Daily Intelligence Update | 14 November 2025

Researchers have identified a campaign by a previously unknown threat actor, UNK_SmudgedSerpent, believed to have operated between June and August 2025, targeting academics and foreign policy experts specializing in Iran. The group used benign conversation openers, spoofed OnlyOffice and Microsoft Teams links, and health-related domains to harvest credentials and deploy Remote Monitoring & Management tools, including PDQConnect and ISL Online. Analysts observed overlaps in tactics with Iranian-aligned groups such as TA453 (Charming Kitten), TA455 (C5 Agent), and TA450 (MuddyWater), suggesting potential coordination or contractor sharing within Iranian intelligence operations. The group reportedly impersonated prominent policy figures such as Suzanne Maloney and Patrick Clawson, adapting lures dynamically when suspicion was detected. Researchers urge heightened vigilance among those working in policy research or Iran-focused fields, recommending proactive credential audits and email domain verification.

In parallel, analysts are investigating a significant alleged data leak involving Knownsec Information Technology Co., Ltd., a leading Chinese cybersecurity firm long speculated to maintain ties with government operations. The leaked dataset, exceeding 12,000 internal files reportedly dating from 2023, includes presentations, databases, and technical manuals allegedly revealing cooperation with the Ministry of Public Security and other national agencies. Posted by an actor using the alias “T1g3r,” the material was first uploaded briefly to GitHub before being sold on dark web forums by October 31, 2025. The seller closed the sale within a week, claiming it was transferred to a single buyer. While authenticity remains unconfirmed, reviewed samples reportedly reference Knownsec’s Chief Security Officer Zhou Jingping and internal tools such as the ZoomEye mapping engine, the GhostX framework, and the “Un-Mail” interception tool, as well as databases cataloging global infrastructure targets across 26 regions. If verified, the leak would represent rare insight into China’s state-linked cyber ecosystem, highlighting both contractor integration and extensive reconnaissance capability.

Meanwhile, researchers detected a coordinated npm supply-chain compromise affecting 18 highly popular JavaScript packages with a combined weekly download count exceeding two billion. Packages such as chalk, debug, ansi-styles, supports-color, and color-convert were found to contain obfuscated code that hijacked cryptocurrency wallet interactions by intercepting browser APIs and redirecting transactions to attacker-controlled addresses. The breach stemmed from a phishing campaign masquerading as npm support via the spoofed domain npmjs[.]help, tricking a maintainer into granting access. Although cleanup has begun, analysts warn that additional packages such as proto-tinker-wc may still be compromised.

Researchers also observed a renewed phishing wave attributed to the Russian state-sponsored group Gamaredon, which exploited the WinRAR path traversal vulnerability (CVE-2025-8088) to deploy HTA malware hidden in PDF decoys. The attack automatically installed payloads upon opening, continuing the group’s persistent targeting of Ukrainian government entities. Simultaneously, a Stealit malware campaign has been uncovered leveraging Node.js’ experimental Single Executable Application (SEA) feature, enabling standalone execution without dependencies. Distributed via fake game and VPN installers hosted on Mediafire and Discord, the campaign’s infrastructure has shifted between stealituptaded[.]lol and iloveanimals[.]shop. Once executed, the malware installs components to steal browser data, credentials, crypto wallets, and gaming profiles, while using PowerShell to disable Windows Defender and establish persistence.

Lastly, researchers disclosed a two-factor authentication bypass in Zyxel ATP/USG devices (CVE-2025-9133) that allows attackers to access sensitive configurations by chaining commands through the zysh-cgi binary. The flaw enables non-privileged users to execute commands like show running-config, facilitating credential and network data exfiltration. Zyxel has confirmed the issue, released patches, and advised administrators to immediately update firmware, disable command chaining, and audit CGI activity to prevent further exploitation.

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.