Daily Intelligence Update | 30 October 2025

Researchers have uncovered a new APT28 campaign leveraging Signal Desktop and cloud infrastructure to covertly target Ukrainian military personnel with malicious macro-enabled Office documents. By abusing the lack of “Mark of the Web” tagging in Signal Desktop, the campaign executed macros that dropped a DLL and PNG with encrypted shellcode, ultimately loading Covenant’s HTTP Grunt Stager through Koofr cloud storage. Subsequent stages deployed the BeardShell backdoor, a C++ PowerShell implant using Icedrive for C2, and SlimAgent, a keylogger and screenshotter, all delivered through lures mimicking Ukrainian military documents to collect intelligence on personnel and logistics. In parallel, researchers identified a rapidly spreading malware campaign in Brazil dubbed Water Saci, which abuses WhatsApp for propagation of a Windows-based infostealer called SORVEPOTEL. The malware spreads through phishing ZIP attachments that, once executed on desktop systems, abuse active WhatsApp Web sessions to resend the malicious file to all contacts and groups. SORVEPOTEL is designed to steal banking and cryptocurrency credentials, relying on PowerShell scripts, .NET DLLs, reflective loading, and HTTPS-based C2, while deploying secondary payloads like Maverick[.]StageTwo and Maverick[.]Agent to perform overlay phishing against major Brazilian financial institutions.

Elsewhere, researchers warned of the evolving role of Android droppers in bypassing Google’s Play Protect and its Pilot Program. Traditionally a tool of banking trojans, droppers are increasingly distributing lightweight malware like SMS stealers and spyware across Asia and India by presenting as harmless apps that only fetch or decrypt their payloads after user interaction. RewardDropMiner was highlighted as a particularly adaptive dropper family, with its latest variant dropping cryptocurrency mining functionality to reduce detection while focusing entirely on payload delivery. Similar families such as SecuriDropper, Zombinder, BrokewellDropper, HiddenCatDropper, and TiramisuDropper are reported to use comparable evasion techniques to bypass Android 13 and Play Protect restrictions. Analysts also noted that the massive Aisuru IoT botnet, responsible for some of the largest DDoS attacks ever recorded, has shifted its focus from disruption to monetization, renting its network of more than 700,000 infected routers and cameras to residential proxy services. This pivot aligns with the explosive growth of the proxy market, with evidence suggesting overlap between Aisuru’s infrastructure and China-linked proxy providers like IPidea. Analysts warn that Aisuru’s botnet is now fueling aggressive AI-related web scraping and anonymizing cybercrime traffic through compromised residential IPs.

Finally, Unity Technologies released critical patches for a high-severity vulnerability (CVE-2025-59489, CVSS 8.4) in its game development platform caused by an untrusted search path weakness that could allow local code execution, privilege escalation, and information disclosure across Android, Windows, Linux, and macOS. Affecting Unity Editor versions from 2017.1 through current builds, the flaw exposes millions of deployed applications to potential compromise, with Android at particular risk due to privilege escalation scenarios and Windows exposed through URI handler abuse. Unity has patched supported versions including 6000.3, 6000.2, 6000.0 LTS, 2022.3 xLTS, and 2021.3 xLTS, as well as legacy versions dating back to 2019.1, though older builds from 2017–2018 remain unsupported.
