

# What is Lumma Stealer?

---

 [gridinsoft.com/spyware/lumma-stealer](https://gridinsoft.com/spyware/lumma-stealer)

Using this site

Please ensure you understand and agree with our data protection policy before using this site. [Review Policy](#).



## Lumma Stealer

---

February 13, 2024

*Newcomers are sometimes treated with disrespect – that’s a rather natural behaviour. It is also natural to be overwhelmed by this newcomer, who turns out to be a rather potent and snappy malware. That is exactly what’s happened with Lumma Stealer.*

Lumma Stealer is an infostealer malware that emerged in early 2023, though some sources say about its first samples detected in the wild in late 2022. For functionality, it is a **classic information and crypto stealer that targets a selection of data sources** across the infected system. Written in C++, it incorporates heavy obfuscation and anti-analysis features, which, in fact, makes this malware so potent and successful.

**Its way towards the top of the charts was rapid.** A couple of months after the launch, Darknet forums were offering Lumma’s logs for sale at the same volume as the renowned leaders of the time – [Vidar](#) and [Raccoon](#). Such a rapid success is generally caused by the tricks this malware uses to avoid detection, as well as the flexible spreading approaches chosen by its masters.

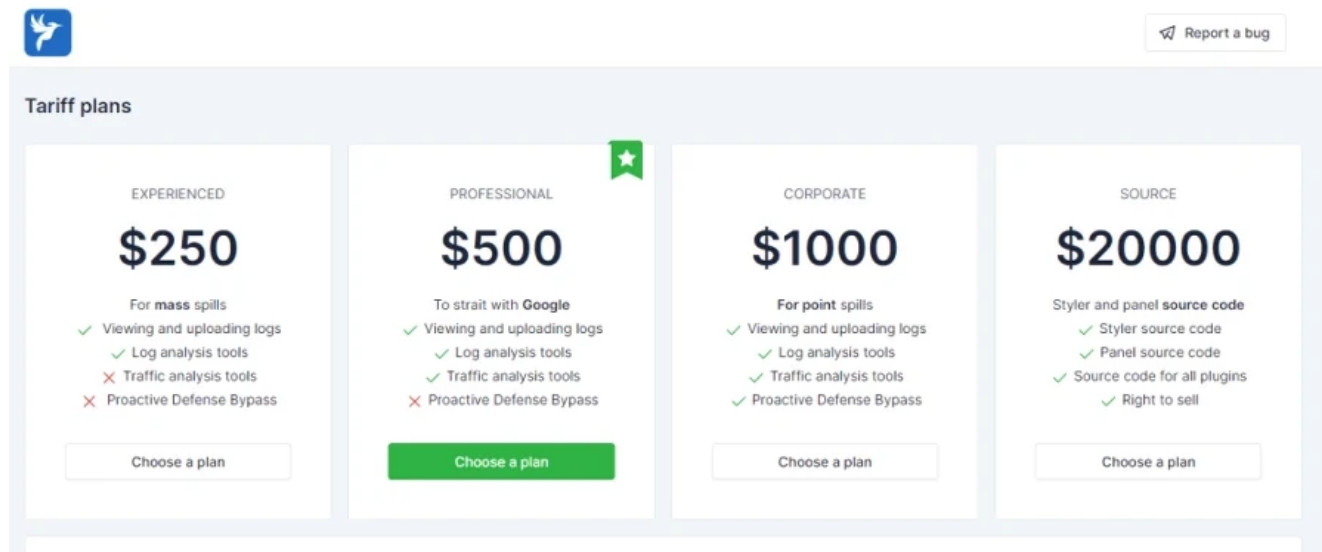
Let’s break down the Lumma Stealer and see what is so unique about it. We will start top to bottom, starting with promotion methods and going all the way down to data exfiltration.

## Received Lumma Stealer Samples

---

## Promotions on Telegram and Darknet

Main ways to market their malware for Lumma developers are posts on Darknet forums and in several Telegram groups. There, **frauds offer a wide range of pricing with different privileges** for each tier. They also provide an extensive description of the stock malware capabilities and its modding potential. Among other things, developers make a special emphasis on absence of any dependencies and complete abundance of high-level WinAPI calls. Such a trick greatly improves both execution stability and detection evasion.



The screenshot shows a webpage titled "Tariff plans" with four columns representing different pricing tiers. Each tier includes a price, a target audience, a list of features with checkmarks or crosses, and a "Choose a plan" button. The Professional plan is highlighted with a green star.

Tier	Price	Target Audience	Features
EXPERIENCED	\$250	For mass spills	Viewing and uploading logs (✓), Log analysis tools (✓), Traffic analysis tools (✗), Proactive Defense Bypass (✗)
PROFESSIONAL	\$500	To strait with Google	Viewing and uploading logs (✓), Log analysis tools (✓), Traffic analysis tools (✓), Proactive Defense Bypass (✗)
CORPORATE	\$1000	For point spills	Viewing and uploading logs (✓), Log analysis tools (✓), Traffic analysis tools (✓), Proactive Defense Bypass (✓)
SOURCE	\$20000	Styler and panel source code	Styler source code (✓), Panel source code (✓), Source code for all plugins (✓), Right to sell (✓)

Different plans for Lumma malware, posted on the Darknet site

Similarly to all the “major” infostealers, **Lumma offers their own hosting for establishing the C2**, praising their stability and anti-DDoS protection. Devs also boast of the anti-detection tricks like HeavensGate exploitation, binary morpher and non-resident loader.

## Lumma Stealer Spreading Methods

For spreading methods, **Lumma opts for common yet unusual approaches**. Such a paradox is explained with arranging the spreading campaigns in a way so it will be much less suspicious to the victim. Some of them include exploiting popular social media platforms to attract as many folks as possible.

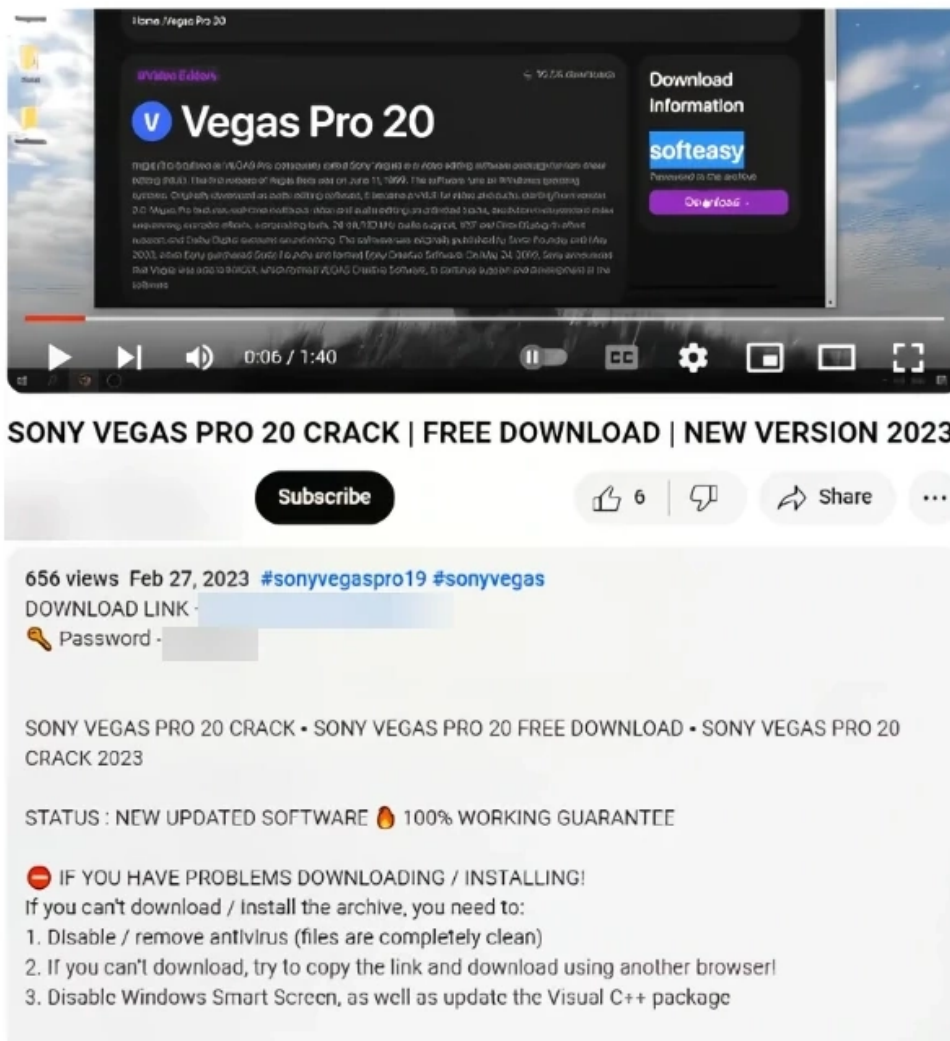
## Pirated a.k.a Cracked Software

One of the oldest malware spreading approaches, cracked software provides **the vast majority of victims to Lumma Stealer**. By embedding a downloading script into the installer, frauds provide themselves with an excellent disguise. Not only does such software usually require the user to disable antivirus tools, it also gets an alibi to any notifications from antivirus afterwards.

Typically for malware that opts for a more sophisticated spreading approach, the topics for spreading are picked among ones that have the biggest traffic. **With the use of SEO poisoning and spam in social media**, frauds attract a lot of people to their website, which offers to download the desired software for free. Such tactic is not new, and was previously used by STOP/Djvu ransomware back in 2021.

## Hacked YouTube Channels Promoting Software Cracks

One particular case of Lumma stealer spreading via pirated software **happened in January 2024**, when a hacked YouTube account started promoting a link to cracked software downloading. Upon downloading the and running file from the link, users were infected with Lumma through the staged loader, that provided additional disguise to the entire operation.

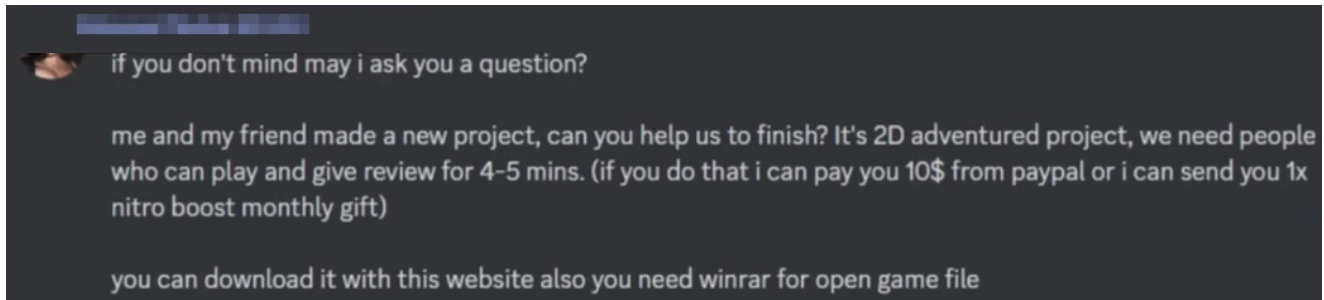


YouTube video that promotes a link to malware downloading

## Discord Spam Messages

One of the earliest spreading tactics for Lumma was **messages sent through Discord**. Despite being a rather simple and straightforward tactic, it is surprisingly effective. There were variations to this approach – with gaining trust on a particular Discord server or with a

direct spam to anyone who does not have their DMs locked.



Spam message that offers to run "a game that requires testing"

The links spread in such a way were directed to the downloading of a payload, **but were offered as a tool the sender wants to test**. In some really sophisticated attacks, frauds were sending malicious files in response to a request for some specific software utility.

## Email Spam

---

Alpha and omega of malware spreading throughout the last decade. There are dozens of ways to hide malware within the email message, **both as a link and inside of the attached file**. However, Lumma went further here, too, targeting specific people online with spear phishing campaigns. Mass-spreading campaigns through email messages are not typical though, for no obvious reason.

## Lumma Stealer Analysis

---

In the vast majority of campaigns, Lumma **is delivered by a staged loader** – the malicious script that does some basic checks and pulls the payload from the command server. Nonetheless, this does not weaken Lumma's evasion methods by any means. The interesting thing about these loaders is the use of GitHub profile as the intermediary C2 server. Main function behind these loaders is ensuring that the system is not a virtual machine or debug environment, doing some basic system review and retrieving the payload from a different command server. **The latter differs depending on the system configuration and location**.

## Startup, Detection & Analysis Evasion

---

The aforementioned staged loader in the form of a script finishes its activity with downloading the DLL file – **an actual Lumma payload**. In the Resources section of this library, there are 3 PNG files that are in fact the encrypted malware code. Upon decryption and launch, Lumma begins its own round of system checks, to ensure that it is not running on the VM or the debugger.

For that purpose, malware calls for Windows function *GetForegroundWindow* and checks whether it contains any of the strings from below. These are the strings **typical for debug environments**.

- ida
- hyperdbg
- debug
- debugger
- x32dbg
- x64dbg
  
- cheat engine
- cheatengine
- windbg
- ollydbg
- immunity debugger
- dnspy

The next step for Lumma is sandboxing evasion. Malware enumerates the DLLs in use, seeking for ones typically used by 360 Total Security, **Sandboxie**, **Cuckoo Sandbox** and Comodo Antivirus. It also pulls the trick to avoid analysis through Wine environment, by seeking for the *wine\_get\_unix\_file\_name* API being used by *kernel32.dll* or *ntdll.dll*.

**Another anti-sandbox round is to seek for matches in usernames.** As most common sandbox environments have default or generic names, it is not that complicated to weed out the simplest honeypots. Malware compares usernames in the system with the following list:

- CurrentUser
- Virus
- Sandbox
- sand box
- test user
- malware
  
- maltest
- Miller
- WDAGUtilityAccount
- John Doe
- Johnson

Things do not stop here, **as Lumma proceeds with reviewing system properties** searching for any signs of virtualization being used. It checks the .sys files in the *system32* folder, seeking for ones that are typical for virtual machines; malware scans the devices in

order to find generic vendor names used as blanking plugs in VMs. At the end, **malware scans the services** to once again see whether there is any evidence of virtual machines.

Match on any of the aforementioned stages makes malware to stop further execution. But when it passes clear, **malware decrypts the rest of the DLL** and the process injection happens, launching the payload.

## C2 Communications & Data Stealing

After such a long detection and analysis evasion cycle, **Lumma eventually switches to its main function** – information stealing. But beforehand, it reports about the new instance to the command server. This is done using HTTP POST message; each sample carries the list of encrypted C2 addresses (1 main + 10 backup) that malware starts resolving after being launched. The first one to be responsive is then used for all further communications, **including data exfiltration.**

..			File folder		
Applications	11,977	6,475	File folder		
Chrome	3,822,417	311,486	File folder		
Cookies	221,304	90,935	File folder		
CreditCards	81	81	File folder		
Edge	3,905,183	367,308	File folder		
GoogleAccounts	3,799	935	File folder		
Opera GX Stable	7,225	3,507	File folder		
Opera Neon	7,146	1,388	File folder		
Wallets	29,815,0...	19,143,4...	File folder		
All Passwords.txt	5,989	872	Text Document	11/8/2023 ...	CAE05...
Brute.txt	242	210	Text Document	11/8/2023 ...	7F3850...
Processes.txt	6,752	1,018	Text Document	11/8/2023 ...	E98A5...
Screen.png	12,681,2...	189,037	PNG File	11/8/2023 ...	ADBC8...
Software.txt	1,039	503	Text Document	11/8/2023 ...	B1DCD...
System.txt	502	346	Text Document	11/8/2023 ...	AB6C8...

Data collection gathered by Lumma

Once the initial connection has been established, **malware starts scanning the user data in the system**, seeking for the files related to crypto wallets, user browser profiles and browser extensions of crypto wallets. As Lumma developers say in the promo post, it is possible to add the needed crypto wallet extension to the seek list in a couple of clicks. Under one of the tariffs, hackers offer to steal persistent cookies – a vulnerable type of ones that provide access to the compromised account even after the password change. When data collection is over, malware encrypts the resulting package and **sends it to the C2.**

```

    "t": 0,
    "p": "%userprofile",
    "m": "*bitcoin*",
    "z": "Important Files/Profile",
    "d": 3
  },
  {
    "t": 0,
    "p": "%userprofile",
    "m": "*binance*",
    "z": "Important Files/Profile",
    "d": 3
  },
  {
    "t": 0,
    "p": "%userprofile",
    "m": "*exodus*",
    "z": "Important Files/Profile",
    "d": 3
  },
  {
    "t": 0,
    "p": "%userprofile",
    "m": "*coinbase*",
    "z": "Important Files/Profile",
    "d": 3
  },
  {
    "p": "%localappdata%\Google\Chrome\User Data",
    "z": "Chrome"
  },
  {
    "p": "%localappdata%\Chromium\User Data",
    "z": "Chromium"
  },
  {
    "p": "%localappdata%\Microsoft\Edge\User Data",
    "z": "Edge"
  },
  {
    "p": "%localappdata%\Kometa\User Data",
    "z": "Kometa"
  },
  {
    "p": "%localappdata%\Opera Software\Opera Stable",
    "z": "Opera"
  },
  {
    "p": "%localappdata%\Opera Software\Opera GX Stable",
    "z": "Opera GX Stable"
  }
}

```

Rows in malware code that specify where to seek for user data/crypto wallets data

The C2 panel is also worth attention. All the methods to avoid detection are accompanied by AI-assisted filtering, **which weeds out the exfiltrated data from “bots”**, i.e. test machines used by analysts. At least, this capability was promoted in one of the publications on the Darknet forum.

## How to Protect Yourself?

As you could have seen from the analysis, **Lumma is an exceptionally cautious malware**. Before running, it does its best to avoid leaving any trails in the system. However, it is not invulnerable, as advanced anti-malware software is still able to catch it rather fast. Still, the best option is to avoid the infection at all.

**Avoid cracked software.** The vast majority of Lumma infection cases are after the malware being injected into pirated software. For the selection of properties, such apps fit exceptionally well as a shell for malware spreading.

**Be careful with sketchy programs you find online.** The continuation of the previous paragraph, low-trust or unknown applications may be used to inject malware. Same as pirated apps, they often require you to disable anti-malware software, and you often simply do not know how the program should work. The latter actually makes it even more convenient for malware distribution.

**Do not interact with suspicious email messages.** Even though Lumma is rarely spread in email attachments, this is universal advice for keeping your system safe. Despite all attempts to jam this approach, it is still the most popular one, and may be used under different

circumstances and in different attack scenarios.

**Use reliable anti-malware software.** The best way to be sure about your system's safety is to have a dedicated software for that case. When combined with precautions from the above, anti-malware programs will act as a gatekeeper, detecting and removing the stuff that managed to get in. [GridinSoft Anti-Malware](#) is a program you can rely on for this purpose.

## Lumma Stealer Indicators of Compromise (IoC)

---

**MD5:** 69abcc261ae76d2b063672df06837966

**MD5:** 757661287c20b63b1c6ae4f66fc0c6d8

**MD5:** 6d07e04a6926d1dd6cc7805f866114a4

**MD5:** 8c2b02f3609019a2ea5af617a1d2556d

**SHA-256:** 48cbeb1b1ca0a7b3a9f6ac56273fbaf85e78c534e26fb2bca1152ecd7542af54

**SHA-256:** 483672a00ea676236ea423c91d576542dc572be864a4162df031faf35897a532

**SHA-256:** 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f

**SHA-256:** 7603c6dd9edca615d6dc3599970c203555b57e2cab208d87545188b57aa2c6b1

**SHA-256:** 674d96c42621a719007e64e40ad451550da30d42fd508f6104d7cb65f19cba51

## IP Addresses

---

176.113.115.224

176.113.115.226

176.113.115.227

176.113.115.229

176.113.115.232

144.76.173.247

45.9.74.78

77.73.134.68

82.117.255.127

82.117.255.80

82.118.23.50

## URLs

---

netovrema[.]pw

opposesicknessopw[.]pw

politefrightenpowoa[.]pw

chincenterblandwka[.]pw

loogsporus[.]pw/api

meayyammgatterre[.]pw/api