CRITICALSTART®

Daily Intelligence Update | 2 October 2025

Researchers have uncovered a sophisticated malware campaign distributing fake cryptocurrency trading applications through thousands of malicious Facebook ads. Tracked as WEEVILPROXY, the campaign has been active since at least March 2024 and relies on a compiled JavaScript malware dubbed *JSCEAL*. Victims are lured through ads impersonating trusted platforms like TradingView and redirected to fraudulent sites that deliver modular JavaScript components designed to work in tandem with a locally installed MSI package. This hybrid setup complicates detection by splitting malicious activity between the browser and local system. Analysts report that JSCEAL employs extensive fingerprinting and anti-analysis techniques, using DLL unpacking, localhost communication, and msedge_proxy[.]exe to blend in visually with legitimate software. Once active, it establishes a local proxy to intercept and manipulate web traffic, injecting malicious scripts into banking and cryptocurrency platforms to harvest credentials, cookies, wallet data, and Telegram information. The malware also supports adversary-in-the-middle attacks and functions as a remote access trojan, providing broad surveillance and persistence capabilities.

In parallel, researchers have analyzed a new Android banking trojan dubbed *Klopatra*, which has been aggressively targeting financial institutions and users in Spain and Italy since March 2025. Operated by what analysts assess to be a Turkish-speaking group, Klopatra leverages Hidden VNC, dynamic overlays, and Accessibility Service abuse to obtain full control of infected devices and perform real-time fraudulent transactions. The malware stands out for its use of *Virbox*, a commercial-grade obfuscation tool uncommon in Android threats, alongside heavy reliance on native code to bypass defenses. Distribution occurs through dropper apps disguised as IPTV services, which trick victims into granting extensive permissions. Researchers highlight Klopatra's rapid evolution, with more than 40 unique builds across three identified botnets now controlling thousands of devices. Command-and-control logs show direct fraud operations, including late-night banking thefts conducted via stealth VNC sessions with stolen PINs. Despite strong evasion measures, OPSEC missteps in the infrastructure allowed analysts to link seemingly distinct campaigns back to the same actor.

On the vulnerability front, Cisco has confirmed active exploitation of a stack overflow flaw in the SNMP subsystem of IOS and IOS XE Software, tracked as CVE-2025-20352 and rated CVSS 7.7. The issue allows remote attackers with SNMPv2c or SNMPv3 credentials to cause denial-of-service conditions or, at higher privilege levels, execute arbitrary code with root access. Impacted devices include widely deployed models such as Meraki MS390 and Catalyst 9300 switches running Meraki CS 17 or earlier. Cisco has released patches in IOS XE 17.15.4a and advises customers to immediately restrict SNMP access, monitor device configurations with the "show snmp host" command, and disable vulnerable OIDs if patching is delayed. The active exploitation underscores the continued focus on network infrastructure devices as high-value targets, with SNMP remaining a persistent weak point in enterprise environments.

Critical Start is a leading provider of Managed Detection and Response (MDR) services, combining AI acceleration with expert human validation to eliminate false positives, reduce alert noise, and deliver fast, reliable threat resolution.

With a US-based, 24/7/365 Security Operations Center and a 90% analyst retention rate, Critical Start delivers both proactive and reactive MDR for large enterprises across North America. Its MDR is built to detect threats early and respond quickly, with every action backed by contractual service-level agreements that ensure trusted outcomes for security teams.

For more information, visit www.criticalstart.com.