Daily Intelligence Update | 10 November 2025

10 November

Researchers report a new malware campaign targeting gamers on Discord, where a Python-based infostealer known as RedTiger has been repurposed from an open-source security testing tool into a credential-harvesting platform focused on French-speaking users. The malware steals Discord authentication tokens, payment information, browser passwords, cryptocurrency wallets, game files, and even webcam images, uploading data to GoFile and notifying operators via Discord webhooks. Analysts note that RedTiger modifies Discord's internal code to maintain long-term access even after password resets and employs heavy anti-analysis techniques, creating large volumes of fake files and processes to obscure forensic traces. It operates across Windows, Linux, and macOS, and although current targeting remains limited, researchers warn that its open-source nature increases the likelihood of broader adoption by threat actors.

In parallel, analysts uncovered a separate campaign linked to China-aligned threat actors repurposing the legitimate open-source monitoring tool Nezha to deploy the Gh0st RAT malware. Activity observed in August 2025 involved poisoning phpMyAdmin logs on vulnerable servers to plant a PHP web shell, followed by the use of the ANTSWORD web shell to gain control, deploy the Nezha agent, and execute remote commands. PowerShell scripts then disabled Microsoft Defender protections and installed Gh0st RAT. Over 100 systems were reportedly compromised across Taiwan, Japan, South Korea, and Hong Kong, with additional victims identified worldwide. Researchers also noted the actors configured the Nezha dashboard in Russian, likely as a deception tactic designed to mislead investigators and obscure attribution.

Meanwhile, researchers assessed that the Russia-linked group InedibleOchotense carried out a phishing campaign in May 2025 impersonating ESET to target Ukrainian users. The operation delivered emails and Signal messages warning victims of supposed suspicious activity and urging them to download fake threat-removal tools. The hosted ZIP archives contained a legitimate ESET AV Remover bundled with the Kalambur backdoor, mimicking previous activity from UAC-0212 and BACKORDER. Analysts identified minor translation inconsistencies from Russian to Ukrainian in the phishing content, reflecting linguistic inaccuracies often observed in Russia-aligned social engineering operations.

Analysts also warn that a newly released AI-enabled security framework known as Hexstrike-AI has been rapidly weaponized by cybercriminals to exploit Citrix NetScaler ADC and Gateway zero-day vulnerabilities, particularly CVE-2025-7775. Initially marketed as a research and red-team toolkit, Hexstrike-AI uses more than 150 AI agents to autonomously scan, exploit, and maintain persistence across large networks. Dark-web chatter indicates that exploitation tasks once requiring days can now be completed in under 10 minutes. The framework integrates models such as Claude, GPT, and Copilot to orchestrate multi-stage operations, raising concerns about accelerated offensive automation. Organizations are urged to patch immediately, restrict access, and monitor for compromise amid increasing abuse of autonomous exploitation tooling.

Finally, Oracle issued a security alert for CVE-2025-61884, a high-severity vulnerability affecting Oracle E-Business Suite versions 12.2.3 through 12.2.14. The flaw allows remote, unauthenticated access to sensitive resources via the Oracle Configurator Runtime UI component. Oracle emphasized the urgency of applying patches or mitigations, warning that unsupported versions are likely vulnerable and that all customers should align with the company's Lifetime Support Policy. The company assigned a CVSS score of 7.5 to the flaw, underscoring potential risk to exposed environments.

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.