

Lazarus Targets the Financial Sector with Memory-Only Malware Toolset

 cognnyte.com/blog/lazarus-targets-the-financial-sector-with-memory-only-malware-toolset

Gilad Zahavi

June 23, 2026

LUMINAR Threat Spotlight

This spotlight analysis examines a newly identified Lazarus campaign targeting financial institutions and cryptocurrency organizations using a sophisticated memory-only malware framework. The report reviews the malware toolset, the techniques used to evade detection, and what this activity reveals about the growing adoption of stealth-focused tradecraft among advanced threat actors.

Key Takeaway

A subgroup of the North Korea-linked Lazarus group has been observed targeting financial institutions and cryptocurrency organizations with a sophisticated malware framework designed to operate almost entirely in memory. The campaign demonstrates the growing adoption of stealth-focused techniques that reduce forensic visibility, evade traditional detection methods and enable long-term access to high-value environments.

Key Findings

Researchers identified a new malware toolset used by Lazarus consisting of three components: DPAPILoader, RemotePELoader and RemotePE.

The malware operates through a multi-stage infection chain designed to minimize detection. The first-stage loader decrypts and launches the next component using Windows Data Protection API (DPAPI), while the second-stage loader retrieves the final payload directly from attacker-controlled infrastructure. The final component, a fully featured remote access trojan (RAT), is executed entirely in memory and provides attackers with extensive control over compromised systems.

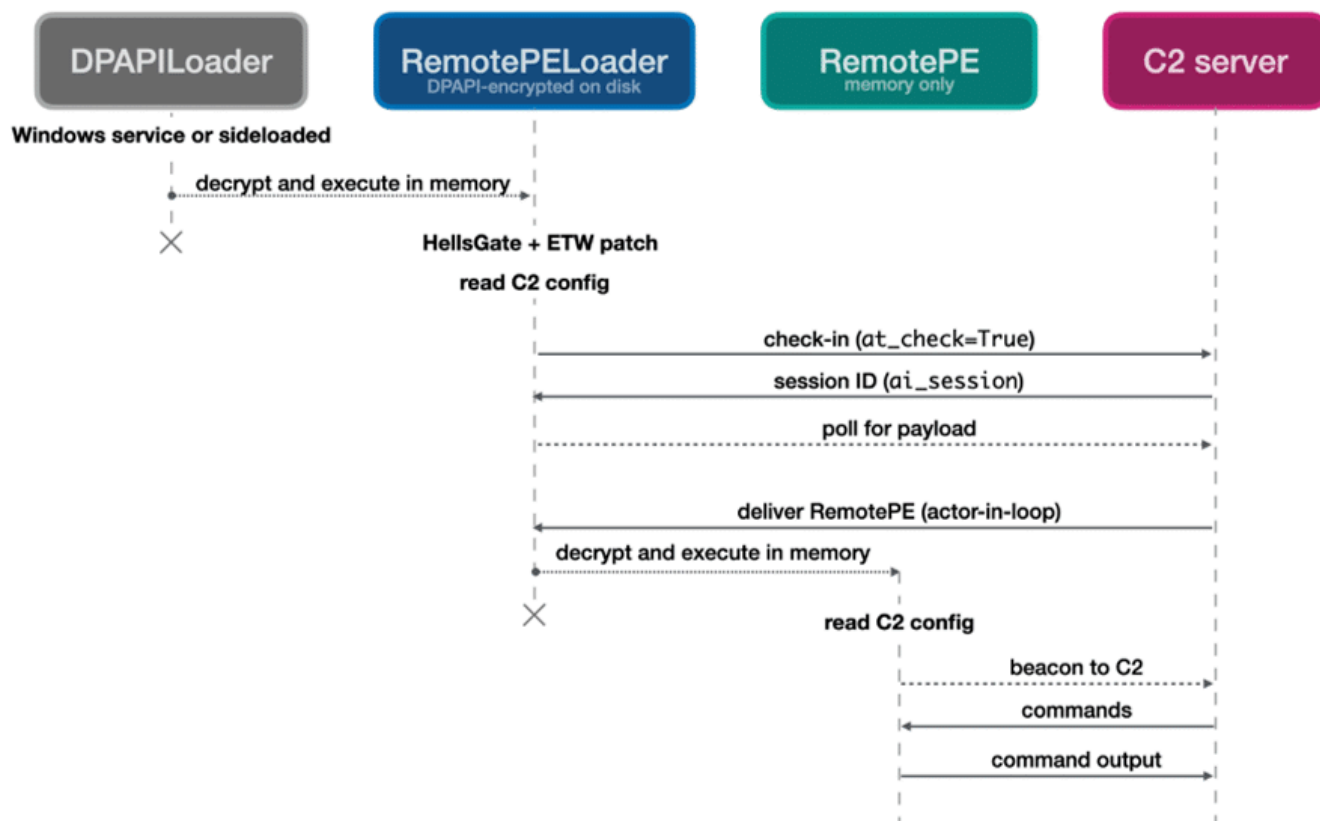


Figure 1: The three-stage attack chain employed by Lazarus in campaigns targeting financial institutions and cryptocurrency organizations. Source: Fox-IT.

A notable aspect of the campaign is the use of environmental keying through Windows DPAPI. This technique binds malware execution to a specific victim environment, making analysis outside the targeted system extremely difficult. Because each deployment generates a unique encrypted payload, traditional hash-based detection methods become significantly less effective.

Once deployed, the RemotePE malware enables command execution, file manipulation, process management and data access, providing attackers with the capabilities needed to support long-term objectives such as financial theft, intelligence collection or data exfiltration. The campaign primarily targets financial institutions and cryptocurrency organizations, sectors that have historically been a focus of Lazarus operations due to their direct financial value and access to digital assets.

Beyond the technical sophistication of the malware itself, the techniques observed in this campaign reflect broader shifts occurring across the threat landscape.

The Overall Trend

This campaign reflects a broader shift toward stealth-first malware development. Rather than relying solely on sophisticated exploitation techniques, advanced threat actors are

increasingly investing in methods that reduce visibility after compromise and complicate incident response efforts.

Memory-only malware, environmental keying and endpoint detection evasion are becoming increasingly common among advanced threat groups. These techniques significantly reduce the forensic footprint left on compromised systems, making traditional signature-based and file-based detection approaches less effective.

The activity also highlights the continued evolution of Lazarus. While the group remains heavily focused on financial gain and cryptocurrency theft, it continues to demonstrate advanced tradecraft typically associated with highly capable nation-state operators.

Assessment

The malware framework used in this campaign appears specifically designed to maintain long-term access while minimizing opportunities for detection and analysis.

The combination of environmental keying, memory-only execution and endpoint evasion techniques indicates a deliberate effort to increase operational security and hinder defensive investigations. These capabilities allow attackers to remain active within victim environments for extended periods while reducing the likelihood of discovery.

Organizations operating within the financial and cryptocurrency sectors should view this activity as a reminder that modern threat actors increasingly prioritize stealth, persistence and operational security rather than simply achieving initial access.

As advanced threat actors continue investing in stealth and persistence, organizations should expect memory-resident malware, environmental keying and endpoint evasion techniques to become increasingly common across financially motivated and nation-state operations.

Indicators of Compromise (IOCs)

[Download IOC](#)

[YARA Detection Rule](#)

Recommendations

Organizations should strengthen their ability to detect and investigate memory-resident threats and suspicious post-compromise activity.

Recommended actions include:

- Restrict unnecessary administrative privileges and enforce least-privilege access controls.
- Implement the IOCs and YARA detection rule included in this report.
- Deploy behavioral detection capabilities focused on memory-only malware techniques.

- Enhance endpoint telemetry collection to improve visibility into memory-resident threats.
- Monitor for suspicious use of Windows DPAPI functions and credential-protected decryption activity.
- Monitor outbound communications for unusual command-and-control activity.
- Conduct threat hunting activities focused on malicious DLL sideloading and suspicious service creation.
- Review and investigate newly created services and suspicious DLL sideloading activity.

June 23, 2026

Related Articles

[May 25 2026 · 5 Min Read](#)

[LUMINAR 2026 Threat Landscape Report Key Takeaways](#)

[Sep 12 2025 · 8 Min Read](#)

[Ransomware Will Make Your Healthcare Organization Sick](#)

[Aug 14 2025 · 9 Min Read](#)

[How Ransomware Gangs Are Evolving and What It Means for Defenders](#)

Gilad is a VP Threat Intelligence at Cognyte, leading the LUMINAR threat intelligence solution. Gilad has over 15 years of cyber security experience and is a leading expert in the threat intelligence domain. Prior to joining Cognyte, Gilad held executive positions at SenseCy Cyber Intelligence Ltd., which was one of the first global threat intelligence vendors. He holds an MA in Near & Middle Eastern Studies and a BA in Islamic Studies and Communications from Tel Aviv University.

[See more from this author](#)