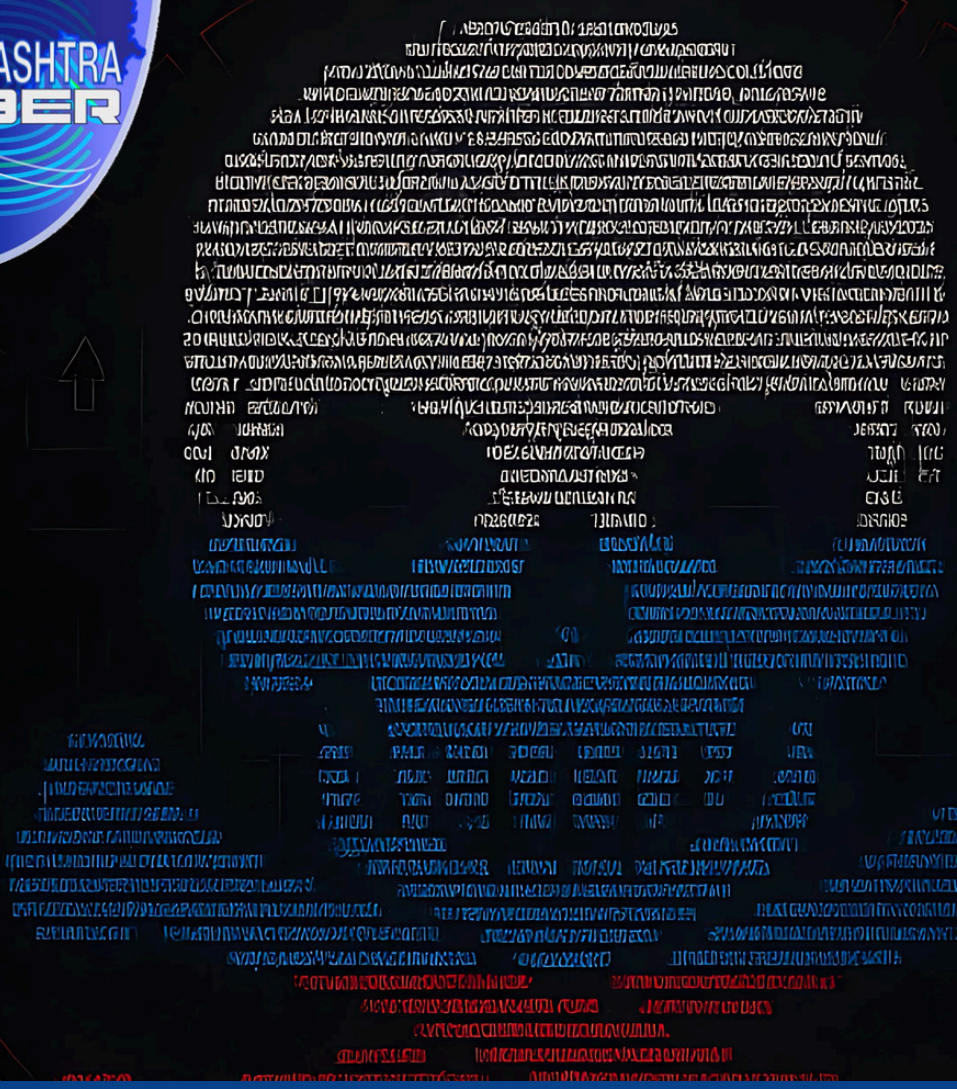
MAHARASHTRA CYBER

TLP:CLEAR



Lumma C2 Malware

CERTMH_CTI_2025_30 04/07/2025

Table of Contents

Summary

Lumma C2 represents one of the most significant and rapidly evolving information-stealing threats in the current cybersecurity landscape. First emerging in August 2022 from Russia-based developers, this sophisticated Malware-as-a-Service (MaaS) offering has transformed from a niche threat into a prolific cybercrime tool responsible for compromising approximately 394,000 Windows systems within a three-month period in early 2025.

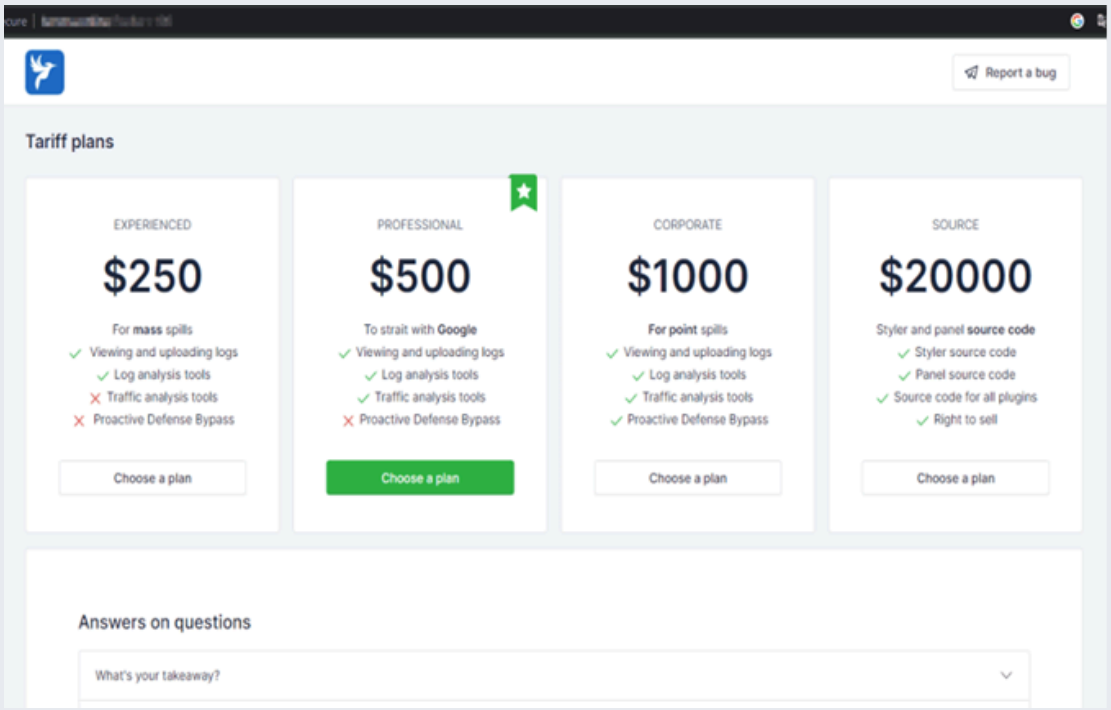
The malware operates through a tiered subscription model ranging from $250 to $20,000, with higher tiers offering advanced capabilities including source code access. This business model has effectively democratized advanced cyber capabilities, allowing even technically unsophisticated actors to deploy sophisticated attacks previously limited to advanced persistent threat (APT) group.

Lumma C2's technical sophistication is evident in its multi-layered evasion techniques, including LLVM-based obfuscation, process hollowing targeting legitimate system utilities, and direct syscall execution to bypass security solutions. The malware's primary focus is comprehensive credential theft, targeting over 86 browser extensions, 42 browser profiles, 25+ cryptocurrency wallets, and various communications applications.

Lumma Website page with logo and description

In May 2025, Microsoft's Digital Crimes Unit spearheaded a major disruption operation against Lumma's infrastructure, taking down approximately 2,300 malicious domains. However, the malware's resilient command and control architecture—featuring multi-tier fallback channels through legitimate services like Steam profiles and Telegram—ensures the threat persists despite these enforcement actions.

Organizations facing this threat must implement a defense-in-depth strategy focusing on memory protection, credential isolation, and behavioral monitoring to effectively counter Lumma's sophisticated evasion techniques and post-exploitation capabilities.



Advertisement on Lumma Website

Attribute	Details
Name	Lumma C2 / Lumma Stealer
Origin Date	Aug 1, 2022
Origin Country	Russia
Aliases	LummaC2, Lummac, Lumma Stealer,"Shamel"
Distribution Model	Malware-as-a-Service (MaaS)
Pricing Structure	$250-$20,000 (tiered subscription)
Number of Attacks (Global)	~394,000 Windows computers
India Impact	Banking, Healthcare, Telecom, and Marketing sectors
Top Targeted Countries	Peru, Poland, Spain, Mexico, Slovakia
Primary Distribution Methods in India	Fake CAPTCHA verification pages, phishing emails, Discord CDN abuse, malvertising
Key Target Sectors	Financial Services, Healthcare, Telecommunications, Marketing
Active Years	2022 - Present (2025)
Affiliated Groups	Independent MaaS provider; used by Octo Tempest (Scattered Spider)

Key Takeaway

01 Comprehensive Evolution Timeline

02 Dual Case-Study Perspective

03 Four-Phase Attack Framework

04 Sector-Specific Threat Landscape

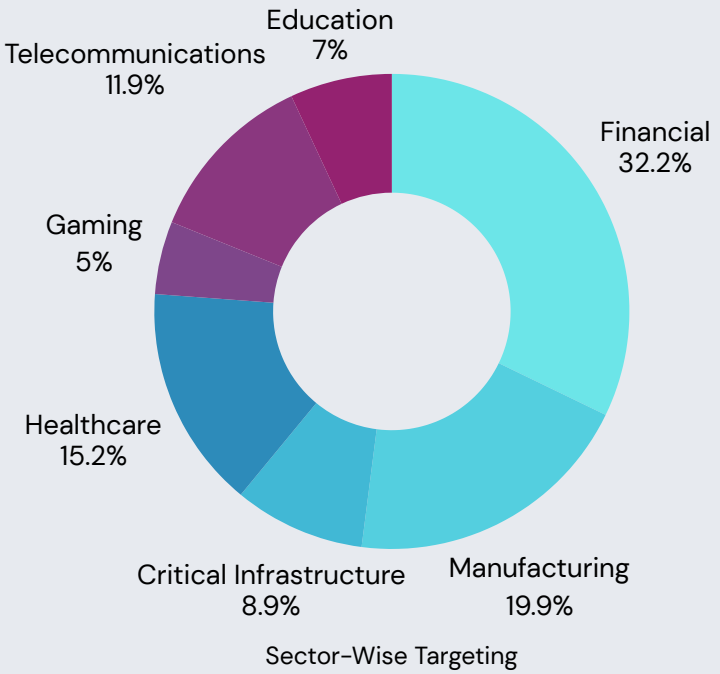
05 MITRE ATT&CK Mapping

Threat Profile

Lumma Stealer is a Malware-as-a-Service infostealer first observed in August 2022 and sold by a Russian-speaking operator "Shamel" under the alias Storm-2477. Affiliates pay a tiered subscription $250/month for an "Experienced" build, $750/month for "Professional," and up to $20 000 for "Corporate"/source-code access—and, by late 2023, Shamel claimed roughly 400 active clients actively using it

Since its debut in August 2022, Lumma Stealer has rapidly evolved from a simple browser-credential dumper into a sophisticated, multi-stage infostealer designed for in-memory execution and EDR evasion:

- v1 (Aug 2022): Browser credential theft
- v2–3 (Early 2023): Added crypto-wallet targeting and basic anti-VM checks
- v4–5 (2024): LLVM(Low Level Virtual Machine) obfuscation with control-flow flattening and custom stack decryption
- v6 (Late 2024–'25): Switched to uid/cid C2 protocol, implemented Heavens Gate for mixed-mode execution, uses direct syscalls to bypass EDR, and leverages multiple encrypted C2 fallbacks (Cloudflare proxy, Steam profiles, Telegram



Sector-Wise Targeting

- Multiple real-world campaigns have confirmed Lumma's reach and impact. In January 2025, Netskope observed a massive fake-CAPTCHA campaign targeting healthcare, banking, telecom, and marketing firms worldwide.
- On April 7, 2025, Microsoft tracked a drive-by download cluster using "EtherHiding" and ClickFix lures on compromised sites, which funneled Canadian organizations into executing mshta-based commands to deploy Lumma in memory.
- In 2024, Lumma was linked to the PowerSchool student-data breach, where stolen credentials facilitated unauthorized database access.
- Finally, on May 13–21, 2025, a multinational takedown led by Microsoft DCU, DOJ, Europol, and others seized over 2 300 C2 domains—Lumma had infected some 394 000 Windows machines in the prior quarter and was a go-to tool for groups like Scattered Spider

Timeline

AUGUST 2022

First appearance of Lumma Stealer on underground forums.

DECEMBER 2022

Official launch with marketing campaign.Over 1k Telegram subscribers by May 2023.

EARLY 2023

Versions 2–3 add cryptocurrency-wallet theft and basic anti-VM checks.Phishing and malvertising deployments.

NOVEMBER 2023

~400 active clients reported by developer

H2 2024

A 369 % increase in Lumma detections between H1 and H2 2024, reflecting rapid affiliate uptake

SEPTEMBER 2024

Lumma campaigns using ClickFix since at least September—fake “I’m not a robot” prompts that drop mshta-based loaders in memory

LATE 2024

Introduction of LLVM-based obfuscation, control-flow flattening, custom stack decryption and CFF techniques to thwart static analysis.

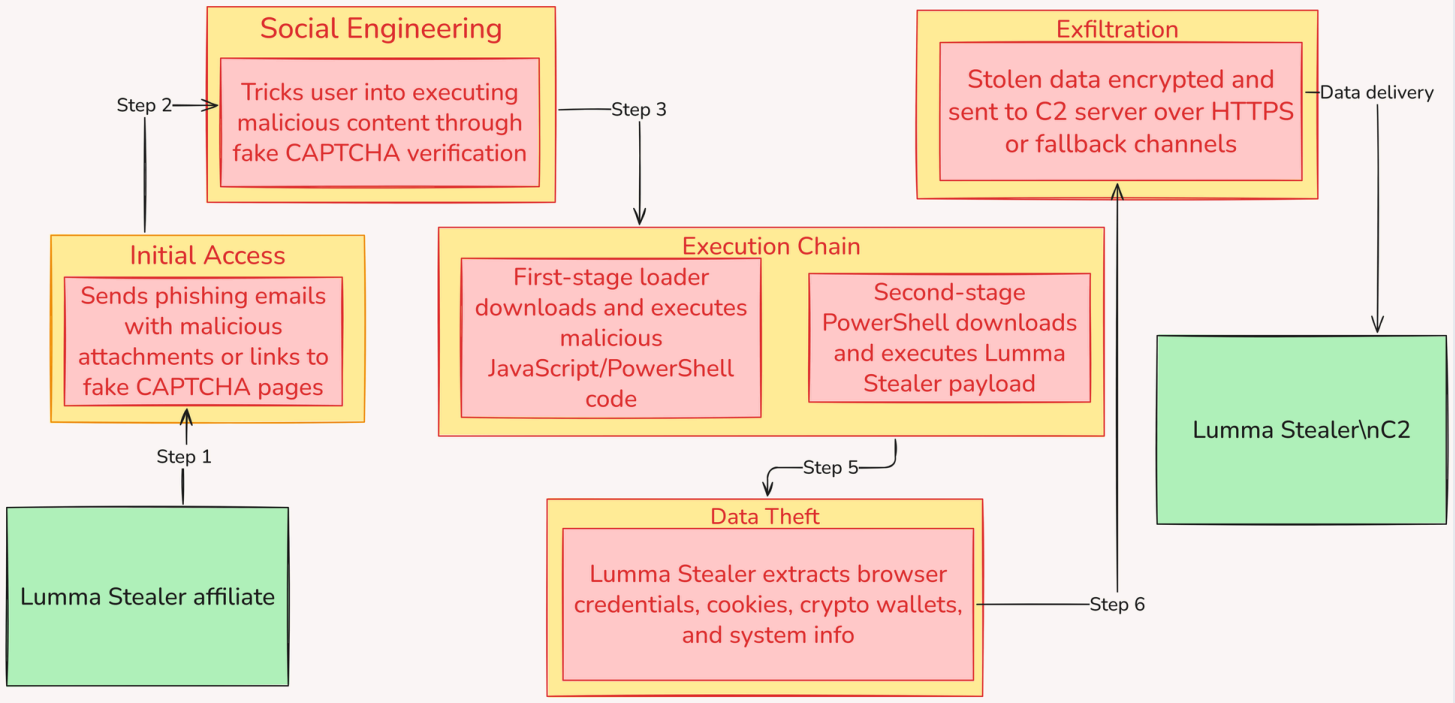
2025

DCU, DOJ, Europol, CISA, ESET, Cloudflare seized 2,300 Lumma domains.

Methodology

This campaign employs a multi-stage strategy, initiating with URLs embedded in PDF documents and progressing through successive dropper URLs. These layered techniques demonstrate sophisticated obfuscation tactics aimed at evading detection while deceiving users into executing malicious payloads.

A notable feature of this operation is the use of a dynamically generated password for each downloaded archive. This added layer of complexity hampers traditional signature-based detection and analysis, underscoring the evolving tactics of threat actors behind malware like Lumma Stealer, who are continuously innovating their delivery mechanisms to stay ahead of security defenses.



Stages of infection process in Lumma campaign

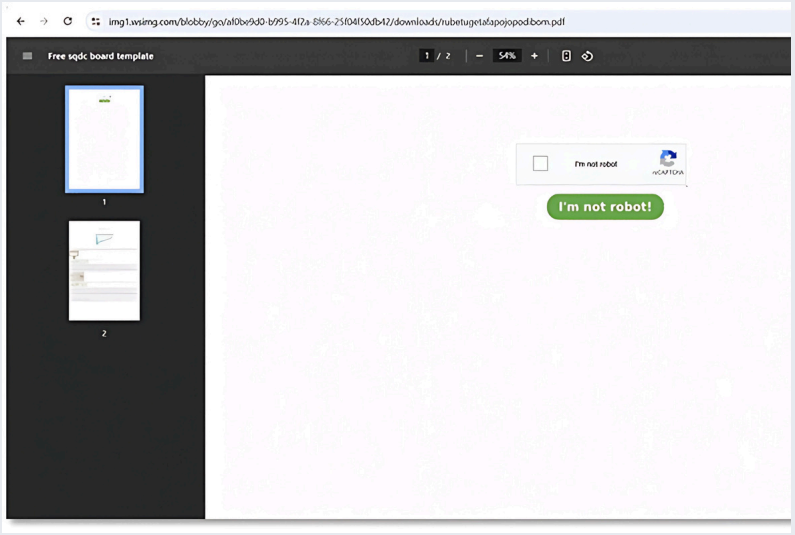
1.Initial Access

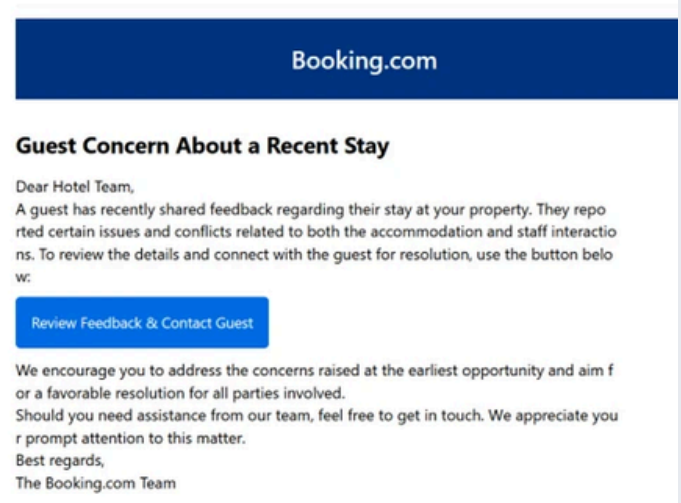
Lumma C2 is developed in C++ and ASM, leveraging advanced obfuscation like LLVM, Control Flow Flattening, and custom stack decryption to resist analysis. Its operators deploy diverse, filter-heavy delivery tactics, recently including EtherHiding via blockchain and ClickFix social engineering.

1 Case 1: PDF Drop Case

- A PDF named Invoice.pdf, hosted on a trusted CDN (wsimg.com), displays a fake "bot check." When clicked, it triggers a silent redirect chain (lusejoripifofo.robazumuxi.com → berapt-medii.com → media.site34l.cyou).

- The final page offers payload.7z and a one-time password embedded in the PDF. Users must extract and manually run lumma.exe (often via cmd.exe), bypassing both reputation-based and sandbox-based detection.




Booking.com

Guest Concern About a Recent Stay

Dear Hotel Team,
A guest has recently shared feedback regarding their stay at your property. They repo rted certain issues and conflicts related to both the accommodation and staff interactio ns. To review the details and connect with the guest for resolution, use the button belo w:

Review Feedback & Contact Guest

We encourage you to address the concerns raised at the earliest opportunity and aim f or a favorable resolution for all parties involved.
Should you need assistance from our team, feel free to get in touch. We appreciate you r prompt attention to this matter.
Best regards,
The Booking.com Team

2 Case 2: Booking.com Case

- Victims receive invoice-themed emails tailored with their addresses, each containing a link to a Prometheus-based TDS hosted on compromised domains.

- The TDS funnels users to binadata[.]com, serving a ClickFix fake CAPTCHA page, which forms part of the broader social engineering chain.

3 MITRE TTPs

- T1566.001 / T1566.002 – Phishing: Spearphishing Link/Attachment
- T1102.001 – Web Service: Malicious Hosting / TDS
- T1204.002 – User Execution: Malicious File
- T1573.001 – Encrypted Channel: password-protected archive
- T1102.001 – Web Service: Traffic Direction System

2.Execution & Evasion

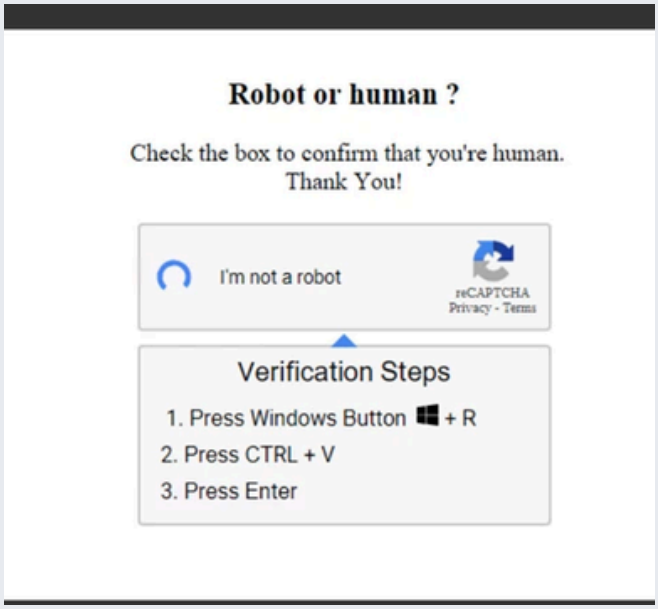
Lumma C2 executes malicious code using a mix of social engineering and technical exploits, employing syscalls and Heaven's Gate to bypass user-mode API hooks. It maintains persistence via process hollowing, injecting into legitimate processes like msbuild.exe, regasm.exe, regsvcs.exe, and explorer.exe.

1 Case 1: PDF Drop Case

- Running lumma.exe (an NSIS installer) drops multiple .accde modules and a batch script into *%Temp%\283528*. Static analysis flags API calls like CreateDirectoryW, CopyFileW, GetTempPathW, and ShellExecuteW.

- The .bat file checks for AV processes (e.g., opsvc, wrsa, Sophos, AVG, Avast).If found it loops via ping -n 188 (sandbox evasion) and exits. If not then merges the NSIS loader with VB code into an AutoIT binary (Alexander.com) and companion script (o.a3x) using copy /b.

- Alexander.com executes o.a3x (AutoIT v3 EA06) entirely in memory. Analysis reveals obfuscated strings, junk code, custom stack-based decryption, and anti-debugging mechanisms.



2 Case 2: Booking.com Case

- A fake CAPTCHA page stealthily copies a malicious mshta command to the clipboard when the user clicks "I'm not a robot."

- mshta.exe executes obfuscated JavaScript in memory, which spawns PowerShell to retrieve and run the stealer.

- loader.hta launches Base64 PowerShell to: Fetch another script from 185.147.125[.]174 Deliver and execute a bundled Lumma Stealer + Xworm payload.

3 MITRE TTPs

- T1059.003 / T1059.001 – Windows Command Shell / PowerShell
- T1218.005 – Signed Binary Proxy Execution (mshta.exe)
- T1497.001 – Virtualization/Sandbox Evasion
- T1027 – Obfuscated Files or information
- T1140 – Deobfuscate/Decode Files or Information

3.Escalation

Lumma maintains persistence through several methods, including modifying registry entries in both HKLM and HKCU hives, creating scheduled tasks with SYSTEM privileges, and placing misleading shortcuts in the Startup folder. It also uses Run key installations and reflective DLL injection to stay memory-resident.

Technically, it allocates memory in legitimate system processes using **VirtualAllocEx**, writes malicious code with **WriteProcessMemory**, and triggers execution using **ResumeThread**. This combination allows Lumma to inject itself into trusted processes and maintain stealthy, long-term access

1 Case 1: PDF Drop Case

- Though the stealer runs once by design, affiliates create a Scheduled Task named Lodging to execute wscript Quantifyr.js every 5 minutes. This JS stub re-downloads and relaunches the AutoIT loader if missing—maintaining persistence with zero user interaction.

- A .url shortcut in *%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup* triggers *mshta.exe //./Quantifyr.js* at startup.

- Additionally, some variants set *HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater* to relaunch on login

2 Case 2: Booking.com Case

- This campaign utilized a one-shot loader that executed Lumma entirely in memory before terminating, without establishing any long-term persistence. Unlike other variants, it did not create services, scheduled tasks, or registry Run keys—relying instead on the likelihood of end-user reinfection for repeated access. However, affiliates may optionally deploy persistence mechanisms like scheduled tasks or Run-key entries in separate campaigns.

3 MITRE TTPs

- T1053.005 – Scheduled Task/Job
- T1547.001 – Registry Run Keys / Startup Folder
- T1543.003 – Create or Modify System Process (Windows Service)
- T1505.003 – Accessibility Features

4.C2 Communication & Exfilteration

Lumma uses a multi-tiered C2 setup with rotating hardcoded domains, fallback channels via Steam/Telegram, and Cloudflare protection. Communications are encrypted (ChaCha20, HTTPS), with custom obfuscation per channel. Commands and parameters evolve by version.

Targets include browser data, crypto wallets, email/FTP clients, messaging apps, documents, and system metadata. Theft is guided by C2-delivered config files with sectioned targeting logic. Techniques include memory scraping and clipboard monitoring for live data capture.

1 Case 1: PDF Drop Case

- Lumma transmits stolen data using a ChaCha20-encrypted custom protocol via POST requests to rotating C2 domains. If primary channels fail (e.g., blocked Cloudflare-protected endpoints), it falls back to Telegram Bot API (sending JSON blobs) and public Steam profile comments with base64-encoded data.

- Harvested data includes browser credentials, MetaMask wallet keys, and 2FA tokens from Authy/WinAuth. Upon successful exfiltration, Lumma wipes its temp directory and self-overwrites with junk data to minimize forensic footprint.

2 Case 2: Booking.com Case

- Lumma exfiltrates stolen data via HTTPS POST requests to rotating, Cloudflare-protected domains using ChaCha20 and custom stack-based encryption. If primary C2s fail, it falls back to the affiliate's Telegram Bot API, then Steam profile comments with base64-encoded payloads.

- Legacy parameters like *act/lid/j* are replaced with *uid/cid* in POST requests (e.g., *POST https://[domain]/api?uid=&cid=*). Data—including browser credentials, wallet keys, and 2FA tokens—is collected, chunked, and exfiltrated with minimal visibility

3 MITRE TTPs

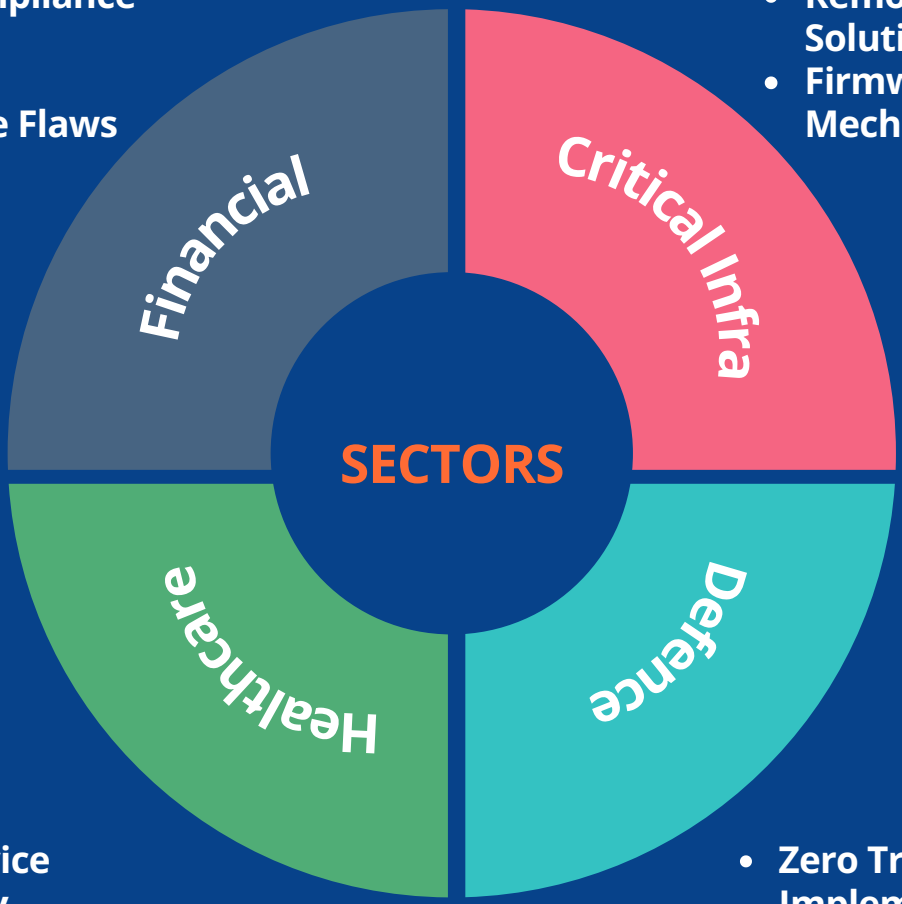
- T1071.001 – Application Layer Protocol: HTTP/S
- T1008 – Fallback Channels
- T1573.001 – Encrypted Channel
- T1105 – Ingress Tool Transfer

Sector Impact

Attack Surface

- Privileged Access Management Gaps
- API Security Weaknesses
- PCI-DSS Compliance Blind Spots
- Credential Architecture Flaws

- OT-IT Network Segmentation Failures
- Legacy SCADA Authentication
- Remote Access Solutions
- Firmware Update Mechanisms:



- Medical Device Connectivity
- EHR Integration Points
- Telehealth Platform Weaknesses
- Legacy Windows Systems

- Zero Trust Implementation Gaps
- Classified/Unclassified Boundary Controls
- Identity Federation Weaknesses
- Procurement System Access

Sector Impact

Attack Pattern

1 Finance Sector

- **Trading Platform Focus:** Recent targeting shift toward retail trading platforms during peak trading hours (9:30-11:00 AM local markets)
- **Weekend Execution Strategy:** 67% of financial sector infections occur Friday-Sunday when monitoring staff is reduced
- **Supply Chain Compromise:** Distribution through compromised financial news aggregators and market analysis tools
- **Crypto-Mixer Integration:** Direct exfiltration to cryptocurrency mixing services (3 hops minimum) for immediate laundering

2 Critical Infrastructure

- **Long-Term Persistence Focus:** Average dwell time of 47 days before active exploitation begins
- **After-Hours Activity:** Command execution primarily occurring during maintenance windows (2:00-4:00 AM local time)
- **Safety System Targeting:** Specific focus on bypassing or disabling safety instrumented systems (SIS) before operational changes
- **Geopolitical Alignment:** Attack spikes correlating with international tensions involving host nation of targeted facilities

3 Healthcare Sector

- **Patient Data Monetization:** Tiered pricing model for stolen health records ($100-$500 per record) based on patient demographics
- **Provider Credential Focus:** Prioritization of physician credentials with prescription capabilities for fraud schemes
- **Hybrid Extortion Tactics:** Combined data theft and encryption with triple extortion (patient notification threat)
- **Insurance Fraud Enablement:** Sale of patient data specifically to groups specializing in insurance and Medicare fraud

4 Defence Sector

- **Slow-and-Low Exfiltration:** Data transfer rates deliberately kept below detection thresholds (avg. 2.3MB/hour)
- **Living-off-the-Land Techniques:** Heavy use of native Windows utilities to avoid introducing malicious executables
- **Credential Harvesting Campaign Structure:** Two-phase operations with initial credential collection followed by targeted access
- **Weekend Privilege Escalation:** Key system compromise activities concentrated during non-business hours

Recommendations

1.Advanced Threat Modeling

Technical Recommendation: Implement MITRE ATT&CK-based threat modeling specifically focused on Lumma C2's attack patterns. Create threat scenarios that map the malware's known delivery mechanisms, persistence techniques, and data exfiltration methods to your organization's critical assets.

Implementation Strategy:

- Conduct adversary emulation exercises that simulate Lumma's specific process hollowing techniques targeting msbuild.exe, regasm.exe, and explorer.exe
- Prioritize security controls that detect syscall-based API invocations outside normal operational parameters
- Evaluate business impact of credential theft from browser stores with specific focus on your organization's critical web applications

2.Supply Chain Risk Management

Technical Recommendation: Implement software supply chain integrity verification to counter Lumma's DLL side-loading techniques. Establish cryptographic verification of all software components before execution, focusing on DLL search order vulnerabilities.

Implementation Strategy:

- Deploy application allowlisting with cryptographic hash verification at the kernel level
- Implement software bill of materials (SBOM) validation for all executed binaries
- Create monitoring specifically for unexpected DLL loading sequences in standard system applications

3.Resilient Credential Architecture

Technical Recommendation: Segment credential storage and implement hardware-backed keystores to neutralize Lumma's browser and wallet credential theft capabilities. Design authentication systems that remain secure even if endpoint browsers are compromised.

Implementation Strategy:

- Deploy hardware security keys for critical administrative access
- Implement temporary credential invalidation (< 1 hour lifetime) for high-value transactions
- Separate browser-based authentication from system-level authentication stores

4.Memory Protection Enforcement

Technical Recommendation: Deploy Kernel Data Protection (KDP) and Memory integrity features in modern operating systems to prevent Lumma's process hollowing techniques and direct memory manipulation.

Implementation Strategy:

- Enable Hardware-enforced Stack Protection on Windows 10/11 enterprise endpoints
- Configure Hypervisor-Protected Code Integrity (HVCI) to block Lumma's code injection attempts
- Deploy memory integrity monitoring with automated remediation for suspicious VirtualAllocEx and WriteProcessMemory sequences.

5. C2 Traffic Analysis & Disruption

Technical Recommendation: Implement specialized network monitoring for Lumma's distinctive C2 protocol patterns and TLS inspection capabilities capable of identifying domain fronting techniques.

Implementation Strategy:

- Deploy traffic shape analysis to detect Lumma's beaconing patterns even through encrypted channels
- Create detection rules for Lumma's specific C2 protocol formats:

// Version 5 pattern
act=receive_message&ver=4.0&lid=[<value>]&j=[<value>]
// Version 6 pattern
uid=<value>&cid=[<value>]&hwid=<value>

- Implement DNS filtering that blocks newly registered domains and monitors connections to Steam profiles and Telegram channels used as C2 fallbacks

6.Process Execution Control

Technical Recommendation: Implement strict application control policies to prevent Lumma's execution techniques, particularly focusing on LOLBin abuse and script-based execution chains.

Implementation Strategy:

- Restrict PowerShell execution using Constrained Language Mode and block encoded commands
- Disable mshta.exe and other commonly abused LOLBins through Software Restriction Policies
- Implement code signing requirements for all script execution

7. Mandatory Security Architecture Review

Technical Recommendation: Implement formal security architecture reviews focused on credential storage, authentication mechanisms, and permission models to counter Lumma's credential harvesting capabilities.

Implementation Strategy:

- Require security architecture reviews focusing on browser credential storage designs
- Mandate formal threat modeling for authentication systems
- Implement zero standing privilege models for administrative access

Reference

Cybereason Analysis Report
https://www.cybereason.com/blog/threat-analysis-lummastealer-2.0

Microsoft Security Blog (2025)
https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

CyberScoop Report
https://cyberscoop.com/lumma-stealer-infostealer-takedown/

CYFIRMA Research Report
https://www.cyfirma.com/research/lumma-stealer-tactics-impact-and-defense-strategies/

Darktrace Blog
https://www.darktrace.com/blog/the-rise-of-the-lumma-info-stealer

Fortinet Threat Research
https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

MITRE ATT&CK Framework
https://attack.mitre.org/

g0njxa Medium Interview
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-lummac2-94111d4b1e11

Microsoft Security Blog (2025)
https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/

Forcepoint Analysis Report
https://www.forcepoint.com/blog/x-labs/unmasking-lumma-stealer-campaign

Annexure

IOCs

Indicator	Type
klipderiq[.]shop	DOMAIN
check[.]qlkwr[.]com	DOMAIN
xian[.]klipderiq[.]shop	DOMAIN
simplerwebs[.]world	DOMAIN
affc[.]klipcewucyu[.]shop	DOMAIN
klipdiheqoe[.]shop	DOMAIN
kliphylj[.]shop	DOMAIN
extranet-captcha[.]com	DOMAIN/IP
77.105.164[.]117	DOMAIN/IP
Ef85ba125184cbb92b3abf780fa9dbf0a1f1d4d0	HASH
172[.]67[.]144[.]135	IP
104[.]21[.]224	IP
172[.]67[.]144[.]135	IP
104[.]21[.]64[.]1	IP

sos-at-vie-1.exo[.]io	DOMAIN
pawpaws.readit-carfanatics[.]com	DOMAIN
anita2[.]snuggleam[.]org	DOMAIN
buck2nd[.]oss-eu-central-1[.]aliyuncs[.]com	DOMAIN
sakura[.]holistic-haven[.]shop	DOMAIN
pub-e62cce9a08224552b513d24397cb4413[.]r2[.]dev	DOMAIN
heavens[.]holistic-haven[.]shop	DOMAIN
hookylucnh[.]click	DOMAIN/IP
104.21.35[.]211	DOMAIN/IP
30b18eb4082b8842fea862c2860255edafc838ab	HASH
f2ec439b1f1b8d7dcc38d979bcf6ad64fe437122	HASH
0551cdbf681c7ce31754247291dc550df0807cee	HASH
decd01a95a05f557720e62ada86fa929f4687e88	HASH
279ec364b8bc3244335c47ed2586d387e448ac7b	HASH
79d7a6e7441d478fc81638e6ed458e898e0ebf2b	HASH
88958d7c9749b7d085ee28d9fa50151a505eba09	HASH
b9ff81cc8ad9e4d30df66fe520d1a0f5231902a6	HASH
a2840e3927351244f253d54389a66342a4f6be33	HASH
60e30eaeedc7abb079fd7e6d2d8f486de5a9af38	HASH
d896764e7ce9e8685ce4e11aa49d556f8a23a547	HASH

klipbyxycaa[.]shop	DOMAIN
goatstuff[.]sbs	DOMAIN
awagama2[.]org	DOMAIN
176[.]113.115[.]170	DOMAIN
t1.awagama2[.]org	DOMAIN
awagama[.]org	DOMAIN
savecoupons[.]store	DOMAIN
klipbazyxui[.]shop	DOMAIN
topofsuper[.]store	DOMAIN
onceletthemcheck[.]com	DOMAIN
dma.sportstalk-musiclover[.]com	DOMAIN
scrutinycheck[.]cash	DOMAIN
atsuka.thrivezest[.]org	DOMAIN
solve.fizq[.]net	DOMAIN
deduhko2.klipzyroloo[.]shop	DOMAIN/IP
172.67.144[.]15	DOMAIN/IP
solve.gevaq[.]com	DOMAIN/IP
104.21.16[.]142	DOMAIN/IP
b133d42502750817aa8e88119ff36158d2f8ecee	HASH
104[.]21.16[.]1	IP