Daily Intelligence Update | 13 November 2025

Researchers have identified a newly emerging Android banking trojan known as **Herodotus**, which appears to be a derivative of the Brokewell malware family and is already circulating as a Malware-as-a-Service offering. Recent campaigns have focused on Italy and Brazil, where operators distributed the malware through side-loaded applications delivered via SMiShing lures. Once deployed, Herodotus abuses Android Accessibility Services to perform overlay attacks that capture credentials and uses a blocking overlay to mask unauthorized transactions taking place in the background. What sets this trojan apart is its effort to imitate human interaction patterns during remote-control sessions—randomizing typing intervals between 0.3 and 3 seconds—to evade behavioral biometric defenses. The malware supports remotely triggered actions such as taps, swipes, and text entry while communicating with its command infrastructure through the MQTT protocol over domains like google-firebase[.]digital. Although code similarities suggest partial reuse from Brokewell, investigators note that Herodotus introduces its own communication logic and task-handling framework.

While mobile-focused threats continue to evolve, analysts have also uncovered a large-scale recruitment-themed phishing operation active throughout Q3 2024, in which adversaries impersonated major brands including Red Bull, Tesla, Google, and Ferrari. The campaign targeted individuals working in marketing and social-media roles, sending emails from messaging-service[@]post.xero[.]com to exploit the trust associated with Xero's legitimate infrastructure. Victims were directed to convincingly crafted spoofed portals that embedded realistic logos, CAPTCHAs, and authentication prompts mimicking services such as Glassdoor, Facebook, or X. Some variants requested résumé uploads, allowing attackers to collect additional personal data suitable for downstream social engineering. Researchers view this activity as a refinement of previous job-themed credential theft techniques, demonstrating continued adversary interest in exploiting trusted enterprise domains and professional recruitment workflows.

Investigators are also tracking a parallel wave of phishing activity leveraging **AI-enabled hosting platforms** such as Lovable, Netlify, and Vercel. Since early 2024, these services have been increasingly abused to host CAPTCHA-based landing pages that appear benign while concealing redirection to phishing portals targeting Microsoft 365 and other enterprise accounts. Analysts identified 98 malicious sites across these platforms, with activity spiking between February and April and rising again in August. The strategy benefits from the platforms' rapid deployment capabilities, free tier usage, and legitimate-looking domains such as vercel[.]app, .netlify[.]app, and lovable[.]app, allowing adversaries to rotate infrastructure quickly while evading automated scanning. Users are commonly lured with delivery notifications or password-reset prompts, underscoring how AI-generated site creation is accelerating the scale and sophistication of phishing ecosystems.

In addition to these social-engineering campaigns, security teams warn of ongoing exploitation of a critical remote code execution vulnerability in the ICTBroadcast autodialing platform, tracked as **CVE-2025-2611**. The flaw results from insufficient validation of session cookie data, allowing attackers to pass shell commands through the BROADCAST cookie and achieve unauthenticated command execution on systems running version 7.4 and earlier. Exploitation observed since October 11 initially involved timing-based probes such as "sleep 3," followed by deployment of reverse shells communicating with localto[.]net URLs and the IP address 143.47[.]53.106—previously associated with Ratty RAT operations in Europe. ICT Innovations released version 7.2.12 with new validation checks, but researchers continue to detect exploitation attempts and cannot yet confirm whether the patch fully eliminates the underlying issue.

These developments coincide with Microsoft's November 2025 Patch Tuesday release, which includes a fix for an actively exploited Windows Kernel vulnerability, **CVE-2025-62215**. The flaw stems from a race condition that allowed local attackers to escalate privileges to SYSTEM, prompting Microsoft to classify it as a zero-day due to observed in-the-wild exploitation. The update cycle addressed 63 vulnerabilities overall, including four rated critical—two enabling remote code execution, one allowing privilege

escalation, and one leading to information disclosure—alongside dozens of additional issues across elevation of privilege, remote code execution, information disclosure, denial-of-service, security feature bypass, and spoofing categories. Given its exploitation status and potential for chaining with other techniques, organizations are urged to prioritize deployment of the kernel patch and validate their endpoint hardening controls.
