Daily Intelligence Update | 7 November 2025

Researchers report a new China-linked phishing operation attributed to APT41 (TA415), which impersonated U.S. Representative John Moolenaar between July and August 2025 to target U.S. government entities, think tanks, and academics focused on U.S.–China trade issues. The campaign used spoofed outreach sharing supposed draft legislation on China sanctions, delivering password-protected files hosted on Zoho and Dropbox that deployed a Python-based loader named WhirlCoil. The malware established remote access, while the actors relied on VS Code Remote Tunnels and Google services for persistence and exfiltration. Analysts attribute the operation to TA415, a Chengdu-based subgroup of APT41 linked to Chengdu 404 Network Technology and China's Ministry of State Security. In parallel, researchers identified a separate campaign from the China-aligned BRONZE BUTLER (Tick) APT group exploiting a zero-day in Motex LANSCOPE Endpoint Manager, tracked as CVE-2025-61932. The vulnerability enabled SYSTEM-level remote command execution that the attackers used to deploy Gokcpdoor, the Havoc C2 framework, and the OAED loader to obfuscate execution. They further abused Remote Desktop, 7-Zip, and goddi for lateral movement and used cloud services such as file[.]io, LimeWire, and Piping Server for exfiltration. Organizations running LANSCOPE are urged to apply updates and audit external attack surfaces.

Separately, researchers uncovered compromise activity against WordPress sites involving malicious edits to the active theme's functions[.]php file, inserting PHP that loaded attacker-controlled JavaScript from external domains. The injected scripts contacted a remote C2 server to retrieve dynamic payloads responsible for forced redirects, pop-ups, and fake Cloudflare verification pages. At least 17 additional sites displayed the same infection pattern, and analysts recommend patching, malware scanning, strong credential hygiene, and WAF deployment to mitigate recurrence.

Hacktivist activity intensified as a coalition of eight pro-Russian and pro-Palestine groups—including NoName057(16), Desinformador Ruso, Mr Hamza, and Z-Alliance—announced coordinated targeting against Belgium. The actors signaled forthcoming DDoS operations, OT-focused disruptions, and potential hack-and-leak claims aimed at government-linked infrastructure and national-level networks. Researchers assess that the campaign aligns with ongoing geopolitical narratives leveraging opportunistic alliances to amplify operational reach.

Meanwhile, analysts disclosed a vulnerability in OpenAI's Atlas product that allows malicious prompt-injection strings to bypass safety controls. The issue stems from omnibox input being improperly treated as trusted intent when malformed strings resemble URLs but embed harmful instructions. When pasted or clicked, Atlas could interpret them as high-trust commands, enabling actions such as navigating to attacker-controlled sites or deleting files. Identified on October 24, 2025 and disclosed publicly the same day, the flaw underscores risks associated with agentic browsing systems. Recommended mitigations include hardened URL parsing, explicit user-mode separation, and treating omnibox interactions as untrusted by default.

Finally, Juniper Networks issued extensive security patches addressing nearly 220 vulnerabilities across Junos OS, Junos Space, and Security Director, including nine critical issues. The most severe, CVE-2025-59978 (CVSS 9.0), is a cross-site scripting flaw in Junos Space that allows administrative-level script injection leading to full system compromise. The 24.1R4 Patch V1 resolves 162 vulnerabilities, including 24 XSS flaws. Another high-severity vulnerability, CVE-2024-47615 (CVSS 8.6), affects GStreamer and may cause memory corruption through unchecked input. While Juniper has not observed active exploitation, customers are urged to apply the updates immediately due to the breadth and impact of the issues.

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.