Daily Intelligence Update | 3 November 2025

Researchers have uncovered that China-based threat actors exploited a critical Microsoft SharePoint zero-day, tracked as CVE-2025-53770 and nicknamed “ToolShell,” to compromise government and private sector networks across Africa, South America, the Middle East, and Europe. Patched in July 2025, the flaw allowed unauthenticated remote code execution on on-premise SharePoint servers and was reportedly weaponized months before disclosure. The attackers deployed multiple payloads, including Zingdoor, a Go-based backdoor linked to the Chinese group Glowworm (also known as FamousSparrow), and KrustyLoader, a Rust-based loader associated with UNC5221, as well as ShadowPad, a modular Trojan tied to APT41 affiliates. Victims included a Middle Eastern telecom firm, several government agencies, and a U.S. university. Attackers leveraged legitimate binaries for DLL sideloading and tools such as Certutil, Revsocks, and PetitPotam for credential theft and lateral movement. Analysts noted overlap with Budworm (Linen Typhoon), Sheathminer (Violet Typhoon), and Storm-2603, with some intrusions culminating in Warlock ransomware deployment, suggesting coordinated espionage and access maintenance across regions.

Meanwhile, a Vietnamese threat actor known as BatShadow has been observed distributing a new Go-based malware family named Vampire Bot, primarily targeting job seekers and digital marketing professionals. The campaign impersonates recruiters and delivers ZIP archives containing decoy PDFs and malicious LNK or executable files. Once launched, PowerShell scripts fetch fake job materials while redirecting victims via spoofed browser messages urging them to open links in Microsoft Edge, triggering the infection chain. The final payload, masquerading as “Marriott_Marketing_Job_Description[.]pdf[.]exe,” steals system data, captures screenshots, and communicates with api3[.]samsungcareers[.]work. Linked to IP 103.124[.]95.161, BatShadow has maintained infrastructure tied to domains like samsung-work[.]com and previously deployed Agent Tesla, Lumma Stealer, and Venom RAT.

Elsewhere, Canada’s national cyber agency warned that hacktivists have begun tampering with exposed industrial control systems (ICS), citing incidents in which water pressure at a local utility was altered, an oil-and-gas tank gauge was manipulated to trigger false alarms, and grain-dryer settings were changed to unsafe levels before staff intervention. The advisory, supported by the RCMP, referenced opportunistic intrusions exploiting weakly secured interfaces. While attribution remains unclear, the warning coincides with broader trends of ICS targeting by hacktivists worldwide, including Russia-aligned CARR’s claimed disruptions of U.S. utilities and Iran-linked CyberAv3ngers’ ICS malware campaigns. Analysts caution that while some claims appear exaggerated or honeypot-related, small utilities, farms, and manufacturing facilities remain especially vulnerable due to inadequate segmentation and exposure management.

Recent reporting further confirms that ICS-targeting hacktivism surged in Q3 2025, accounting for roughly one-quarter of all hacktivist operations—nearly double Q2’s share. Russia-aligned crews including Z-Pentest, Dark Engine, Inteid, and Sector 16 led attacks against energy, manufacturing, and agriculture sectors across NATO and Ukraine. Some groups expanded beyond disruption to data theft and ransomware, with Team BD Cyber Ninja promoting a Windows MBR locker and Liwa’ Muhammad advertising a cross-platform RaaS named BQTLock. Geopolitical realignments also shifted targeting: Southeast Asia cooled as Thai-Cambodian tensions eased, while activity in the Philippines, Saudi Arabia, and Finland spiked. Ukraine remained the top target, and groups like NoName057(16), Z-Pentest, and Hezi Rash grew increasingly active despite enforcement actions.

Within that ecosystem, researchers observed Hezi Rash—a Kurdish hacktivist collective founded in 2023—conducting roughly 350 DDoS attacks over two months against targets in Japan, Türkiye, Israel, Germany, Iran, and Iraq, citing ideological and retaliatory motives. The group reportedly leveraged rented DDoS-as-a-Service tools such as EliteStress and Abyssal DDoS v3, collaborating with Keymous+, Killnet, and NoName057(16), illustrating the professionalization of hacktivism through shared platforms and service models.

In parallel, Russian authorities announced the arrest of three individuals in Moscow accused of developing and operating Meduza Stealer, an information-stealing malware also linked to Aurora Stealer. Distributed under a malware-as-a-service model, Meduza enabled subscribers to steal credentials, cryptocurrency wallet data, and browser-stored information, including the ability to “revive” expired Chrome cookies for account takeover. The suspects face prosecution under Russia’s Criminal Code Article 273, and investigators continue to trace the group’s supporting botnet infrastructure and accomplices.

Finally, researchers have reported active exploitation of CVE-2025-5947, a critical vulnerability in the Service Finder WordPress theme’s bundled Bookings plugin that allows unauthenticated attackers to bypass authentication and assume administrative privileges. The flaw, affecting versions up to 6.0 and patched in version 6.1, has seen over 13,800 exploitation attempts since August 2025. Exploited sites have been hijacked for code injection, malware hosting, and redirect campaigns. Administrators are advised to update immediately and audit for anomalous activity to prevent persistence or reinfection.
