11 September 2025

Researchers have uncovered a new campaign attributed to a Lazarus subgroup targeting cryptocurrency and financial organizations with custom malware. The operation relied on social engineering through fake trading firm personas on Telegram and fraudulent meeting websites, with at least one incident suspected to involve a Chrome zero-day. Persistence was achieved through phantom DLL loading via the SessionEnv service, using PerfhLoader to deploy multiple implants. PondRAT, acting both as a loader and backdoor, was among the first deployed, sharing traits with the previously observed POOLRAT. This was followed by ThemeForestRAT, an advanced in-memory tool active since at least 2020, which offered expanded capabilities and stealth. After conducting network discovery and credential harvesting, the group reportedly transitioned to RemotePE, a more secure post-exploitation RAT retrieved via a DPAPI-encrypted loader, suggesting a deliberate progression toward operational security and persistence.

In parallel, researchers reported several new malware campaigns. A Linux-focused operation was observed exploiting unsanitized filename handling in shell scripts to deliver the VShell backdoor. Spam emails carrying malicious RAR archives contained specially crafted filenames with embedded Base64-encoded Bash commands. When executed through common utilities such as eval or echo, these filenames triggered a downloader that retrieved architecture-specific ELF binaries. The final payload was executed in memory using fexecve(), disguised as a kernel worker thread to blend into normal processes. Analysts linked the campaign to the Snowlight dropper and noted its cross-platform capability on x86, x64, ARM, and ARM64 systems, with fallback installation paths designed to ensure resilience.

On mobile platforms, researchers identified a spyware campaign called LunaSpy distributed through Telegram and other messaging apps as fake antivirus and banking protection software. Active since at least February 2025, LunaSpy simulated security scans to trick users into granting full device permissions. Once installed, it was capable of stealing browser and messenger passwords, recording audio and video, accessing geolocation data, and even issuing shell commands. More than 150 C2 domains and IPs were tied to the campaign, highlighting its broad infrastructure and likely global reach.

Another campaign tracked during this period involved the abuse of QR codes in phishing operations. Labeled “Scanception,” the activity embedded malicious QR codes into PDF attachments designed to bypass email and endpoint defenses. Victims scanning the codes with mobile devices were redirected through legitimate services such as YouTube, Google, Bing, Cisco, and Medium before reaching phishing sites mimicking Microsoft 365 portals. The attack incorporated Adversary-in-the-Middle infrastructure capable of harvesting credentials, MFA tokens, and one-time passcodes in real time. Analysts observed over 600 unique phishing PDFs in just three months, the majority of which had no detections on VirusTotal, underscoring the campaign’s stealth.

Meanwhile, CISA added a previously disclosed vulnerability in TP-Link TL-WA855RE Wi-Fi Range Extenders (CVE-2020-24363, CVSS 8.8) to its Known Exploited Vulnerabilities catalog following confirmation of active exploitation. The flaw, stemming from missing authentication, allowed remote attackers to trigger a factory reset and set new administrative credentials through crafted POST requests. Although fixed in a 2020 firmware update, the affected device has reached end-of-life, and CISA urged organizations to replace unsupported hardware. No attribution or exploitation details have yet been released.

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.