Lumma Stealer targets YouTubers via Spear-phishing Email

By S2W

Published: 2023-02-27 · Archived: 2026-04-05 22:53:56 UTC

8 min read

Feb 27, 2023

Author: Jiho Kim & Sebin Lee | S2W TALON

> ***Last Modified*** *: Feb 27, 2023*

Press enter or click to view image in full size

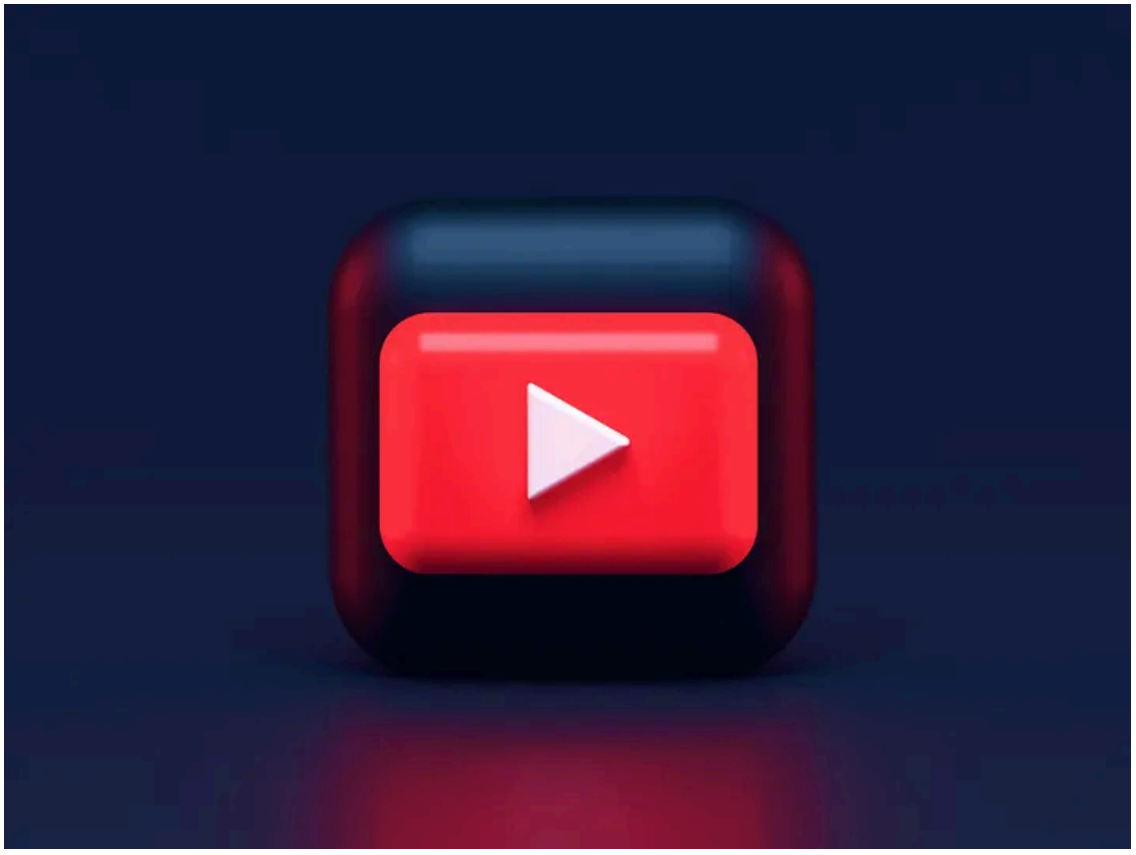

Photo by Alexander Shatov on Unsplash

Executive Summary

- Lumma Stealer is an info stealer malware written in C language and has been sold on underground forums since August 2022.

- The seller of Lumma Stealer has been actively promoting it since at least April 2022.
- The seller posts the announcement about version updates, inquiries, etc. on the underground forum, telegram channel, and his own site.
- On February 6th, 2023, a spear-phishing email **impersonating a Bandai Namco** game company was used to target **a voice actor YouTuber in Korea**, and Lumma Stealer malware was distributed through the email.
- A normal video file and a malicious PDF document were downloaded from a Dropbox link in the email, and the PDF file installed an additional malware called **Pure Crypter**.
- Pure Crypter, a loader that drops and executes additional malware, injects the Lumma Stealer payload based on the configuration value.
- Once installed, Lumma Stealer steals information from browsers, cryptocurrency wallets, and 2FA extensions on the infected system and sends them to a C&C server.

Introduction

Lumma Stealer sellers use the name “LummaC” on an underground forum called XSS, which is based in Russia. The seller has been actively promoting the malware since April 2022. In August of that year, the seller posted a new promotional article under the name LummaC Stealer. Then, the seller continuously updates the malware, including changing its name to LummaC2 Stealer, as seen in a post title from December 2022.

Press enter or click to view image in full size

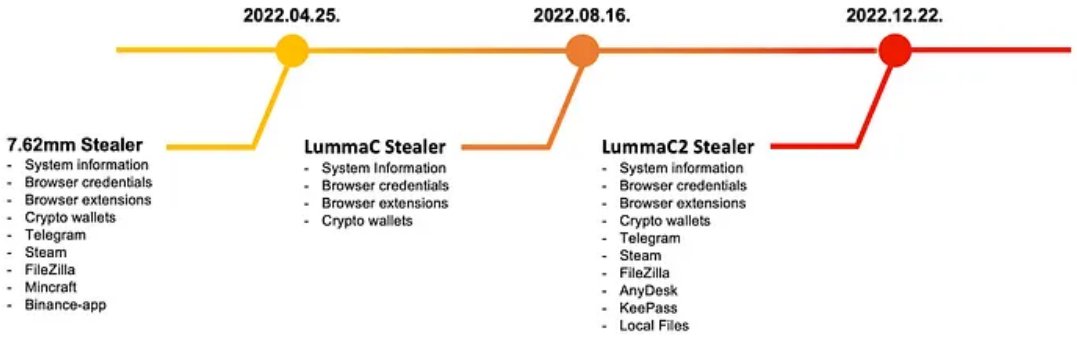

Figure 1. Activity history of LummaC users

Press enter or click to view image in full size

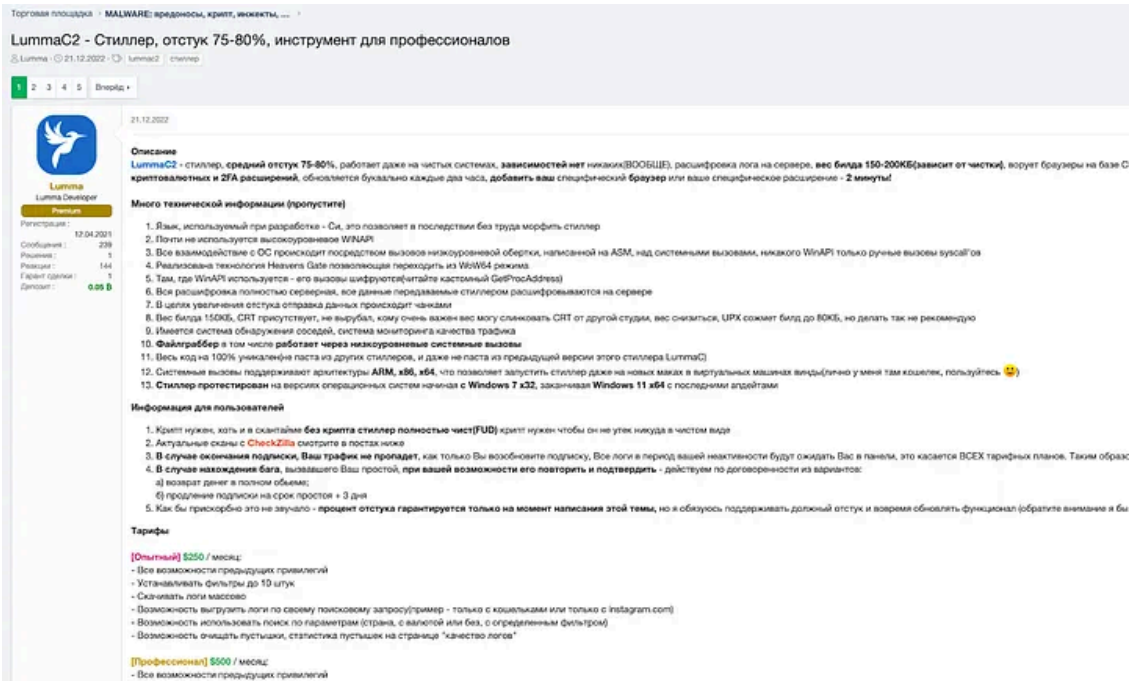

Figure 2. LummaC2 Stealer promotional post

Seller Information

Not only the underground forum, but the seller also uses Telegram to notify users of updates to the malware and to respond to inquiries. The seller also operates a separate website for selling the malware. The Telegram channels operated by the seller are divided into different categories, such as providing updated information, offering support, and allowing users to report bugs.

- @LummaC2Stealer: Channel for updated information
- @lummaseller126: Channel for offering support
- @Lummanowork: Channel for reporting bugs

Press enter or click to view image in full size

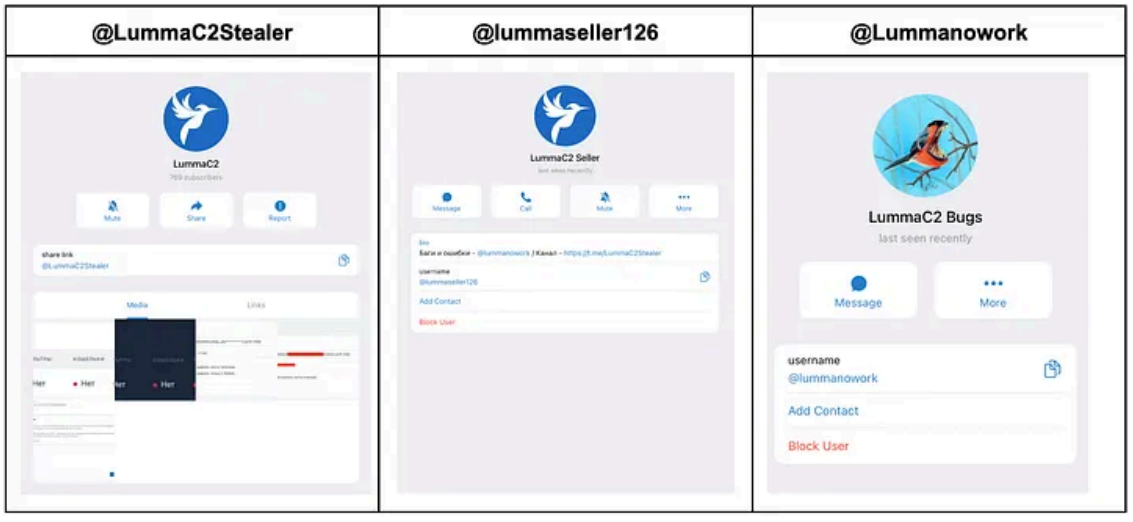

Table 1. Terelgram channels operated by Lumma Stealer sellers

Price Policy

The seller has created their own website to sell the malware and has set different functions and pricing policies depending on the type of level. According to a promotional post on the underground forum, the seller also offers the ability to install a control panel on the server when using the corporate level of the service.

Press enter or click to view image in full size

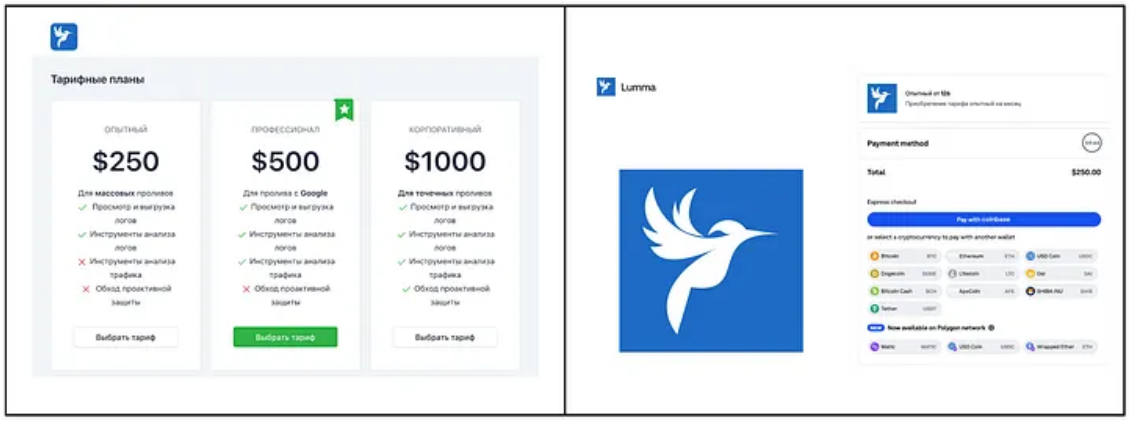

Figure 3. Pricing policies and supported cryptocurrency for trading

Payment for the Lumma Stealer is made through Coinbase, and a unique coin address is generated and provided for each payment.

Press enter or click to view image in full size

	Experienced	Professional	Corporate
Price (Month)	$250	$500	$1000
View Upload Log	O	O	O
Log Analysis Tool	O	O	O
Traffic Analysis Tool	X	O	O
Proactive Defense Bypass	X	X	O
Payment	Bitcoin, Ethereum, USD Coin, Dogecoin, Litecoin, Dai, Bitcoin Cash, ApeCoin, SHIBA INU, Tether		

Table 2. Features by pricing policy

Targeted a voice actor YouTuber in South Korea

On February 6, 2023, a voice actor YouTuber in Korea received an e-mail impersonating a Bandai Namco game company. The e-mail embedded a Dropbox link downloading malware, then the YouTuber downloaded the malware and executed it. Later, his YouTube channel was compromised and changed to a **Tesla US** channel.

Fortunately, the YouTuber was able to regain access to his compromised account and posted a video explaining how the attack had taken place. Thanks to the information provided by him, we were able to obtain the original

spear-phishing email and malware from VirusTotal. We would like to express our gratitude to him for their bravery in sharing the details of the attack and helping to uncover the truth.

Based on our analysis, we have identified the following attack flow:

1. The attacker sends a spear-phishing email targeting the YouTuber.
2. Downloads a ZIP file containing malware via the Dropbox link in the spear-phishing email.
3. Executes the malware, which is disguised as a PDF document inside the ZIP file.
4. The malware downloads additional malware from the command and control (C&C) server.
5. The malware loads the additional malware, Pure Crypter.
6. The Pure Crypter injects the Lumma Stealer into the process.
7. The Lumma Stealer steals information from the victim's system and sends it to the C&C server.

Press enter or click to view image in full size

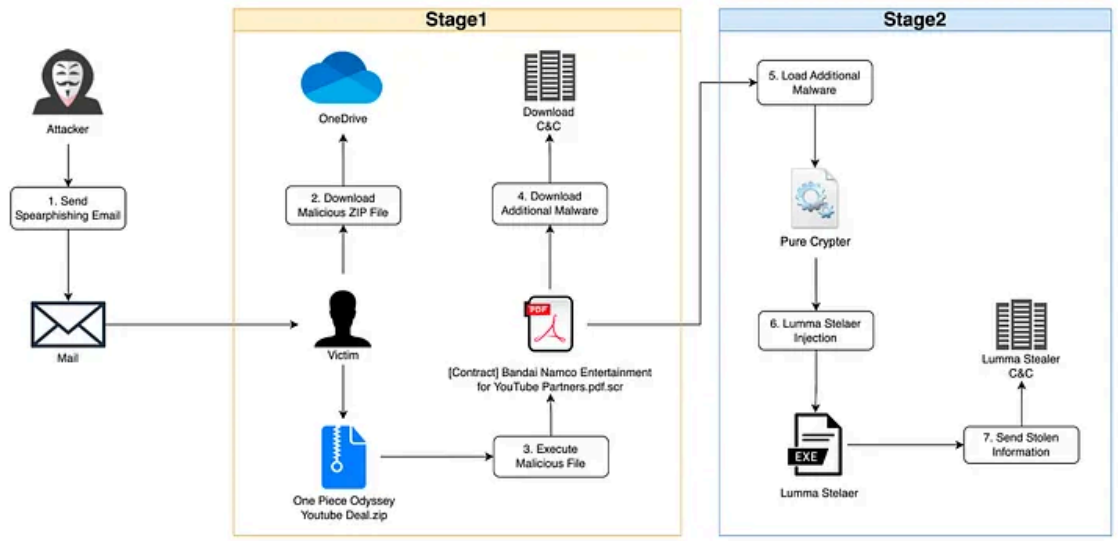

Figure 4. Lumma Stealer infection and execution flow

It has been confirmed that the victim's YouTube account, which was infected with Lumma Stealer, was hacked and the channel name was changed to "Tesla US".

Press enter or click to view image in full size

Figure 5. Victim’s YouTube channel changed to the Tesla advertising account

> The channel name and thumbnail changed, but the previously uploaded channel notices not changed.

Distributed via Spear-phishing

The e-mail used the “bandai.namco.ma[@]kakao.com” account to impersonate Bandai Namco game company. The email requested the victim’s cooperation in promoting a new game and urged them to download and execute the file via the Dropbox link included in the email.

- Title : Re: Bandai Namco YT Offer 2023
- Sender : bandai.namco.ma[@]kakao.com

Although Bandai Namco is a Japanese company, the email was sent through the account from kakao.com, one of the most used mail domains in Korea. As the targeted YouTuber is also Korean, we assess with low-confidence that there is a possibility that the attacker is also Korean.

Press enter or click to view image in full size

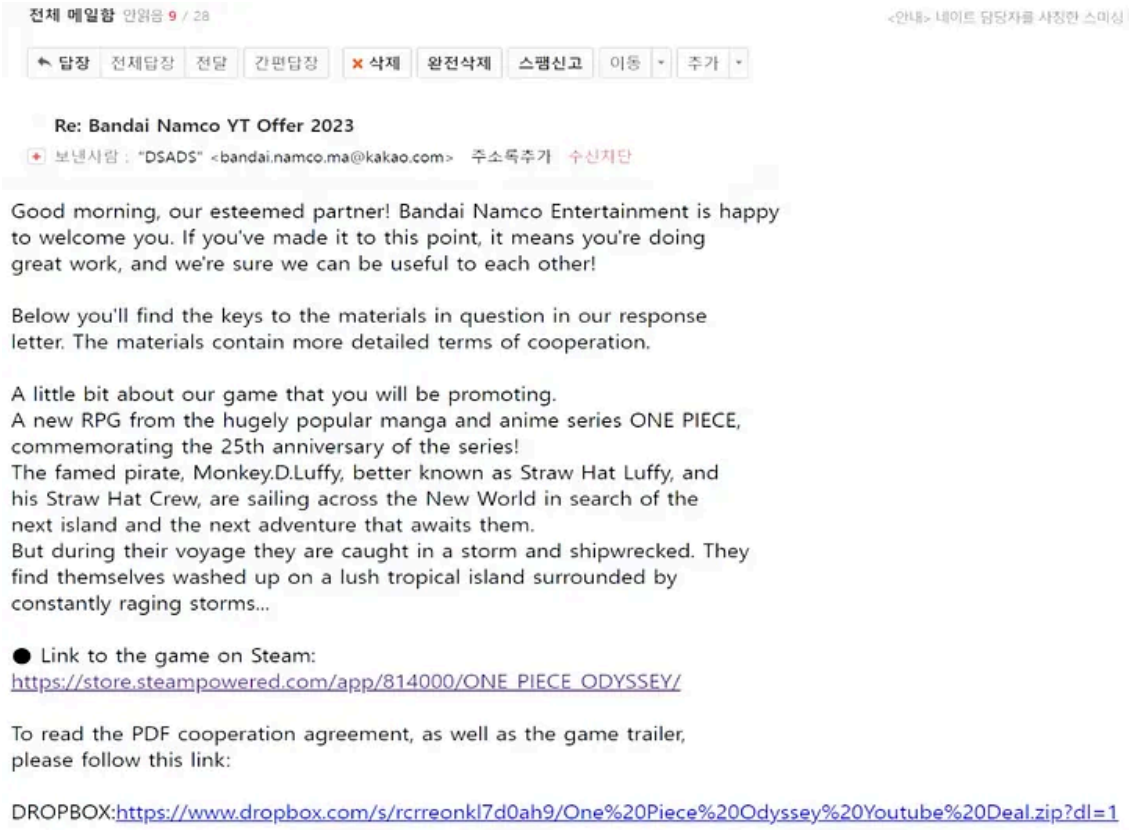

Figure 6. A phishing email masquerading as a game company (Source: Victim's YouTube channel)

The file downloaded through the Dropbox link contained a normal video file and a malicious file disguising a PDF document. Once executed, additional malware is downloaded from the C&C server, and Lumma Stealer is finally installed.

- Downloaded filename from Dropbox: One Piece Odyssey Youtube Deal.zip
- Dropbox Link: hxxps[:]//www.dropbox[.]com/s/rcrreonkI7d0ah9/One%20Piece%20Odyssey%20Youtube%20Deal.zip?dl=1

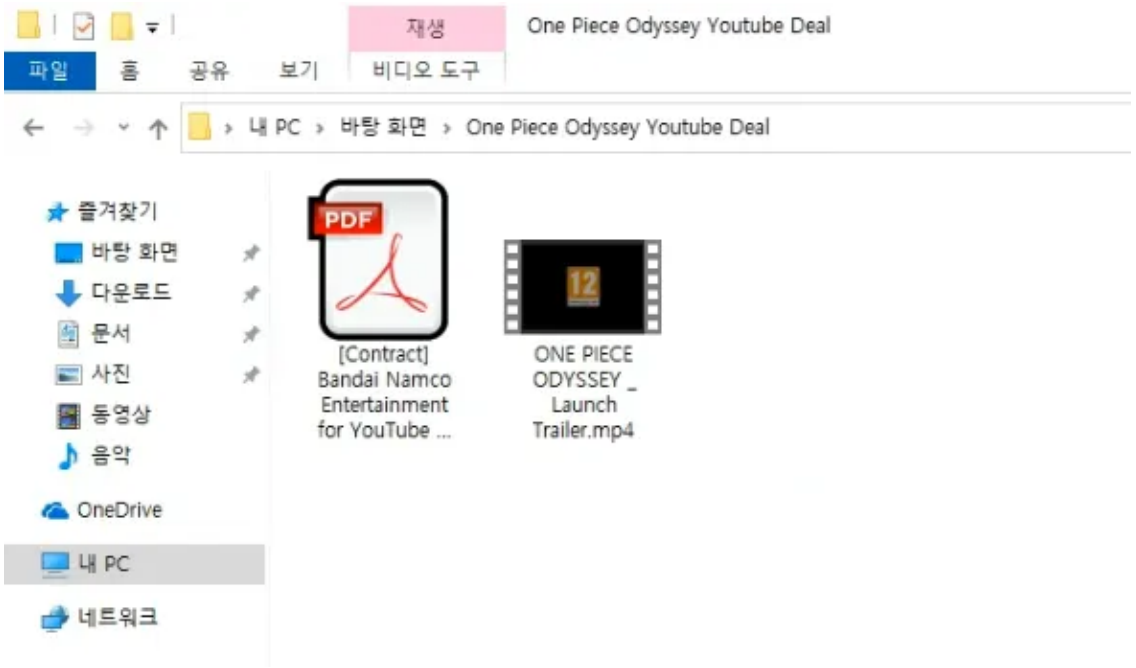

Figure 7. Malicious attachments in the phishing email

Pure Crypter

Upon analyzing the downloaded from the C&C server, it was identified as a Pure Crypter. Pure Crpyter is a tool written in C# and developed by an individual known as “PureCoder,” which is available for sale on underground forums in the form of software as a service (SaaS). This tool includes features designed to bypass security products, including obfuscation and process injection, and is commonly used to drop additional malware.

Press enter or click to view image in full size

Pure Crypter Function		
Shared STUB C#	.NET and Native Support	Inject 32Bit & 64Bit
Command Line	Various Output Extensions	Time-Stamp
Exclusion Region	Hardened Name	Crypters Killer
Memory Bombing	Anti File Delete	Anti Sample Submission
Discord and Telegram Execution Notification	Icon, Assembly and Certificate Cloner	Advanced Injection
Fake Message Box	Three Startup Technique	Binder
Delay	Scanner Run time and Scan Time	Fake App Builder
Macro Excel Builder	Downloader Builder	CLI and GUI

Table 3. Features provided by Pure Crypter

Press enter or click to view image in full size

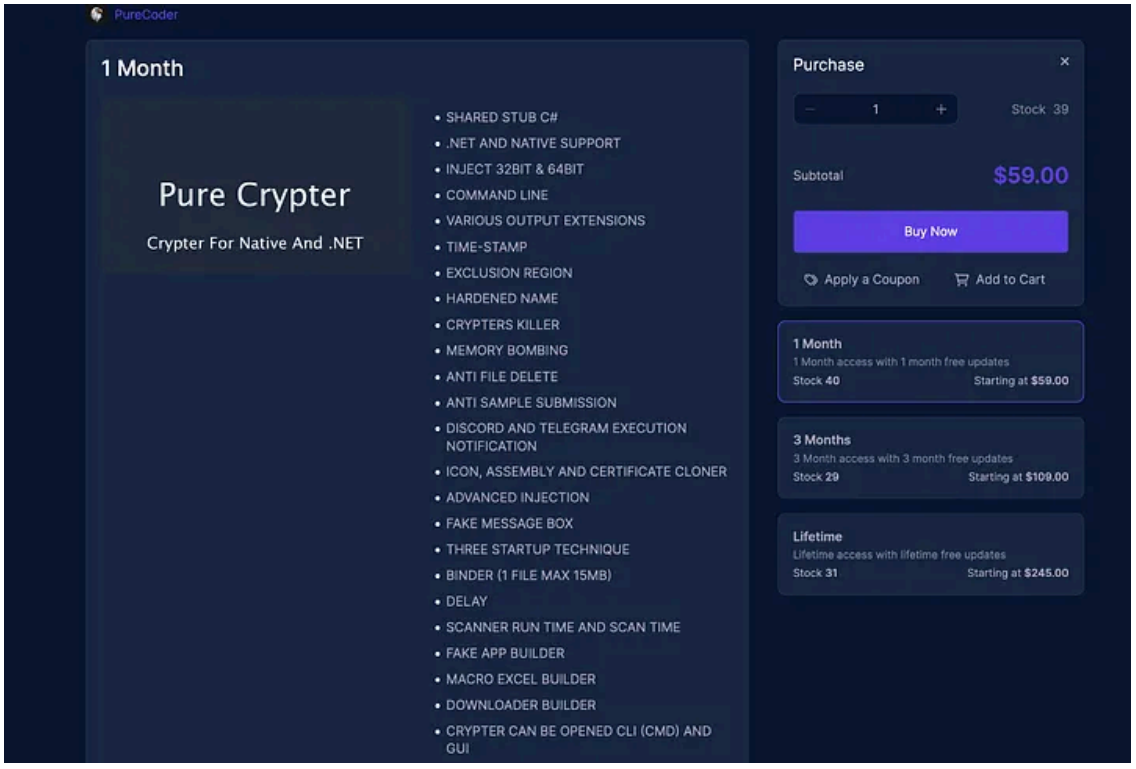

Figure 8. Pure Crypter sales site

The Pure Crypter reads the separate data included within and then decrypts it to obtain configuration values for performing malicious actions set as desired.

Press enter or click to view image in full size

Config Field							
1	Delay	9	IsAnti	17	EnumInjection	25	MemoryBombingLevel
2	InjectionPath	10	IsFakeMessage	18	IsExclusionRegion	26	IsLogger
3	CommandLine	11	FakeMessageType	19	ExclusionRegionname	27	IsLoggerBuffer
4	IsMutex	12	FakeMessageText	20	IsHardenedName	28	LoggerSettings
5	MutexString	13	IsExclude	21	SaveFileName	29	OnlyLogger
6	BinderSettings	14	Notification	22	IsCrypterkiller	30	PatchANSI
7	StartupSettings	15	IsDelay	23	IsMemoryBombing	31	DisableInternet
8	IsMelt	16	Is64bit	24	IsAntiDelete	32	RunPowershell

Table 4. Fields in configuration

```
{"1":0,"2":"Itself","3":"","4":false,"5":"Vszbhncwjwcaklzwbvyio","6":{"1":false,"2":false,"3":null,"
```

After extracting the configuration values, an additional malware payload is read from the resource and decrypted. In this case, the Lumma Stealer malware is loaded and injected into a separate process for execution. If the file name specified in the injection-related configuration does not exist, Pure Crypter performs injection using the Process Hollowing technique in the current process.

Stolen Information via Lumma Stealer

The types of information that the finally executed Lumma Stealer steals are as follows.

Press enter or click to view image in full size

Collected Item		
System Information	Browser Credentials	Browser Extension Wallets
Crypto Wallets	Browser Extension 2FA/Authenticator	Telegram
Steam	FileZilla	AnyDesk
KeePass	Local Files	

Table 5. Target information that Lumma Staeler steals

- **Browser list**

Chrome, Chromium, Edge, Kometa, Vivaldi, Brave, Opera Stable, Opera GX Stable, Opera Neon, Firefox

- **Browser extension list**

[Crypto wallet] Metamask, TronLink, Ronnin Wallet, Binance Chain Wallet, Yoroi, Nifty, Math, Guarda, Coinbase, EQUAL, Jaxx Liberty, BitApp, Exodus Web3, Terust Wallet, iWlt, EnKrypt, Wombat, NEW CX, Cuild, Satrun, NeoLine, Clover, Liquality, Terra Station, Keplr, Sollet, Auro, Polymesh, ICOnex, Nabox, KHC, Temple, TezBox, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98, Cyano, Byone, OneKey

[**2FA**] Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager

[**Browser**] Leaf

- **Crypto wallet list**

Binance, Electrum, Ethereum, Exodus, Ledge Live, Atomic, Coinomi

The stolen information is transmitted to the C&C server via HTTP communication, with the HWID of the victim system, Packet ID, and an identification value set by the attacker appended to the end. To disguise the communication as browser traffic, the Tesla Browser is set as the User-Agent.

Press enter or click to view image in full size

Figure 9. Exfiltration traffic

The Admin Panel of Lumma Stealer is as follows. As explained in an advertisement in the forum, the panel has functions such as damage status by country, infection status, number of items stolen, and downloading log files.

Press enter or click to view image in full size

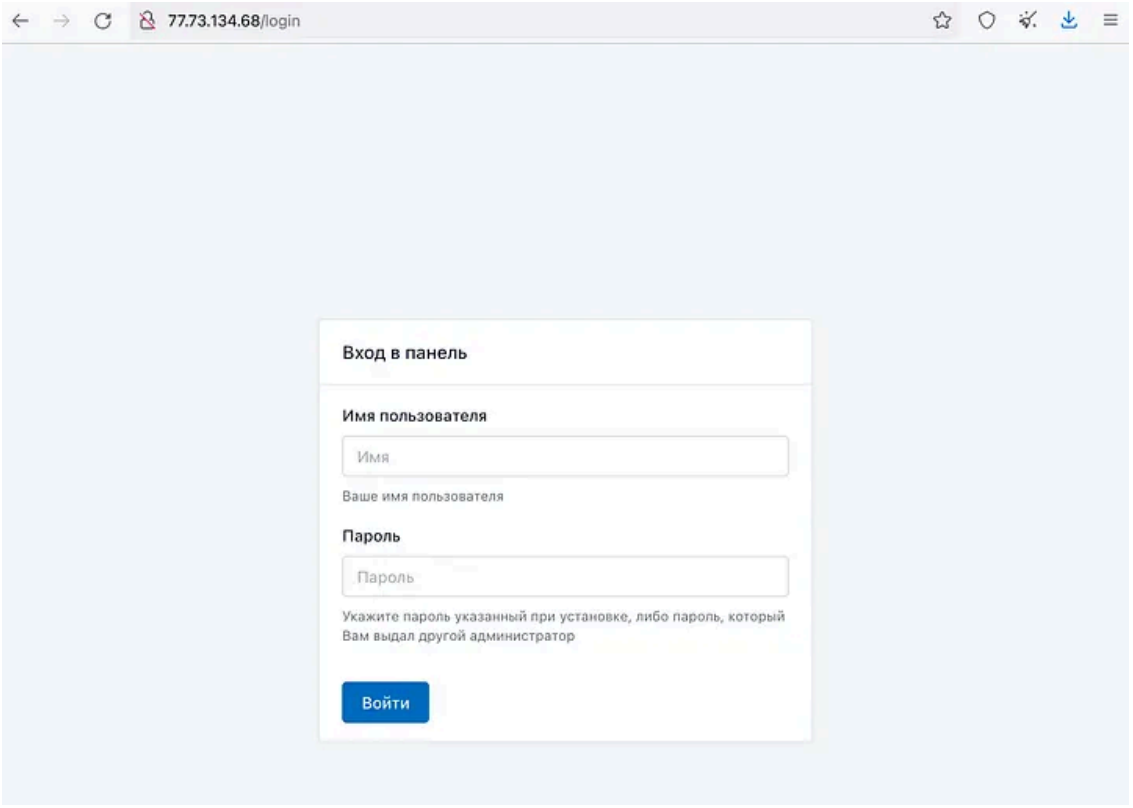

Figure 10. Lumma Stealer Admin Panel

Conclusion

- Lumma Stealer is a malware written in C language that steals user credentials from infected systems.
- The Lumma Stealer seller has been continuously updating since April 2022 and classifies telegram channels by purpose

- The Lumma Stealer has been distributed from phishing sites disguised as legitimate software and phishing emails, then the victim's Youtube channel changed to an advertisement for Tesla
- To prevent infection and minimize damage, users are advised to block automatic redirection and pop-ups, verify that the software download site is legitimate, and change passwords regularly.

Latest trends regarding Lumma Stealer

- On Feb 22, 2023, Lumma Stealer was distributed from a phishing site disguised as ChatGPT.
- On Feb 06, 2023, Lumma Stealer was distributed via a phishing email disguised as a game company.
- On Jan 31, 2023, Lumma Stealer was distributed from phishing sites disguised as VLC downloads.
- On Dec 22, 2022, a LummaC2 Stealer promotion was posted in the forum.
- On Aug 16, 2022, a LummaC Stealer promotion was posted in the forum.
- On Apr 25, 2022, a 7.62mm Stealer promotion was posted in the forum.

IoCs

```
17a9e53240082bd288d35b02986769a0
d18a31b0b3d20a86fc0647d7f47332d648499d52eee68d34857eec61f3b042ce
817ee46423164cf2502ae2accffecaa1
350edaca28b1572c31165431bafc7d1e0552c45f3186ffa039de33a58e55144e
efb9b1da0d5db39485c469cd5fe3aa1e
cdfecffbdda4075ee4eae8b44c3740b2450c64564d949a84a7f707d3d1a32449
5aac51312dfd99bf4e88be482f734c79
9b742a890aff9c7a2b54b620fe5e1fcfa553648695d79c892564de09b850c92b
9cd90bc5d586721862744403d80debfc
351366b6c0522c8d7454173844b7d2420b33ef245f5c7f6c8f72dd6e2c6a7571
11b6c32ffdb72904d0813e7df93cef79
1beadc5a862d28e69431756324b07aa61d8a077f60f81c72bc3ff324b415e3c6
2bc31e3b4d6623e6053b4b77a1bce062
c466284d938e9d9d40b785c346e142762f3069cc0f69bbfb81f6d5c59e720bb3
ec89c94613bf3208d975b9b3c758f81d
89fe11874357f3fbf17e938d91957f8c4a0291853dd7f5f10077b6144162ad04
c265357447e7e4910769b1817d6277cb
61a9884307317bbd93aad885dc646aebbcbeb840616e36f1be314af9bcce4284
16685b20847f33924fb8d849229c41f0
81b16b8e152322da3b81e7703e430c77d3f06e53b0ba24a5a82e0c3e371c9a21
254d7550e25a597539d67ffd01e3f1bd
e57cfd368ad71d81543c22d1e12ef620eca6677254556cc00375fda768f2487f
1e085b39d5dae93c6f5e6f4ef31e211e
0f40b111497b78b928a42f3c4f2e0c988be7ee5b3b0d523300685b75a2aadf06
24c3a967a34b6657e3f84bab979d5f67
72d6cd338baba81b7cef1bcd1ea4eed199adcce0ac57fe1e674527ad7258ea8d
c9c0e32e00d084653db0b37a239e9a34
d932ee10f02ea5bb60ed867d9687a906f1b8472f01fc5543b06f9ab22059b264
eb99b5d6ca92e932c02a8108a7512bf3
```

```
f33e6f4e62b30c7e4b74c5ec9710f8481853300e1da16056efc85c01475d8913
6908f7af68011665fbe453a628171101
0f86014f6c59f187274a7467a58b4fd4c7f8816bd8efa12af08eb0169333897f
53200921c95e7e4ce8c9959d06870416
f8e52c2fd7447d6eb87394f70c6f9d6c0290ffa16bd5833b390790a1521133bd
16685b20847f33924fb8d849229c41f0
81b16b8e152322da3b81e7703e430c77d3f06e53b0ba24a5a82e0c3e371c9a21
25110b76d4543e7dcd9b9737fb47005c
004f2b62840a91b011eaaafbcc429b374835b9274610f89c6a9ef6f9bfdde768
fc146adbe18d3cbdd7989a02b7bcc761
5aebbe7f3cee0b66e325844bfc4837a7dc36831c4b0d7201520b07530a2ad881
358e7b13098e126d884b121217d10fce
066fe4bb2fe09cad7df4e01f0eacc046faa304c9eb76812a636811acb44e936d
```

```
hxxp[:]//77[.]73[.]134[.]68/c2sock
hxxp[:]//45[.]9[.]74[.]78/c2sock
hxxp[:]//195[.]123[.]226[.]91/c2sock
hxxp[:]//144[.]76[.]173[.]247/c2sock
hxxp[:]//217[.]12[.]206[.]197/c2sock
hxxp[:]//195[.]123[.]226[.]167/c2sock
```

MITRE ATT&CK

Initial Access

- Drive-by Compromise (T1189)
- Spearphishing Link (T1566.002)

Execution

- User Execution (T1204)

Defense Evasion

- Deobfuscate/Decode Files or Information (T1140)

Credential Access

- Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
- Unsecured Credentials: Credentials In Files (T1552.001)

Discovery

- System Information Discovery (T1082)

Command and Control

- Application Layer Protocol (T1071)

Exfiltration

- Exfiltration Over C2 Channel (T1041)

Reference

- https://www.youtube.com/watch?v=LI9fwFEU8z0
