Relatório de Inteligência - RIT-001

Lumma Stealer Analysis

João Pedro Rosa Cezarino

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 Introduction

The Cyber Threat Intelligence (CTI) team is responsible for monitoring emerging and persistent threats to protect brand integrity and prevent the exposure of sensitive information. This proactive monitoring aims to identify prevalent malware campaigns, new Tactics, Techniques, and Procedures (TTPs), and threat actor activities that may affect the organization, its employees, or its partners. This report focuses on the Lumma Stealer, a significant information-stealing malware.

3 Executive Summary

Lumma Stealer (also known as LummaC2) is a prominent information-stealing malware operating on a Malware-as-a-Service (MaaS) model, making it accessible to a wide range of financially motivated threat actors. Developed by an actor known as “Shamel,” Lumma Stealer poses a significant threat by exfiltrating sensitive data from compromised Windows systems. Its distribution is opportunistic and relies heavily on sophisticated social engineering, malvertising, and abuse of trusted platforms, making it a persistent risk to organizations across all sectors.

4 Threat Details

The primary function of Lumma Stealer is to harvest and exfiltrate a wide variety of sensitive data from victim machines. The malware is written in C and is continuously updated with advanced features to evade detection and maximize data theft. Its MaaS model allows affiliates to customize and deploy the malware easily. The primary types of data targeted include:

- Browser Credentials: Usernames, passwords, cookies, and autofill data from over 10 major web browsers.
- Cryptocurrency Wallets: Data from numerous cryptocurrency wallet applications and browser extensions.
- Two-Factor Authentication (2FA) Tokens: Information from 2FA extensions, potentially allowing attackers to bypass multi-factor authentication.
- System Information: Detailed information about the compromised machine, including hardware, OS version, and IP address.
- Application Data: Credentials and data from various applications, including FTP clients and messaging apps like Telegram.

The malware employs a multi-stage, often fileless, execution chain using obfuscated PowerShell scripts and Living Off the Land Binaries (LOLBINs) like mshta.exe to evade detection. A particularly effective delivery method is the “ClickFix” technique, where victims are tricked by fake CAPTCHA pages into pasting and executing malicious commands in the Windows Run dialog, bypassing browser-based security controls. Data is exfiltrated via HTTP POST requests to a resilient and frequently changing Command and Control (C2) infrastructure.

5 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

6 Threat Actor Profile

The threat actor “Shamel” (also known as “Lumma”) is a Russian-speaking developer responsible for creating and maintaining the Lumma Stealer. The malware has been advertised on Russian-language underground forums since August 2022. Shamel operates a Malware-as-a-Service (MaaS) business, selling subscriptions to the stealer via Telegram and a dedicated website. This model allows a broad range of cybercriminals, from low-skilled individuals to sophisticated groups like the ransomware operator Octo Tempest, to use the malware for initial access and data theft. Subscription tiers range from approximately $250 per month to $20,000 for access to the source code, making it a commercially successful and widely distributed threat.

7 Forum Post by the Attacker

A representative advertisement for the Lumma Stealer MaaS on an underground forum.

```
Lumma Stealer v4.0 - The Best Infostealer on the Market
Hey, I am selling subscriptions to the Lumma Stealer MaaS platform. Stable,
    reliable, and FUD (Fully Undetectable).
Features:
- Steals from all major browsers (Chrome, Firefox, Edge, etc.)
- Grabs Crypto Wallets (Metamask, Exodus, and 80+ more)
- 2FA Extension support
- Advanced anti-sandbox and anti-debug techniques
- Resilient C2 infrastructure with fallback mechanisms
- Loader functionality to drop additional payloads (EXE, DLL, PS)
Pricing:
- Basic: $250/month
- Professional: $500/month
- Source Code Access: $20,000 (one-time)
PM me for offers and details. Serious buyers only.
```

8 Infection Chain

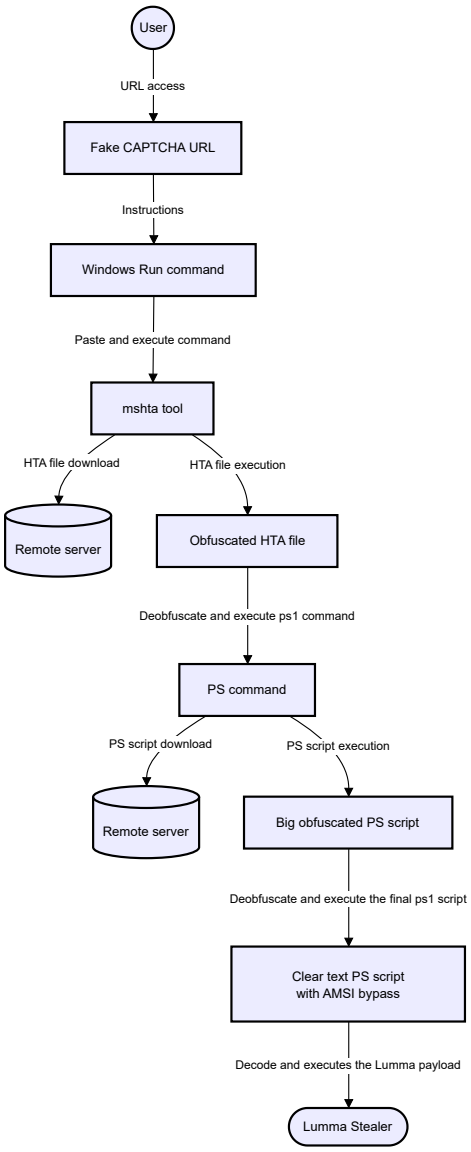

Figure 1: Lumma stealer infection chain

9 Mitigation Recommendations

1. **User Awareness Training**: Educate employees to recognize phishing, malvertising, and social engineering tactics like the “ClickFix” fake CAPTCHA. Emphasize caution against downloading software from untrusted sources or executing commands from websites.
2. **Endpoint Detection and Response (EDR)**: Deploy and configure an EDR solution to monitor for anomalous process behavior, such as mshta.exe spawning PowerShell, or unauthorized processes accessing browser credential stores.
3. **Restrict Script Execution**: Use application control policies to restrict the execution of PowerShell and other scripting languages for users who do not require them for their job functions.
4. **Network Filtering**: Block connections to known malicious domains and newly registered domains (NRDs), which are frequently used for C2 infrastructure. Use DNS filtering and web gateways to prevent access to malware distribution sites.
5. **Credential Hygiene**: Encourage the use of password managers instead of saving credentials in browsers. Enforce Multi-Factor Authentication (MFA) across all critical services to mitigate the impact of stolen credentials.
6. **Regular Software Updates**: Keep operating systems, browsers, and other software patched and up-to-date to protect against vulnerabilities that could be exploited in multi-stage attacks.

10 Conclusion

The Lumma Stealer represents a mature and resilient threat within the cybercrime ecosystem, amplified by its accessible MaaS model. Its reliance on sophisticated social engineering and evasive execution techniques makes it a danger that bypasses traditional signature-based defenses. Organizations must adopt a multi-layered security posture that combines advanced technical controls with robust user education to effectively mitigate the risk of credential theft and subsequent network compromise.

11 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

12 Artifacts

12.1 Endpoint Artifacts

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

12.2 Network Artifacts

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

13 Malware

13.1 Malware Hashes

Type	File Hash	Description	Kill Chain Stage
SHA256	65eb366739361b97fb68c0ac4b9fbaad2ac26e0cb0a21af0ad0a75817[illegible]	Lumma Stealer v4	Installation, C2

13.2 Vulnerabilities

CVE #	CVSS Score	Patch Available (Y/N)	Remediation	Date Reported	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

14 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_IOC	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_Exfil	Detects anomalous HTTPS POST exfiltration	Suricata Rule

15 Confidence Levels

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

16 Source Reliability (A–F)

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

17 Information Credibility (1–6)

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

18 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).