

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-10,

Defendants.

Case No. 1:25-CV-2695-MHC

**FILED UNDER SEAL**

**DECLARATION OF JAKUB TOMANEK IN SUPPORT OF  
MICROSOFT'S MOTION FOR TEMPORARY RESTRAINING ORDER  
AND RELATED RELIEF**

I, Jakub Tomanek, declare as follows:

1. I am a Malware Analyst at ESET Research Czech Republic s.r.o., a subdivision of ESET spol. s.r.o. ('ESET'). I make this declaration in support of Plaintiffs' Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge, and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. ESET is an Internet security company that investigates malicious threat actors, including the present threat known as LummaStealer, and offers anti-virus products. In my role at ESET, I investigate incidents related to online attacks,

security threats and botnets. In particular, over the past nine years I have been involved in identifying and mitigating online threats for millions of ESET product end users.

3. My role at ESET, with my education, has provided me an in-depth insight into how malware authors deploy and utilize online threats for their monetary gain. In 2015, I received a Bachelor of Engineering degree in Computer Science from Czech Technical University in Prague. In 2017, I received a Master of Engineering degree in Computer Security from Czech Technical University in Prague, Czech Republic. I am contributor to ESET's security blog: [welivesecurity.com](http://welivesecurity.com). A true and correct copy of the current version of my curricula vitae is attached to this declaration as Exhibit 1.

4. During the investigation I was part of a team that reverse engineered the LummaStealer malware and monitored threat activity associated with the LummaStealer malware. From that work, I am familiar with the operation and structure of LummaStealer and conclude that the core functionalities of LummaStealer are stealing sensitive and valuable data from the victim machines. As of May 2025, this threat is primarily detected by ESET products as Win32/Spy.LummaStealer.A, Win32/Spy.LummaStealer.B, Win32/Spy.LummaStealer.C, and so forth through Win32/Spy.LummaStealer.AD.

5. During my investigation, I observed several indications that convince me that LummaStealer operates as malware-as-a-service (MaaS). These indications include advertisements on hacking forums where a LummaStealer reseller account offers the infostealer as a service with three tier options (Figure 1 in Exhibit 2), open documentation of the LummaStealer management panel for affiliates (Figure 2 and Figure 3 in Exhibit 2), the existence of Telegram marketplace maintained by LummaStealer operators for their affiliates to sell stolen data (Figure 4 in Exhibit 2), a special affiliate identifier embedded in the LummaStealer infostealer binaries, and a substantial amount of existing cybersecurity research documenting LummaStealer infections.

6. The LummaStealer operators develop the infostealer malware and maintain exfiltration network infrastructure. They advertise the malware service on hacking forums and Telegram channels. The LummaStealer affiliates pay a monthly fee to receive the latest LummaStealer malware builds from LummaStealer operators, the network infrastructure necessary for data exfiltration, and an account at management panel for stolen data withdrawal. The exfiltrated data is then exploited or traded by LummaStealer affiliates, leading to further and more severe cyber-attacks.

7. In the latest versions of LummaStealer malware, we distinguish three types of Command & Control (C&C) servers. Each LummaStealer sample contains a protected list of nine C&C URLs, along with two additional URLs. These additional URLs point to a *Telegram channel* and a *Steam profile*, and act as *dead drop resolvers*<sup>1</sup>. The Telegram URL is not included in all LummaStealer samples. When present, it serves as the primary source for the C&C server. The Steam profile URL, on the other hand, is used as a backup source for the C&C server.

8. During the first phase of execution, LummaStealer selects an active C&C server. The selection order is as follows: at first, it uses the Telegram dead drop resolver; if unsuccessful, it then tries the hardcoded list of C&C servers; and if none of these responds, LummaStealer attempts to obtain a C&C server from the Steam profile dead drop resolver.

9. During our investigation of LummaStealer, we found that all extracted C&C domains are consistently proxied through Cloudflare services, which are used to conceal LummaStealer's actual C&C infrastructure. The Cloudflare proxy services are also employed for dead drop resolved C&C servers.

---

<sup>1</sup> A dead drop resolver refers to a technique where adversaries utilize an existing, legitimate external web service to host information that directs to additional C&C infrastructure (<https://attack.mitre.org/versions/v17/techniques/T1102/001/>)

10. Our investigation revealed that LummaStealer malware exfiltrates a wide range of sensitive data from victim machines. The LummaStealer primary focus is on stealing data from browsers<sup>2</sup>, password managers, VPNs, FTP clients, cloud services, remote desktop applications, email clients, cryptocurrency wallets, and note-taking applications. Moreover, the LummaStealer malware have ability to exfiltrate any other data from victim machines based on custom configuration created by LummaStealer operators or affiliates.

11. The LummaStealer malware also includes an additional payload delivery feature, leading to further compromise of the victim's machine and potential monetary harm. This feature is not always used by LummaStealer affiliates. In cases where the payload was not empty, our research has predominantly observed the delivery of malware classified as Coinminers, which exploit the victim's computer power to mine cryptocurrency, which scan the victim's clipboard for cryptocurrency wallet addresses to replace them with the attacker's addresses, tricking the victims into transferring cryptocurrency to the attackers. Other types of malwares have been observed with lower frequency.

12. LummaStealer malware causes harm to victim end-users who are targeted by the LummaStealer operators and affiliates. The LummaStealer malware

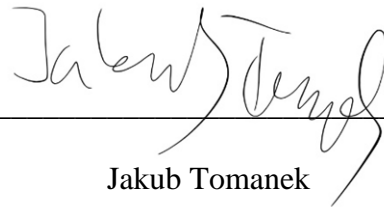
---

<sup>2</sup> browser-saved credentials, session cookies, web history, autofill data

enables the Defendants to infect victim computers, steal sensitive data, and deploy additional malicious payloads. Consequently, the victims' machines, digital identities, and valuable assets are further exposed to subsequent cyber-attacks facilitated by the stolen data.

13. ESET telemetry confirms that LummaStealer has been one of the most prevalent infostealers over the past two years, targeting regions globally without exception.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 12th day of May in Prague, Czech Republic.



---

Jakub Tomanek

# **EXHIBIT 1**

# JAKUB TOMANEK

## EXPERIENCE

2016 – PRESENT

**MALWARE ANALYST**, ESET

For the past nine years, I have dedicated my career to working as a malware analyst, deeply involved in researching various malware families such as TrickBot, BumbleBee, Numando, Zumanek, RecordBreaker, and currently LummaStealer. My expertise extends beyond malware research to include Windows digital forensic analysis. Additionally, I have contributed to enhancing the security infrastructure by participating in the development of the detection rules of the ESET Endpoint Detection and Response (EDR) ruleset, ensuring the system remains robust against evolving threats.

## EDUCATION

2015-2017

**ING. (MASTER OF ENGINEERING)**, CZECH TECHNICAL UNIVERSITY, PRAGUE

Computer Security

2012-2015

**BC. (BACHELOR OF ENGINEERING)**, CZECH TECHNICAL UNIVERSITY, PRAGUE

Computer Science

## SKILLS

**Reverse Engineering:** IDA, ollydbg, Scylla, dnspy, hiew, Wireshark, PEiD, Frida, Unicorn engine, Sysinternals Suite, Volatility, Burp Suite

**Threat Intelligence:** YARA, VirusTotal, Shodan, Censys


**Programming skills:** Python, C++, .NET




# **EXHIBIT 2**

LummaC2 - malware, knock 90% x

hackforums.net/showthread.php?tid=6250298&page=1



**LummaStealer** •  
LummaC2 Seller  
\$\$



Posts:	144
Threads:	1
Credibility:	0 0
Popularity:	107
Bytes:	35.75
Game XP:	0

**Pricing plans:**

**EXPERIENCED**

- Set filters up to 10 .
- Download logs in bulk
- Possibility to upload logs by your search query (for example - only with wallets or only with instagram.com)
- Ability to use search by parameters (country, with or without currency, with a specific filter)
- Ability to clear dumps, dumps statistics on the "quality of logs" page
- 3 build tags

**PRICE: \$250/month**

**PROFESSIONAL**

- All features of previous privileges
- Unlimited number of filters
- Logs can be deleted in bulk (by zeroing the counter)
- Share your stats with others
- Logs quality widget available
- Filter widget is available
- Unlimited build tags
- Search widened, logs search and downloading is available by request (in cookies/passwords)
- Ability to monitor number of neighbors in logs
- Logs quality rating system available
- Ability to create and edit grabber profiles
- Ability to add and remove extensions
- Ability to add and remove browsers
- Ability to add and remove paths for looting
- Ability to use masks as well as variable paths
- Ability to edit the data to be collected and the order of data collection, e.g. someone needs to collect cid phrases first and someone needs to collect chrome first
- Ability to customize the depth of data collection
- Ability to always roll back to default settings
- Ability to create an unlimited number of rules in the profile
- Ability to edit profile "hot", to change data collected by the malware right during spreading
- Non-residential Loader

**PRICE: \$500/month**

**CORPORATE**

- Previous privileges features
- Dedicated build cleanup line, build is cleaned more often
- Improved bypass of proactive protection (no message LummaC2.exe tries to access password store), build lives longer
- Great for you-know-where point-level security breaches
- Generation of random builds by our morpher, each build is individual, different from the other

**PRICE: \$1.000/month**

Figure 1: Screenshot of Defendant's advertisement on hacking forum (12<sup>th</sup> of May 2025)



## Полное описание LummaC2

Обзор на панель

Виды подписок

Сбор данных

FAQ

### РУКОВОДСТВО

Основные термины

Входим в криптокошельки из лога

Входим в приложения из лога

Проверка билда на отстук

Фильтры для популярных запросов

Нерезидентный Loader

Восстанавливаем cookies Google

Ink билдер

Безопасность вашей учетной записи

Создание уникальной  
ссылки воркера

Виджеты

### МАРКЕТ

Описание @lummamarketbot

Пользовательское соглашение

Информация для продавцов

Инструкция по  
использованию @lummamarketbot

Powered by GitBook

## Полное описание LummaC2



**LummaC2** - стиллер не имеющий аналогов, **средний отстук 75-85%**, работает даже на чистых системах, зависимостей нет никаких (ВООБЩЕ), расшифровка лога на сервере, вес билда 150-300КБ, ворует **браузеры на базе Chromium и Mozilla**, ворует **~70 браузерных криптовалютных и 2FA расширений, токены Discord**, имеется возможность **ВОССТАНОВИТЬ УБИТЫЕ COOKIES GOOGLE**, нерезидентный **Loader**, низкоуровневый адаптивный файлгаббер, интегрированные **Reverse proxy, Ink builder, AI для определения ботов в панели**, а также новейшая уникальная разработка - **МОРФЕР**.

**LummaC2** обновляется буквально каждые два часа, добавить ваш специфический браузер или ваше специфическое расширение - **2 клика!**

### Важная информация о нашем продукте:

- Язык, использовавшийся при разработке данного продукта - **C++**
- Практически не используется высокоуровневое **WinAPI**
- Работаем по модели **Malware-as-a-Service**, панель и билдер находятся в web'e
- Вся расшифровка полностью серверная, все данные передаваемые стиллером расшифровываются на сервере
- В целях увеличения отстука отправка данных происходит chunk'ами
- Вес билда составляет **150-300КБ**
- Доступна система обнаружения соседей, а также система мониторинга качества трафика
- Системные вызовы поддерживают архитектуры ARM, x86, x64
- Стиллер работает на версиях операционных систем начиная с Windows 7 x32, заканчивая Windows 11 x64 с последними update'ами
- Все взаимодействие с ОС происходит посредством вызовов низкоуровневой обертки, написанной на ASM, над системными вызовами, никакого WinAPI только ручные вызовы syscall'ов (корпоративный тариф)

Figure 2: Screenshot of Defendant's official documentation (12<sup>th</sup> of May 2025)



## Full description of LummaC2

Panel overview

Types of subscriptions

Data collection

FAQ

### MANAGEMENT

Basic terms

Logging into the crypto wallet from the log

Logging into applications from the log

Checking the build for knockback

Filters for popular queries

Non-resident Loader

Recovering Google cookies

Ink builder

Security of your account

Creating a unique worker link

Widgets

### MARKET

Description @lummamarketbot

User Agreement

Information for sellers

Instructions for using @lummamarketbot

## Full description of LummaC2



**LummaC2** is a stealer that has no analogues, the average knockback is 75-85%, it works even on clean systems, there are no dependencies (AT ALL), log decryption on the server, the build weight is 150-300 KB, it steals **browsers based on Chromium and Mozilla**, steals **~70 browser cryptocurrency and 2FA extensions, Discord tokens**, it is possible to **RESTORE KILLED GOOGLE COOKIES**, non-resident **Loader**, low-level adaptive file grabber, integrated **Reverse proxy**, Ink builder, **AI for detecting bots in the panel**, as well as the latest unique development - **MORPHER**. **LummaC2** is updated literally every two hours, add your specific browser or your specific extension - **2 clicks!**

### Important information about our product:

- The language used in the development of this product is **C++**
- **High-level WinAPI** is hardly used
- We work on the **Malware-as-a-Service model**, the panel and builder are located on the web
- All decryption is completely server-based, all data transmitted by the stealer is decrypted on the server
- In order to increase the response time, data is sent in chunks.
- The build weight is **150-300KB**
- A neighbor detection system is available, as well as a traffic quality monitoring system.
- System calls support ARM, x86, x64 architectures
- Still works on operating system versions from Windows 7 x32 to Windows 11 x64 with the latest updates.
- All interaction with the OS occurs through calls to a low-level wrapper written in ASM over system calls, no WinAPI, only manual calls to syscalls (corporate rate)

Figure 3: Screenshot of Defendant's official documentation – english translated  
(12<sup>th</sup> of May 2025)

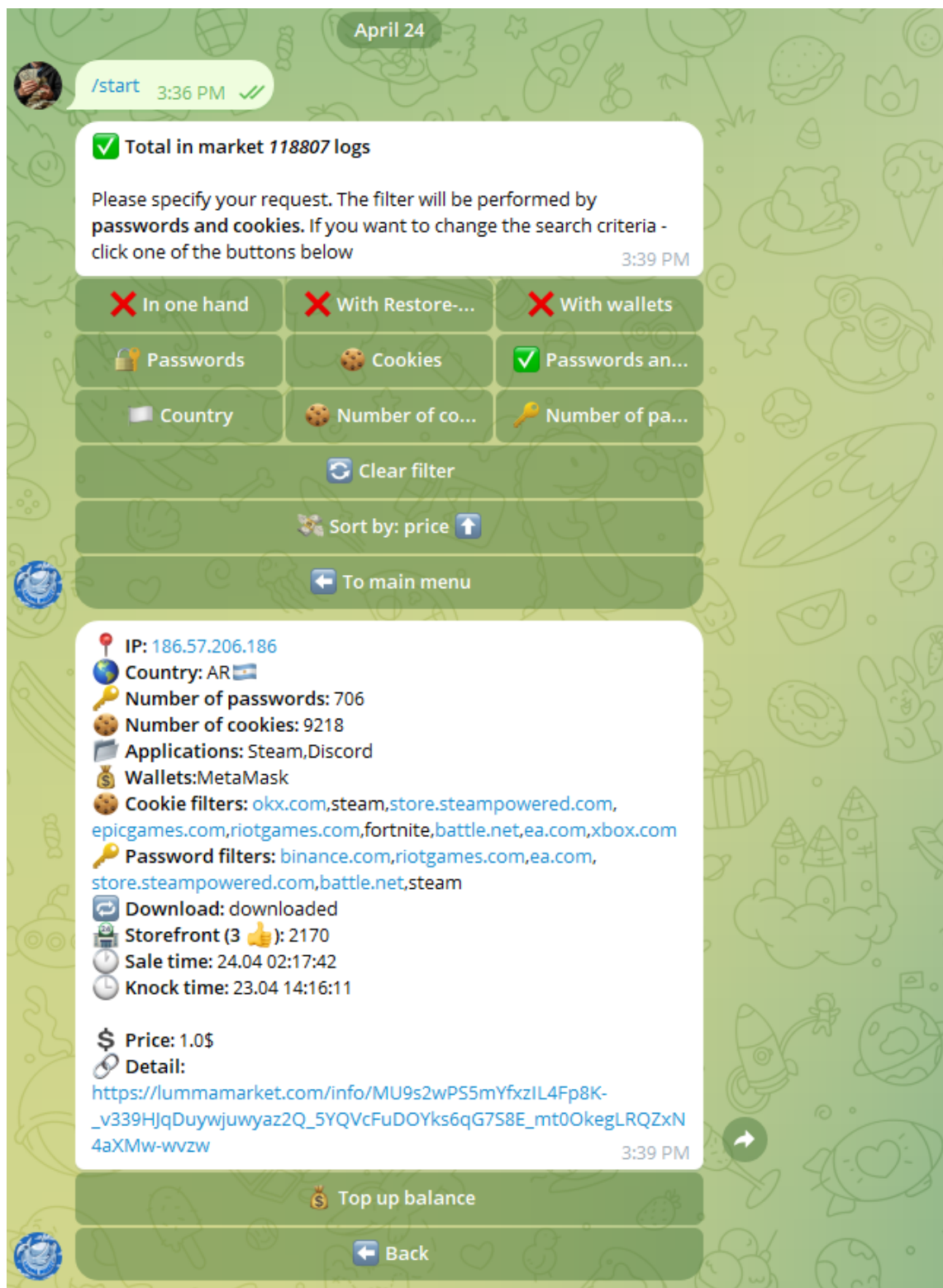


Figure 4: Screenshot of Defendant's marketplace on Telegram (24<sup>th</sup> of April 2025)