Daily Intelligence Update | 23 September 2025

Researchers have uncovered a stealthy espionage campaign dubbed *Fire Ant*, which has been active since early 2025 and highlights virtualization infrastructure as a key weak point for enterprise security. The campaign reportedly targeted VMware ESXi, vCenter, and related network components by exploiting flaws such as CVE-2023-34048 and CVE-2023-20867, enabling attackers to compromise hypervisors and execute commands inside guest VMs without credentials. Once inside, the actors deployed unsigned VIBs, rogue VMs, and backdoors such as *ksmd* and *autobackup.bin*, while tampering with logging to avoid detection. They also leveraged F5 load balancers, pivot hosts, and internal web servers to tunnel across segmented environments, bypass firewalls, and evade ACLs. Even after remediation, Fire Ant reportedly re-compromised assets using rotated toolsets and mimicked forensic tools to remain persistent. Analysts note strong overlap with UNC3886 activity, though attribution remains unconfirmed.

At the same time, researchers are warning of a new evolution of the ClickFix social engineering technique—this time turning AI summarizers into malware delivery vectors. By embedding malicious instructions into HTML via CSS-based obfuscation, such as zero-width characters and off-screen rendering, attackers can invisibly inject ransomware-style commands into content that AI summarizers are asked to process. Proof-of-concept testing showed these instructions dominating the summarizer's context window and being echoed back as PowerShell execution steps, simulating ransomware behavior. With AI summarizers now widely integrated into email clients, browser extensions, and productivity platforms, analysts warn this method bypasses traditional phishing cues and creates a high-trust malware delivery channel. Amplified through SEO poisoning and syndication, the technique is considered a growing threat with a low barrier to adoption.

Further highlighting the risks of offensive AI, researchers have also discovered an emerging class of malware that directly leverages LLMs like GPT-4 to generate malicious logic at runtime. Early families include *MalTerminal*, which can dynamically create ransomware or reverse shells, and *LameHug* (PROMPTSTEAL), linked to APT28, which embeds stolen API keys and prompt injections to exfiltrate data and issue commands. Analysts note that this malware is especially difficult to detect due to its unpredictable behavior and legitimate-seeming API traffic, though researchers have started hunting for hardcoded prompts and unique API key usage patterns as indicators. The findings point to broader offensive experimentation with LLMs in vulnerability injection, phishing, and unauthorized data mining operations.

Meanwhile, ransomware activity continues to escalate. Analysts are tracking the Warlock ransomware operation, also referred to as GOLD SALEM, which has gained traction since March 2025 and compromised over 60 victims across North America, Europe, and South America. Some researchers suggest a link to Chinese state-aligned actor Storm-2603, though attribution remains debated. GOLD SALEM is said to exploit SharePoint servers through multi-CVE chains, maintaining access with custom Golang payloads and deploying advanced techniques such as Bring Your Own Vulnerable Driver (BYOVD) and stealth tunneling via Visual Studio Code. The group runs a Tor-based leak site, listing victims, staging data sales, and using public countdowns to pressure ransom payments. Analysts warn that several victims had already suffered previous ransomware attacks, underscoring the risks of re-compromise through unpatched vectors and recycled access.

In a major law enforcement development, UK authorities announced on September 18 the arrests of two teenagers, Thalha Jubair and Owen Flowers, tied to the August 2024 Transport for London attack and linked to the Scattered Spider group. Both face charges under the UK Computer Misuse Act, including the first prosecutions under provisions related to national security, carrying potential life sentences. U.S. authorities have also unsealed charges against Jubair, connecting him to more than 120 attacks across the U.S. with an estimated $115 million in ransom payments. These coordinated prosecutions mark a significant escalation in holding high-profile cybercriminal groups accountable.

On the vulnerability front, CISA has issued an urgent warning after confirming active exploitation of a critical remote code execution flaw in Dassault Systèmes' DELMIA Apriso manufacturing platform. The bug, tracked as CVE-2025-5086 and rated CVSS 9.0, arises from deserialization of untrusted data in all Apriso versions from Release 2020 to 2025. Attackers have been observed sending malicious SOAP requests containing compressed .NET executables, which execute on vulnerable systems. Researchers traced active payloads to IP 156.244.33[.]162, suggesting widespread automated scanning and exploitation is already underway. CISA has added the flaw to its Known Exploited Vulnerabilities catalog and urged immediate patching, given Apriso's prevalence in automotive, aerospace, and industrial environments.
