Lazarus Group Targets Crypto-Wallets and Financial Data while employing new Tradecrafts

By [Submitted on 27 May 2025 (v1), last revised 30 Jun 2025 (this version, v2)]

Archived: 2026-04-05 17:44:48 UTC

View PDF HTML (experimental)

Abstract:This report presents a comprehensive analysis of a malicious software sample, detailing its architecture, behavioral characteristics, and underlying intent. Through static and dynamic examination, the malware core functionalities, including persistence mechanisms, command-and-control communication, and data exfiltration routines, are identified and its supporting infrastructure is mapped. By correlating observed indicators of compromise with known techniques, tactics, and procedures, this analysis situates the sample within the broader context of contemporary threat campaigns and infers the capabilities and motivations of its likely threat actor.
Building on these findings, actionable threat intelligence is provided to support proactive defenses. Threat hunting teams receive precise detection hypotheses for uncovering latent adversarial presence, while monitoring systems can refine alert logic to detect anomalous activity in real time. Finally, the report discusses how this structured intelligence enhances predictive risk assessments, informs vulnerability prioritization, and strengthens organizational resilience against advanced persistent threats. By integrating detailed technical insights with strategic threat landscape mapping, this malware analysis report not only reconstructs past adversary actions but also establishes a robust foundation for anticipating and mitigating future attacks.

Submission history

From: Alessio Di Santo [view email]
[v1] Tue, 27 May 2025 20:13:29 UTC (13,716 KB)
[v2] Mon, 30 Jun 2025 19:42:53 UTC (10,369 KB)