Daily Intelligence Update | 1 October 2025

Researchers have uncovered a new in-memory malware strain, dubbed the *EggStreme Framework*, which is believed to be linked to Chinese APT groups targeting military-related entities in the Philippines. The campaign, thought to be motivated by Beijing's strategic interest in the region amid ongoing South China Sea disputes, involves a multi-stage process with components known as EggStremeFuel and EggStremeLoader deploying the main EggStremeAgent payload. This agent monitors Windows user sessions, injects a keylogger into *explorer[.]exe*, fingerprints systems, escalates privileges, executes arbitrary commands, and exfiltrates sensitive data, while EggStremeWizard is used for DLL sideloading. Operating entirely in memory with encrypted components, the framework is designed to remain stealthy and evade traditional detection.

Separately, analysts reported a highly unusual cyber intrusion campaign against banking infrastructure that relied on physical access to ATM networks. A threat group tracked as UNC2891 was observed installing Raspberry Pi devices connected via 4G and Dynamic DNS, creating covert remote access tunnels. The attackers deployed custom Linux-based malware and backdoors disguised as legitimate processes, leveraging a previously unknown anti-forensics technique that thwarted conventional analysis tools. Only advanced memory and network forensics uncovered persistent outbound connections and disguised processes. Researchers believe the operation was intended to deploy the *CAKETAP* rootkit, which manipulates Hardware Security Module responses to enable large-scale ATM fraud.

In Russia, researchers identified a sophisticated Android spyware campaign targeting executives of major businesses through malicious apps masquerading as domestic antivirus tools allegedly developed by the FSB and the Central Bank. The malware, tracked as *Android.Backdoor[.]916.origin*, has been active since January 2025 and distributed under names like GuardCB, SECURITY_FSB, and ФСБ. Once installed, the apps request extensive permissions, including full device access, screen recording, and Accessibility Services, enabling audio and video surveillance, keylogging, and data theft from apps such as Telegram, WhatsApp, Gmail, Chrome, and Yandex. The spyware maintains stealth and persistence through background execution and dynamic switching between up to 15 different hosting providers for resilience. Researchers note that the malware shows no code overlap with known families, underscoring its unique design and singular targeting of sensitive domestic communications.

In the cybercriminal ecosystem, intelligence surfaced of a newly created Telegram channel on September 30 allegedly linked to a coalition of Lapsus$, ShinyHunters, and Scattered Spider actors. The channel, labeled "Scattered LAPSUS$ Hunters," has not yet posted data for sale but announced "DLS coming within the next 48 hours," which analysts interpret as a forthcoming data leak site. While impersonator channels continue to resell or repost stolen material from ShinyHunters, this new collaboration may signal a consolidation or rebranding effort by established extortion groups. Monitoring will continue for confirmation of actor involvement, victim disclosures, or tactical shifts.

Finally, researchers disclosed a significant zero-click, service-side data exfiltration attack against ChatGPT's Deep Research agent, which they dubbed *ShadowLeak*. The attack relies on a single crafted email containing hidden HTML-based prompt injections—such as white-on-white text and invisible layout elements—that trick the agent into retrieving personally identifiable information from Gmail inboxes, encoding it in Base64, and transmitting it to attacker-controlled servers using the agent's *browser.open()*

function. Because the traffic originates from OpenAI’s cloud infrastructure, the exfiltration is invisible to traditional endpoint or enterprise web monitoring. Testing showed a 100% success rate in repeated trials, with attackers using social engineering cues like urgency, authority, and reassurance to bypass safeguards. Analysts warn that the method generalizes to any connected Deep Research integration, including Drive, SharePoint, Outlook, GitHub, and Notion, broadening the potential attack surface. Recommended mitigations include sanitizing HTML inputs before agent ingestion and continuous behavioral monitoring to detect agent activity that diverges from user intent.

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.