Daily Intelligence Update | 23 October 2025

Researchers attributed a large-scale cyber espionage campaign to Iran-aligned APT MuddyWater, which leveraged a compromised mailbox accessed through NordVPN to distribute phishing emails delivering Phoenix backdoor version 4. The operation, which targeted more than 100 government, diplomatic, and humanitarian organizations across MENA and beyond, relied on malicious Microsoft Word attachments that prompted macro execution to install Phoenix alongside the FakeUpdate loader. The campaign featured updated persistence through registry changes and COM-based components, while command-and-control infrastructure was registered via NameCheap and briefly exposed through SSL certificate data. In addition to Phoenix, MuddyWater deployed a credential stealer disguised as a calculator app and used legitimate remote management tools such as Action1 and PDQ, aligning with prior campaigns and Iranian geopolitical targeting. In parallel, researchers uncovered the TamperedChef campaign, which disguised malware as a fake PDF editor distributed via Google ads and compromised websites. First detected in June 2025, the operation relied on heavily obfuscated JavaScript components, persistence via scheduled tasks and registry edits, and exfiltration of browser credentials and tokens, with infections traced to European organizations through domains such as inst[.]productivity-tools[.]ai and vault[.]appsuites[.]ai, and C2 activity linked to mka3e8[.]com. At the same time, a new ransomware leak site branded **GENESIS** emerged, listing nine victims dating back to late September. The operators describe themselves as financially motivated and independent of affiliate programs, threatening data exposure, reputational damage, and customer notifications if deadlines are missed, while claiming not to re-target victims and to spare live systems in healthcare and non-profits. GENESIS further increases pressure by publishing parsed data folders and promoting leaks on dark web forums.

On the vulnerability front, researchers disclosed the Phoenix RowHammer variant (CVE-2025-6202), a DDR5-targeting attack capable of bypassing both on-die ECC and TRR mitigations, achieving root access in under two minutes under default configurations. The attack impacts SK Hynix DDR5 chips manufactured between 2021 and 2024, with scenarios including breaking RSA-2048 SSH keys in co-located VMs and exploiting sudo for privilege escalation. Because hardware cannot be patched, researchers recommend significantly increasing refresh rates to mitigate the risk, though exposure will persist long-term. Separately, researchers revealed the Gemini Trifecta—a set of three prompt injection vulnerabilities in Google's Gemini suite—affecting Cloud Assist, Search Personalization, and the Browsing Tool. These flaws allowed stealthy data exfiltration via poisoned log fields, malicious search history injections, and browsing tool abuse to send user data to attacker-controlled domains, with proof-of-concept demos confirming feasibility. Google responded by rolling back vulnerable models, tightening outputs, and layering new defenses against prompt injection attacks. Finally, CISA confirmed that the Oracle E-Business Suite zero-day (CVE-2025-61884) has been exploited in an ongoing Cl0p-led extortion campaign tied to FIN11, mandating federal agencies patch by November 10. The campaign has already impacted organizations including Harvard University, Envoy Air, and the University of the Witwatersrand, with Emerson the only publicly named target yet to confirm compromise. Analysts note that Scattered LAPSUS$ Hunter's leaked proof-of-concept exploit accelerated attacker adoption, leaving many enterprises potentially breached before Oracle's emergency patch closed the window.
