trick them into executing a PowerShell script. Over the past few weeks, the Trellix Advanced Research Center observed a sophisticated phishing campaign targeting Microsoft OneDrive users.

'LockBit of phishing' EvilProxy used in more than a million attacks every month

The Register - 30 July 2024 15:33

Leaves a trail of ransomware infections, data theft, business email compromise in its wake Insight The developers of EvilProxy – a phishing kit dubbed the "LockBit of phishing" – have produced guides on using legitimate Cloudflare services to disguise malicious traffic.

UK related

UK govt links 2021 Electoral Commission breach to Exchange server

BleepingComputer - 30 July 2024 09:00

The United Kingdom's Information Commissioner's Office (ICO) revealed today that the Electoral Commission was breached in August 2021 because it failed to patch its on-premise Microsoft Exchange Server against ProxyShell vulnerabilities. [...]