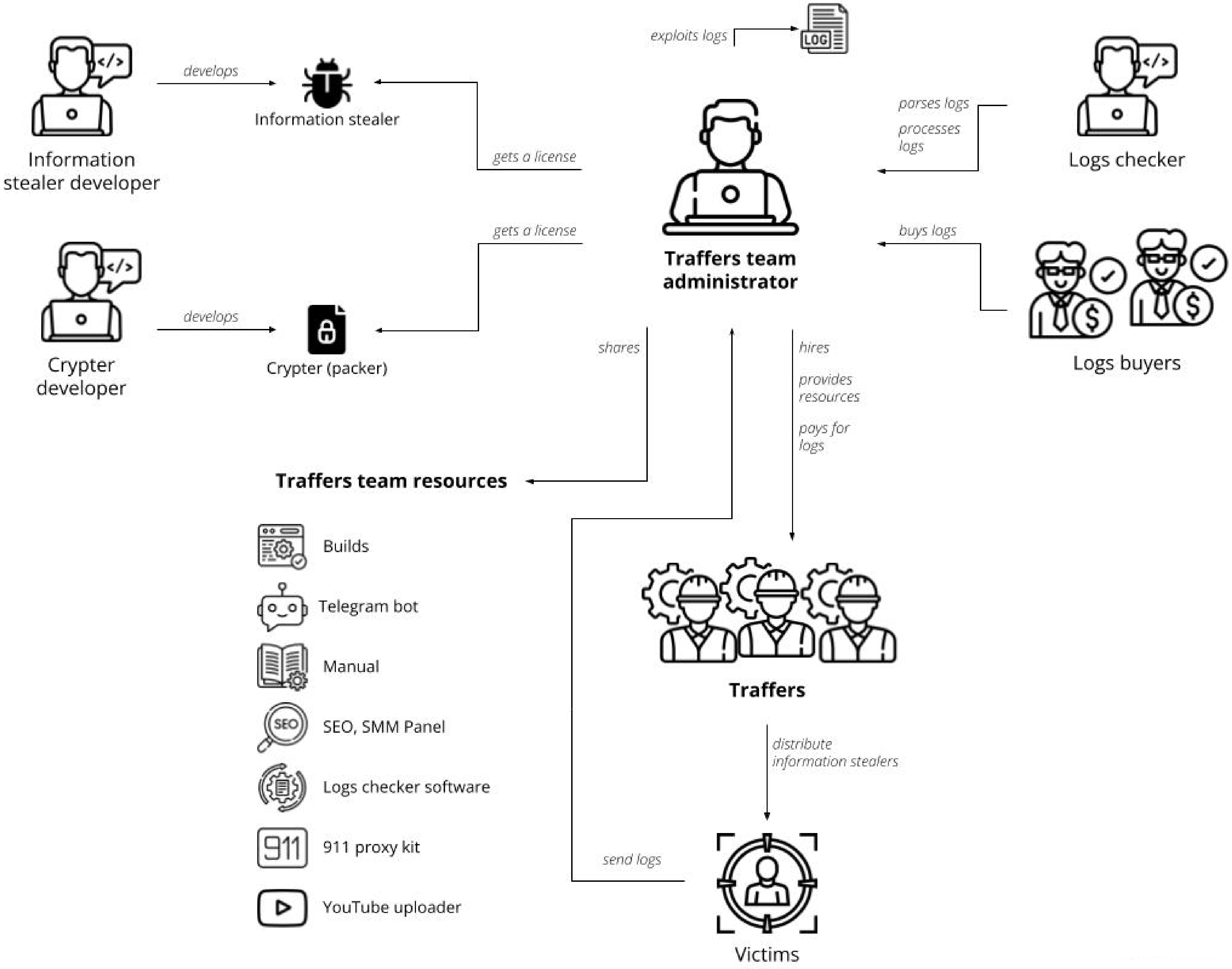
Log Stealer Market Places

è il momento degli acquisti per i Threat Actors!

Massimo Giaimo - Team Leader Cyber Security

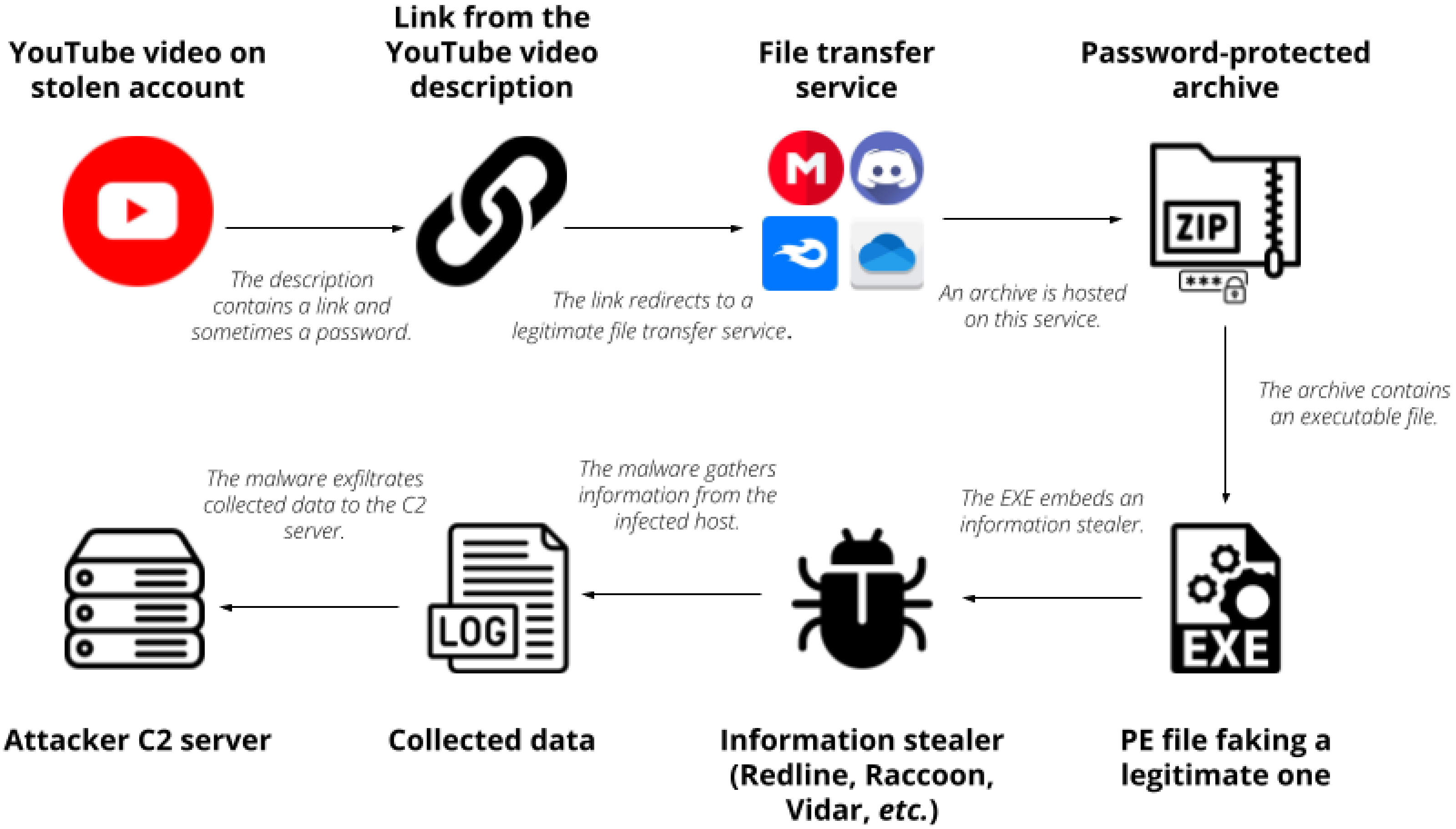


What is a log stealer malware?

Log (or information) stealer malware is a type of Trojan that gathers data in order to send it to the attacker. Typical targets are credentials saved in browser profiles.

Log stealer malware infection chain

- YouTube video on stolen account
- websites masquerading as blogs to deliver password-protected archives
- software installation pages to deliver password-protected archives
- phishing emails



YouTube video on stolen account

The description contains a link and sometimes a password.

Link from the YouTube video description

The link redirects to a legitimate file transfer service.

File transfer service

An archive is hosted on this service.

Password-protected archive

The archive contains an executable file.

PE file faking a legitimate one

The EXE embeds an information stealer.

Information stealer (Redline, Raccoon, Vidar, *etc.*)

The malware gathers information from the infected host.

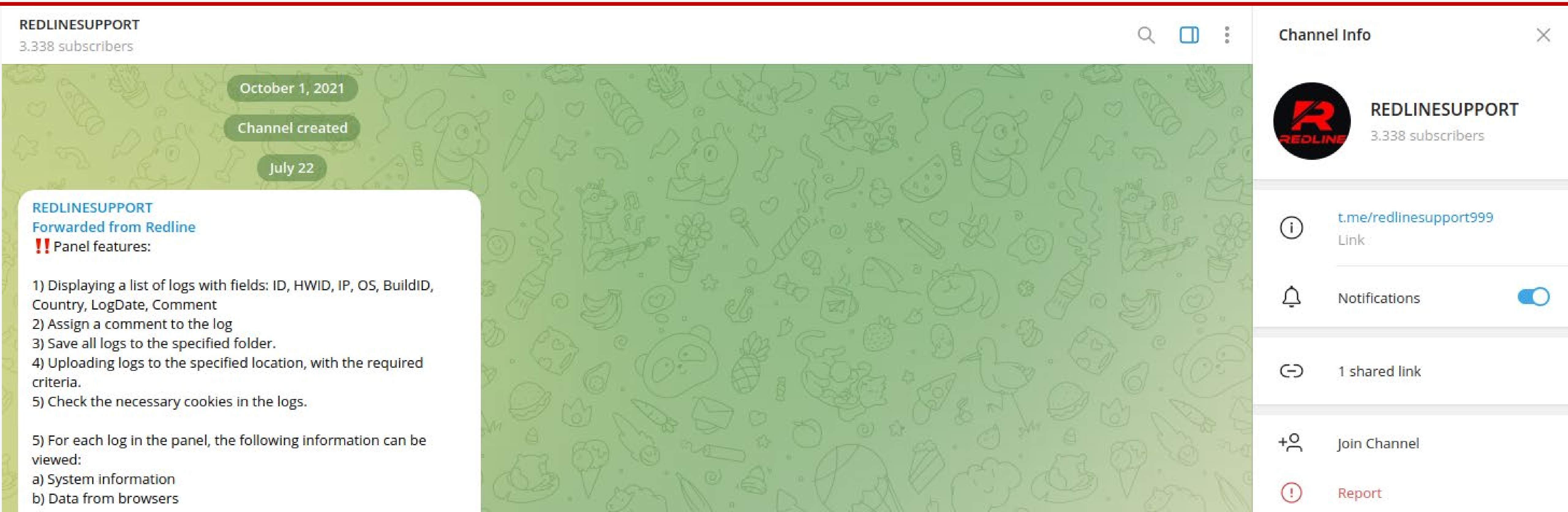
Collected data

The malware exfiltrates collected data to the C2 server.

Attacker C2 server

Redline

- available from: February 2020 (on WWH Club and BHF forum)
- owners: Glade aka REDGlade
- Telegram channel: https://t.me/REDLINESELLER | https://t.me/redlinesupport_new
- nationality: Russian
- other info: 2241632 records on Russian Market



REDLINESUPPORT
3.338 subscribers

October 1, 2021

Channel created

July 22

REDLINESUPPORT
Forwarded from Redline
‼️Panel features:

1) Displaying a list of logs with fields: ID, HWID, IP, OS, BuildID, Country, LogDate, Comment
2) Assign a comment to the log
3) Save all logs to the specified folder.
4) Uploading logs to the specified location, with the required criteria.
5) Check the necessary cookies in the logs.

5) For each log in the panel, the following information can be viewed:
a) System information
b) Data from browsers

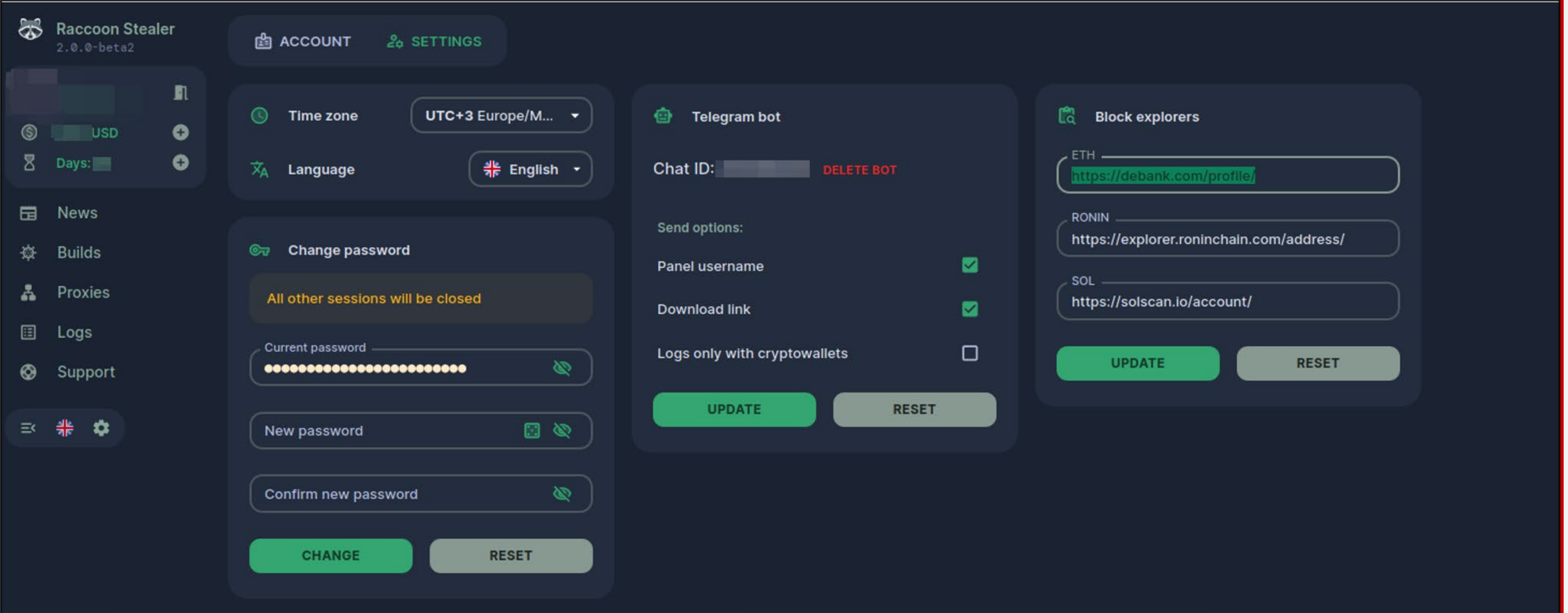
Channel Info

REDLINESUPPORT
3.338 subscribers

t.me/redlinesupport999
Link

Raccoon

- available from: 20/05/2019, version 2.0 from 15/09/2022 (on XSS forum)
- owners: @raccoonstealer on XSS forum
- Telegram channel: https://t.me/miaranimator | https://t.me/gr33nl1ght
- nationality: Ukrainian
- other info: 997005 records on Russian Market, FBI disclosure site on https://raccoon.ic3.gov/home



[redacted]

[redacted] USD

Days: [redacted]

Time zone: UTC+3 Europe/M...

Language: English

Change password

All other sessions will be closed

Current password: ●●●●●●●●●●●●●●●●●●●●●●●●●

New password

Confirm new password

CHANGE RESET

Telegram bot

Chat ID: [redacted] DELETE BOT

Send options:

Panel username ☑

Download link ☑

Logs only with cryptowallets □

UPDATE RESET

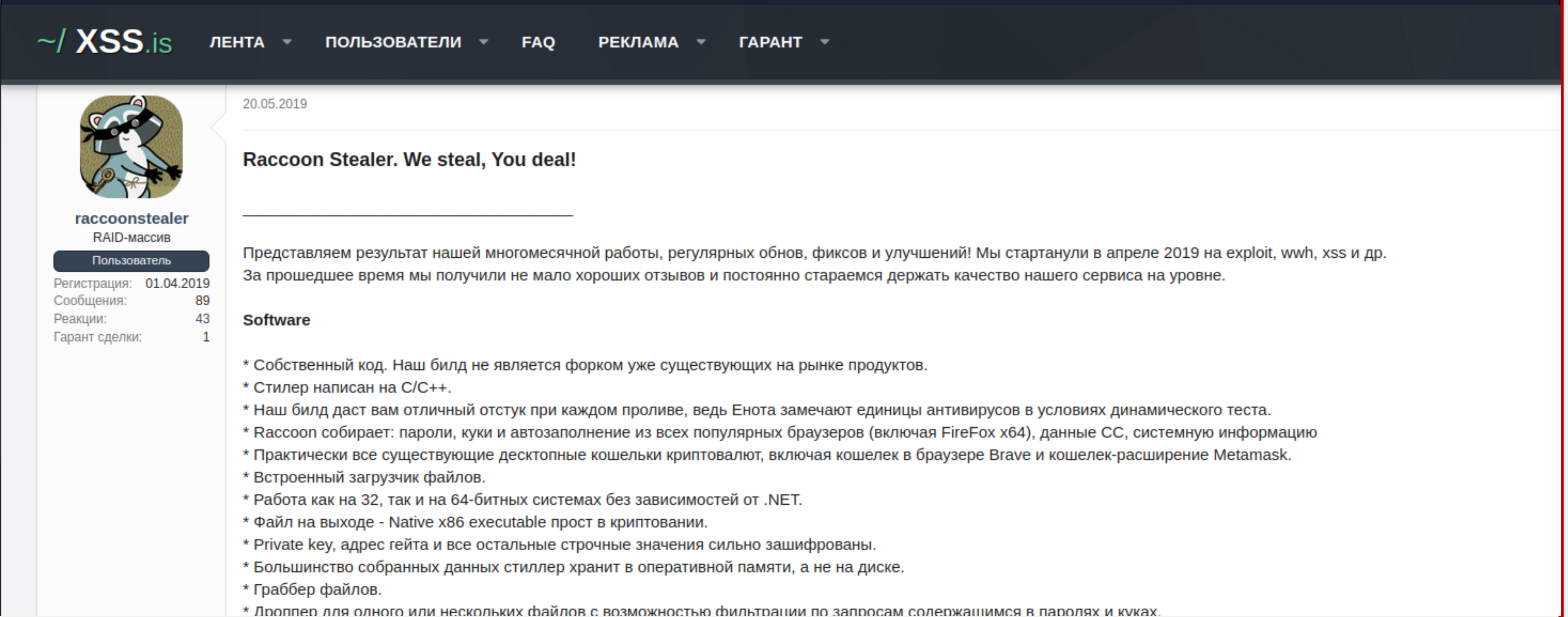
Block explorers

ETH: https://debank.com/profile/

RONIN: https://explorer.roninchain.com/address/

SOL: https://solscan.io/account/

UPDATE RESET



raccoonstealer
RAID-массив
Пользователь

Регистрация: 01.04.2019
Сообщения: 89
Реакции: 43
Гарант сделки: 1

20.05.2019

Raccoon Stealer. We steal, You deal!

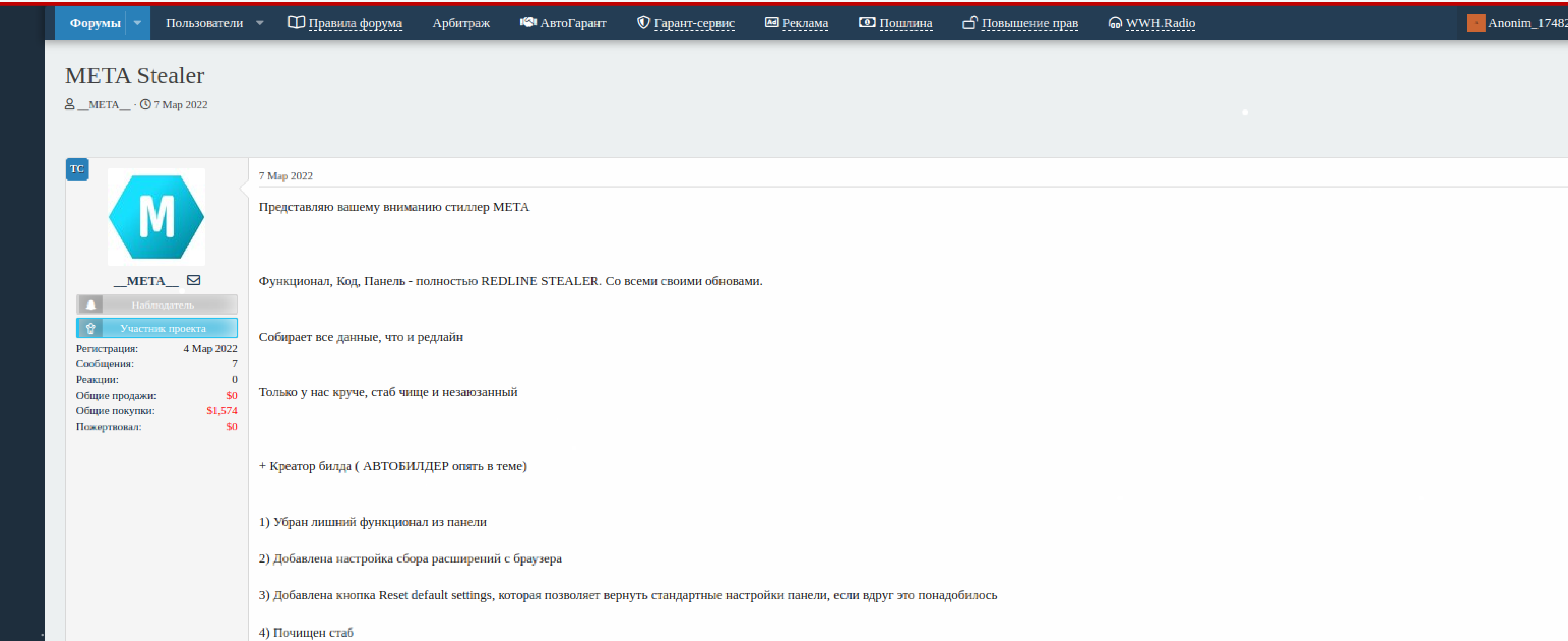
Представляем результат нашей многомесячной работы, регулярных обнов, фиксов и улучшений! Мы стартанули в апреле 2019 на exploit, wwh, xss и др.
За прошедшее время мы получили не мало хороших отзывов и постоянно стараемся держать качество нашего сервиса на уровне.

Software

* Собственный код. Наш билд не является форком уже существующих на рынке продуктов.
* Стилер написан на C/C++.
* Наш билд даст вам отличный отстук при каждом проливе, ведь Енота замечают единицы антивирусов в условиях динамического теста.
* Raccoon собирает: пароли, куки и автозаполнение из всех популярных браузеров (включая FireFox x64), данные CC, системную информацию
* Практически все существующие десктопные кошельки криптовалют, включая кошелек в браузере Brave и кошелек-расширение Metamask.
* Встроенный загрузчик файлов.
* Работа как на 32, так и на 64-битных системах без зависимостей от .NET.
* Файл на выходе - Native x86 executable прост в криптовании.
* Private key, адрес гейта и все остальные строчные значения сильно зашифрованы.
* Большинство собранных данных стиллер хранит в оперативной памяти, а не на диске.
* Граббер файлов.
* Дроппер для одного или нескольких файлов с возможностью фильтрации по запросам содержащимся в паролях и куках.

Metastealer

- available from: 07/03/2022 (on WWH Club forum)
- owners: @__META__
- other info: from 150$ (1 month) to 1000$ (lifetime)
- Telegram channel: https://t.me/METASTEALER_bot



META Stealer

__META__ · 7 Мар 2022

Регистрация:	4 Мар 2022
Сообщения:	7
Реакции:	0
Общие продажи:	$0
Общие покупки:	$1,574
Пожертвовал:	$0

7 Мар 2022

Представляю вашему вниманию стиллер META

Функционал, Код, Панель - полностью REDLINE STEALER. Со всеми своими обновами.

Собирает все данные, что и редлайн

Только у нас круче, стаб чище и незаюзанный

+ Креатор билда (АВТОБИЛДЕР опять в теме)

1) Убран лишний функционал из панели

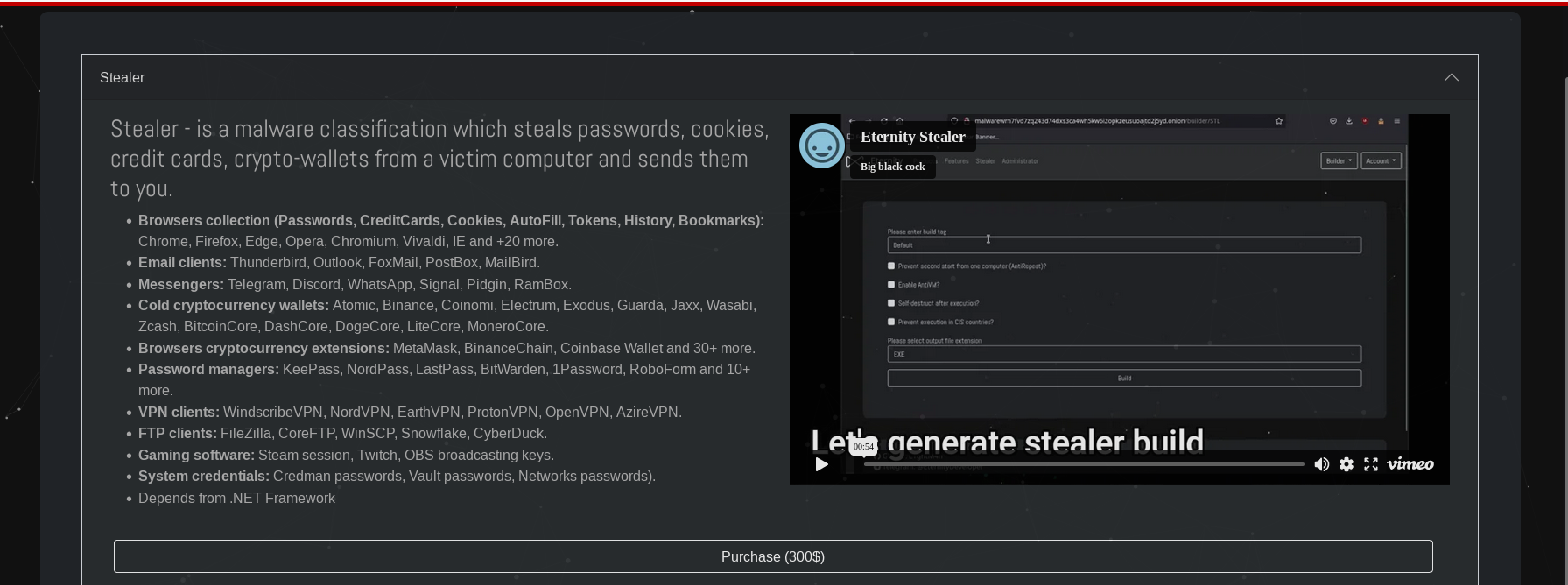
2) Добавлена настройка сбора расширений с браузера

3) Добавлена кнопка Reset default settings, которая позволяет вернуть стандартные настройки панели, если вдруг это понадобилось

4) Почищен стаб

Eternity

- available from: 26/03/2022
- owners: @LightM4n on TG, @EternityTeam on XSS forum
- nationality: Ukrainian
- other info: 300$
- Telegram channel: https://t.me/EternityDeveloper+immagine eternity



Stealer

Stealer - is a malware classification which steals passwords, cookies, credit cards, crypto-wallets from a victim computer and sends them to you.

- **Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks):** Chrome, Firefox, Edge, Opera, Chromium, Vivaldi, IE and +20 more.
- **Email clients:** Thunderbird, Outlook, FoxMail, PostBox, MailBird.
- **Messengers:** Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.
- **Cold cryptocurrency wallets:** Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.
- **Browsers cryptocurrency extensions:** MetaMask, BinanceChain, Coinbase Wallet and 30+ more.
- **Password managers:** KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.
- **VPN clients:** WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.
- **FTP clients:** FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.
- **Gaming software:** Steam session, Twitch, OBS broadcasting keys.
- **System credentials:** Credman passwords, Vault passwords, Networks passwords).
- Depends from .NET Framework

Eternity Stealer

Big black cock

malwarewm7fvd7zq243d74dxs3ca4wh5kw6i2opkzeusuoajtd2j5yd.onion/builder/STL

Please enter build tag

Default

□ Prevent second start from one computer (AntiRepeat)?

□ Enable AntiVM?

□ Self-destruct after execution?

□ Prevent execution in CIS countries?

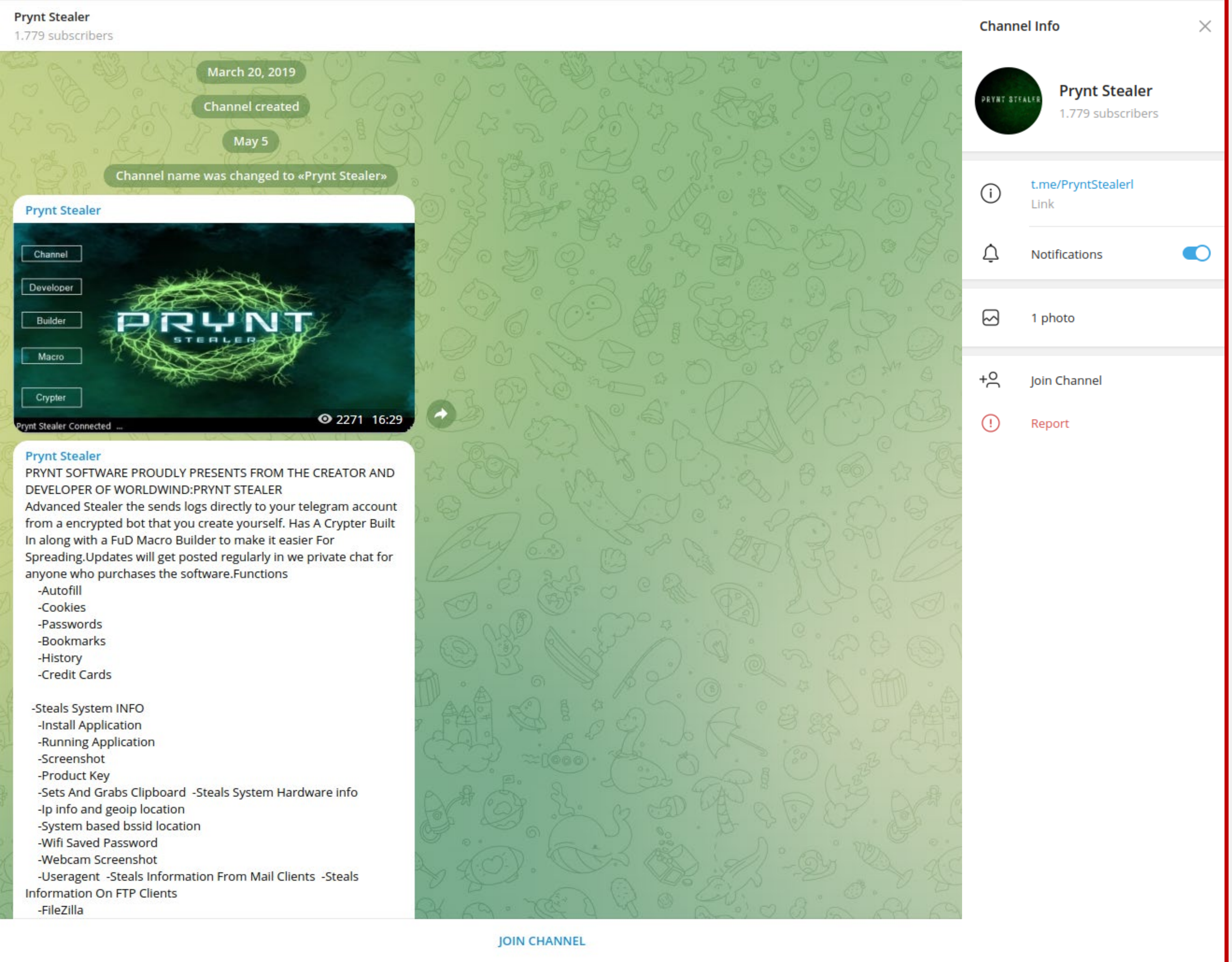
Please select output file extension

EXE

Build

Let's generate stealer build

Purchase (300$)



Prynt Stealer
1.779 subscribers

March 20, 2019

Channel created

May 5

Channel name was changed to «Prynt Stealer»

Prynt Stealer

Prynt Stealer
PRYNT SOFTWARE PROUDLY PRESENTS FROM THE CREATOR AND DEVELOPER OF WORLDWIND:PRYNT STEALER
Advanced Stealer the sends logs directly to your telegram account from a encrypted bot that you create yourself. Has A Crypter Built In along with a FuD Macro Builder to make it easier For Spreading.Updates will get posted regularly in we private chat for anyone who purchases the software.Functions
-Autofill
-Cookies
-Passwords
-Bookmarks
-History
-Credit Cards

-Steals System INFO
-Install Application
-Running Application
-Screenshot
-Product Key
-Sets And Grabs Clipboard -Steals System Hardware info
-Ip info and geoip location
-System based bssid location
-Wifi Saved Password
-Webcam Screenshot
-Useragent -Steals Information From Mail Clients -Steals Information On FTP Clients
-FileZilla

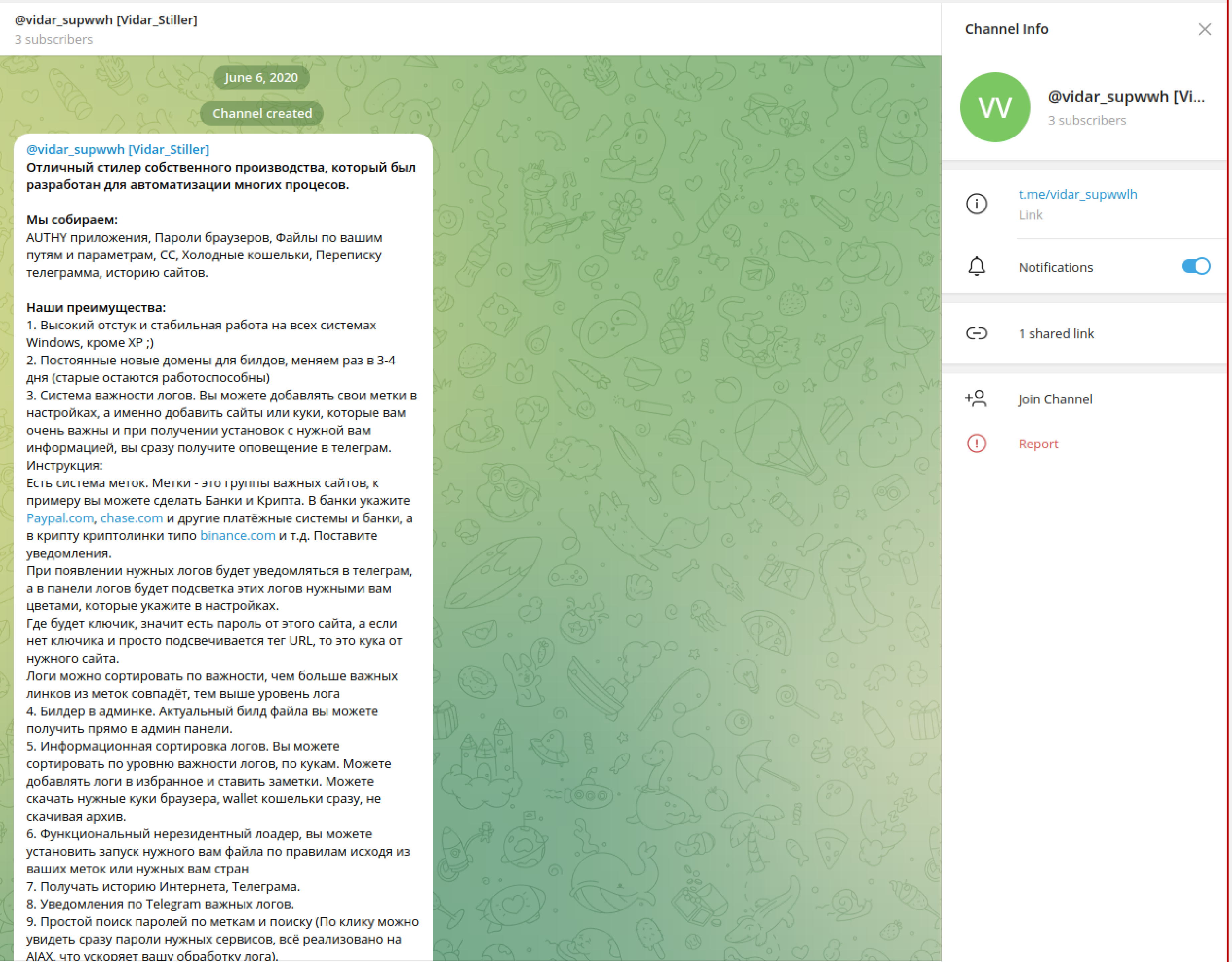
Channel Info

Prynt Stealer
1.779 subscribers

t.me/PryntStealerl
Link

Pryntstealer

- available from: 04/2022
- owners: @FlatLineStealerOfficial
- other info: from 50$ (3 days) to 200$ (lifetime)
- Telegram channel: https://t.me/PryntStealerl



@vidar_supwwh [Vidar_Stiller]

3 subscribers

June 6, 2020

Channel created

@vidar_supwwh [Vidar_Stiller]

Отличный стилер собственного производства, который был разработан для автоматизации многих процесов.

Мы собираем:
AUTHY приложения, Пароли браузеров, Файлы по вашим путям и параметрам, CC, Холодные кошельки, Переписку телеграмма, историю сайтов.

Наши преимущества:
1. Высокий отстук и стабильная работа на всех системах Windows, кроме XP ;)
2. Постоянные новые домены для билдов, меняем раз в 3-4 дня (старые остаются работоспособны)
3. Система важности логов. Вы можете добавлять свои метки в настройках, а именно добавить сайты или куки, которые вам очень важны и при получении установок с нужной вам информацией, вы сразу получите оповещение в телеграм.
Инструкция:
Есть система меток. Метки - это группы важных сайтов, к примеру вы можете сделать Банки и Крипта. В банки укажите Paypal.com, chase.com и другие платёжные системы и банки, а в крипту криптолинки типо binance.com и т.д. Поставите уведомления.
При появлении нужных логов будет уведомляться в телеграм, а в панели логов будет подсветка этих логов нужными вам цветами, которые укажите в настройках.
Где будет ключик, значит есть пароль от этого сайта, а если нет ключика и просто подсвечивается тег URL, то это кука от нужного сайта.
Логи можно сортировать по важности, чем больше важных линков из меток совпадёт, тем выше уровень лога
4. Билдер в админке. Актуальный билд файла вы можете получить прямо в админ панели.
5. Информационная сортировка логов. Вы можете сортировать по уровню важности логов, по кукам. Можете добавлять логи в избранное и ставить заметки. Можете скачать нужные куки браузера, wallet кошельки сразу, не скачивая архив.
6. Функциональный нерезидентный лоадер, вы можете установить запуск нужного вам файла по правилам исходя из ваших меток или нужных вам стран
7. Получать историю Интернета, Телеграма.
8. Уведомления по Telegram важных логов.
9. Простой поиск паролей по меткам и поиску (По клику можно увидеть сразу пароли нужных сервисов, всё реализовано на AJAX, что ускоряет вашу обработку лога).

Channel Info

VV

@vidar_supwwh [Vi...

3 subscribers

t.me/vidar_supwwlh

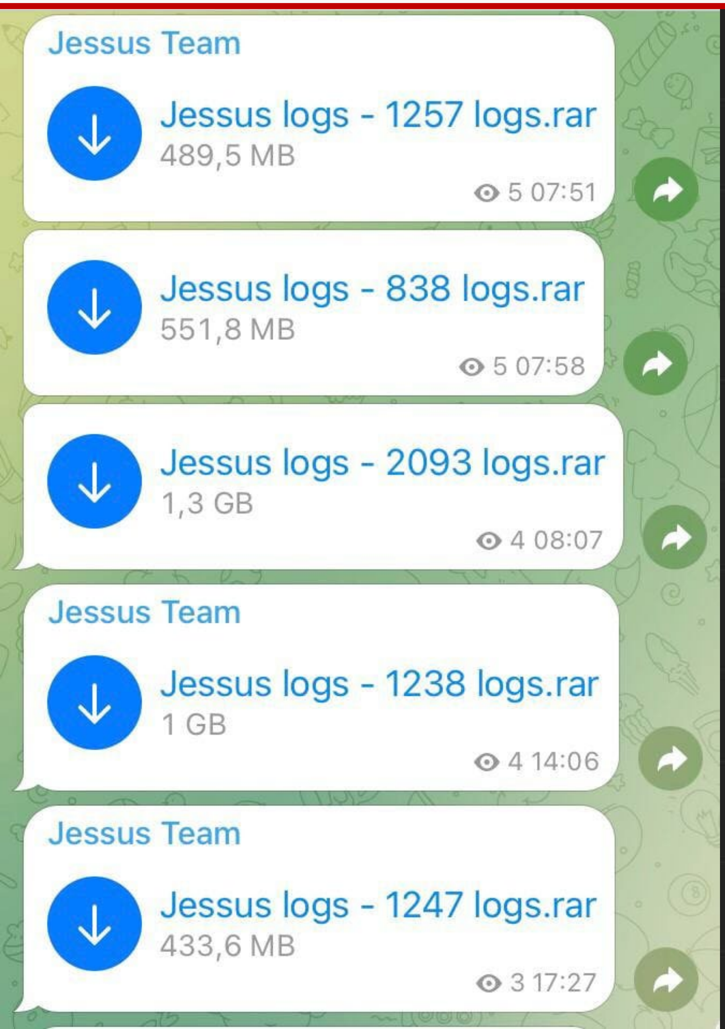
Link

Vidar

- available from: 11/2018
- owners:
- other info: 1642758 records on Russian Market
- Telegram channel: https://t.me/vidar_supwwlh

Telegram markets

- independent sellers
- go here https://github.com/fastfire/deepdarkCTI/blob/main/telegram.md and search for 'logs'



Jessus Team

Jessus logs - 1257 logs.rar
489,5 MB
5 07:51

Jessus logs - 838 logs.rar
551,8 MB
5 07:58

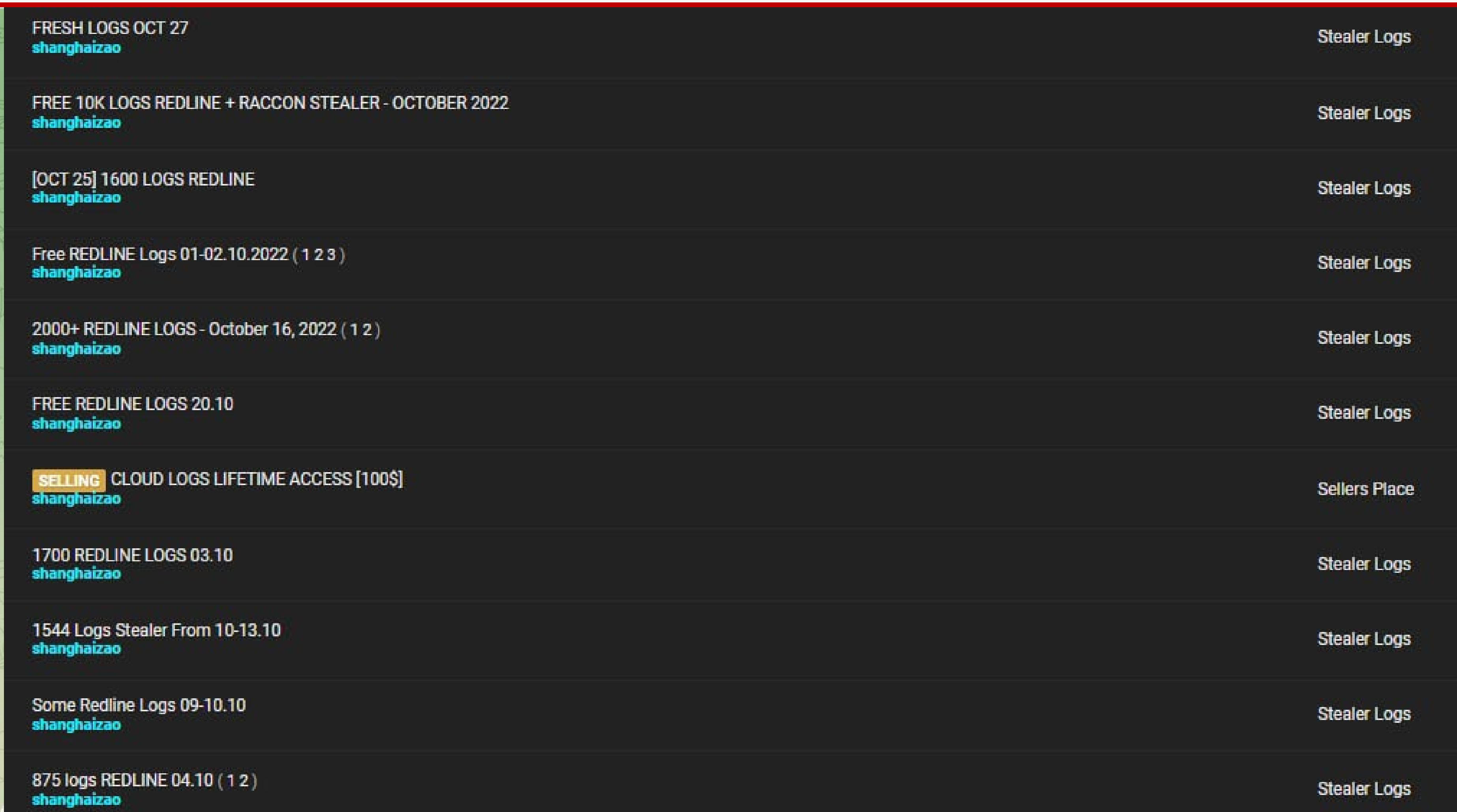
Jessus logs - 2093 logs.rar
1,3 GB
4 08:07

Jessus Team

Jessus logs - 1238 logs.rar
1 GB
4 14:06

Jessus Team

Jessus logs - 1247 logs.rar
433,6 MB
3 17:27



FRESH LOGS OCT 27
shanghaizao
Stealer Logs

FREE 10K LOGS REDLINE + RACCON STEALER - OCTOBER 2022
shanghaizao
Stealer Logs

[OCT 25] 1600 LOGS REDLINE
shanghaizao
Stealer Logs

Free REDLINE Logs 01-02.10.2022 (1 2 3)
shanghaizao
Stealer Logs

2000+ REDLINE LOGS - October 16, 2022 (1 2)
shanghaizao
Stealer Logs

FREE REDLINE LOGS 20.10
shanghaizao
Stealer Logs

SELLING CLOUD LOGS LIFETIME ACCESS [100$]
shanghaizao
Sellers Place

1700 REDLINE LOGS 03.10
shanghaizao
Stealer Logs

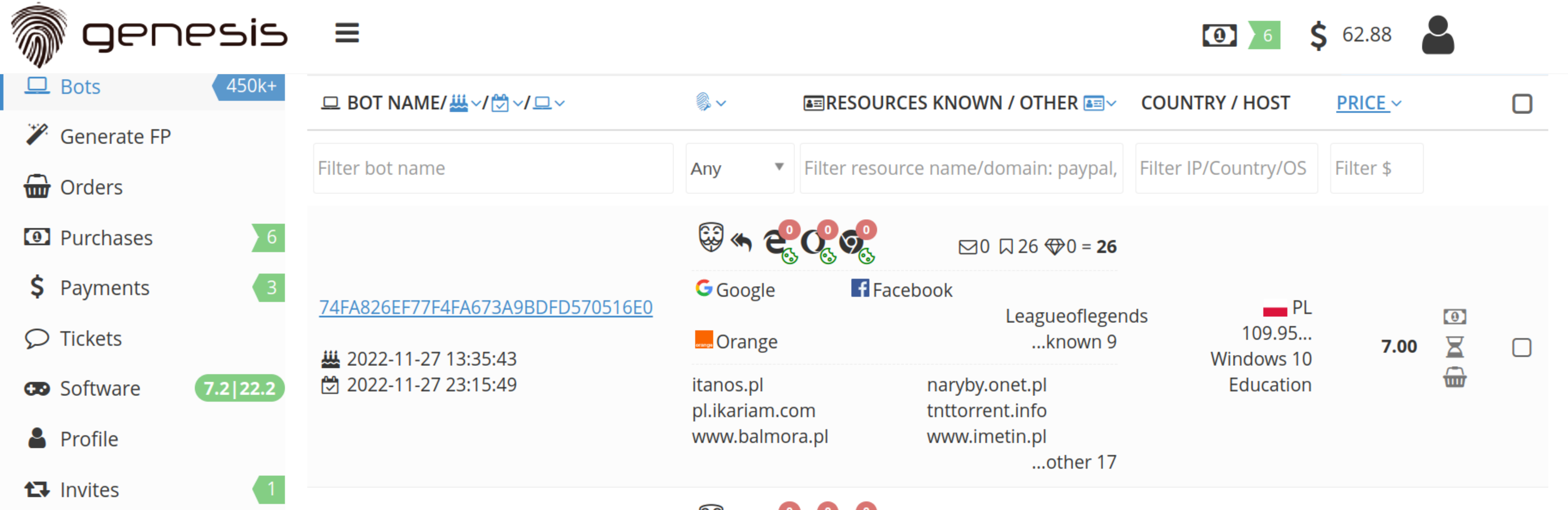
1544 Logs Stealer From 10-13.10
shanghaizao
Stealer Logs

Some Redline Logs 09-10.10
shanghaizao
Stealer Logs

875 logs REDLINE 04.10 (1 2)
shanghaizao
Stealer Logs

Genesis Market

- 450000 record
- invitation access
- sell only logs
- deposit available in: Bitcoin BTC, Litecoin LTC, Monero XMR, Dashs
- offer tools as Genesis Security Plugin & Genesium Browser
- log name format: 32 exadecimal chars (i.e. 7B034E8C77F92627192802CCCE2AB3DD.zip)
- can search for: bot name, name, domain, IP, country, OS, $
- available metadata: Links, Country, # of Resources, # of Browsers, Installed Date, Updated Date, Ip (first 2 triplets), Os, Price Usd
- Online Support



genesis ≡ 6 $ 62.88

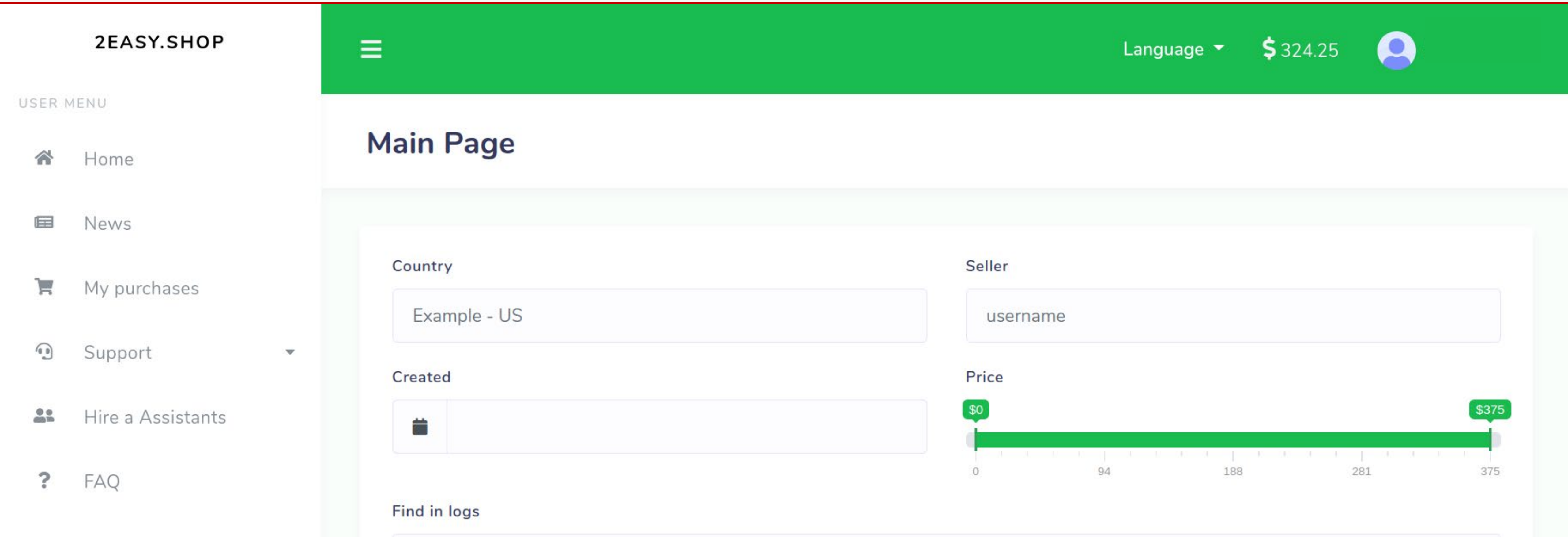
- Bots 450k+
- Generate FP
- Orders
- Purchases 6
- Payments 3
- Tickets
- Software 7.2|22.2
- Profile
- Invites 1

BOT NAME/ / /		RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE	□
Filter bot name	Any ▾	Filter resource name/domain: paypal,	Filter IP/Country/OS	Filter $	
74FA826EF77F4FA673A9BDFD570516E0 2022-11-27 13:35:43 2022-11-27 23:15:49	0 0 0	0 26 0 = 26 Google Facebook Orange Leagueoflegends ...known 9 itanos.pl naryby.onet.pl pl.ikariam.com tnttorrent.info www.balmora.pl www.imetin.pl ...other 17	PL 109.95... Windows 10 Education	7.00	□

2Easy Market

- 630000 record
- paid access
- sell only logs
- log name format: prefix+unique numbers chars (i.e. 2easy_logs_651587.zip)

- deposit available in: Bitcoin BTC, Bitcoincash BCH, Dash DASH, Dogecoin DOGE, Ethereum ETH, Ethereumclassic ETC, Litecoin LTC, Monero XMR, Zcash
- can search for: Seller, Date, Country, Wordavailable metadata: Links, Seller, Country, Installed Date, Price, Seller Rating
- Online Support + Telegram chat for updates



Main Page

Country: Example - US

Seller: username

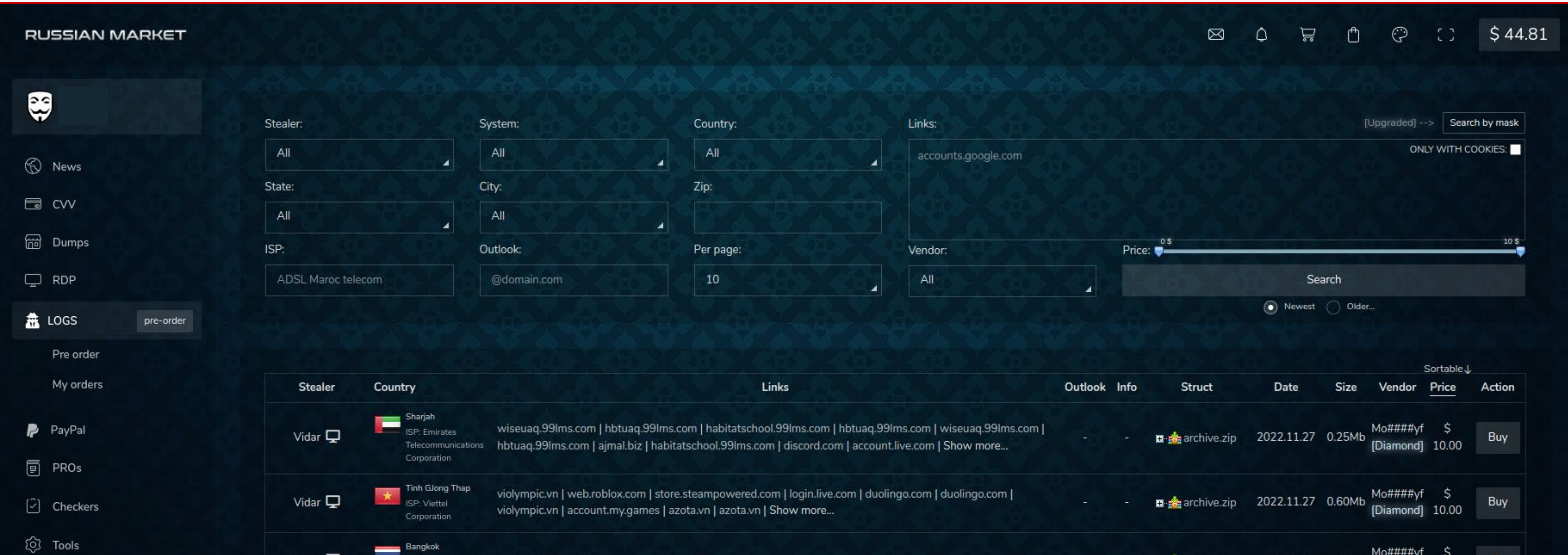
Created

Price

Find in logs

Russian Market

- 5000000 record
- paid access
- sell logs, RDP access, PayPal accounts, credit cards
- log name format: prefix+unique numbers chars (i.e. LOGID-5260493.zip)
- deposit available in: Bitcoin BTC, Ethereum ETH, Litecoin LTC
- can search for: stealer, state, ISP, System, City, Outlook, Country, Zip, Links
- available metadata: Links, Stealer, Country, Structure, Installed Date, Size, Vendor, Price UsdOnline Support



Stealer: All

System: All

Country: All

Links: accounts.google.com

ONLY WITH COOKIES: □

State: All

City: All

Zip:

ISP: ADSL Maroc telecom

Outlook: @domain.com

Per page: 10

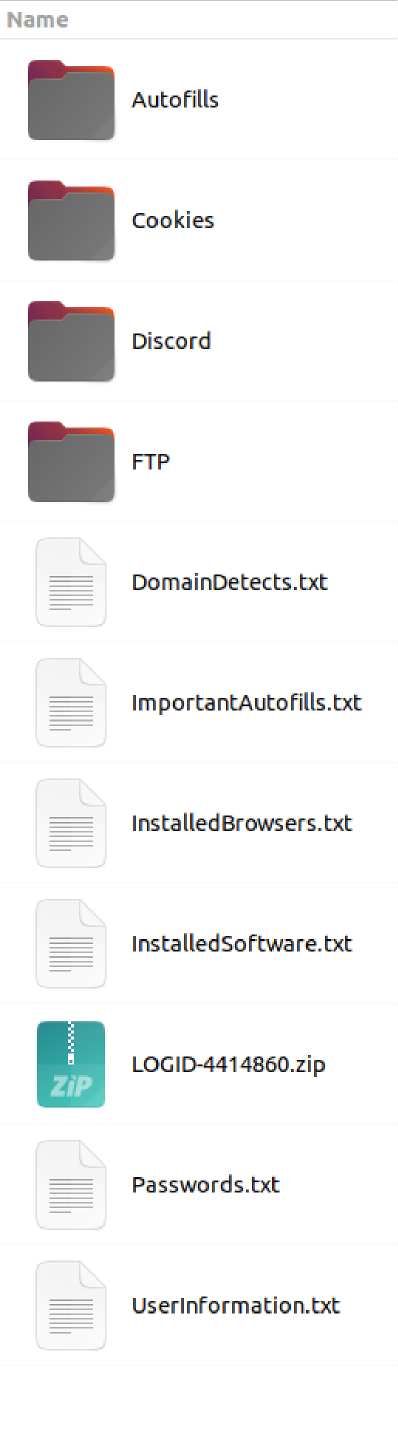
Vendor: All

Price: 0 $ – 10 $

● Newest ○ Older...

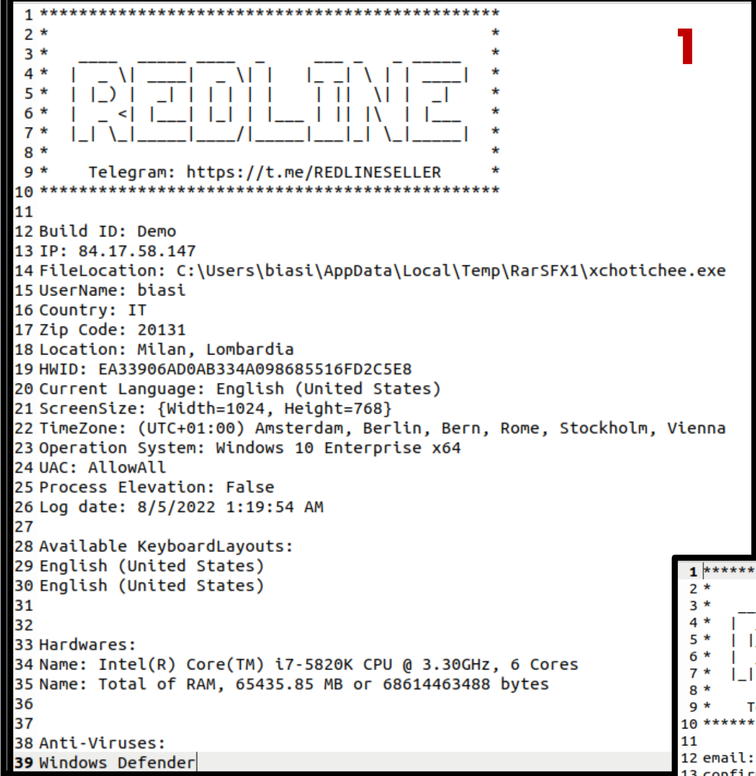
Sortable↓

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Vidar	Sharjah ISP: Emirates Telecommunications Corporation	wiseuaq.99lms.com | hbtuaq.99lms.com | habitatschool.99lms.com | hbtuaq.99lms.com | wiseuaq.99lms.com | hbtuaq.99lms.com | ajmal.biz | habitatschool.99lms.com | discord.com | account.live.com | Show more...	-	-	archive.zip	2022.11.27	0.25Mb	Mo####yf [Diamond]	$ 10.00	Buy
Vidar	Tinh GJong Thap ISP: Viettel Corporation	violympic.vn | web.roblox.com | store.steampowered.com | login.live.com | duolingo.com | duolingo.com | violympic.vn | account.my.games | azota.vn | azota.vn | Show more...	-	-	archive.zip	2022.11.27	0.60Mb	Mo####yf [Diamond]	$ 10.00	Buy
	Bangkok							Mo####yf	$	



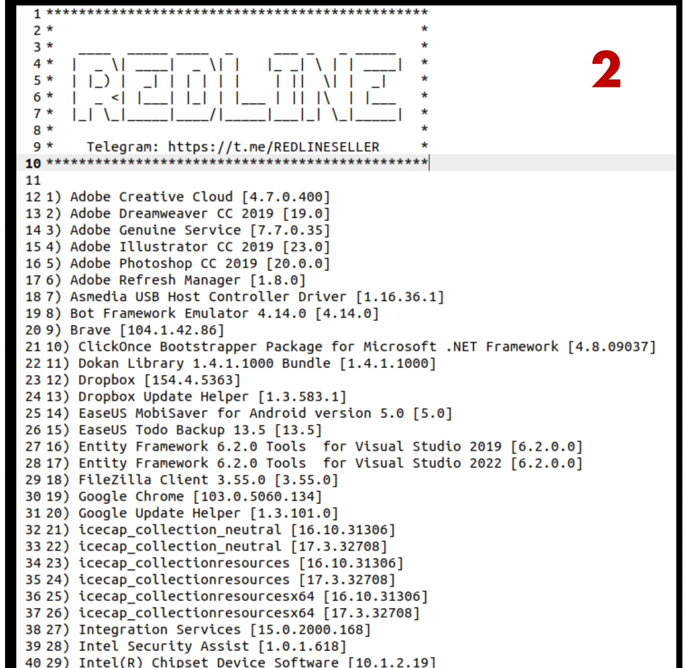
```
Name
Autofills
Cookies
Discord
FTP
DomainDetects.txt
ImportantAutofills.txt
InstalledBrowsers.txt
InstalledSoftware.txt
LOGID-4414860.zip
Passwords.txt
UserInformation.txt
```

1



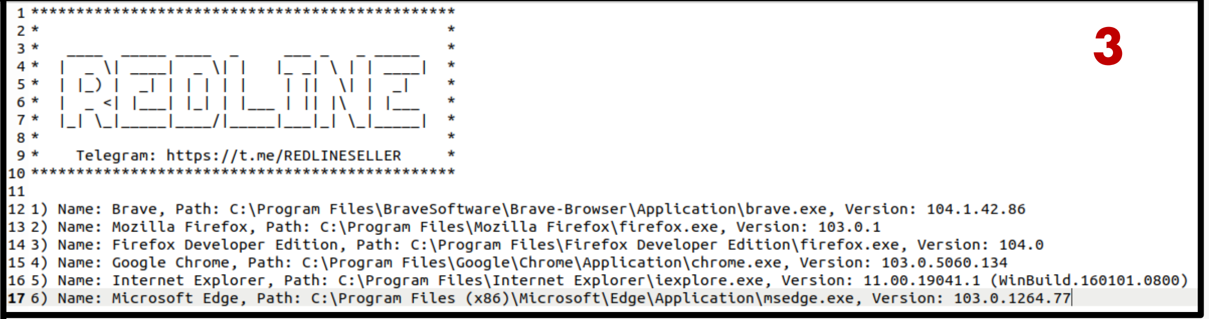
```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

Build ID: Demo
IP: 84.17.58.147
FileLocation: C:\Users\biasi\AppData\Local\Temp\RarSFX1\xchotichee.exe
UserName: biasi
Country: IT
Zip Code: 20131
Location: Milan, Lombardia
HWID: EA33906AD0AB334A098685516FD2C5E8
Current Language: English (United States)
ScreenSize: {Width=1024, Height=768}
TimeZone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Operation System: Windows 10 Enterprise x64
UAC: AllowAll
Process Elevation: False
Log date: 8/5/2022 1:19:54 AM

Available KeyboardLayouts:
English (United States)
English (United States)


Hardwares:
Name: Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz, 6 Cores
Name: Total of RAM, 65435.85 MB or 68614463488 bytes


Anti-Viruses:
Windows Defender
```

2



```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

1) Adobe Creative Cloud [4.7.0.400]
2) Adobe Dreamweaver CC 2019 [19.0]
3) Adobe Genuine Service [7.7.0.35]
4) Adobe Illustrator CC 2019 [23.0]
5) Adobe Photoshop CC 2019 [20.0.0]
6) Adobe Refresh Manager [1.8.0]
7) Asmedia USB Host Controller Driver [1.16.36.1]
8) Bot Framework Emulator 4.14.0 [4.14.0]
9) Brave [104.1.42.86]
10) ClickOnce Bootstrapper Package for Microsoft .NET Framework [4.8.09037]
11) Dokan Library 1.4.1.1000 Bundle [1.4.1.1000]
12) Dropbox [154.4.5363]
13) Dropbox Update Helper [1.3.583.1]
14) EaseUS MobiSaver for Android version 5.0 [5.0]
15) EaseUS Todo Backup 13.5 [13.5]
16) Entity Framework 6.2.0 Tools  for Visual Studio 2019 [6.2.0.0]
17) Entity Framework 6.2.0 Tools  for Visual Studio 2022 [6.2.0.0]
18) FileZilla Client 3.55.0 [3.55.0]
19) Google Chrome [103.0.5060.134]
20) Google Update Helper [1.3.101.0]
21) icecap_collection_neutral [16.10.31306]
22) icecap_collection_neutral [17.3.32708]
23) icecap_collectionresources [16.10.31306]
24) icecap_collectionresources [17.3.32708]
25) icecap_collectionresourcesx64 [16.10.31306]
26) icecap_collectionresourcesx64 [17.3.32708]
27) Integration Services [15.0.2000.168]
28) Intel Security Assist [1.0.1.618]
29) Intel(R) Chipset Device Software [10.1.2.19]
```

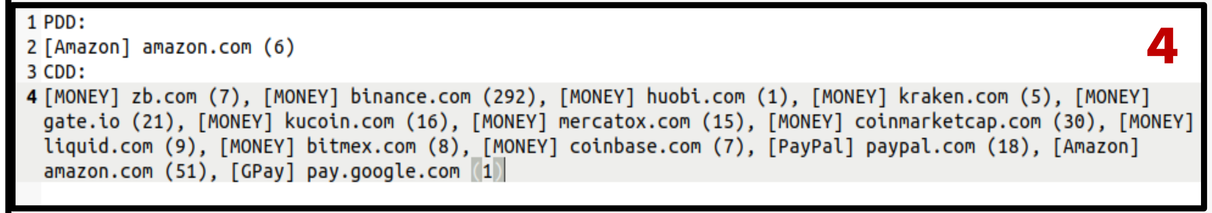
3



```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

1) Name: Brave, Path: C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe, Version: 104.1.42.86
2) Name: Mozilla Firefox, Path: C:\Program Files\Mozilla Firefox\firefox.exe, Version: 103.0.1
3) Name: Firefox Developer Edition, Path: C:\Program Files\Firefox Developer Edition\firefox.exe, Version: 104.0
4) Name: Google Chrome, Path: C:\Program Files\Google\Chrome\Application\chrome.exe, Version: 103.0.5060.134
5) Name: Internet Explorer, Path: C:\Program Files\Internet Explorer\iexplore.exe, Version: 11.00.19041.1 (WinBuild.160101.0800)
6) Name: Microsoft Edge, Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Version: 103.0.1264.77
```

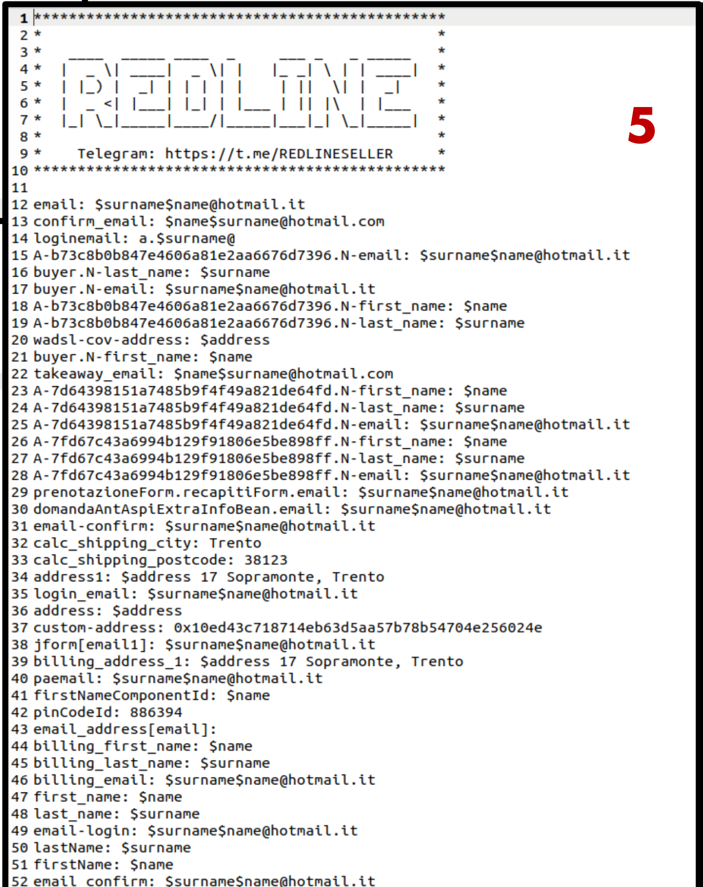
Log example

4



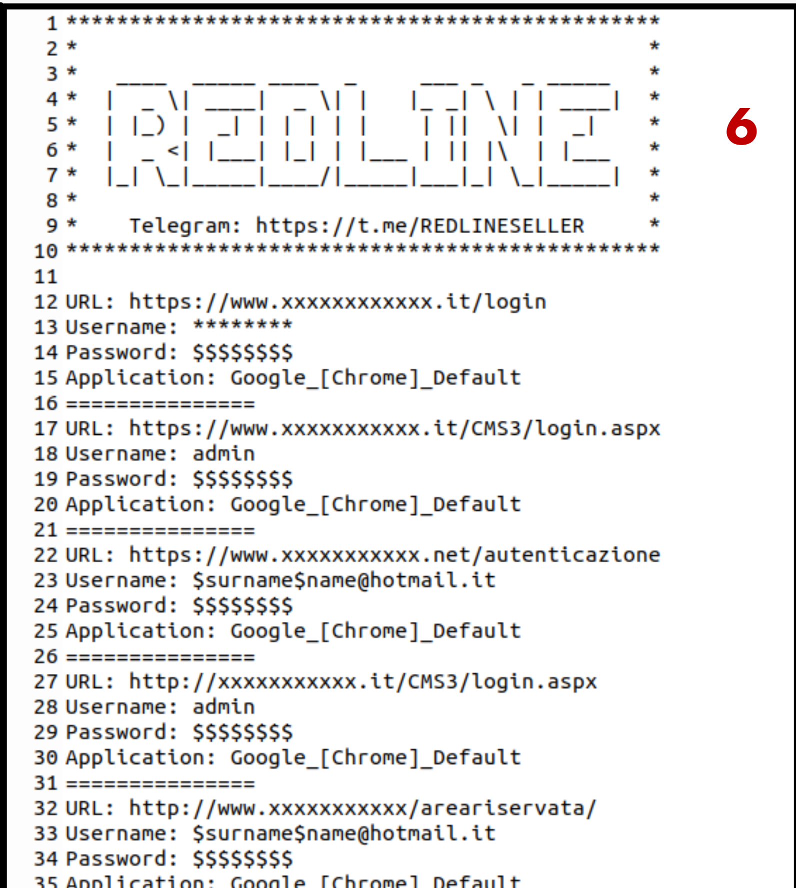
```
PDD:
[Amazon] amazon.com (6)
CDD:
[MONEY] zb.com (7), [MONEY] binance.com (292), [MONEY] huobi.com (1), [MONEY] kraken.com (5), [MONEY] gate.io (21), [MONEY] kucoin.com (16), [MONEY] mercatox.com (15), [MONEY] coinmarketcap.com (30), [MONEY] liquid.com (9), [MONEY] bitmex.com (8), [MONEY] coinbase.com (7), [PayPal] paypal.com (18), [Amazon] amazon.com (51), [GPay] pay.google.com (1)
```

5



```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

email: $surname$name@hotmail.it
confirm_email: $name$surname@hotmail.com
loginemail: a.$surname@
A-b73c8b0b847e4606a81e2aa6676d7396.N-email: $surname$name@hotmail.it
buyer.N-last_name: $surname
buyer.N-email: $surname$name@hotmail.it
A-b73c8b0b847e4606a81e2aa6676d7396.N-first_name: $name
A-b73c8b0b847e4606a81e2aa6676d7396.N-last_name: $surname
wadsl-cov-address: $address
buyer.N-first_name: $name
takeaway_email: $name$surname@hotmail.com
A-7d64398151a7485b9f4f49a821de64fd.N-first_name: $name
A-7d64398151a7485b9f4f49a821de64fd.N-last_name: $surname
A-7d64398151a7485b9f4f49a821de64fd.N-email: $surname$name@hotmail.it
A-7fd67c43a6994b129f91806e5be898ff.N-first_name: $name
A-7fd67c43a6994b129f91806e5be898ff.N-last_name: $surname
A-7fd67c43a6994b129f91806e5be898ff.N-email: $surname$name@hotmail.it
prenotazioneForm.recapitiForm.email: $surname$name@hotmail.it
domandaAntAspiExtraInfoBean.email: $surname$name@hotmail.it
email-confirm: $surname$name@hotmail.it
calc_shipping_city: Trento
calc_shipping_postcode: 38123
address1: $address 17 Sopramonte, Trento
login_email: $surname$name@hotmail.it
address: $address
custom-address: 0x10ed43c718714eb63d5aa57b78b54704e256024e
jform[email1]: $surname$name@hotmail.it
billing_address_1: $address 17 Sopramonte, Trento
paemail: $surname$name@hotmail.it
firstNameComponentId: $name
pinCodeId: 886394
email_address[email]:
billing_first_name: $name
billing_last_name: $surname
billing_email: $surname$name@hotmail.it
first_name: $name
last_name: $surname
email-login: $surname$name@hotmail.it
lastName: $surname
firstName: $name
email_confirm: $surname$name@hotmail.it
```

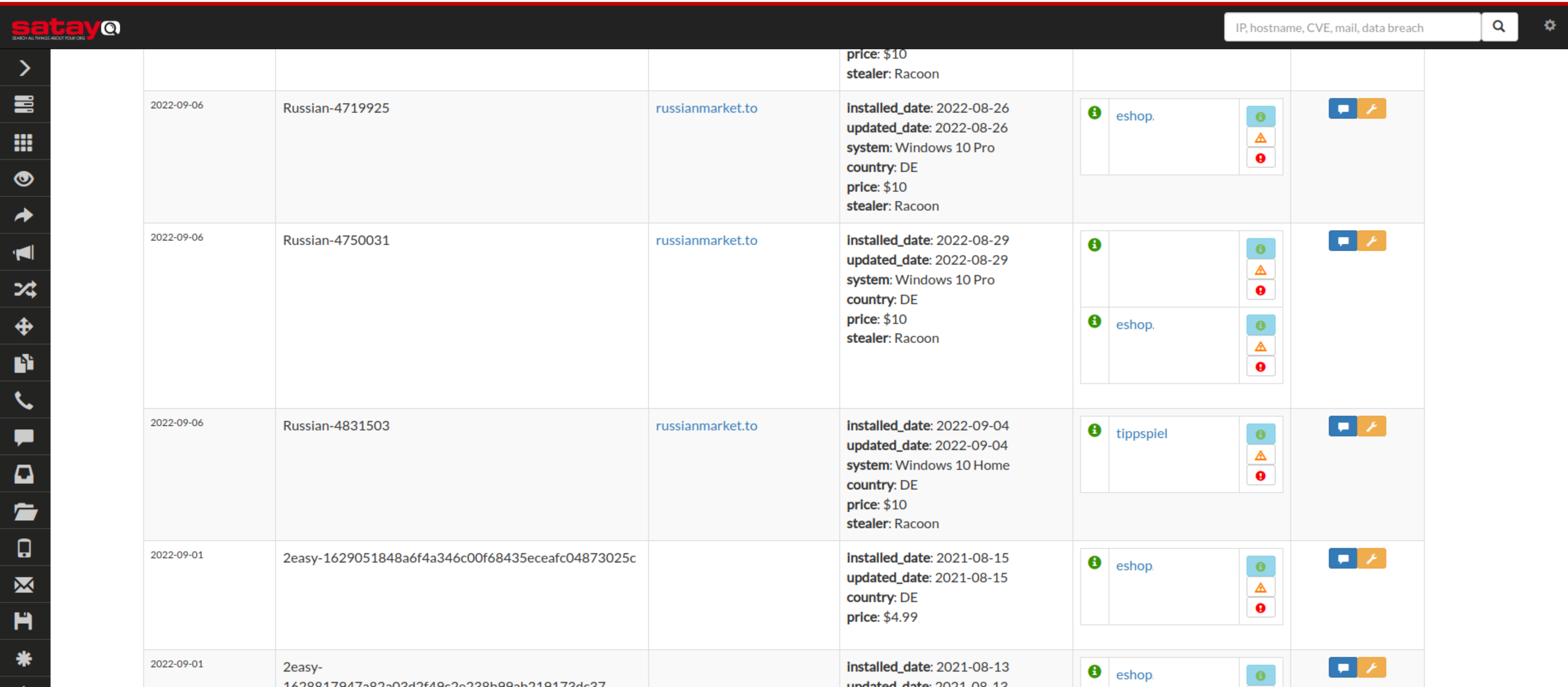
6



```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

URL: https://www.xxxxxxxxxxxx.it/login
Username: ********
Password: $$$$$$$$
Application: Google_[Chrome]_Default
===============
URL: https://www.xxxxxxxxxxx.it/CMS3/login.aspx
Username: admin
Password: $$$$$$$$
Application: Google_[Chrome]_Default
===============
URL: https://www.xxxxxxxxxxx.net/autenticazione
Username: $surname$name@hotmail.it
Password: $$$$$$$$
Application: Google_[Chrome]_Default
===============
URL: http://xxxxxxxxxxx.it/CMS3/login.aspx
Username: admin
Password: $$$$$$$$
Application: Google_[Chrome]_Default
===============
URL: http://www.xxxxxxxxxxx/areariservata/
Username: $surname$name@hotmail.it
Password: $$$$$$$$
Application: Google_[Chrome]_Default
```

SATAYO - markets scrapers

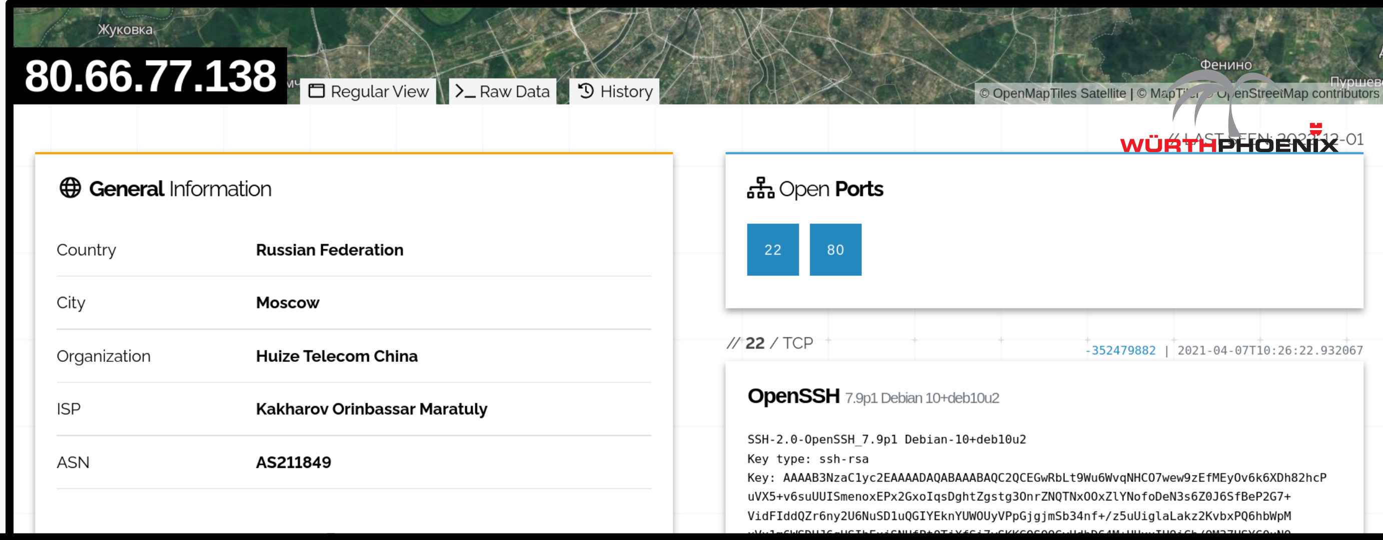
We have developed scrapers able to monitor the 3 major market places (Russian, 2Easy, Genesis)search in OPSEC mode


satayo
SEARCH ALL THINGS ABOUT YOUR ORG
IP, hostname, CVE, mail, data breach

			price: $10 **stealer**: Racoon		
2022-09-06	Russian-4719925	russianmarket.to	**installed_date**: 2022-08-26 **updated_date**: 2022-08-26 **system**: Windows 10 Pro **country**: DE **price**: $10 **stealer**: Racoon	eshop.	
2022-09-06	Russian-4750031	russianmarket.to	**installed_date**: 2022-08-29 **updated_date**: 2022-08-29 **system**: Windows 10 Pro **country**: DE **price**: $10 **stealer**: Racoon	eshop.	
2022-09-06	Russian-4831503	russianmarket.to	**installed_date**: 2022-09-04 **updated_date**: 2022-09-04 **system**: Windows 10 Home **country**: DE **price**: $10 **stealer**: Racoon	tippspiel	
2022-09-01	2easy-1629051848a6f4a346c00f68435eceafc04873025c		**installed_date**: 2021-08-15 **updated_date**: 2021-08-15 **country**: DE **price**: $4.99	eshop.	
2022-09-01	2easy-1628817947a82a03d2f49c2e238b99ab219173dc37		**installed_date**: 2021-08-13 **updated_date**: 2021-08-13	eshop.	

Traffers analysis

Open Shodan and search using this dork: http.html:"stealer"



80.66.77.138

General Information

Country	**Russian Federation**
City	**Moscow**
Organization	**Huize Telecom China**
ISP	**Kakharov Orinbassar Maratuly**
ASN	**AS211849**

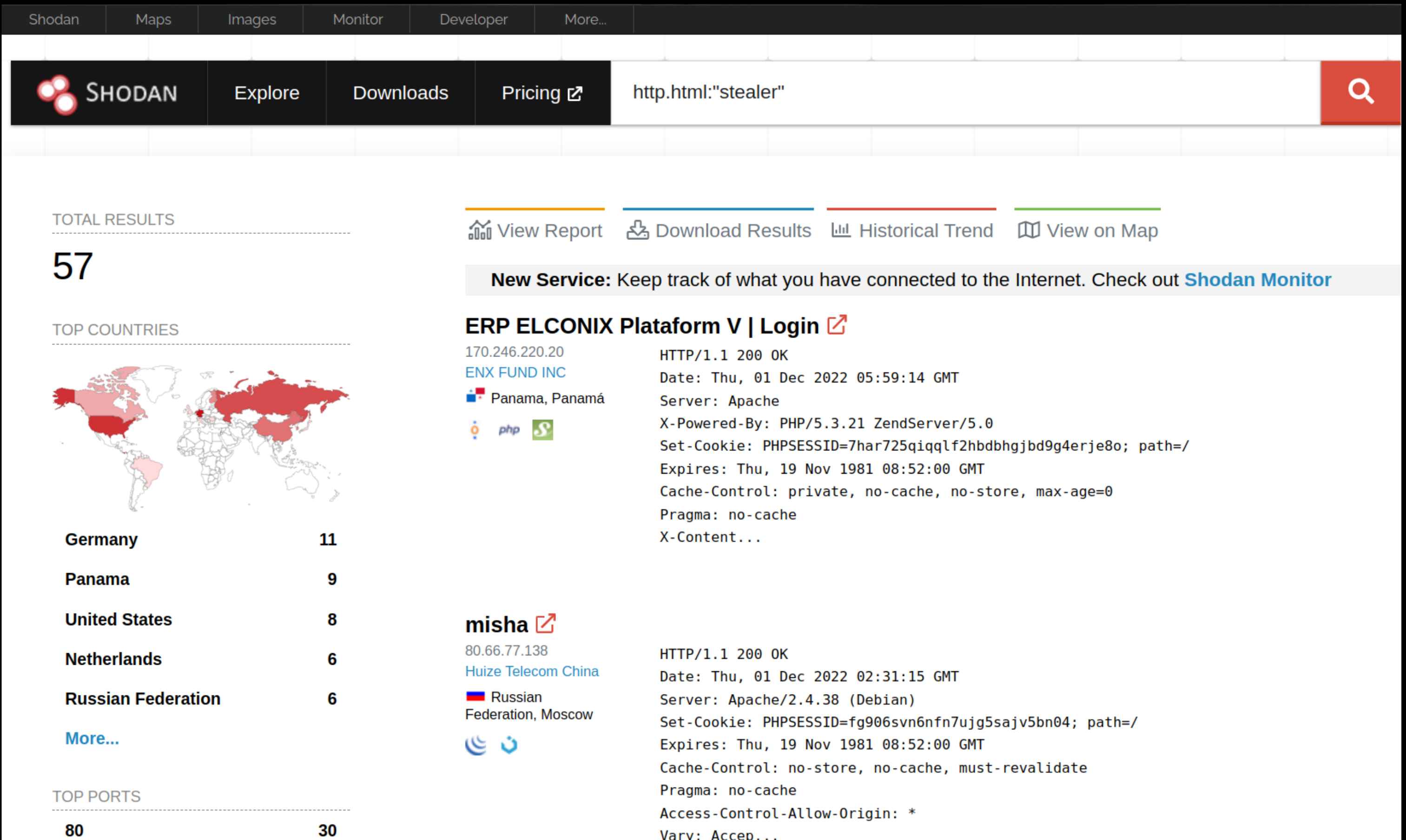
Open Ports

22 80

// **22** / TCP -352479882 | 2021-04-07T10:26:22.932067

OpenSSH 7.9p1 Debian 10+deb10u2

```
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC2QCEGwRbLt9Wu6WvqNHCO7wew9zEfMEyOv6k6XDh82hcP
uVX5+v6suUUISmenoxEPx2GxoIqsDghtZgstg3OnrZNQTNxOOxZlYNofoDeN3s6Z0J6SfBeP2G7+
VidFIddQZr6ny2U6NuSD1uQGIYEknYUWOUyVPpGjgjmSb34nf+/z5uUiglaLakz2KvbxPQ6hbWpM
```



http.html:"stealer"

TOTAL RESULTS

57

TOP COUNTRIES

Germany	11
Panama	9
United States	8
Netherlands	6
Russian Federation	6

More...

TOP PORTS

80	30

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

ERP ELCONIX Plataforma V | Login

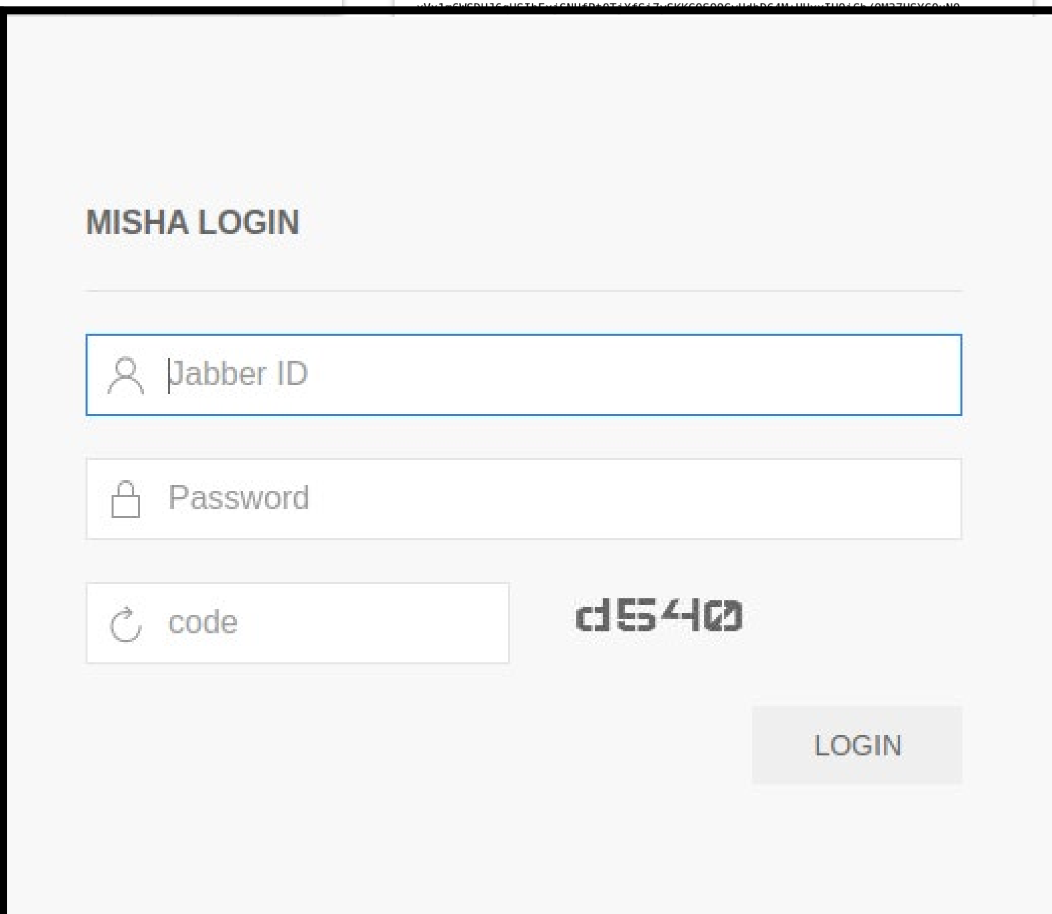
170.246.220.20
ENX FUND INC
Panama, Panamá

```
HTTP/1.1 200 OK
Date: Thu, 01 Dec 2022 05:59:14 GMT
Server: Apache
X-Powered-By: PHP/5.3.21 ZendServer/5.0
Set-Cookie: PHPSESSID=7har725qiqqlf2hbdbhgjbd9g4erje8o; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, no-cache, no-store, max-age=0
Pragma: no-cache
X-Content...
```

misha

80.66.77.138
Huize Telecom China
Russian Federation, Moscow

```
HTTP/1.1 200 OK
Date: Thu, 01 Dec 2022 02:31:15 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=fg906svn6nfn7ujg5sajv5bn04; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Vary: Accep...
```



MISHA LOGIN

Jabber ID

Password

code

d5540

LOGIN

info@wuerth-phoenix.com
www.wuerth-phoenix.com

WÜRTHPHOENIX

Thank you
Grazie Danke

#WEINNOVATE