Daily Intelligence Update | 19 September 2025

Researchers have reported several significant developments across the ransomware, malware, and vulnerability landscapes this week. A coordinated campaign attributed to the Crypto24 ransomware group has been observed targeting enterprises in finance, manufacturing, and technology sectors across Asia, Europe, and the United States. The attackers leveraged legitimate tools such as PSExec, AnyDesk, and Group Policy scripts alongside custom malware to establish access, move laterally, and maintain persistence through malicious services and scheduled tasks. Their operations included the deployment of a customized RealBlindingEDR variant to evade endpoint detection and response, use of keyloggers and Google Drive for data theft, and the abuse of administrative utilities like gpscript[.]exe to disable protections. Once established, Crypto24 deployed its VMProtect-hardened ransomware that encrypts files with a .crypto24 extension, selectively avoids system-critical directories, deletes logs and forensic traces, and drops ransom notes to pressure victims.

Another long-running campaign tied to the group RevengeHotels, also tracked as TA558, has expanded its phishing operations targeting hotels across Brazil and Spanish-speaking countries. Researchers noted that the threat actor is now using AI-generated JavaScript and PowerShell loaders in invoice- and job-themed phishing emails, allowing them to execute VenomRAT, a customized fork of QuasarRAT. VenomRAT comes with AES-encrypted configuration, strong anti-analysis features, persistence mechanisms, and modules to disable Windows Defender, clear event logs, tunnel remote sessions through ngrok, and spread via USB drives. The campaign's use of clean, structured loader code and Portuguese- and Spanish-themed lures highlights both geographic expansion and the operational advantages gained through large language model–generated code.

Researchers also uncovered "GPUGate," a sophisticated malware campaign using poisoned Google Ads and GitHub links to distribute a malicious MSI installer disguised as GitHub Desktop. The installer is deliberately bloated with over 100 dummy executables to evade sandboxes, while the actual payload only decrypts on physical systems with a GPU, excluding most virtual machines and headless environments. Once active, the malware elevates privileges, disables Windows Defender, establishes persistence, and delivers additional payloads, including ransomware modules. The campaign primarily targeted IT professionals in Western Europe, with a macOS variant observed dropping AMOS Stealer. Researchers noted Russian-language scripting and code overlaps with ransomware ecosystems, pointing toward likely Russian-speaking operators with strong anti-analysis expertise.

Elsewhere, analysts tracked renewed activity by the Underground ransomware gang, which re-emerged in May 2024 and has continued to launch targeted attacks into 2025. The group employs AES and RSA encryption with per-file random keys, encrypts small files entirely while using stripe-based partial encryption for larger ones, and embeds encrypted metadata locally to avoid reliance on command-and-control servers. The ransomware deletes shadow copies, halts recovery services, and removes forensic traces with wevtutil[.]exe, while excluding system-critical folders. Customization per victim is evident, with ransom notes including Tor portal credentials and traces of prior compromise.

On the vulnerability front, Samsung has patched a critical zero-day in its proprietary Quram image library (CVE-2025-21043), already exploited in active attacks. The flaw, an out-of-bounds write in libimagecodec.quram[.]so, affected Android versions 13 through 16 and could allow remote code execution through maliciously crafted image files. Samsung confirmed that exploitation has occurred in the wild but withheld details to prevent replication.

Meanwhile, chatter on cybercrime forums in August 2025 showed sustained interest in exploiting recent vulnerabilities. Threat actors were actively seeking or offering proof-of-concept code for critical flaws such as CVE-2025-7775 in NetScaler ADC and Gateway devices, CVE-2025-6543 in the same products, and CVE-2025-53770 in Microsoft SharePoint Server. Discussions also surfaced around a purported zero-day in Microsoft IIS, allegedly enabling unauthenticated wormable remote code execution. The seller claimed it could propagate automatically across vulnerable servers, advertising availability via Telegram for a limited time. However, doubts were raised regarding the credibility of the offer, given the actor’s lack of history and reputation on underground markets.

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.