CTI Report - Lumma Stealer

Cyber Threat Intelligence Report

Independent Researcher

September 9, 2025

Threat Intelligence

Summary

1 Report Metadata

- **Report ID:** CTI-2025-009
- **Date:** 09/09/2025
- **Priority:** High
- **Company Name:** Independent Research
- **Report Title:** Lumma Stealer Activity Report
- **Source Reliability:** B (Usually reliable)
- **Information Sensitivity:** TLP:AMBER

2 Intelligence Requirements Addressed

- Identify Lumma Stealer campaigns active in 2025
- Understand distribution vectors and capabilities
- Assess impact on victims and potential mitigation strategies

3 Data Sources

- Dark Web forums (exploit[.]in, RAMP)
- MalwareBazaar samples
- VirusTotal submissions
- Hybrid Analysis sandbox reports
- Shodan queries

4 Threat Actor

- **Name:** Unknown affiliates (Malware-as-a-Service operators)

- **Profile:** Lumma Stealer is sold as a MaaS since 2022. The operators advertise updates on Telegram and dark web forums.
- **Motivation:** Financial gain through credential theft, crypto-wallet hijacking, and resale of access.

5 Victim Information

- **Location:** Global (notably Europe and LATAM)
- **Sectors:** Finance, E-commerce, Corporate IT
- **Actor Motivation:** Monetization of stolen credentials and resale on markets

6 Capabilities, Adversary Infrastructure & Victim

- Credential harvesting (browsers, crypto wallets, extensions)
- System reconnaissance (hostname, hardware ID, geolocation)
- Exfiltration via Telegram bots & C2 servers
- MaaS infrastructure with tiered subscription models

7 Cyber Kill Chain

- **S1 Reconnaissance:** Actor monitors infected hosts for valuable credentials
- **S2 Weaponization:** Malware builder creates customized stealer payload
- **S3 Delivery:** Malspam with malicious attachments and cracked software installers
- **S4 Exploitation:** User executes dropper disguised as legitimate software
- **S5 Installation:** Persistence achieved via scheduled tasks and registry keys
- **S6 Command & Control (C2):** Communication over HTTPS to C2 panels

- **S7 Actions on Objective:** Exfiltration of browser data, wallets, and credentials

8 Artifacts

8.1 Endpoint Artifacts

Type	Description	Tactic
Registry Key	HKCU\Software\Microsoft\Windows\Run	Persistence
File Drop	%AppData%\Roaming\lumma\client.exe	Execution, Persistence

8.2 Network Artifacts

Type	Description	Kill Chain Stage
HTTP POST	Data exfiltration to C2	C2, Exfiltration
Telegram API	Bot used for credential uploads	C2

9 Malware

9.1 Malware Hashes

Type	File Hash	Description	Kill Chain Stage
SHA256	65eb366739361b97fb68c0ac4b9fbaad2ac26e0cb0a21af0ad0a7561f7e22e94	Lumma Stealer v4	Installation, C2

9.2 Vulnerabilities

CVE #	CVSS Score	Patch Available (Y/N)	Remediation	Date Re-ported	Patch Applied (Y/N/N/A)
CVE-2017-11882	7.8	Y	Apply Microsoft Office patch KB2553204	2017-11-15	N/A
CVE-2021-40444	8.8	Y	Block ActiveX controls, apply MS patch	2021-09-07	N/A

10 Detection & Response

Tactic	Technique	Procedure	D3FEND Control	Rule / Query Name	Type	Description	Reference
Credential Dump	T1555.003	Harvest browser credentials	Credential Harden-ing	Lumma_Browser_Acc	Sigma	Detects abnormal access to browser files	MITRE ATT&CK
Persiste	T1547.(	Registry Run Key persistence	Registry Monitor-ing	Lumma_	Sigr	Alerts when suspicious Run key is created	Sysmon Logs
Exfiltrati	T1041	Exfiltration over C2 HTTPS	Network Segmen-tation	Lumma_Exfil	Sigma/Suri	Detects anomalous HTTPS POST exfiltration	Suricata Rule

11 Confidence Levels

- **Assessment:** Highly Likely (75–85%)
- **Severity:** High – threat requires immediate containment and monitoring.

12 Source Reliability (A–F)

B – Usually reliable (consistent reporting across multiple vendors).

13 Information Credibility (1–6)

2 – Probably true (validated by sandbox analysis and multiple AV engines).

14 Traffic Light Protocol (TLP)

TLP:AMBER – Restricted to organization and trusted partners.

15 CTI Team Roles

Role	Name	Title	Contact
Head of CTI	John Doe	CTI Manager	j.doe@company.com
CTI Lead	Jane Smith	Senior CTI Analyst	j.smith@company.com
CTI Analyst	João Pedro Cezarino	Report Author	researcher@example.com

16 Glossary

- **Lumma Stealer:** Malware-as-a-Service (MaaS) focused on credential and wallet theft.
- **MaaS:** Malware-as-a-Service, subscription-based criminal business model.
- **C2:** Command & Control infrastructure used for data exfiltration.
- **IOC:** Indicator of Compromise.
- **TTP:** Tactics, Techniques, and Procedures (MITRE ATT&CK framework).