A Quick Look at:

LummaC2/Lumma Stealer

Document Control

Version Number	Date	Change Summary
0.1	11 Feb 2024	Initial draft.

Table of Contents

What is LummaC2/Lumma Stealer?

The Lumma stealer gets its name from the threat actor “Shamel” – who originally offered the stealer for sale on various different underground markets, “Shamel” used the alias “Lumma” in making the posts. “Shamel” is also responsible for the 7.62mm Stealer [1]. The stealer first emerged in 2022, appearing in tweets from August/September 2022.

Lumma primarily targets cryptocurrency wallets, browser extensions and two factor authentication. Lumma is able to pull information from compromised targets including: system data, installed program data, cookies, usernames, passwords, credit card numbers, connection history, cryptocurrency wallet data [2].

Lumma is priced from $250 (The “Experienced” edition) up to $1000 (the “Corporate” edition). The source code for Lumma was also available to purchase for a time for $20000 [2]. Payments are processed via Coinbase using a wide range of cryptocurrency options [3].

Distribution of Lumma

Lumma has typically been distributed under the guise of cracked/fake popular software. This has been seen in the form of a fake crack for Nitro Pro, other variants include claiming to be popular software like VLC or Sony VEGAS Pro, or even as a fake browser update [4]. However, as recently as Jan 2024, Lumma has been seen distributed via malicious URLs on YouTube videos, the videos offer free software to users and encourage them to download a malicious zip file [5].

Lumma has also seen distribution via Discord. A user will receive a message from someone, asking them to test out their new game and offering to pay for their time. Upon accessing the link sent, the Lumma download is triggered multiple times, and if executed, it will talk back to its C2 server and attempt to exfiltrate sensitive information from the machine [6].

Lumma has also been seen targeting YouTubers in spear-phishing campaigns [7]. The download links to the software are typically for well known, trusted file hosting services like SharePoint/OneDrive, Mediafire and DropBox.

Execution of Lumma

Once the stealer has acquired a foothold on a victim machine via direct execution, the malware reaches out to a command and control server to transfer pilfered data. The stealer itself is heavily obfuscated, using many techniques including Control Flow Flattening to make it very hard to determine exactly what is going on.

When a connection is established, Lumma sends a POST request to its C2 server with a hardcode user agent and a parameter “act=life” to check in. Next, another POST request is sent with the Lumma ID and parameter “act=receive-message”, which will then upload a compressed version of any stolen data to the C2 server at URI “/api.” [8] Lumma is still being actively developed and updated to better evade anti-virus detections.

Stealer Sample 1

Stealer sample acquired from:
https[://]bazaar[.]abuse[.]ch/sample/
19fefb958bd9c9280d07754ab903022a3dc9fc380a6964733a1dcc016aba8150/

Stealer SHA-256: 19fefb958bd9c9280d07754ab903022a3dc9fc380a6964733a1dcc016aba8150

Integrity Checking

Once extracted, the sample is confirmed to be a Windows PE32 Executable with command: file [filename]. The integrity is confirmed by running sha256sum [filename] where the output returns: 19fefb958bd9c9280d07754ab903022a3dc9fc380a6964733a1dcc016aba8150.

Threat Actors, Associated Accounts and Other Intel

Telegram

Display Name	Link	Description	State
@LummaC2Link Figure 1 Figure 2	hxxps[://]t[.]me/s/LummaC2Link	Channel with master list of Lumma telegram contacts.	ONLINE
@LummaC2Stealer Figure 3 Figure 4	hxxps[://]t[.]me/LummaC2Stealer	Main channel for Lumma stealer, posts updates.	ONLINE
@LummaC2Team Figure 5	hxxps[://]t[.]me/LummaC2Team	Main public channel for the Lumma C2 Team, no preview available.	ONLINE
@lummaseller126 Figure 6	hxxps[://]t[.]me/lummaseller126	Main account for the primary(?) verified seller of Lumma.	ONLINE
Lumma C2 – reviews Figure 7	hxxps[://]t[.]me/+zq0CE4r--ZEyM2Fi	Channel to post reviews for Lumma.	ONLINE
@lummanowork Figure 8	hxxps[://]t[.]me/lummanowork	Bug reporting user account for Lumma.	ONLINE
@LummaC2Blacklist Figure 9 Figure 10	hxxps[://]t[.]me/LummaC2Blacklist	Blacklist of scammers/false sellers of Lumma.	ONLINE

Documentation

Document	Link	Description	Stable [Safe] Link
About Lumma Document (ENG)	hxxps[://]telegra[.]ph/LummaC2---universal-stealer-a-malware-for-professionals-07-27	Document written by the creators outlining the current capabilities of Lumma.	https://github.com/contrxl/malware/blob/main/Lumma_Documents/Lumma_About_ENG.md
About Lumma Document (RU)	hxxps[://]telegra[.]ph/LummaC2---unikalnyj-stiller-instrument-dlya-professionalov-07-05	Document written by the creators outlining the current capabilities of Lumma.	https://github.com/contrxl/malware/blob/main/Lumma_Documents/Lumma_About_RU.md

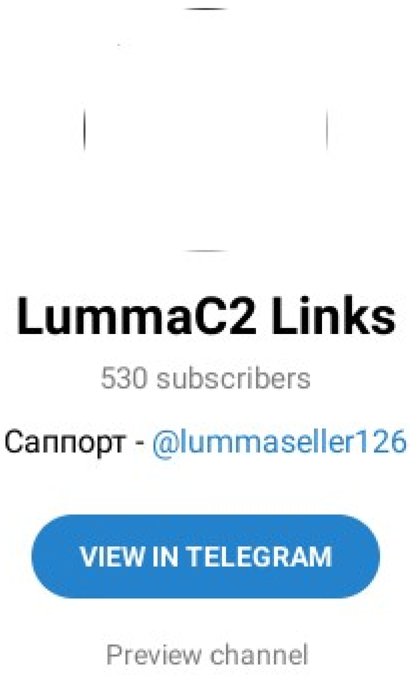
Indicators of Compromise

IP Addresses

82[.]117[.]255[.]80

Files

Appendices

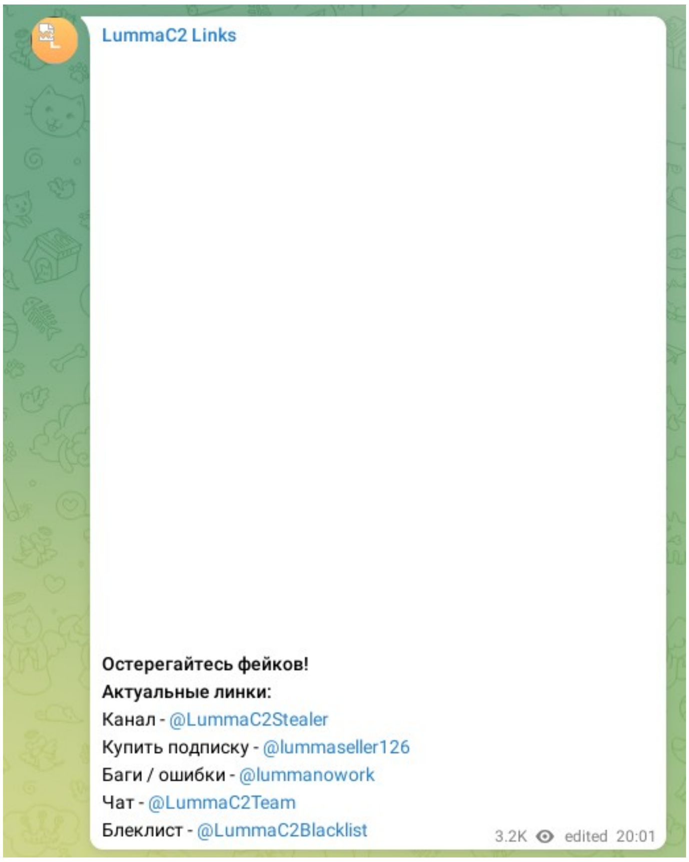


LummaC2 Links

530 subscribers

Саппорт - @lummaseller126

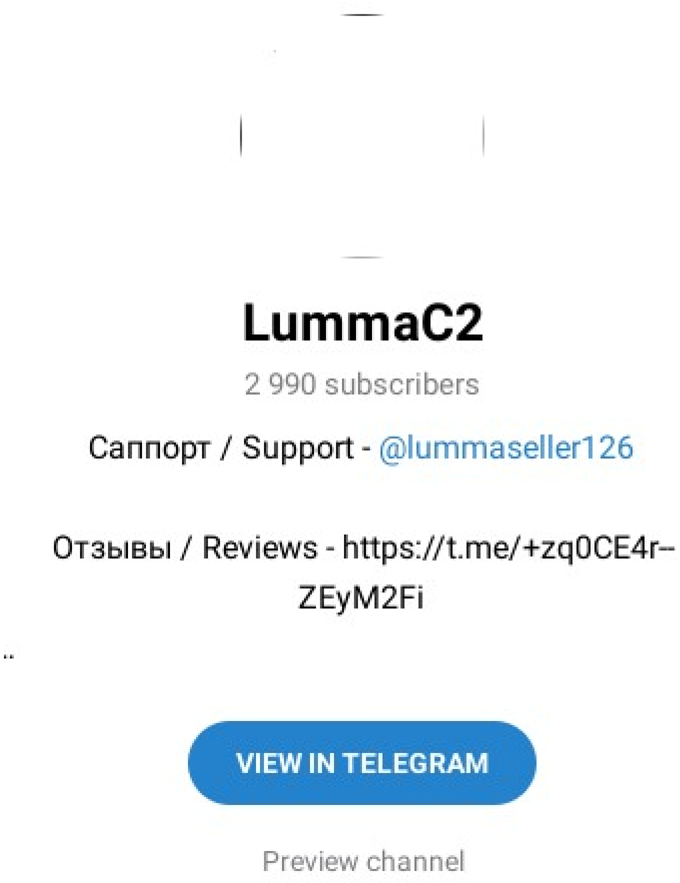
Figure 1: Lumma links Telegram channel.



LummaC2 Links

Остерегайтесь фейков!
Актуальные линки:
Канал - @LummaC2Stealer
Купить подписку - @lummaseller126
Баги / ошибки - @lummanowork
Чат - @LummaC2Team
Блеклист - @LummaC2Blacklist

Figure 2: Inside Lumma links Telegram channel.



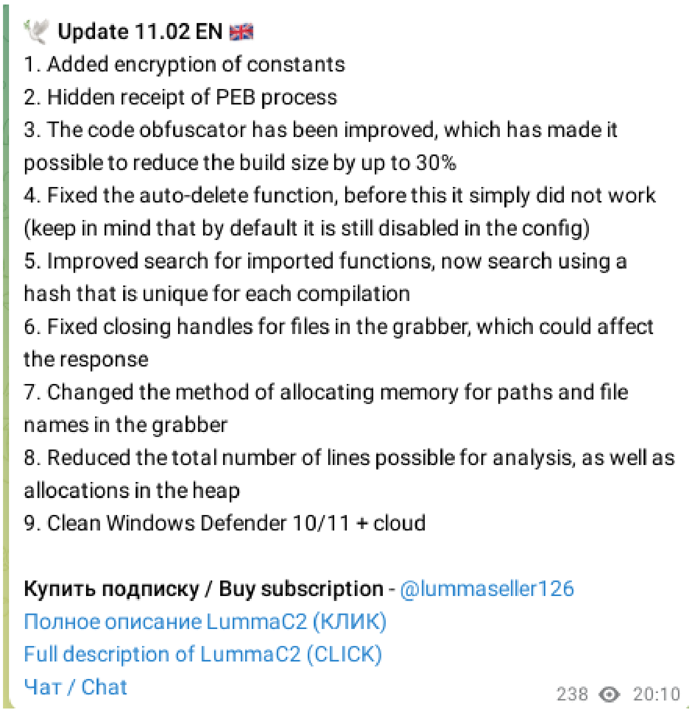
LummaC2

2 990 subscribers

Саппорт / Support - @lummaseller126

Отзывы / Reviews - https://t.me/+zq0CE4r--ZEyM2Fi

Figure 3: Lumma Stealer Telegram channel.

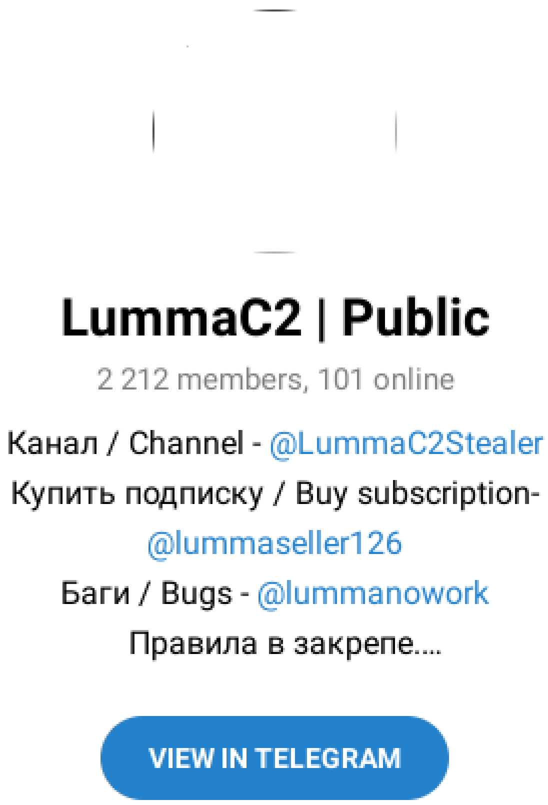


Update 11.02 EN 🇬🇧

1. Added encryption of constants
2. Hidden receipt of PEB process
3. The code obfuscator has been improved, which has made it possible to reduce the build size by up to 30%
4. Fixed the auto-delete function, before this it simply did not work (keep in mind that by default it is still disabled in the config)
5. Improved search for imported functions, now search using a hash that is unique for each compilation
6. Fixed closing handles for files in the grabber, which could affect the response
7. Changed the method of allocating memory for paths and file names in the grabber
8. Reduced the total number of lines possible for analysis, as well as allocations in the heap
9. Clean Windows Defender 10/11 + cloud

Купить подписку / Buy subscription - @lummaseller126
Полное описание LummaC2 (КЛИК)
Full description of LummaC2 (CLICK)
Чат / Chat

Figure 4: Most recent update notes from Luma stealer Telegram channel.

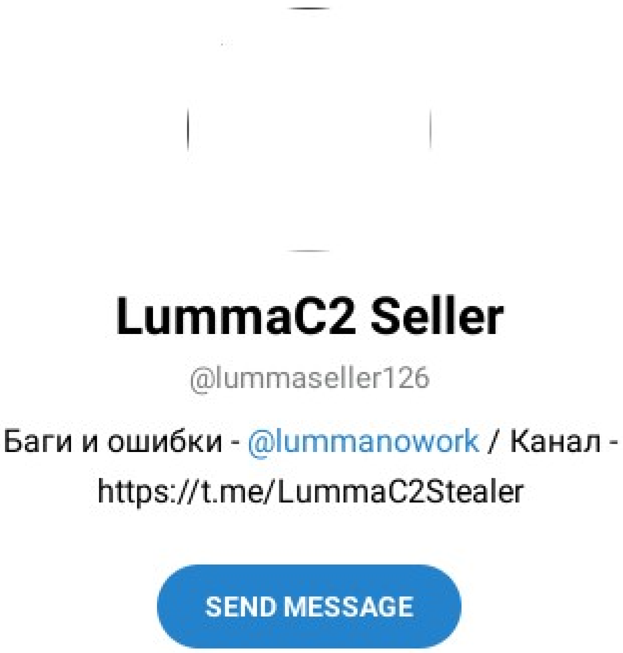


LummaC2 | Public

2 212 members, 101 online

Канал / Channel - @LummaC2Stealer
Купить подписку / Buy subscription-
@lummaseller126
Баги / Bugs - @lummanowork
Правила в закрепе....

Figure 5: Lumma C2 Team Telegram channel.

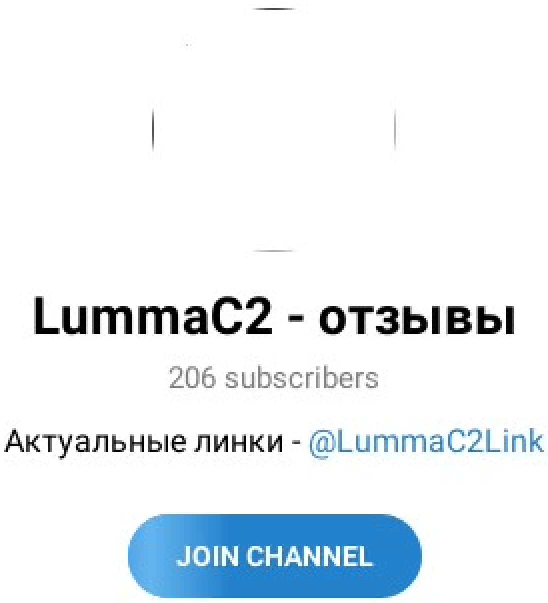


LummaC2 Seller

@lummaseller126

Баги и ошибки - @lummanowork / Канал -
https://t.me/LummaC2Stealer

Figure 6: Lumma seller Telegram channel.

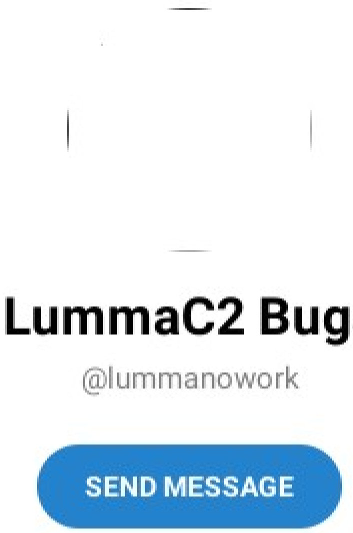


LummaC2 - отзывы

206 subscribers

Актуальные линки - @LummaC2Link

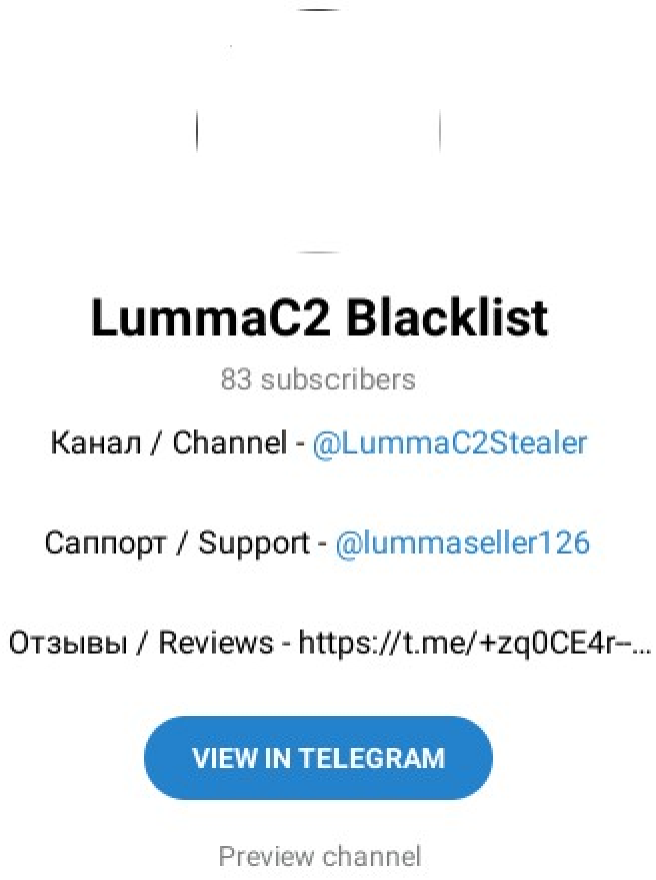
Figure 7: Lumma reviews Telegram channel.



LummaC2 Bugs

@lummanowork

Figure 8: Lumma bug reporting Telegram user.



LummaC2 Blacklist

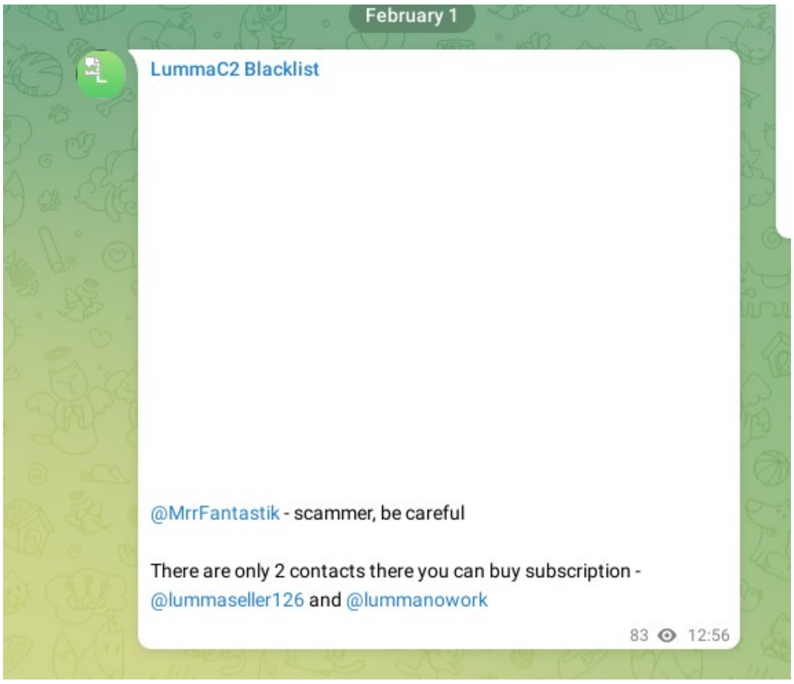
83 subscribers

Канал / Channel - @LummaC2Stealer

Саппорт / Support - @lummaseller126

Отзывы / Reviews - https://t.me/+zq0CE4r-...

Figure 9: Lumma blacklist Telegram channel.



@MrrFantastik - scammer, be careful

There are only 2 contacts there you can buy subscription - @lummaseller126 and @lummanowork

Figure 10: Inside Lumma blacklist telegram channel.

Bibliography

1: KELA Cyber Intelligence Centre, The Next Generation of Info Stealers, 2022
2: Emily Megan Lim, The Rise of the Lumma Info-Stealer, 2023
3: Alberto Marin, Everything you need to know about the LummaC2 stealer: leveraging IDA Python and Unicorn to deobfuscate Windows API hashing, 2023
4: eSentire Threat Response Unit, Fake Browser Updates Distribute LummaC Stealer, Amadey and PrivateLoader Malware , 2023
5: Cyware Alerts - Hacker News, Researchers Disclose New Lumma Stealer Campaign Distributed via YouTube., 2024
6: Carl Malipot, Beware: Lumma Stealer Distributed via Discord CDN, 2023
7: Jiho Kim, Sebin Lee, Lumma Stealer targets YouTubers via Spear-phishing Email, 2023
8: Cara Lin, Deceptive Cracked Software Spreads Lumma Variant on YouTube, 2024

Table of Figures