CyOps Lighthouse: Vidar Stealer

cynet.com/blog/cyops-lighthouse-vidar-stealer/

January 12, 2023

The Darknet is home to many underground hacking forums. In these forums, cybercriminals talk freely: Sharing stories, tactics, success stories, and failures. Their conduct allows us to peek into the politics and ethics of those groups and actors, as they talk about recent activities.

CyOps Lighthouse aims to shed a light on those dark places. Apart from the underground forums, we will also provide information regarding ongoing ransomware groups' publications and worthy mentions from the last month.

Vidar Stealer – the attacker's perspective

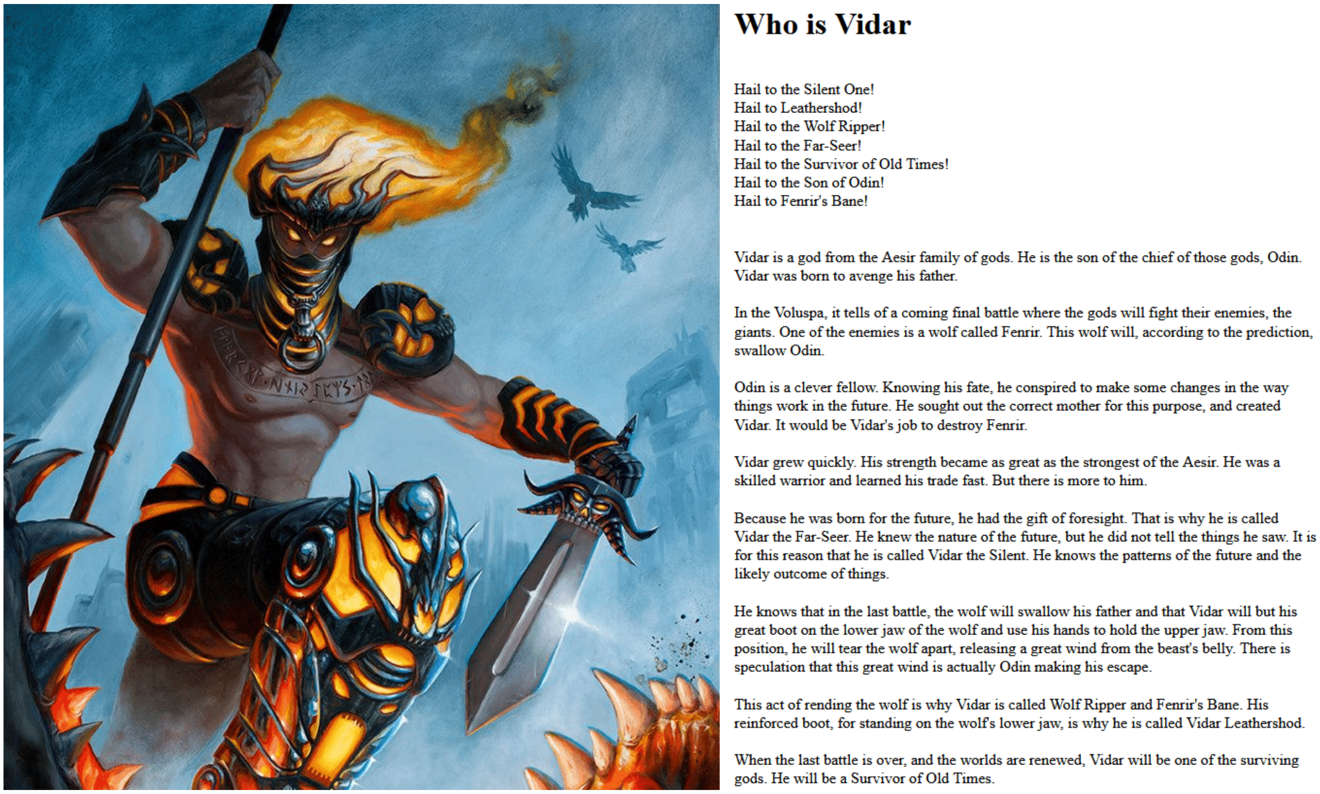
Executive summary:

Vidar stealer is a malware that is offered for sale in the MAAS (Malware as a service) model.

It is present since 2018, and it is a variant of the "Arkei stealer".
Vidar is currently one of the top stealers that are available for sale and is responsible for a large sum of compromised credentials offered for sale on underground forums and marketplaces.

Analysis:

Vidar stealer works as a MAAS, but unlike other stealers where buyers need to set their C2 and operate from it, all Vidar admin operations are done via a dedicated website, that can be accessed either with a dedicated Onion address or a regular “Clearnet” website, when entering the main URL we are greeted with the following:



Who is Vidar

Hail to the Silent One!
Hail to Leathershod!
Hail to the Wolf Ripper!
Hail to the Far-Seer!
Hail to the Survivor of Old Times!
Hail to the Son of Odin!
Hail to Fenrir's Bane!

Vidar is a god from the Aesir family of gods. He is the son of the chief of those gods, Odin. Vidar was born to avenge his father.

In the Voluspa, it tells of a coming final battle where the gods will fight their enemies, the giants. One of the enemies is a wolf called Fenrir. This wolf will, according to the prediction, swallow Odin.

Odin is a clever fellow. Knowing his fate, he conspired to make some changes in the way things work in the future. He sought out the correct mother for this purpose, and created Vidar. It would be Vidar's job to destroy Fenrir.

Vidar grew quickly. His strength became as great as the strongest of the Aesir. He was a skilled warrior and learned his trade fast. But there is more to him.

Because he was born for the future, he had the gift of foresight. That is why he is called Vidar the Far-Seer. He knew the nature of the future, but he did not tell the things he saw. It is for this reason that he is called Vidar the Silent. He knows the patterns of the future and the likely outcome of things.

He knows that in the last battle, the wolf will swallow his father and that Vidar will but his great boot on the lower jaw of the wolf and use his hands to hold the upper jaw. From this position, he will tear the wolf apart, releasing a great wind from the beast's belly. There is speculation that this great wind is actually Odin making his escape.

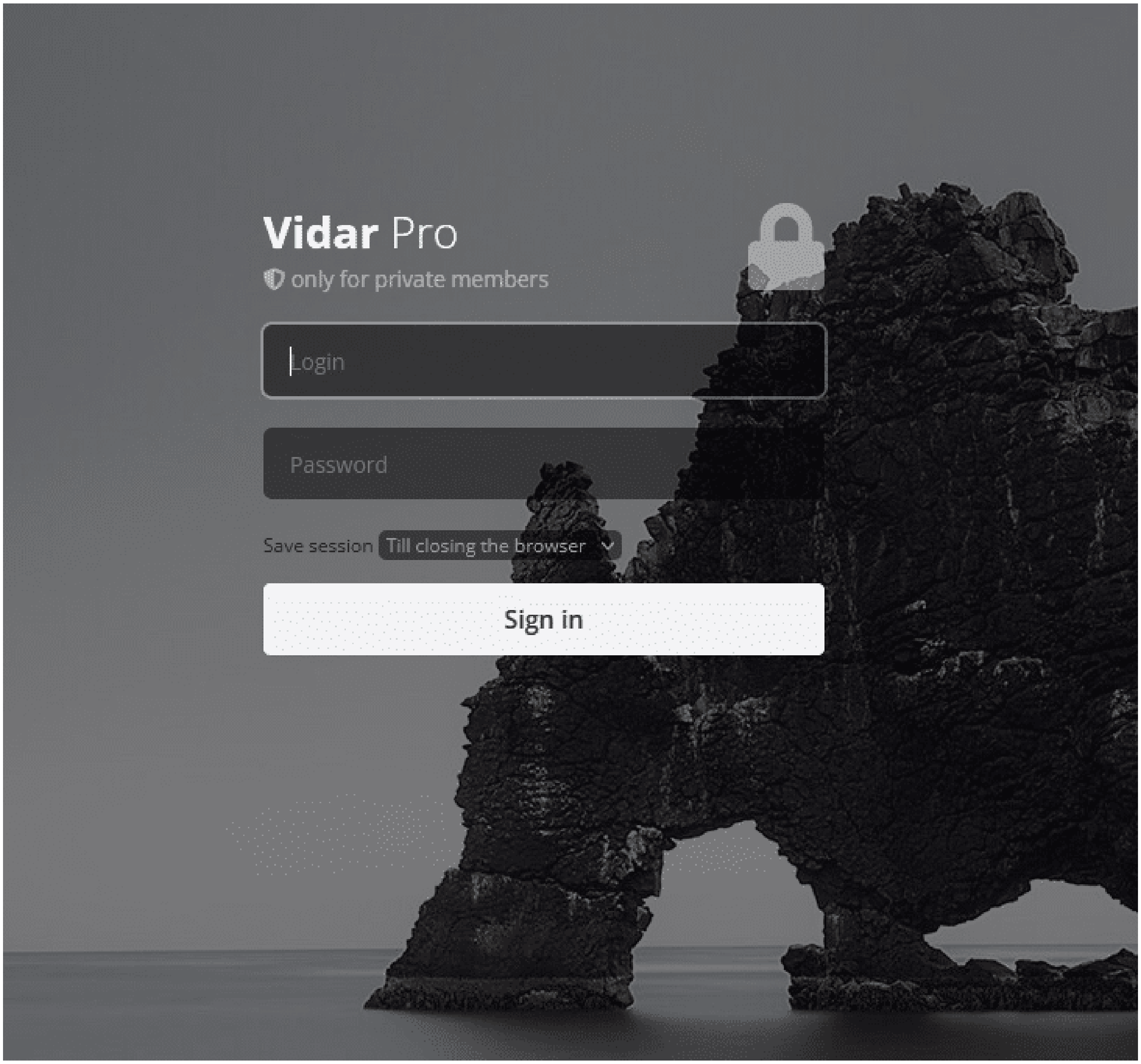
This act of rending the wolf is why Vidar is called Wolf Ripper and Fenrir's Bane. His reinforced boot, for standing on the wolf's lower jaw, is why he is called Vidar Leathershod.

When the last battle is over, and the worlds are renewed, Vidar will be one of the surviving gods. He will be a Survivor of Old Times.

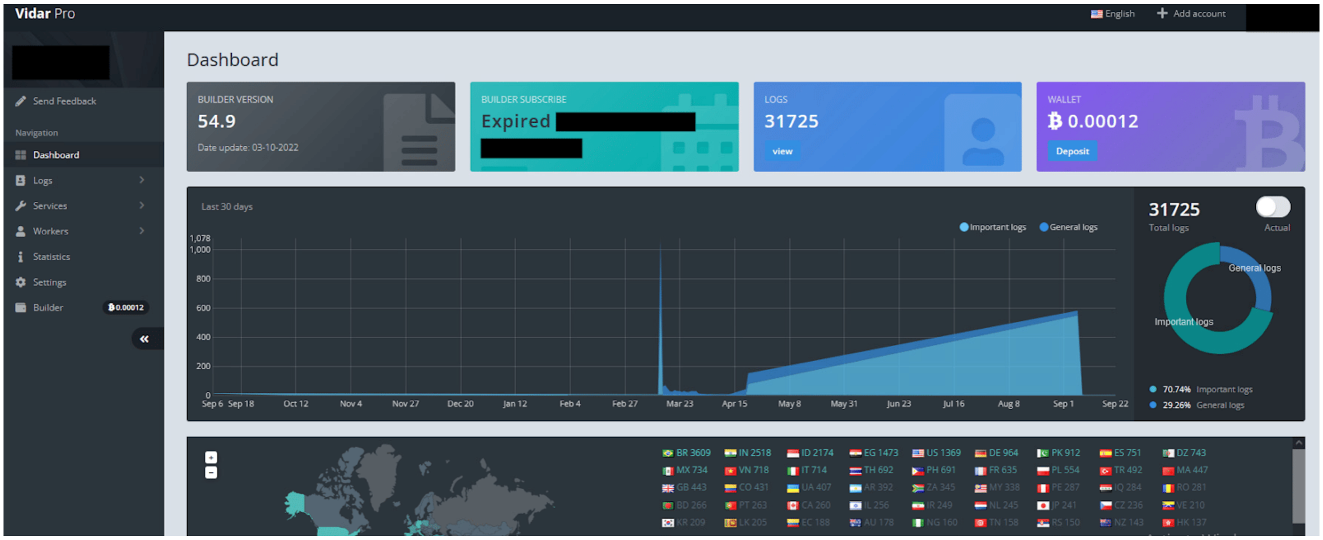
An ode to Vidar, son of Odin and the god of vengeance.

Once we add the “Login” prompt to the URL, we can see Vidar’s operator login page:

Upon successful login, we will be greeted with the main Vidar panel:



Save session Till closing the browser



[redacted]

[redacted]

Builder ฿0.00012

BUILDER VERSION 54.9
Date update: 03-10-2022

BUILDER SUBSCRIBE Expired [redacted]
[redacted]

LOGS 31725

WALLET ฿ 0.00012

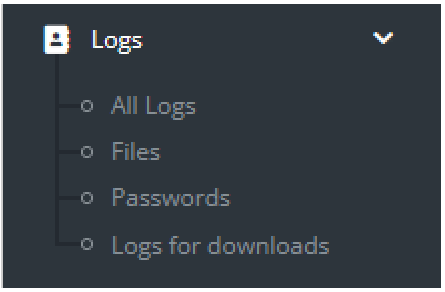
31725 Total logs

● 70.74% Important logs
● 29.26% General logs

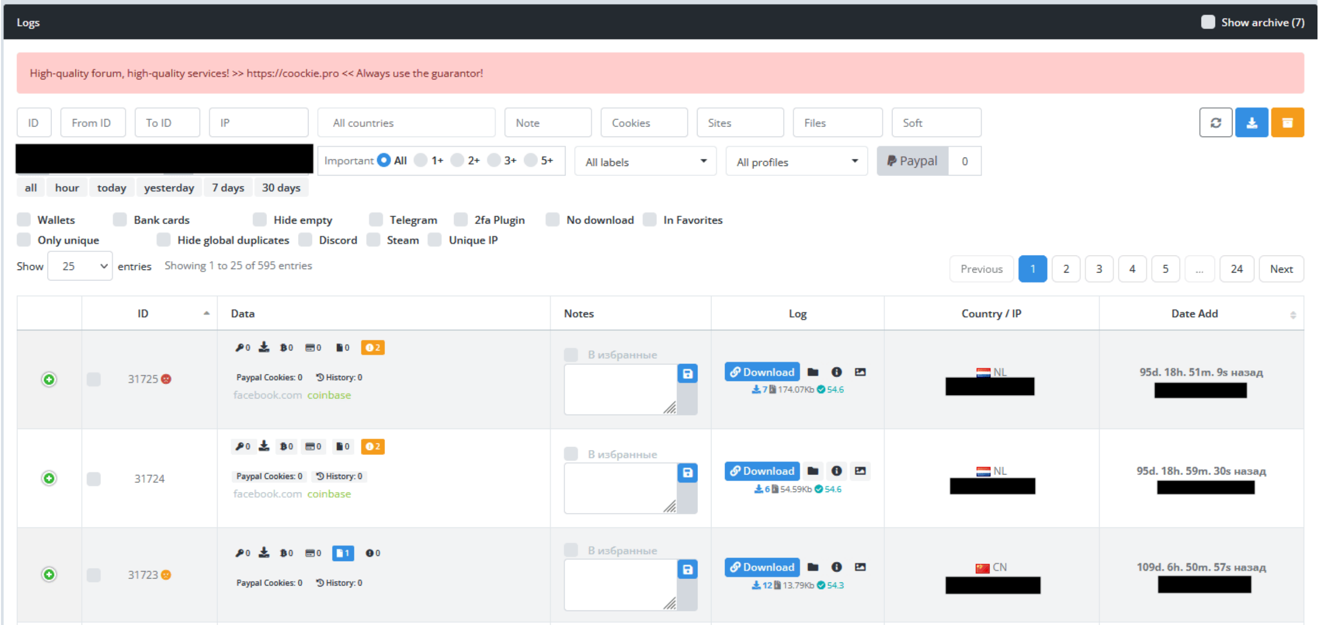
BR 3609	IN 2518	ID 2174	EG 1473	US 1369	DE 964	PK 912	ES 751	DZ 743
MX 734	VN 718	IT 714	TH 692	PH 691	FR 635	PL 554	TR 492	MA 447
GB 443	CO 431	UA 407	AR 392	ZA 345	MY 338	PE 287	IQ 284	RO 281
BD 266	PT 263	CA 260	IL 256	IR 249	NL 245	JP 241	CZ 236	VE 210
KR 209	LK 205	EC 188	AU 178	NG 160	TN 158	RS 150	NZ 143	HK 137

The default login will show us the "Dashboard", a summary of all the operations taken by the operator, the number of infected machines, geolocation, Builder version (Updates automatically), the current funds available at the crypto wallet, and all the stealers' options and possibilities on the left.

The "Logs" section is divided into several subcategories:



"All logs" is like the dashboard, it will show all logs in a given timeframe, with emphasis on the log contents:



Logs — □ Show archive (7)

High-quality forum, high-quality services! >> https://coockie.pro << Always use the guarantor!

ID | From ID | To ID | IP | All countries | Note | Cookies | Sites | Files | Soft

[redacted] Important ● All ○ 1+ ○ 2+ ○ 3+ ○ 5+ | All labels | All profiles | Paypal 0

all | hour | today | yesterday | 7 days | 30 days

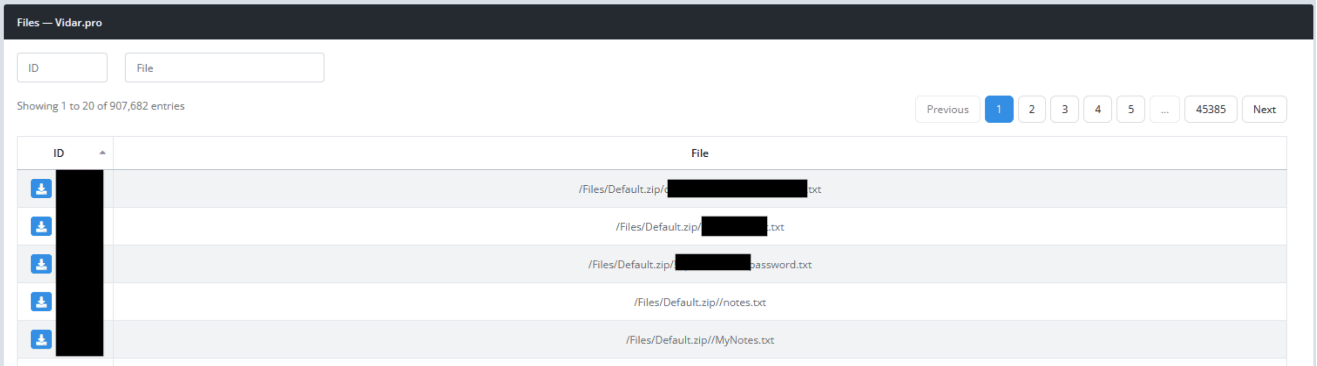
□ Wallets □ Bank cards □ Hide empty □ Telegram □ 2fa Plugin □ No download □ In Favorites
□ Only unique □ Hide global duplicates □ Discord □ Steam □ Unique IP

Show 25 entries Showing 1 to 25 of 595 entries

Previous 1 2 3 4 5 ... 24 Next

	ID	Data	Notes	Log	Country / IP	Date Add
⊕	□ 31725	0 B0 0 0 2 Paypal Cookies: 0 History: 0 facebook.com coinbase	□ В избранные	Download 7 174.07Kb 54.6	NL [redacted]	95d. 18h. 51m. 9s назад [redacted]
⊕	□ 31724	0 B0 0 0 2 Paypal Cookies: 0 History: 0 facebook.com coinbase	□ В избранные	Download 6 54.59Kb 54.6	NL [redacted]	95d. 18h. 59m. 30s назад [redacted]
⊕	□ 31723	0 B0 0 1 0 Paypal Cookies: 0 History: 0	□ В избранные	Download 12 13.79Kb 54.3	CN [redacted]	109d. 6h. 50m. 57s назад [redacted]

"Files" will show all files that were exfiltrated by the stealer:



Files — Vidar.pro

ID | File

Showing 1 to 20 of 907,682 entries

Previous 1 2 3 4 5 ... 45385 Next

ID	File
[redacted]	/Files/Default.zip/[redacted]txt
[redacted]	/Files/Default.zip/[redacted].txt
[redacted]	/Files/Default.zip/[redacted]assword.txt
[redacted]	/Files/Default.zip//notes.txt
[redacted]	/Files/Default.zip//MyNotes.txt

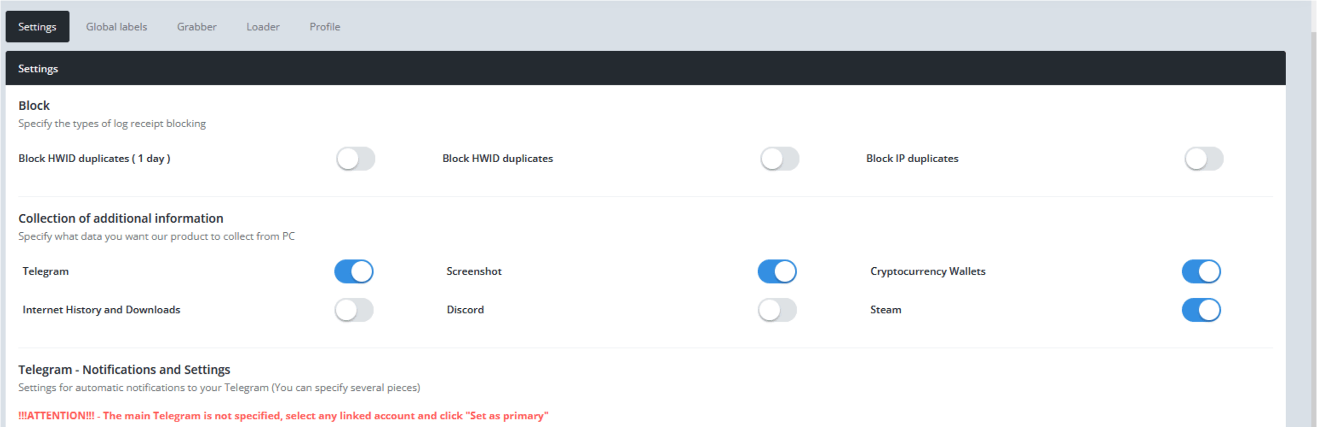
“Passwords” is self-explanatory, and “Logs for download” will show all logs that are ready for download.

As Vidar aims to be a “One stop shop”, it also provides the operators with a “Services” panel, where they can filter and sign in directly to any SMTP/Banking/Cpanels/WordPress websites that were found in the logs.

Moving over the “Workers” (Active bots) and “Statistics”, the settings panel is one of the most important assets of an operator.

Under the main page, an operator can decide what assets to target on the infected host, as well as set rules for “Grabber” – file exfiltration module, or “Loader” – set a rule for a follow-up activity on infected hosts.

Settings:



Settings

Block

Specify the types of log receipt blocking

Block HWID duplicates (1 day)	☐	Block HWID duplicates	☐	Block IP duplicates	☐

Collection of additional information

Specify what data you want our product to collect from PC

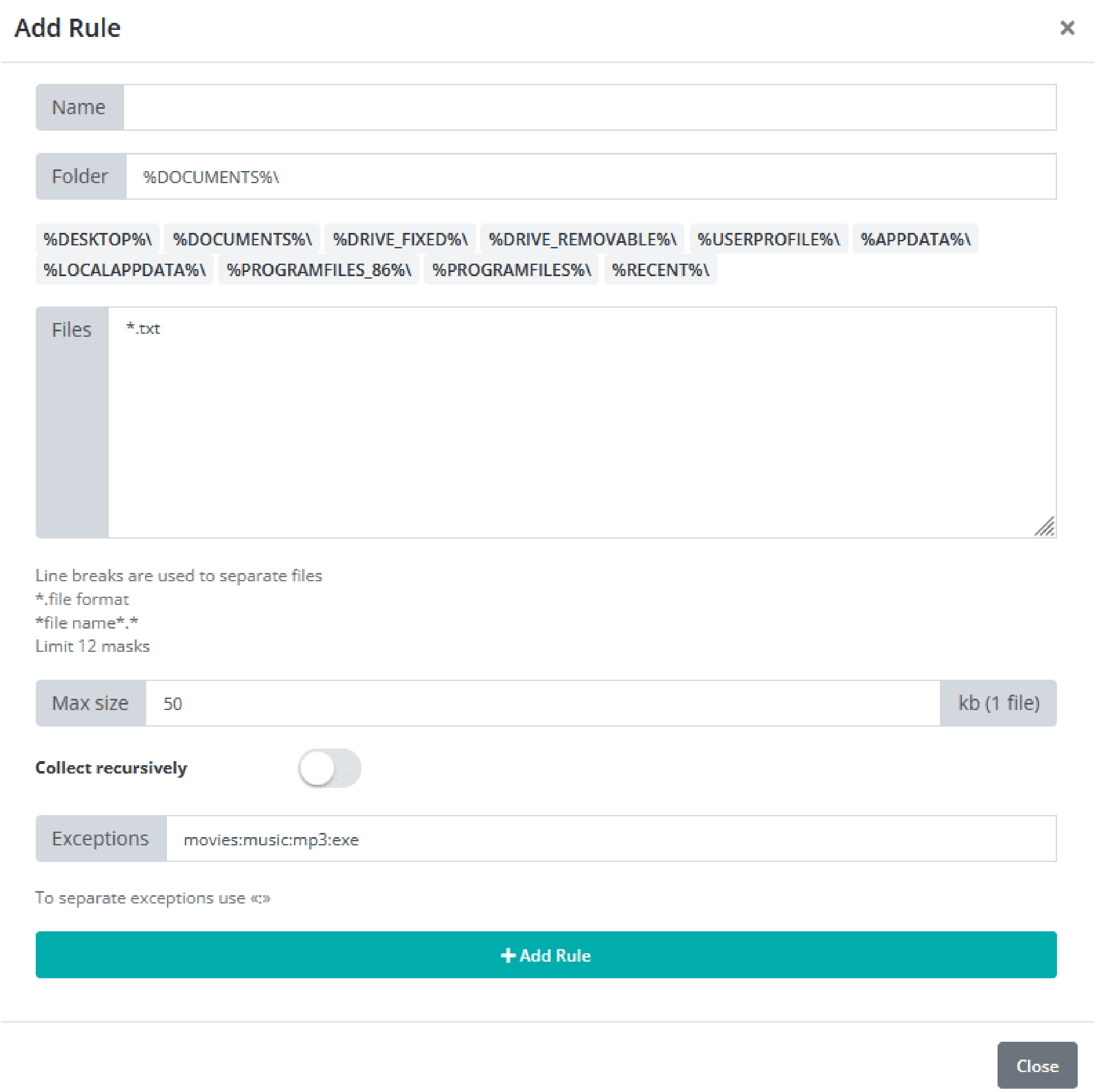
Telegram	☑	Screenshot	☑	Cryptocurrency Wallets	☑
Internet History and Downloads	☐	Discord	☐	Steam	☑

Telegram - Notifications and Settings

Settings for automatic notifications to your Telegram (You can specify several pieces)

!!!ATTENTION!!! - The main Telegram is not specified, select any linked account and click "Set as primary"

Grabber (Specify files type, max size, and folders to exfiltrate data):



Add Rule

Name

Folder: %DOCUMENTS%\

%DESKTOP%\ %DOCUMENTS%\ %DRIVE_FIXED%\ %DRIVE_REMOVABLE%\ %USERPROFILE%\ %APPDATA%\ %LOCALAPPDATA%\ %PROGRAMFILES_86%\ %PROGRAMFILES%\ %RECENT%\

Files: *.txt

Line breaks are used to separate files
*.file format
file name.*
Limit 12 masks

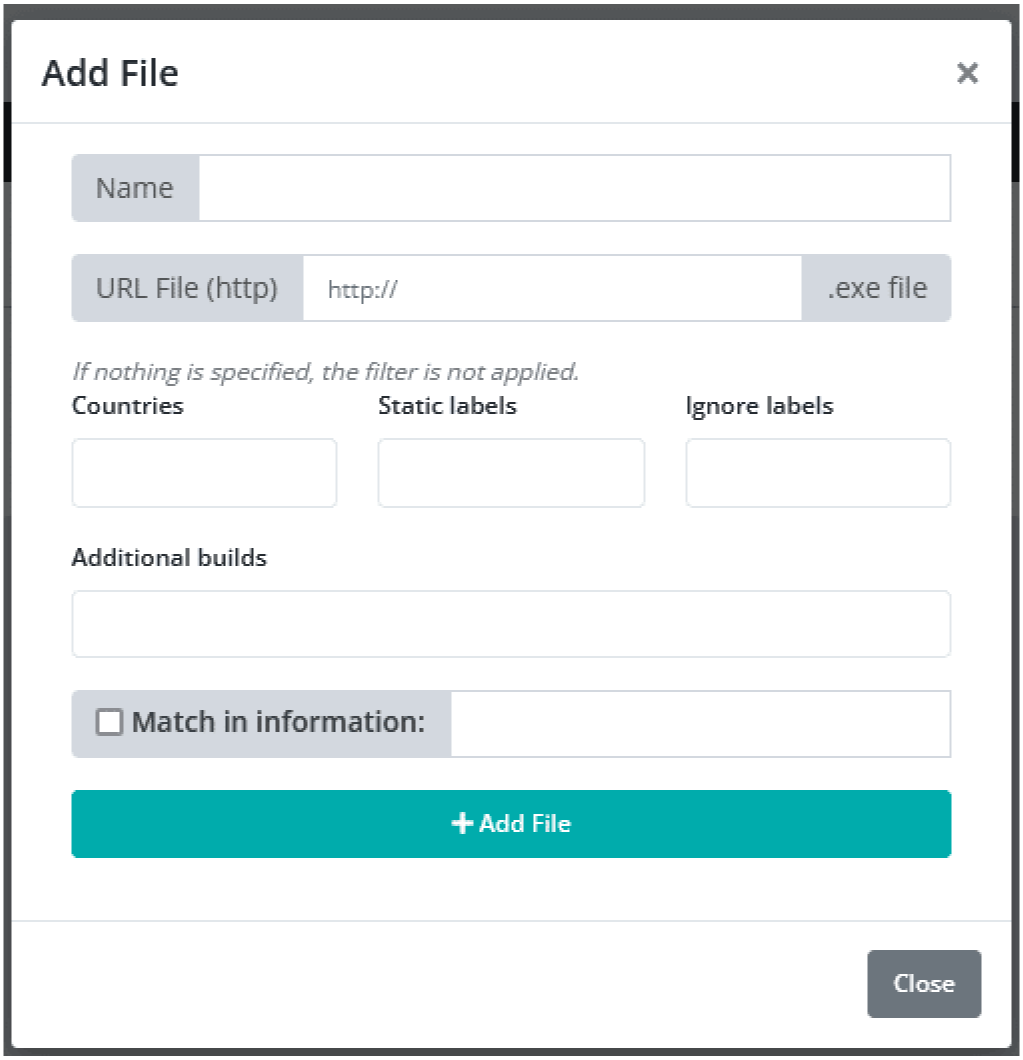
Max size: 50 kb (1 file)

Collect recursively: off

Exceptions: movies:music:mp3:exe

To separate exceptions use «:»

Loader:



Add File ×

Name

URL File (http) http:// .exe file

If nothing is specified, the filter is not applied.

Countries

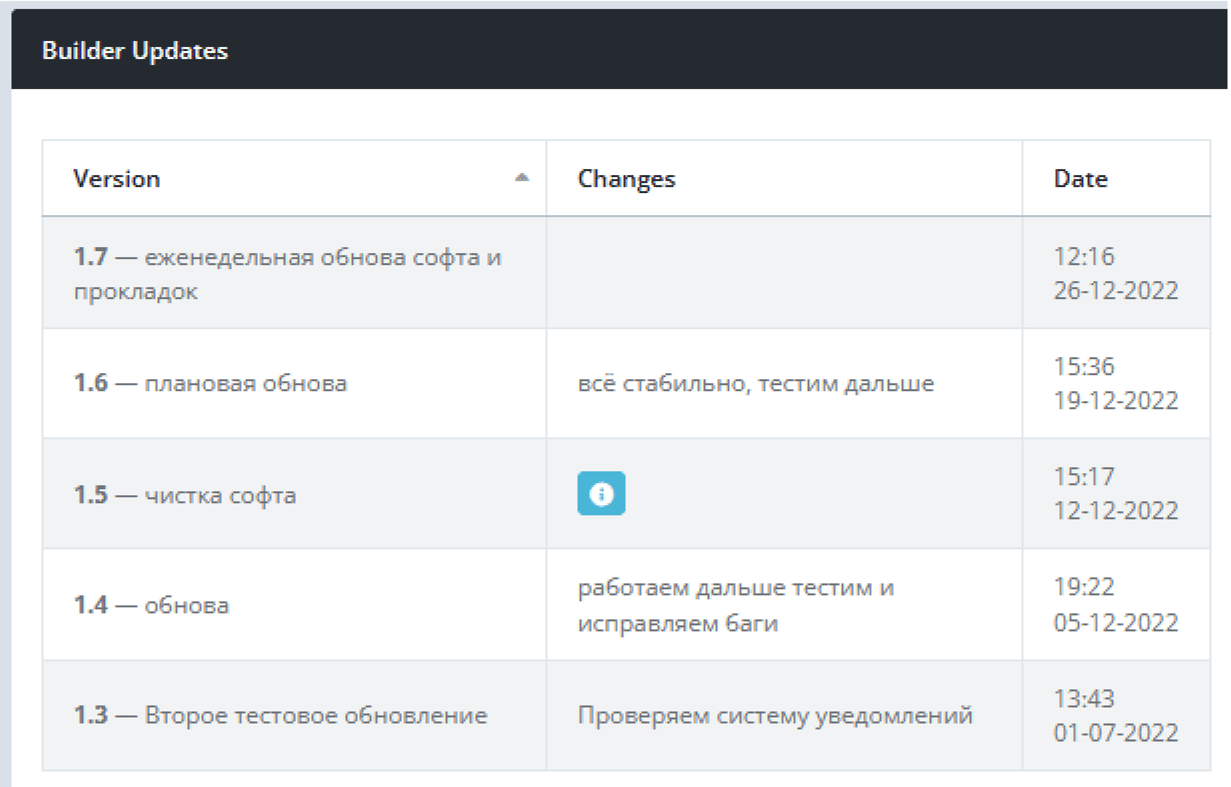
Static labels

Ignore labels

Additional builds

□ Match in information:

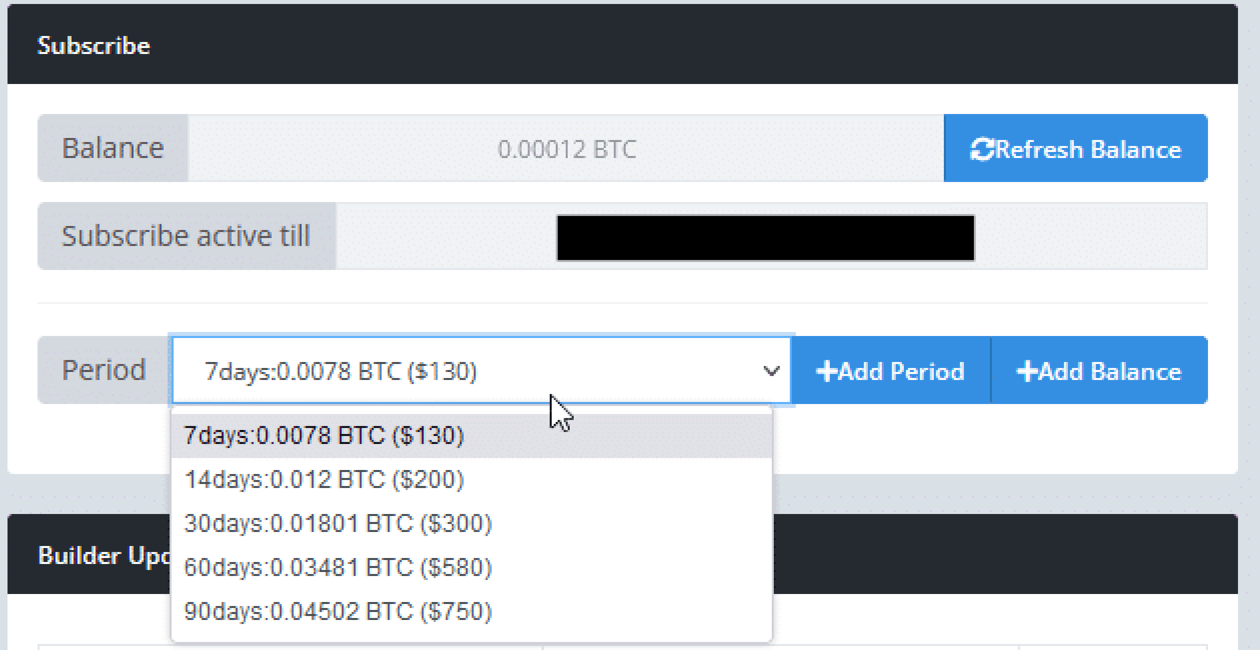
The “Builder” tab related to creating an executable from the panel, can be adjusted to set multiple running campaigns with different targets in mind, it also includes all the “Builder updates” – any constant updates that are pushed by the Vidar team:



Builder Updates

Version	Changes	Date
1.7 — еженедельная обнова софта и прокладок		12:16 26-12-2022
1.6 — плановая обнова	всё стабильно, тестим дальше	15:36 19-12-2022
1.5 — чистка софта	ℹ	15:17 12-12-2022
1.4 — обнова	работаем дальше тестим и исправляем баги	19:22 05-12-2022
1.3 — Второе тестовое обновление	Проверяем систему уведомлений	13:43 01-07-2022

The builder tab is also where operators activate their subscription, according to the required timeframe:



Subscribe

Balance 0.00012 BTC

Subscribe active till [redacted]

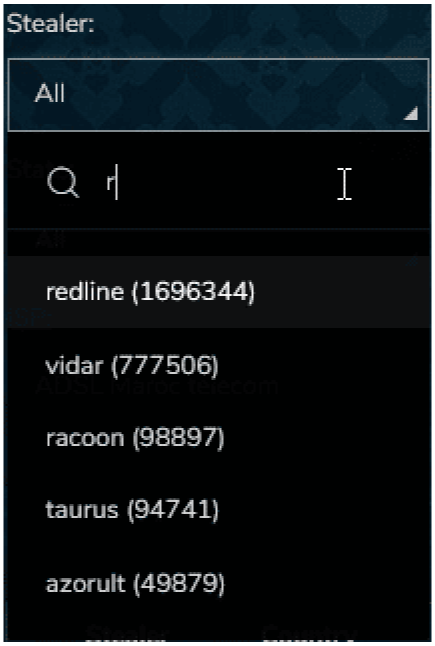
Period 7days:0.0078 BTC ($130)

Conclusion:

Vidar is among the top info stealers on the MAAS market.

It offers multiple “Follow up” activities as seen above, and all in the same Operator panel, this makes their pricing a bit higher than other info stealers, but as the operation is going for a long period, Vidar has already amassed a reputation of a reliable malware.

As we noticed in May 2022, Vidar is also one of the main sources for info stealer logs on underground markets like “Russian Marketplace”:



Stealer: All

r

redline (1696344)

vidar (777506)

racoon (98897)

taurus (94741)

azorult (49879)

Vidar, like other info stealers, is not “just” a stealer, it is responsible for most compromised credentials offered on the darknet and can also be used as a loader for Ransomware to follow up after a successful infection.

We strongly believe that unless an OPSEC mistake was to happen from the Vidar team, they will remain a top threat to reckon with in 2023.