Daily Intelligence Update | 18 November 2025

Plump Spider is a financially motivated criminal group operating primarily in Brazil, functioning much like a structured business where social engineering specialists, intrusion operators, and monetization teams work in coordination to compromise organizations that handle high-value payment workflows. Their campaigns focus on obtaining control over systems responsible for initiating and signing Pix pacs.008 transactions, manipulating legitimate approval processes to authorize attacker-generated transfer messages while leaving minimal forensic traces.

Recent analysis of emerging ransomware activity shows a parallel trend in operational sophistication. Gunra ransomware, active globally since early 2025, deploys Windows EXE and Linux ELF variants that allow attackers to fine-tune the encryption process through user-supplied arguments, controlling threads, paths, extensions, encryption ratios, and key-handling behavior. The ELF variant relies on ChaCha20 but uses a time-seeded rand() loop that repeatedly generates predictable key material, enabling brute-force recovery of encrypted data. In contrast, the Windows version uses CryptGenRandom and ChaCha8, making its encryption irreversible under current analysis. This divergence underscores how threat groups optimize tooling differently for target environments while still maintaining operational consistency.

The broader threat landscape also continues to shift as major vendors respond to security issues that expose downstream risks. SonicWall recently urged customers to reset passwords, rebind MFA, and rotate VPN keys after attackers accessed firewall configuration backups stored in MySonicWall cloud accounts. Although encrypted credentials were not directly compromised, the exposed configuration data could still help adversaries exploit affected devices. SonicWall attributed the issue to brute-force activity and issued regenerated preference files with randomized credentials and keys, advising administrators to verify configuration integrity before redeployment.

Similar concerns emerged when Logitech confirmed a data-theft incident linked to exploitation of a third-party zero-day vulnerability believed to be the same Oracle E-Business Suite flaw used in Clop's July data-exfiltration campaign. While Logitech reported no operational impact, attackers accessed limited employee, consumer, customer, and supplier information. Clop, claiming responsibility, added the company to its extortion site and allegedly leaked nearly 1.8 TB of data. The intrusion mirrors patterns seen in other Clop victims—including Harvard, Envoy Air, and The Washington Post—where organizations received ransom demands threatening public release of E-Business Suite data.

Adding further urgency, researchers and federal agencies confirmed active exploitation of CVE-2025-33073, a high-severity Windows SMB client vulnerability affecting both client and server versions of Windows, even though Microsoft patched it in June. The flaw allows attackers to coerce a system into authenticating to a malicious SMB server, enabling privilege escalation and lateral movement. Given SMB's prevalence in enterprise networks, CISA added the vulnerability to its Known Exploited Vulnerabilities catalog and urged organizations to apply June's patches, monitor for unusual outbound SMB traffic, and restrict SMB exposure to reduce coercion-based attack opportunities.
