Scottish
Cyber
Coordination
Centre

Daily threat bulletin

7 May 2024

Vulnerabilities

Android bug leaks DNS queries even when VPN kill switch is enabled

BleepingComputer - 03 May 2024 18:02

A Mullvad VPN user has discovered that Android devices leak DNS queries when switching VPN servers even though the "Always-on VPN" feature was enabled with the "Block connections without VPN" option. [...]

Critical Tinyproxy Flaw Opens Over 50,000 Hosts to Remote Code Execution

The Hacker News - 06 May 2024 20:30

More than 50% of the 90,310 hosts have been found exposing a Tinyproxy service on the internet that's vulnerable to a critical unpatched security flaw in the HTTP/HTTPS proxy tool.

Xiaomi Android Devices Hit by Multiple Flaws Across Apps and System Components

The Hacker News - 06 May 2024 16:33

Multiple security vulnerabilities have been disclosed in various applications and system components within Xiaomi devices running Android. "The vulnerabilities in Xiaomi led to access to arbitrary activities, receivers and services with system privileges, theft of arbitrary files with system privileges, [and] disclosure of phone, settings and Xiaomi account data".

Citrix Addresses High-Severity Flaw in NetScaler ADC and Gateway

darkreading - 07 May 2024 01:18

The flaw was nearly identical to last year's CitrixBleed flaw, though not as severe.

Threat actors and malware

NATO and EU condemn Russia's cyberattacks against Germany, Czechia

BleepingComputer - 03 May 2024 12:47

NATO and the European Union, with international partners, formally condemned a long-term cyber espionage campaign against European countries conducted by the Russian threat group APT28. [...]

Blackbasta gang claimed responsibility for Synlab Italia attack

Security Affairs - 04 May 2024 16:38

The Blackbasta extortion group claimed responsibility for the attack that in April severely impacted the operations of Synlab Italia. Since April 18, Synlab Italia, a major provider of medical diagnosis services, has been experiencing disruptions due to a cyber attack. The company initially cited technical issues as the cause leading to “temporary interruption of access […]

Russia-linked APT28 and crooks are still using the Moobot botnet

Security Affairs - 03 May 2024 19:39

The Ubiquiti EdgeRouter botnet is still used by Russia-linked group APT28 and cybercriminals organizations. Trend Micro researchers reported that the EdgeRouter botnet, called Moobot, used by the APT28 group is still active and is also used by cyber criminal organizations. In January, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and […]

Dirty stream attack poses billions of Android installs at risk

Security Affairs - 03 May 2024 14:17

Microsoft devised an attack technique, dubbed ‘Dirty Stream,’ impacting widely used Android applications, billions of installations are at risk. Microsoft is warning Android users about a new attack technique, named Dirty Stream, that can allow threat actors to take control of apps and steal sensitive data.

China-Linked Hackers Suspected in ArcaneDoor Cyberattacks Targeting Network Devices

The Hacker News - 06 May 2024 20:17

The recently uncovered cyber espionage campaign targeting perimeter network devices from several vendors, including Cisco, may have been the work of China-linked actors, according to new findings from attack surface management firm Censys.
Dubbed ArcaneDoor, the activity is said to have commenced around July 2023, with the first confirmed attack against an unnamed victim

New ‘Cuckoo’ Persistent macOS Spyware Targeting Intel and Arm Macs

The Hacker News - 06 May 2024 14:18

Cybersecurity researchers have discovered a new information stealer targeting Apple macOS systems that’s designed to set up persistence on the infected hosts and act as a spyware.
Dubbed Cuckoo by Kandji, the malware is a universal Mach-O binary that’s capable of running on both Intel- and Arm-based Macs.The exact distribution vector is currently unclear, although there are

Iranian Cyberspies Hit Targets With New Backdoors

SecurityWeek - 06 May 2024 13:41

Iranian state-sponsored group APT42 is targeting NGOs, government, and intergovernmental organizations with two new backdoors. The post Iranian Cyberspies Hit Targets With New Backdoors appeared first on SecurityWeek.