Daily Intelligence Update | 28 October 2025

CTI Intelligence Update October 28, 2025

Researchers reported that the ransomware-as-a-service group Qilin, also tracked as Agenda, is expanding its operations by deploying a Linux-based ransomware binary on Windows systems in attacks targeting VMware ESXi and Nutanix AHV environments. The attack chain begins with fake CAPTCHA pages hosted on Cloudflare R2 that deliver information stealers used to harvest authentication tokens, cookies, and credentials. Once access is established, the actors rely on legitimate remote management tools including WinSCP, AnyDesk, ScreenConnect, and Splashtop to move and execute the Linux payload on Windows machines. The binary is configurable, supporting command-line parameters, file and folder allow/deny lists, and is specifically tuned to encrypt VMFS hypervisor paths while excluding critical system directories to maintain operational stability.

In parallel, a global smishing campaign attributed to the China-linked Smishing Triad has surged, with activity observed across 121 countries. The group impersonates trusted entities including banks, healthcare providers, government agencies, and e-commerce platforms to deliver SMS-based phishing lures. Researchers identified more than 194,000 domains (with 136,933 unique root domains) registered since early 2024 to support the operation, with domain infrastructure concentrated in Hong Kong and the United States. The campaign leverages a Phishing-as-a-Service ecosystem that includes Telegram channels advertising kits, data brokers supplying phone number lists, registrars providing rapid registrations, and SMS spammer networks distributing lures. Roughly 29% of observed domains remain active for less than two days, highlighting the group's heavy reliance on fast-flux infrastructure to evade takedowns.

Separately, researchers detailed a campaign linked to UNC6229, an emerging Vietnam-based threat cluster, that relies on fraudulent job postings to deliver malware and harvest credentials. The group posts fabricated listings on legitimate freelance and recruitment platforms targeting digital advertising and marketing professionals. After establishing credibility through convincing recruiter profiles, the actor delivers malware via file attachments or directs applicants to phishing portals designed to capture corporate credentials. The campaign further leverages business email and CRM platforms to manage communications, while exploiting remote access tools for persistence and post-compromise activities, underscoring the continued effectiveness of social engineering in credential theft campaigns.
