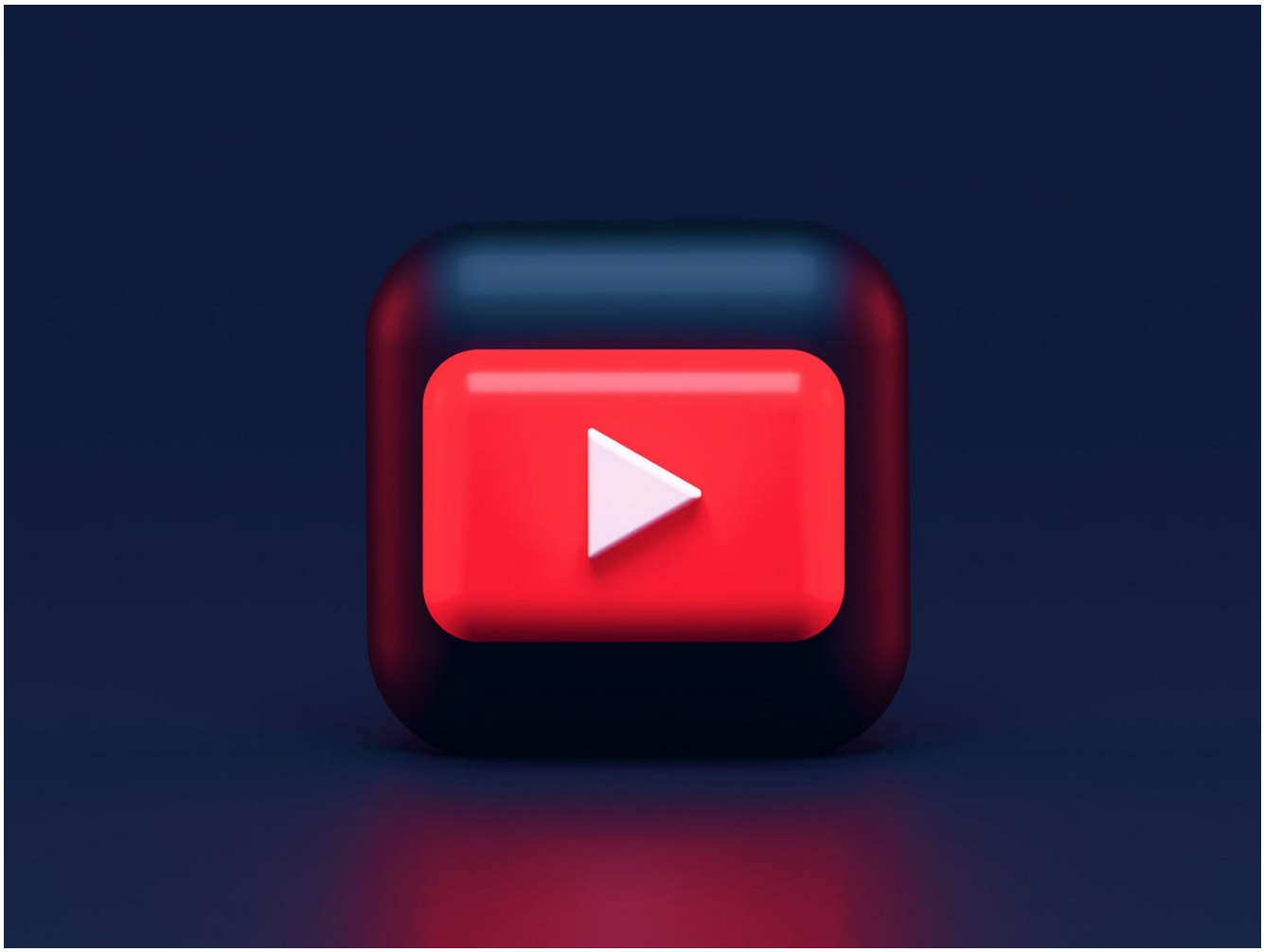
Lumma Stealer targets YouTubers via Spear-phishing Email

medium.com/s2wblog/lumma-stealer-targets-youtubers-via-spear-phishing-email-ade740d486f7

S2W February 27, 2023



S2W

Feb 27

.

8 min read

Author: Jiho Kim & Sebin Lee | S2W TALON

> *: Feb 27, 2023*

Photo by on

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 game company was used to target, 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, 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.

Figure 1. Activity history of LummaC users
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

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.

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.

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.

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".

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.

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.

Table 3. Features provided by Pure Crypter
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.

Table 4. Fields in configuration


```
{"1":0,"2":"Itself","3":"","4":false,"5":"Vszbhncwjwcaklzwbvyio","6":
{"1":false,"2":false,"3":null,"4":null,"5":false},"7":
{"1":false,"2":0,"3":0,"4":null},"8":false,"9":false,"10":false,"11":0,"12":null,"13":false,"14":
2022.4.en-
US.win64.installer.exe","22":false,"23":false,"24":false,"25":0,"26":false,"27":null,"28":null,"2
```


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.

Table 5. Target information that Lumma Staeler steals

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

[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

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.

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.

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 .
- 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

```
17a9e53240082bd288d35b02986769a0d18a31b0b3d20a86fc0647d7f47332d648499d52eee68d34857eec61f3b042ce8

hxxp[:]//77[.]73[.]134[.]68/c2sockhxxp[:]//45[.]9[.]74[.]78/c2sockhxxp[:]//195[.]123[.]226[.]91/c
```

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