Daily Intelligence Update | 4 November 2025

Researchers report that the China-linked espionage group UNC6384 has been actively targeting European diplomatic entities using a Windows LNK zero-day tracked as ZDI-CAN-25373 (ZDI-25-148), weaponized since September 2025. Phishing emails themed around EU and NATO events deliver malicious shortcut files that launch obfuscated PowerShell scripts, which in turn drop a tar bundle containing a signed Canon utility (cnmpaui[.]exe), a malicious loader (cnmpaui[.]dll), and an RC4-encrypted payload (cnmplog[.]dat). The loader leverages DLL side-loading to execute the PlugX (SOGU[.]SEC) backdoor in memory, aligning UNC6384's activity with Mustang Panda tradecraft. Analysts note the campaign's use of HTA and CloudFront JavaScript for delivery, HTTPS fronted C2 infrastructure masquerading as legitimate domains such as racineupci[.]org, dorareco[.]net, and naturadeco[.]net, and rapid iteration of "CanonStager" loaders, which were slimmed down from roughly 700KB to 4KB between September and October to minimize forensic footprint. Confirmed victims include diplomatic and governmental targets in Hungary, Belgium, Serbia, Italy, and the Netherlands, indicating a multi-team intelligence collection effort supporting China's geopolitical interests in Europe.

Elsewhere, researchers have detailed a significant supply-chain compromise within the Visual Studio Code and Open VSX ecosystems. Over 550 leaked secrets were discovered, enabling threat actors to publish malicious extensions; several compromised Open VSX access tokens were abused days later in the GlassWorm campaign, which used invisible Unicode steganography to hide payloads, steal developer credentials, and target cryptocurrency wallets. The Eclipse Foundation confirmed that the incident was contained by October 21, with all malicious extensions removed and token lifetimes shortened. Analysts report that GlassWorm was credential-stealing rather than self-replicating, with inflated download counts attributed to bots. The same actor has since pivoted to GitHub, reusing the Unicode-based techniques against JavaScript repositories, highlighting the persistence of open-source supply-chain threats and the challenges of securing developer ecosystems dependent on public contribution workflows.

In a separate development, Operation SkyCloak has emerged as an advanced espionage campaign targeting Russian and Belarusian defense personnel, including VDV units and Spetsnaz operators, through phishing ZIP archives containing LNK files masquerading as appointment and training documents. Execution initiates multi-stage PowerShell scripts that perform anti-sandbox checks, drop nested archives, and establish covert command-and-control infrastructure by exposing local services through Tor with obfs4 bridges. The backdoor uses embedded OpenSSH binaries disguised as benign applications to publish hidden services over custom ports and beacon in a format identifying user, onion address, and tag metadata. Infrastructure overlaps indicate onion bridges hosted in Germany, France, Poland, and Canada. Attribution remains uncertain, but researchers assess that the campaign's tooling and operational style more closely align with pro-Ukrainian intrusion sets such as Angry Likho or Awaken Likho than with Russian groups like APT28, suggesting escalation in cross-border targeting of Eastern European military networks.

Hacktivist activity in October 2025 continued at elevated levels, dominated by groups including Malaysia Hacktivist, Tengkorak Cyber Crew, Laskar Pembebasan Palestina, Hezi Rash, and BD Anonymous, with attacks primarily consisting of DDoS, data theft, and website defacement. Russia-aligned Z-Pentest claimed OT intrusions in Taiwan as part of its ongoing anti-Western campaign, while groups like RipperSec, Keymous, Team Fearless, and We Are RootSec launched operations against Israel, the U.S., and Pacific nations surrounding the October 7 anniversary. Later in the month, pro-Iran and pro-Palestine collectives such as Cyber Toufan pledged to pause activity in recognition of the Israel–Gaza ceasefire, though they warned of renewed attacks upon any escalation.

One of the fastest-rising hacktivist collectives, Hezi Rash ("Black Force"), was credited with over 350 DDoS attacks between August and October 2025, positioning it as one of the most aggressive Kurdish-aligned operations observed this year. The group frames its activity through nationalist and religious narratives, striking targets in Japan, Turkey, Israel, Germany, Iran, and Iraq, and amplifies its impact

through alliances with Keymous+, Killnet, and NoName057(16). Its use of DDoS-as-a-Service platforms such as EliteStress and custom tools like Abyssal DDoS v3 exemplifies the commercialization and accessibility of hacktivist capabilities. Analysts recommend that organizations prioritize scalable DDoS mitigation, web application firewall enforcement, and continuous monitoring for high-volume traffic anomalies from residential IP sources as threat activity intensifies heading into Q4.
