Cybersecurity trends from dark web

Outpost24

Cybersecurity trends from dark web

- Victor Acin

- Working in cybersecurity since 2014
- Experience as:
  - Ethical hacker
  - Reverse engineering
  - Threat actor tracking

- Currently leading KrakenLabs
  - Team of 22 persons
  - Producing Threat Intelligence for our product and services

*Conference approved picture

Credential theft

> *A credential is evidence of who you are as a user, that will be used for authenticating your identity, and authorize access to a set of resources*

Credential theft - Introduction

- Phishing
- Vulnerabilities
- Brute-force attacks
- Malware
- DNS Hijacking
- Man-in-the-Middle
- Leaked databases
- Social engineering

Credential theft - Introduction

Phishing

Vulnerabilities

Brute-force attacks

Malware

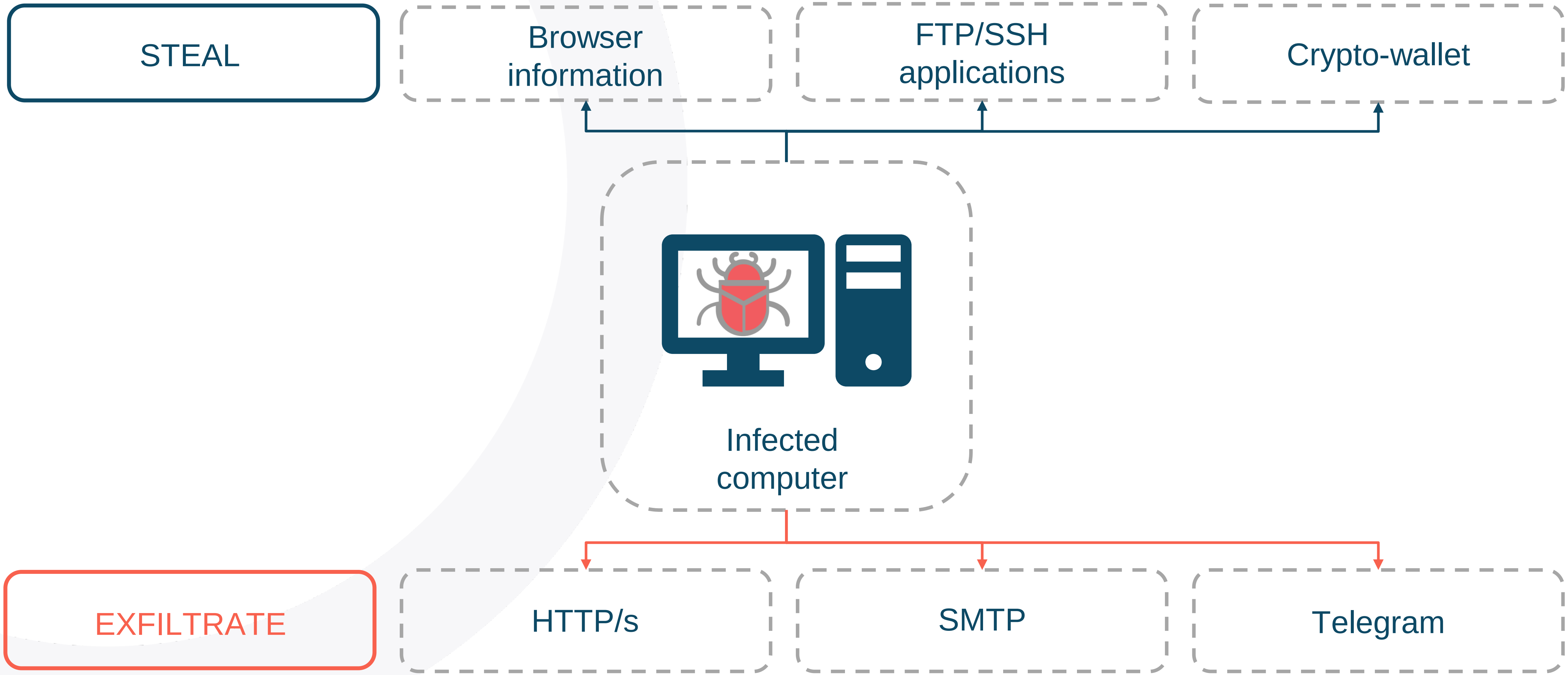
DNS Hijacking

Man-in-the-Middle

Leaked databases

Social engineering

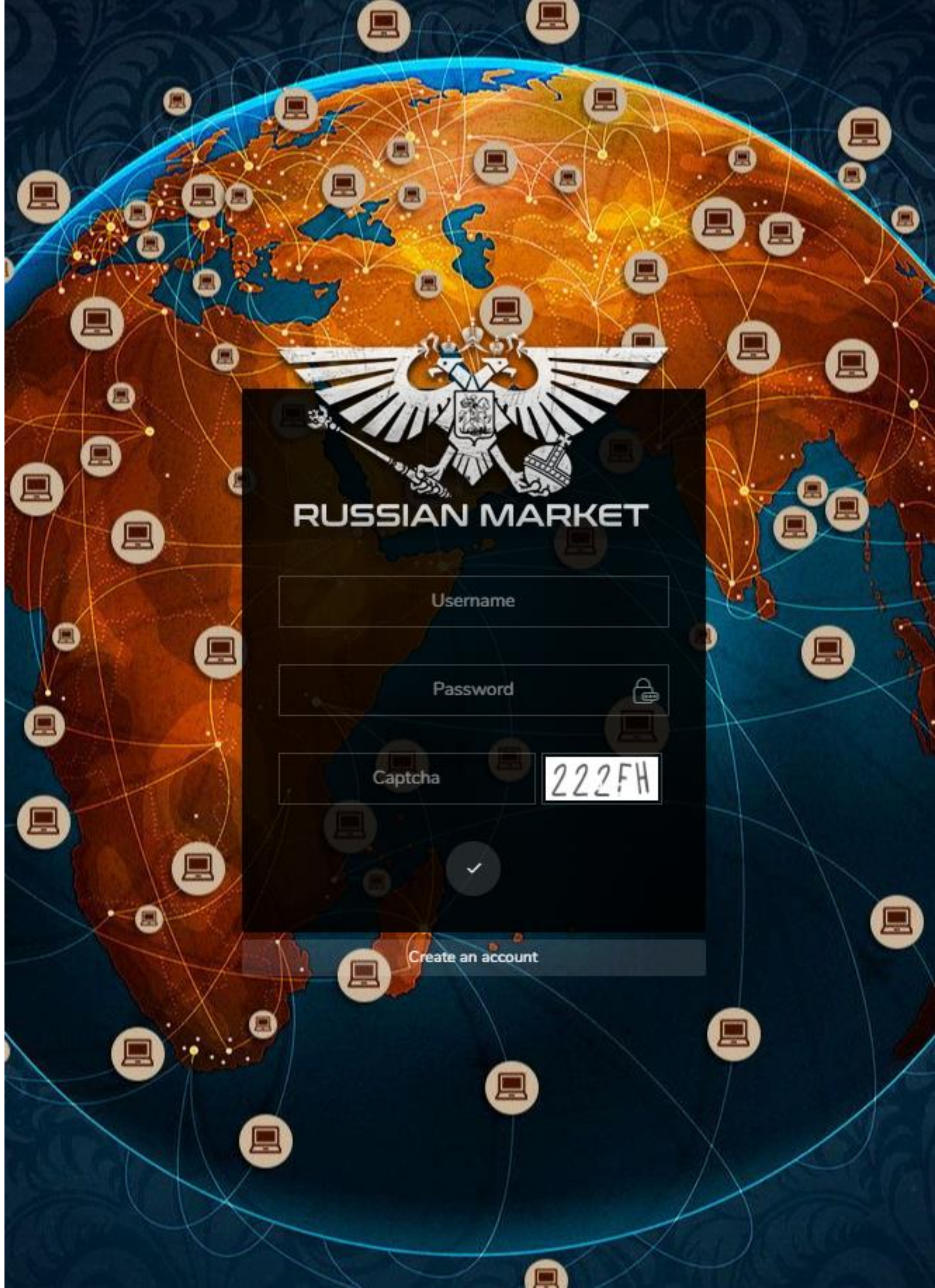
Credential theft - Introduction

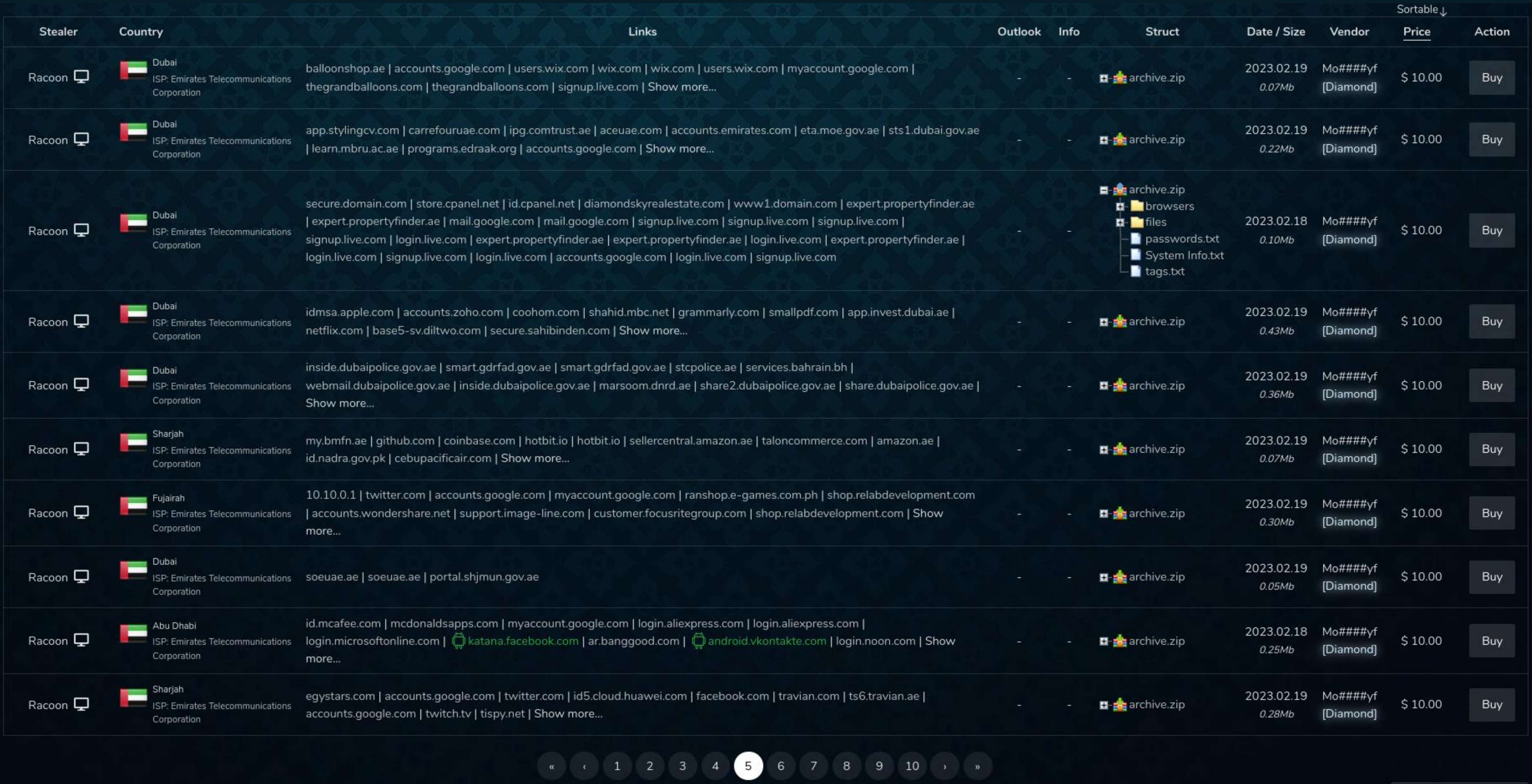


Credential theft - Introduction

Use for credentials

- Filtering of credentials
  - Look for interesting opportunities
- Give them for free
- Sell individual “infections”
- Sell in bulk





Sortable ↓

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Racoon	Dubai ISP: Emirates Telecommunications Corporation	balloonshop.ae | accounts.google.com | users.wix.com | wix.com | wix.com | users.wix.com | myaccount.google.com | thegrandballoons.com | thegrandballoons.com | signup.live.com | Show more...	-	-	archive.zip	2023.02.19 *0.07Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Dubai ISP: Emirates Telecommunications Corporation	app.stylingcv.com | carrefouruae.com | ipg.comtrust.ae | aceuae.com | accounts.emirates.com | eta.moe.gov.ae | sts1.dubai.gov.ae | learn.mbru.ac.ae | programs.edraak.org | accounts.google.com | Show more...	-	-	archive.zip	2023.02.19 *0.22Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Dubai ISP: Emirates Telecommunications Corporation	secure.domain.com | store.cpanel.net | id.cpanel.net | diamondskyrealestate.com | www1.domain.com | expert.propertyfinder.ae | expert.propertyfinder.ae | mail.google.com | mail.google.com | signup.live.com | signup.live.com | signup.live.com | signup.live.com | login.live.com | expert.propertyfinder.ae | expert.propertyfinder.ae | login.live.com | expert.propertyfinder.ae | login.live.com | signup.live.com | login.live.com | accounts.google.com | login.live.com | signup.live.com	-	-	archive.zip browsers files passwords.txt System Info.txt tags.txt	2023.02.18 *0.10Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Dubai ISP: Emirates Telecommunications Corporation	idmsa.apple.com | accounts.zoho.com | coohom.com | shahid.mbc.net | grammarly.com | smallpdf.com | app.invest.dubai.ae | netflix.com | base5-sv.diltwo.com | secure.sahibinden.com | Show more...	-	-	archive.zip	2023.02.19 *0.43Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Dubai ISP: Emirates Telecommunications Corporation	inside.dubaipolice.gov.ae | smart.gdrfad.gov.ae | smart.gdrfad.gov.ae | stcpolice.ae | services.bahrain.bh | webmail.dubaipolice.gov.ae | inside.dubaipolice.gov.ae | marsoom.dnrd.ae | share2.dubaipolice.gov.ae | share.dubaipolice.gov.ae | Show more...	-	-	archive.zip	2023.02.19 *0.36Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Sharjah ISP: Emirates Telecommunications Corporation	my.bmfn.ae | github.com | coinbase.com | hotbit.io | hotbit.io | sellercentral.amazon.ae | taloncommerce.com | amazon.ae | id.nadra.gov.pk | cebupacificair.com | Show more...	-	-	archive.zip	2023.02.19 *0.07Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Fujairah ISP: Emirates Telecommunications Corporation	10.10.0.1 | twitter.com | accounts.google.com | myaccount.google.com | ranshop.e-games.com.ph | shop.relabdevelopment.com | accounts.wondershare.net | support.image-line.com | customer.focusritegroup.com | shop.relabdevelopment.com | Show more...	-	-	archive.zip	2023.02.19 *0.30Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Dubai ISP: Emirates Telecommunications Corporation	soeuae.ae | soeuae.ae | portal.shjmun.gov.ae	-	-	archive.zip	2023.02.19 *0.05Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Abu Dhabi ISP: Emirates Telecommunications Corporation	id.mcafee.com | mcdonaldsapps.com | myaccount.google.com | login.aliexpress.com | login.aliexpress.com | login.microsoftonline.com | katana.facebook.com | ar.banggood.com | android.vkontakte.com | login.noon.com | Show more...	-	-	archive.zip	2023.02.18 *0.25Mb*	Mo####yf [Diamond]	$ 10.00	Buy
Racoon	Sharjah ISP: Emirates Telecommunications Corporation	egystars.com | accounts.google.com | twitter.com | id5.cloud.huawei.com | facebook.com | travian.com | ts6.travian.ae | accounts.google.com | twitch.tv | tispy.net | Show more...	-	-	archive.zip	2023.02.19 *0.28Mb*	Mo####yf [Diamond]	$ 10.00	Buy

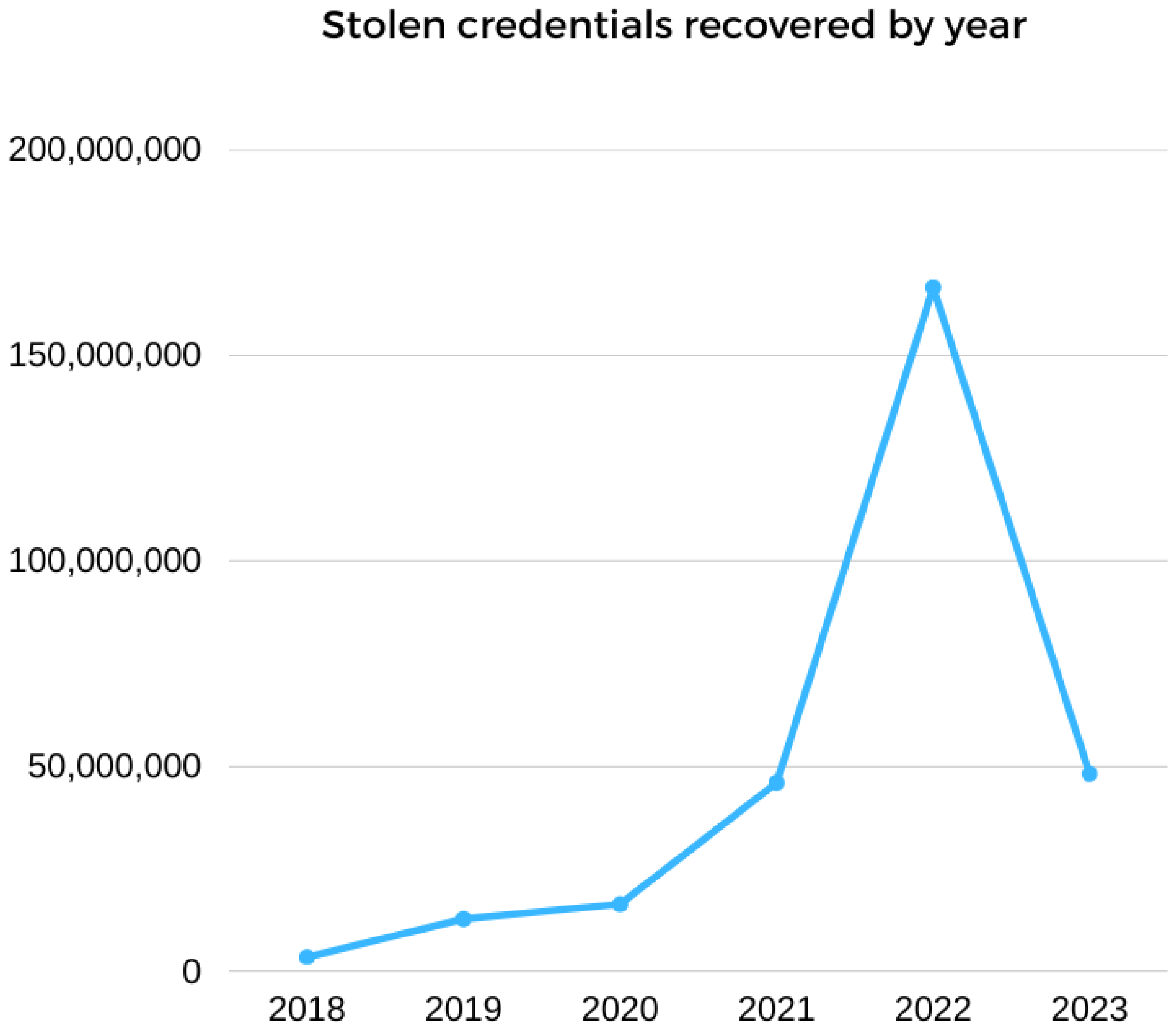
Credential theft - Introduction

Total number of recovered credentials:

- ~300.000.000

Change in methodology

- Industrialize and scale

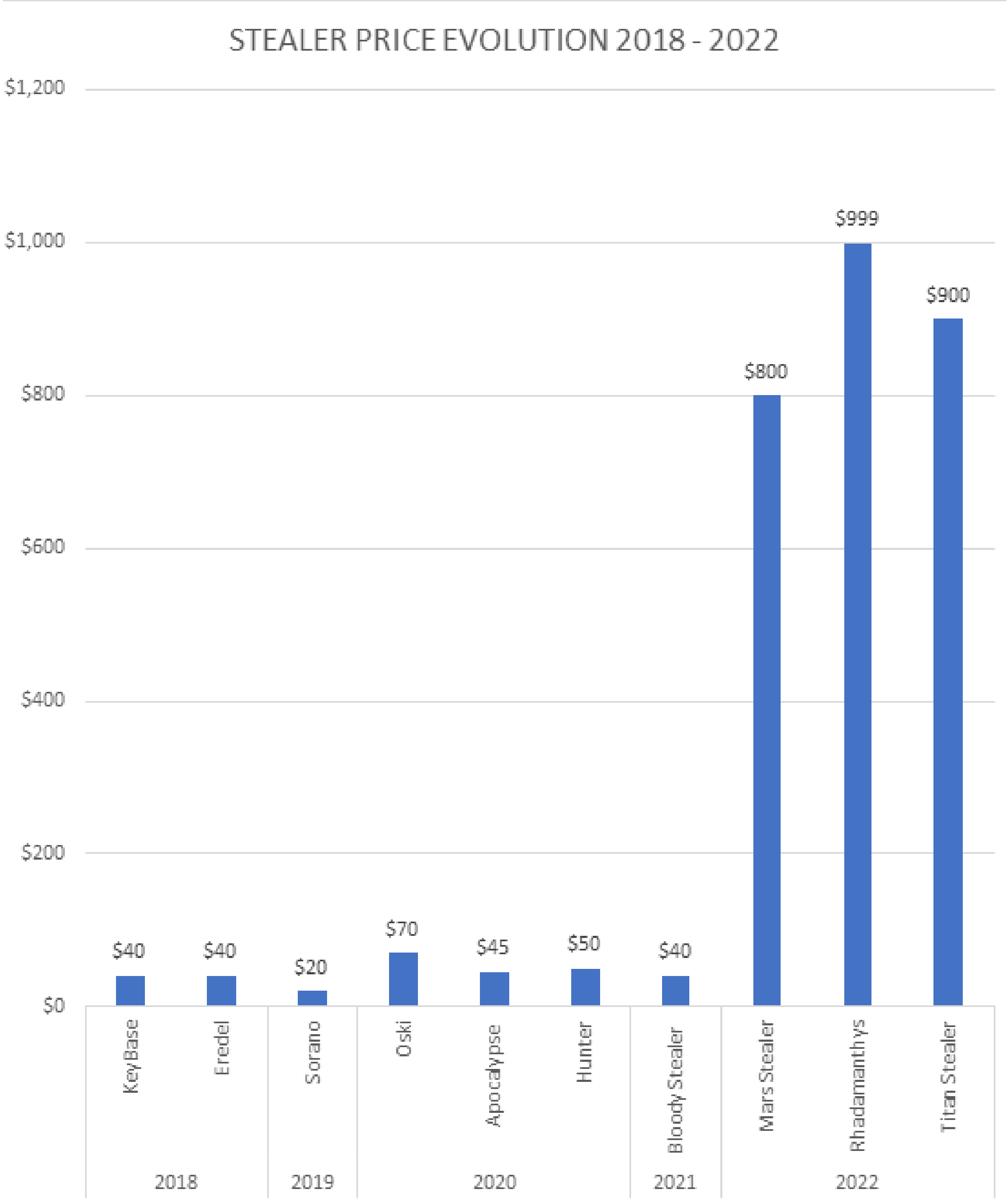


Outpost24

Credential theft - Introduction

The right conditions:

- Ransomware as a Service
- Proliferation of IAB's
- Maturity of the credential ecosystem



Outpost24

Traffers ecosystem

Traffers ecosystem – What are traffers

Traffers are groups that leverage Malware as a Service to recruit low-skilled cybercriminals in order to steal credentials and sell them in bulk through “Clouds”

DEALER TEAM
FREE SEO
THE BEST STEALER - 000
HIGH-QUALITY AND FREE MANUAL FILLING!
@DEALLERTEAM
@DEALLERTEAM

Traffers ecosystem – What are traffers

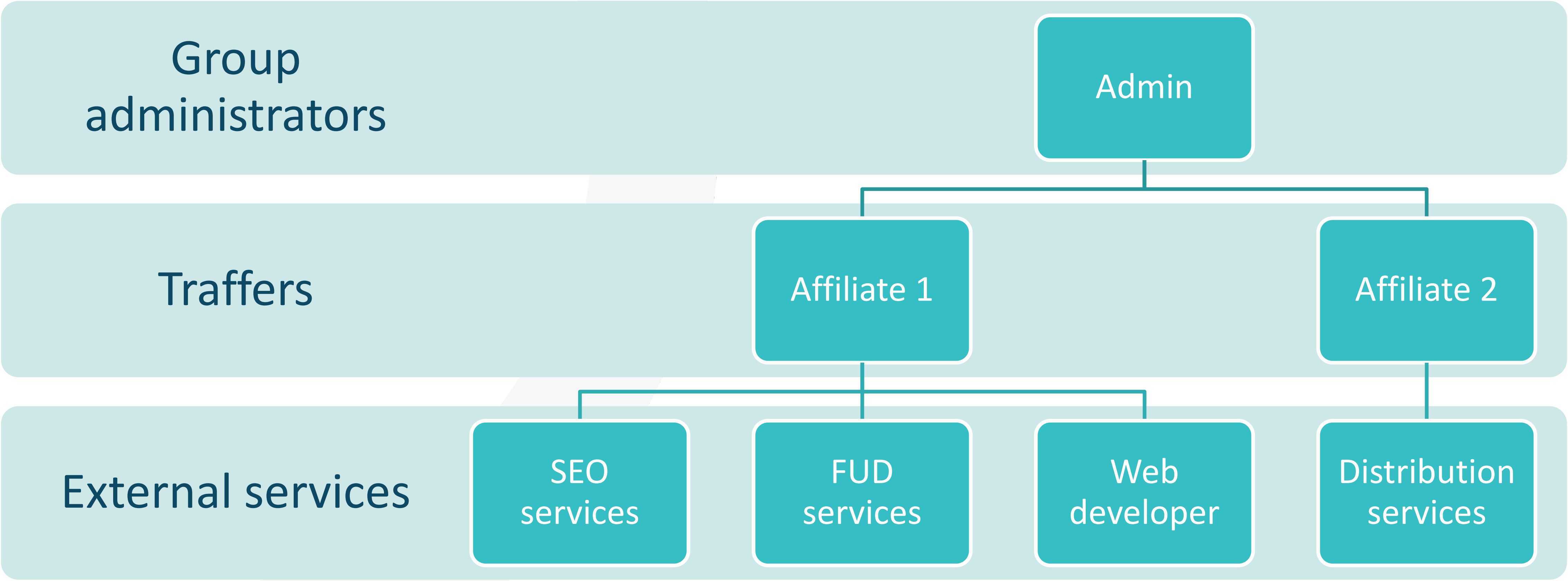
TRAFFERS

High demand for credentials

Malware Stealers as a Service

Social media and communication platforms

Traffers ecosystem – How are they organized



Group administrators

Admin

Traffers

Affiliate 1

Affiliate 2

External services

SEO services

FUD services

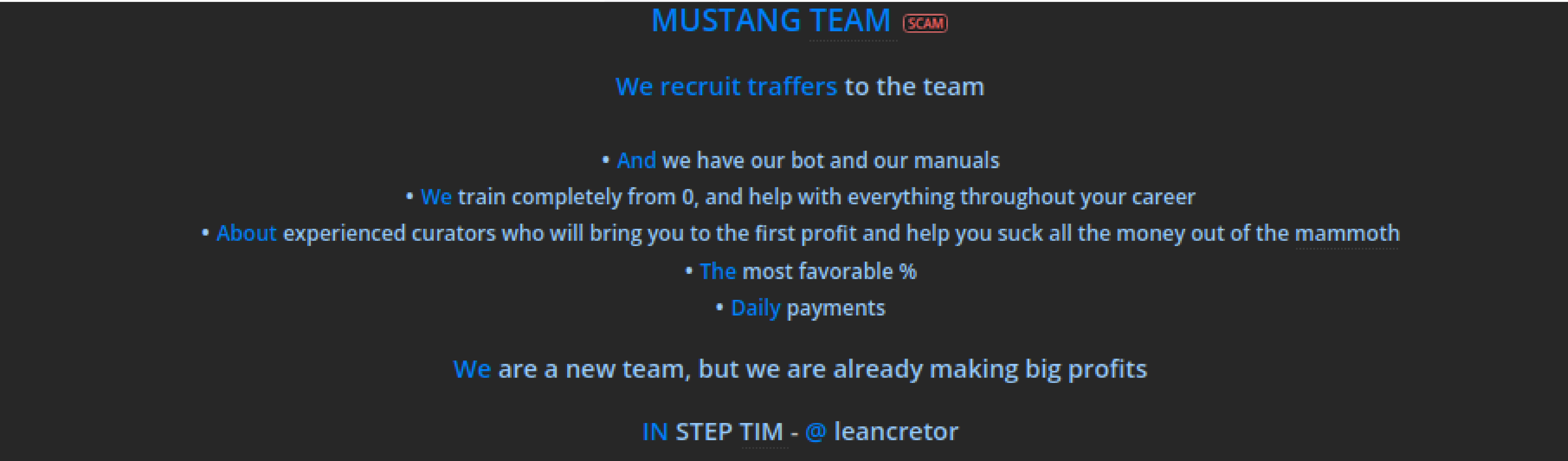
Web developer

Distribution services

Traffer groups – Admins

Responsibilities

- Manage the group
- Recruiting new members
- Evaluating current members
- Invests in new tooling
- Creates tutorials for new members
- Selling the credentials



MUSTANG TEAM SCAM

We recruit traffers to the team

• And we have our bot and our manuals

• We train completely from 0, and help with everything throughout your career

• About experienced curators who will bring you to the first profit and help you suck all the money out of the mammoth

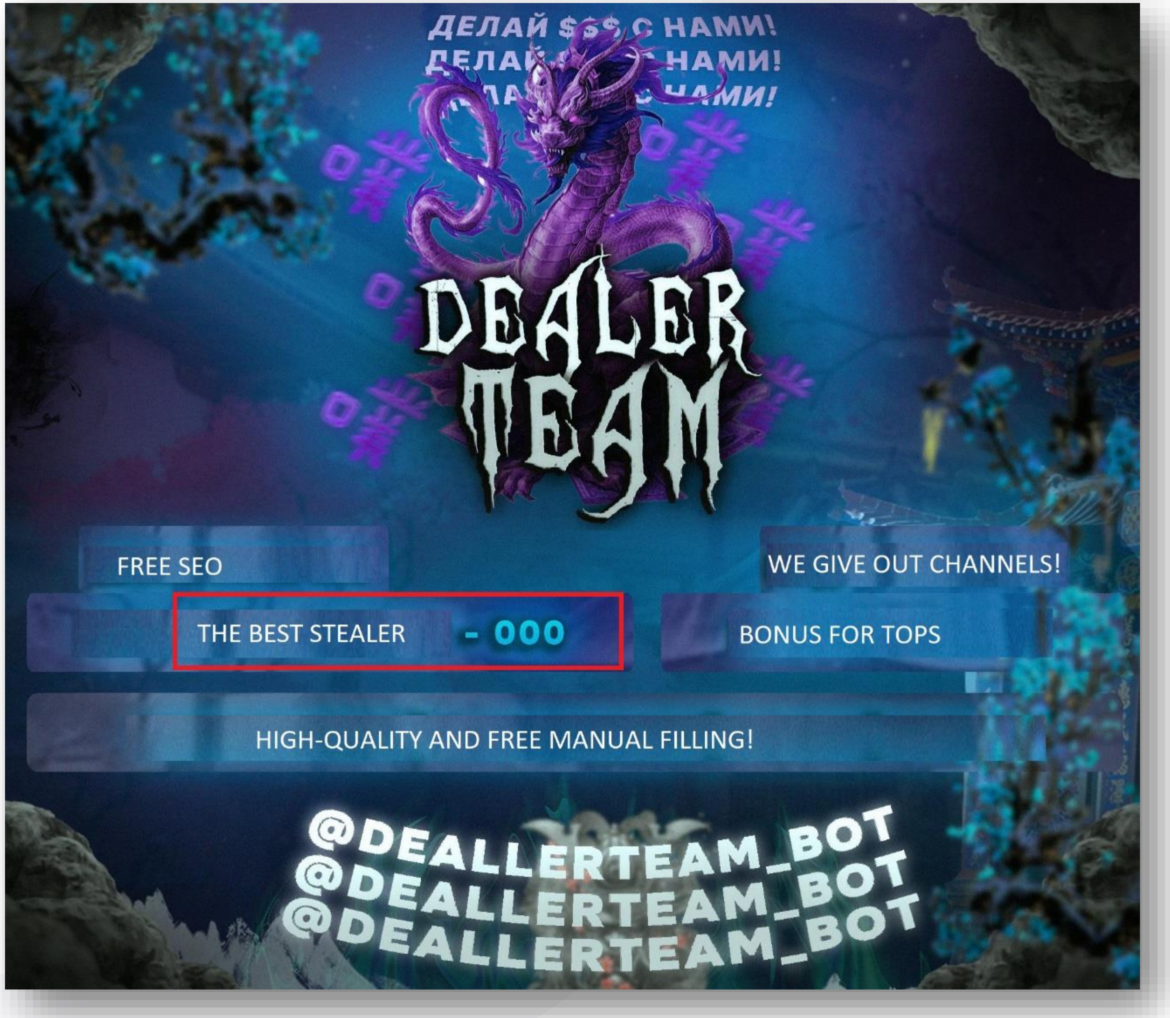
• The most favorable %

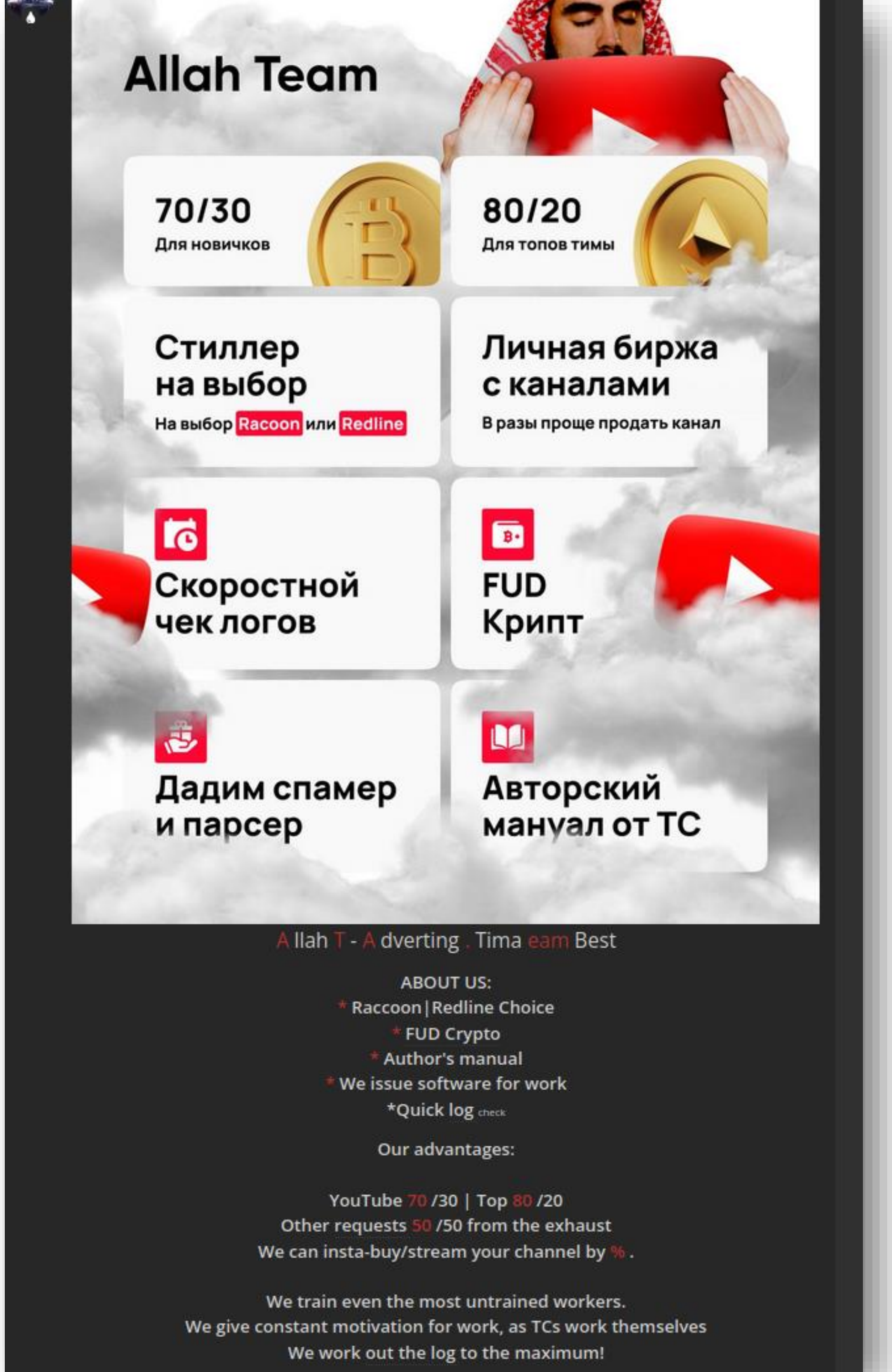
• Daily payments

We are a new team, but we are already making big profits

IN STEP TIM - @ leancretor

Traffer groups – Admins





Allah Team

70/30
Для новичков

80/20
Для топов тимы

Стиллер на выбор
На выбор Racoon или Redline

Личная биржа с каналами
В разы проще продать канал

Скоростной чек логов

FUD Крипт

Дадим спамер и парсер

Авторский мануал от ТС

A llah T - A dverting . Tima eam Best

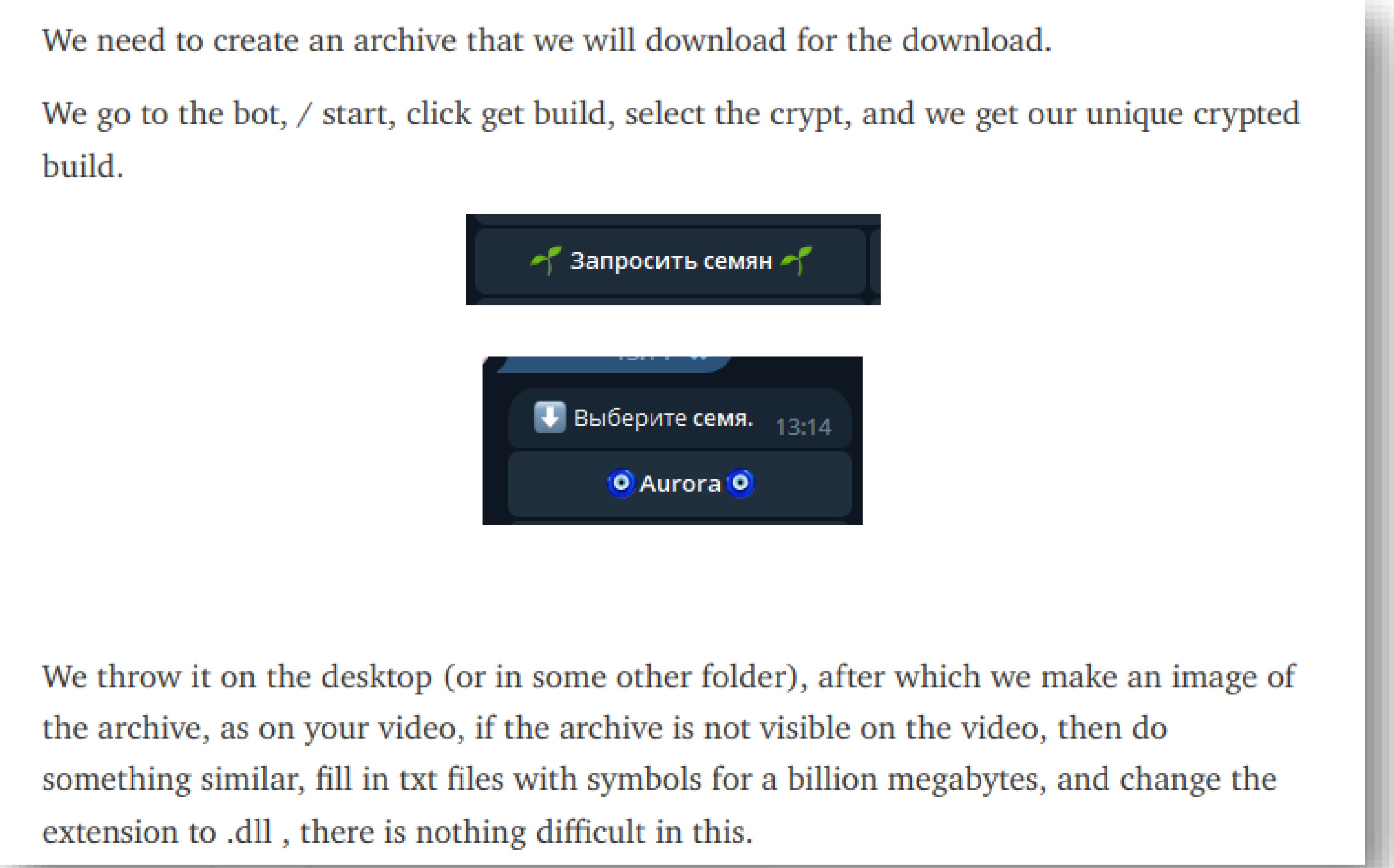
ABOUT US:
* Raccoon|Redline Choice
* FUD Crypto
* Author's manual
* We issue software for work
*Quick log check

Our advantages:

YouTube 70 /30 | Top 80 /20
Other requests 50 /50 from the exhaust
We can insta-buy/stream your channel by % .

We train even the most untrained workers.
We give constant motivation for work, as TCs work themselves
We work out the log to the maximum!

Traffer groups – Admins



We need to create an archive that we will download for the download.

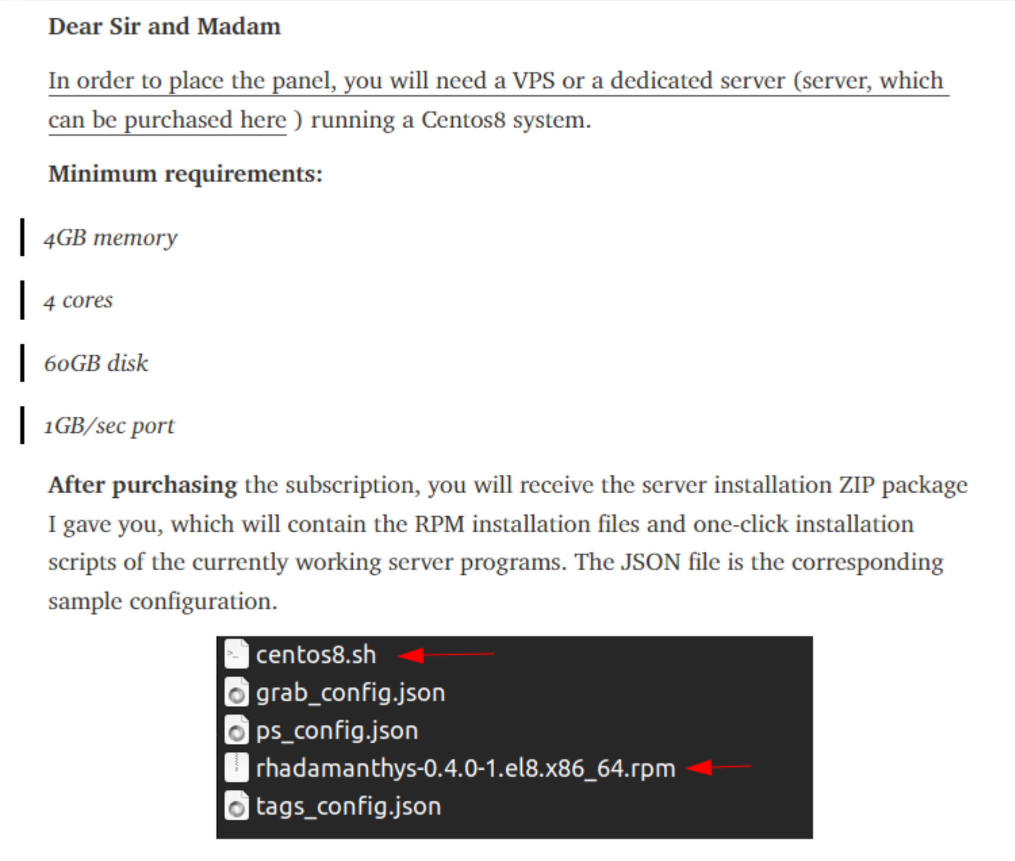
We go to the bot, / start, click get build, select the crypt, and we get our unique crypted build.

Запросить семян

Выберите семя. 13:14

Aurora

We throw it on the desktop (or in some other folder), after which we make an image of the archive, as on your video, if the archive is not visible on the video, then do something similar, fill in txt files with symbols for a billion megabytes, and change the extension to .dll , there is nothing difficult in this.



Dear Sir and Madam

In order to place the panel, you will need a VPS or a dedicated server (server, which can be purchased here) running a Centos8 system.

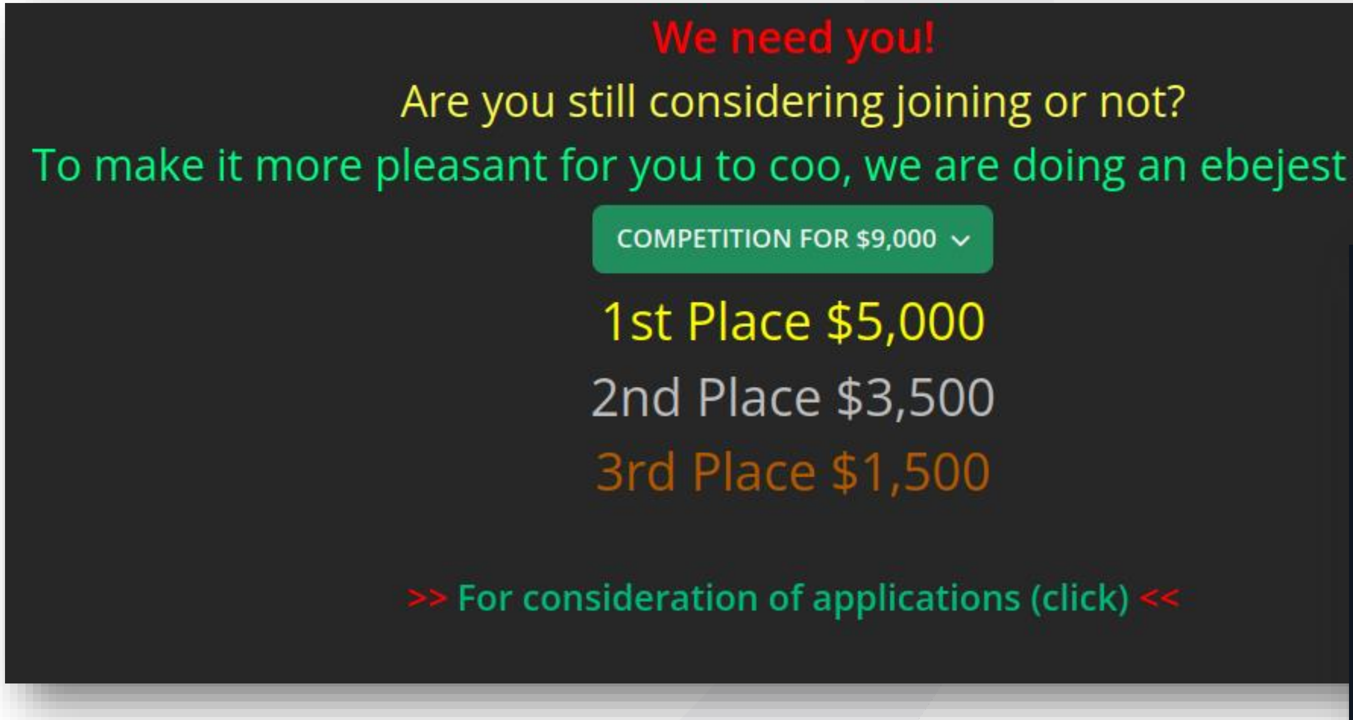
Minimum requirements:

> *4GB memory*
>
> *4 cores*
>
> *60GB disk*
>
> *1GB/sec port*

After purchasing the subscription, you will receive the server installation ZIP package I gave you, which will contain the RPM installation files and one-click installation scripts of the currently working server programs. The JSON file is the corresponding sample configuration.

```
centos8.sh
grab_config.json
ps_config.json
rhadamanthys-0.4.0-1.el8.x86_64.rpm
tags_config.json
```

Traffer groups – Admins



We need you!

Are you still considering joining or not?

To make it more pleasant for you to coo, we are doing an ebejest contest !!!

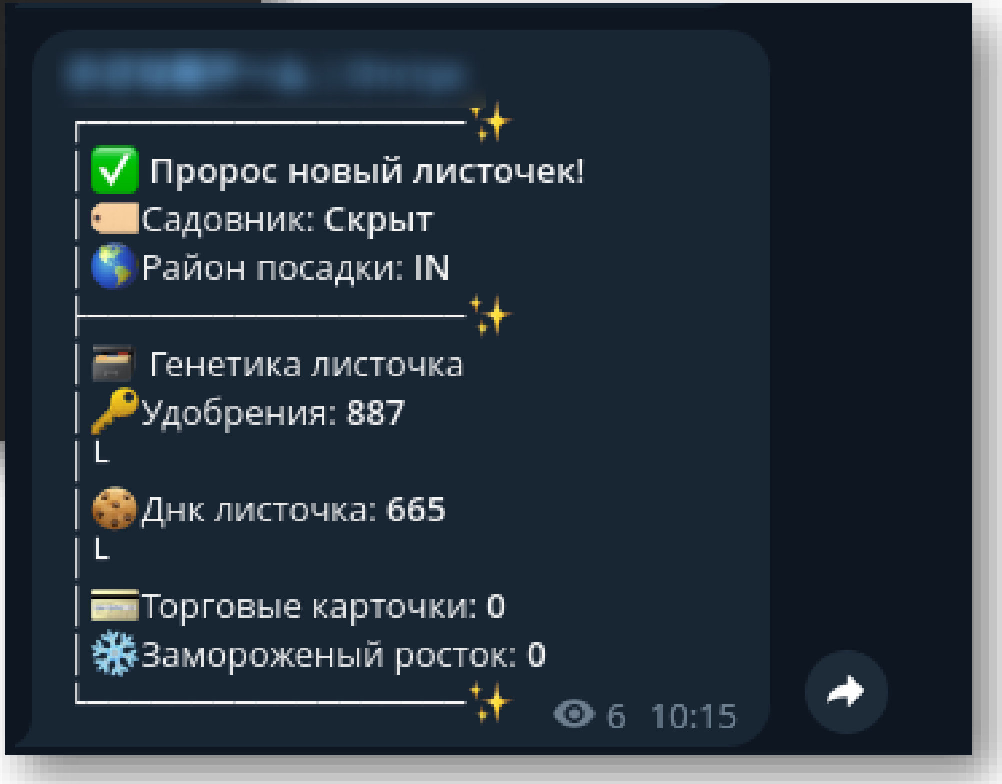
COMPETITION FOR $9,000 ⌄

1st Place $5,000

2nd Place $3,500

3rd Place $1,500

>> For consideration of applications (click) <<



[redacted]

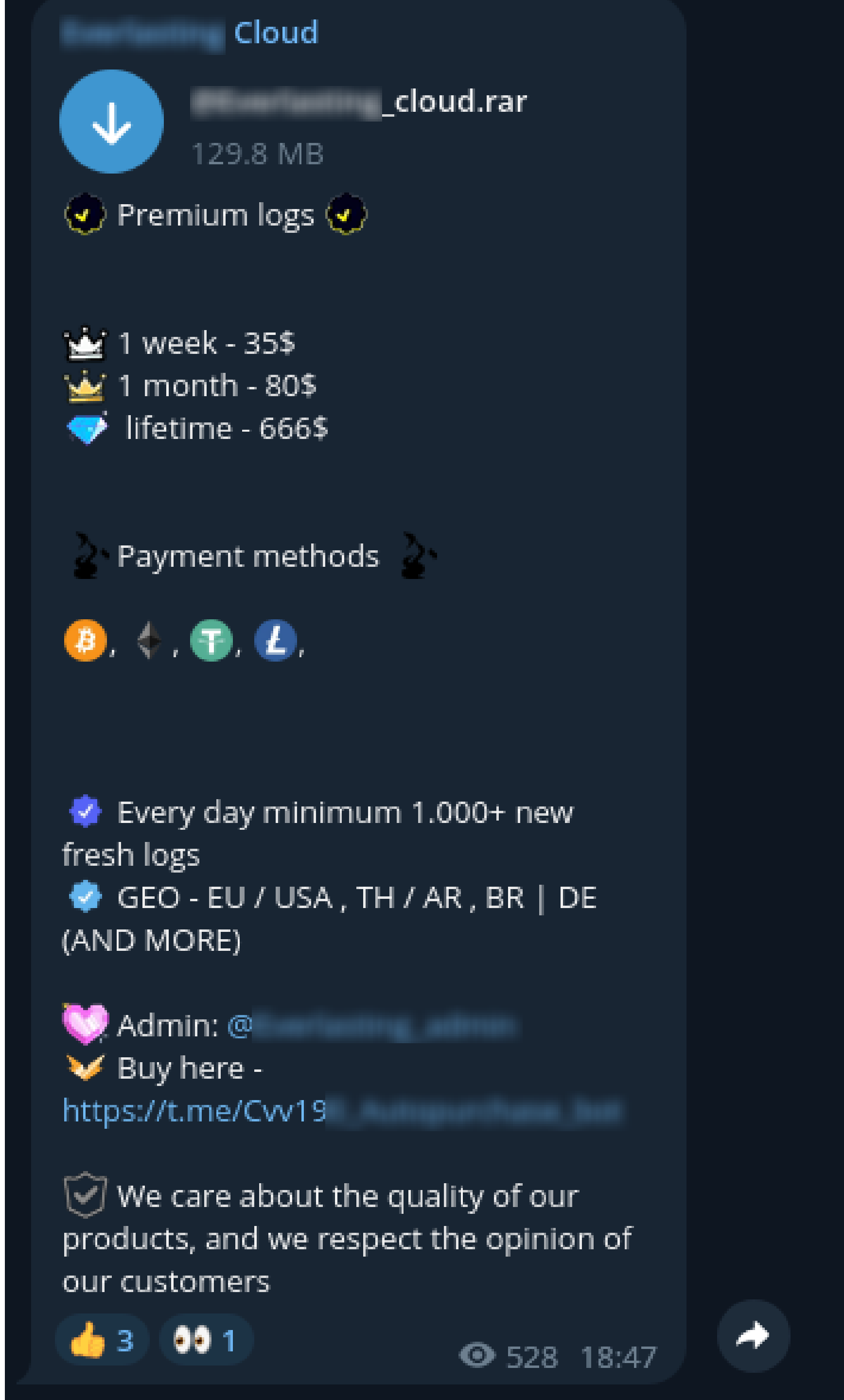
┌────────────────✨
│✅ Пророс новый листочек!
│🏷Садовник: Скрыт
│🌎Район посадки: IN
├────────────────✨
│💳 Генетика листочка
│🔑Удобрения: 887
│└
│🍪Днк листочка: 665
│└
│💳Торговые карточки: 0
│❄️Замороженый росток: 0
└────────────────✨

👁 6 10:15

Traffer groups – Admins

Responsibilities

- Manage the group
- Recruiting new members
- Evaluating current members
- Invests in new tooling
- Creates tutorials for new members
- **Selling the credentials**



[redacted] Cloud

[redacted]_cloud.rar
129.8 MB

Premium logs

👑 1 week - 35$
👑 1 month - 80$
💎 lifetime - 666$

Payment methods

₿, Ξ, ₮, Ł,

✓ Every day minimum 1.000+ new fresh logs
✓ GEO - EU / USA , TH / AR , BR | DE (AND MORE)

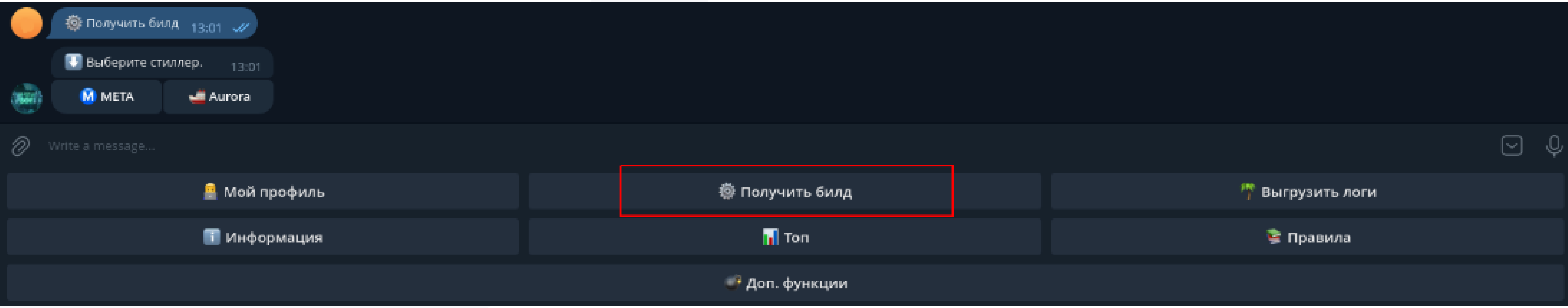
💝 Admin: @[redacted]
Buy here -
https://t.me/Cvv19[redacted]

We care about the quality of our products, and we respect the opinion of our customers

Traffer groups – Traffers

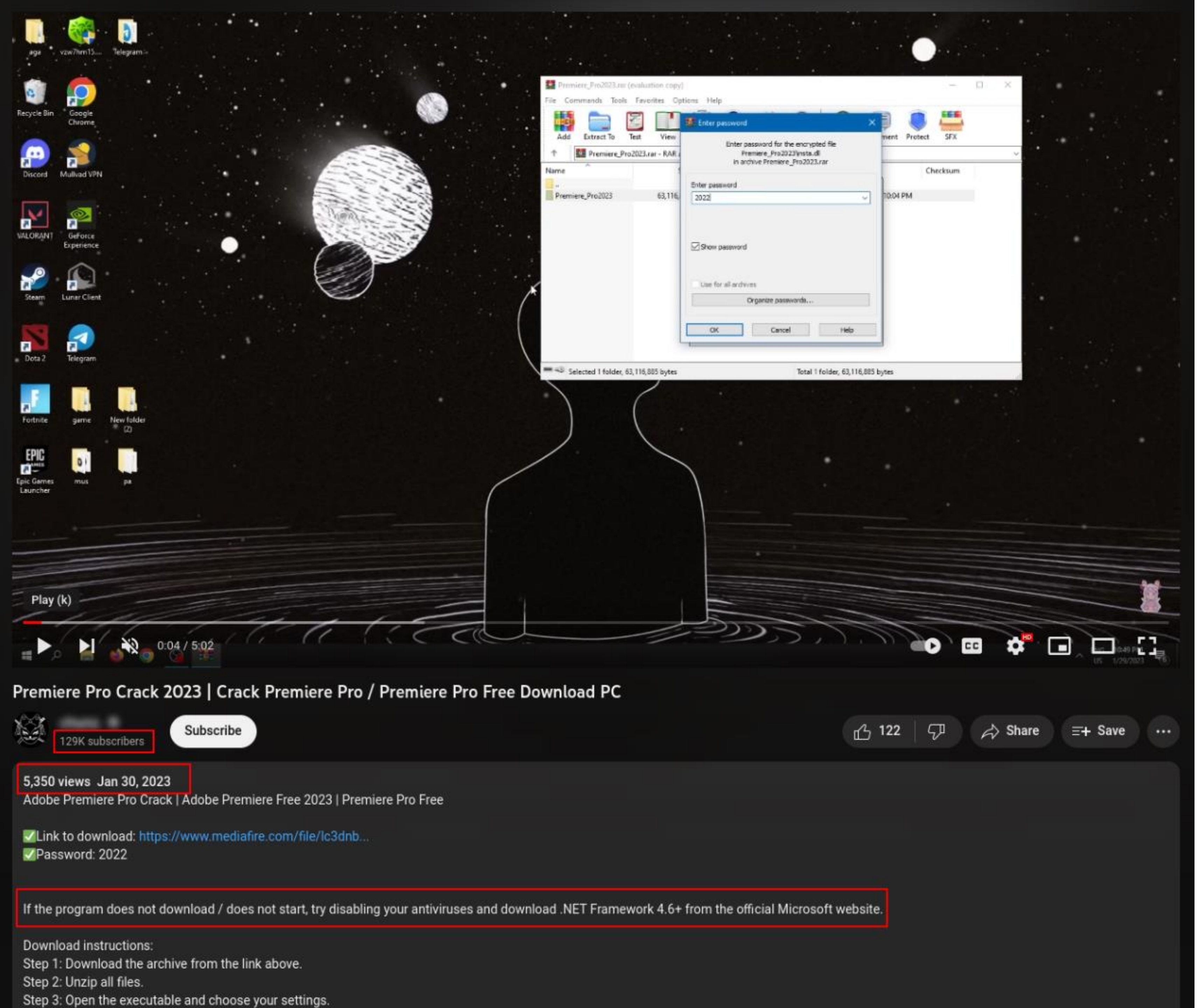
Characteristics:

- Sole goal of stealing credentials
- Typically low technical skill
- Leverages SEO, social media



⚙ Получить билд 13:01

⬇ Выберите стиллер. 13:01



Enter password

Enter password for the encrypted file
Premiere_Pro2023\insta.dll
in archive Premiere_Pro2023.rar

Enter password: 2022

☑ Show password

□ Use for all archives

Selected 1 folder, 63,116,885 bytes

Total 1 folder, 63,116,885 bytes

Premiere Pro Crack 2023 | Crack Premiere Pro / Premiere Pro Free Download PC

[redacted]
129K subscribers

5,350 views Jan 30, 2023
Adobe Premiere Pro Crack | Adobe Premiere Free 2023 | Premiere Pro Free

✅Link to download: https://www.mediafire.com/file/lc3dnb...
✅Password: 2022

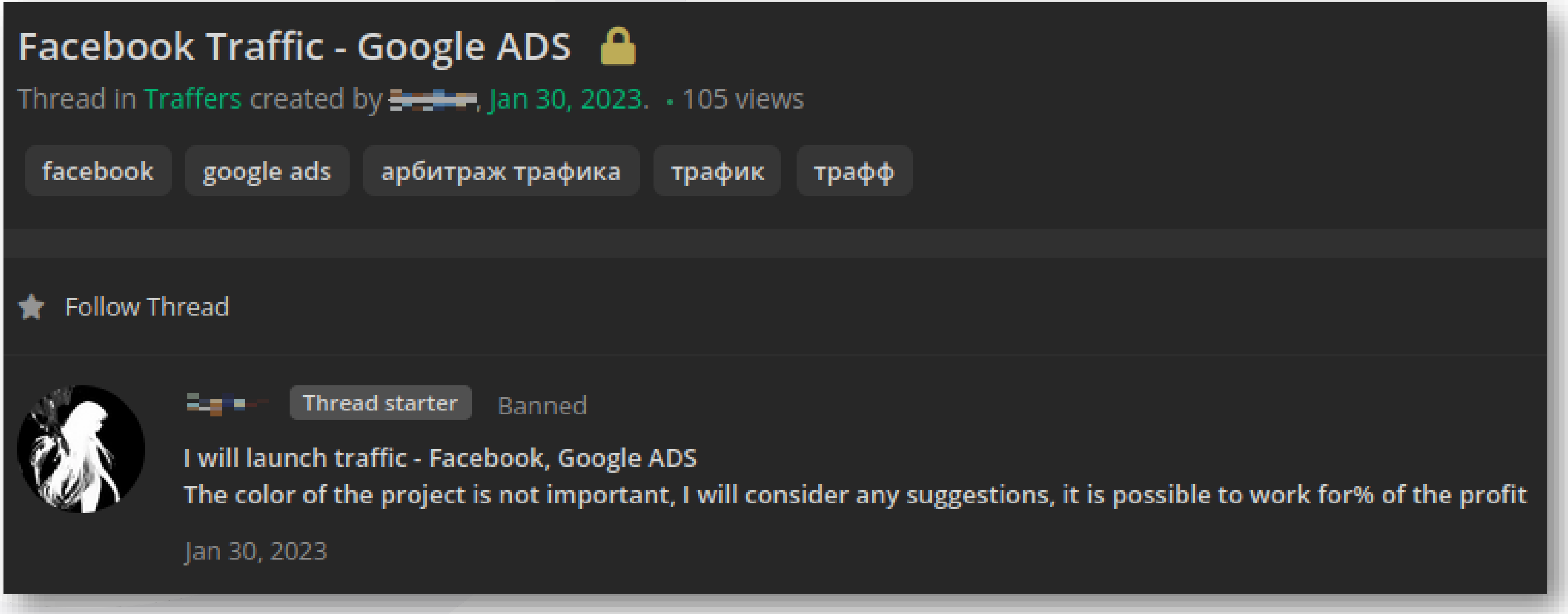
If the program does not download / does not start, try disabling your antiviruses and download .NET Framework 4.6+ from the official Microsoft website.

Download instructions:
Step 1: Download the archive from the link above.
Step 2: Unzip all files.
Step 3: Open the executable and choose your settings.

Characteristics:

- Sole goal of stealing credentials
- Typically low technical skill
- **Leverages SEO, social media, google ads**

Traffer groups – Traffers



Facebook Traffic - Google ADS 🔒

Thread in Traffers created by [redacted], Jan 30, 2023. • 105 views

facebook | google ads | арбитраж трафика | трафик | трафф

★ Follow Thread

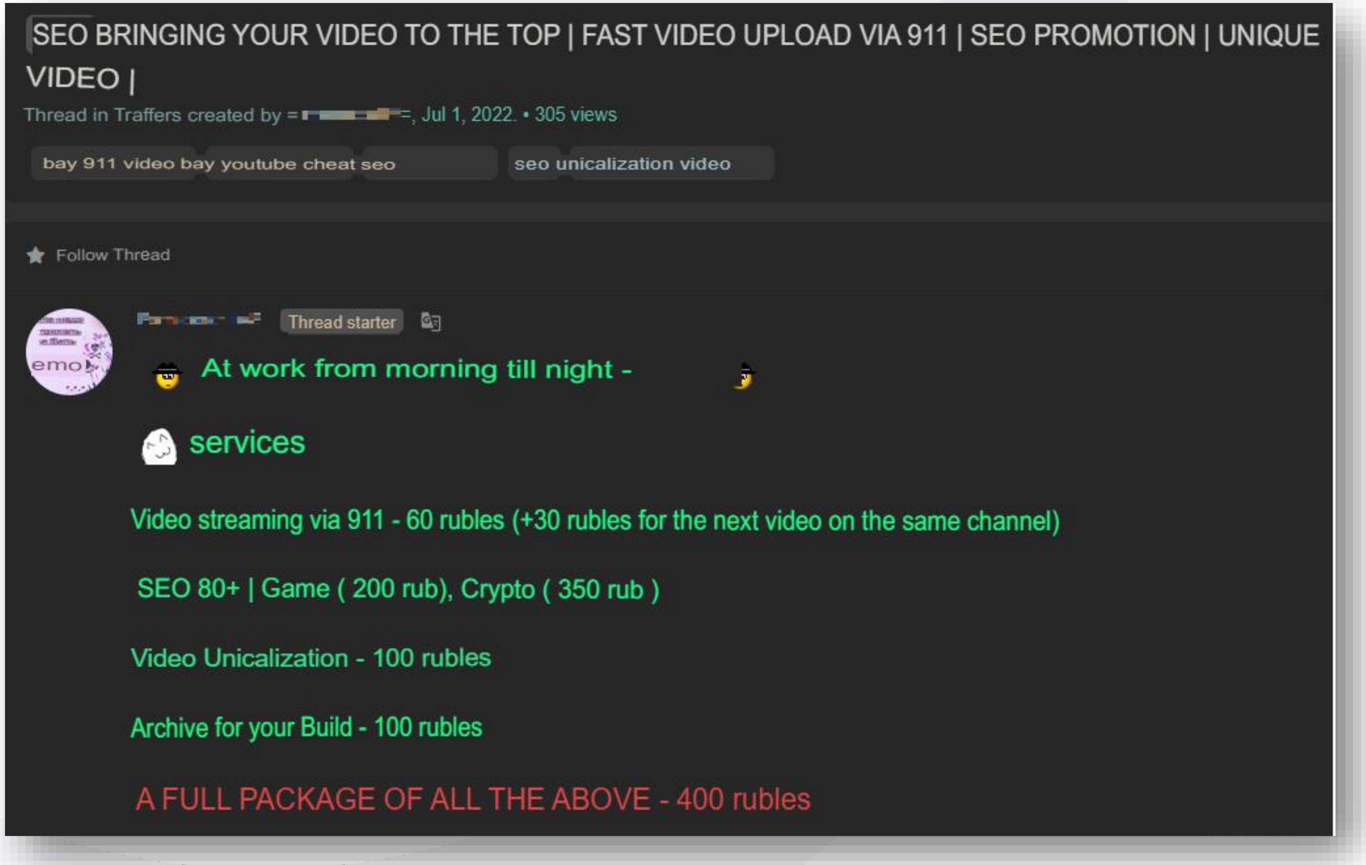
[redacted] Thread starter Banned

I will launch traffic - Facebook, Google ADS
The color of the project is not important, I will consider any suggestions, it is possible to work for% of the profit

Jan 30, 2023

Outpost24

Traffer groups – Traffers



SEO BRINGING YOUR VIDEO TO THE TOP | FAST VIDEO UPLOAD VIA 911 | SEO PROMOTION | UNIQUE VIDEO |

Thread in Traffers created by =[redacted]=, Jul 1, 2022. • 305 views

bay 911 video bay youtube cheat seo

seo unicalization video

Follow Thread

[redacted] Thread starter

At work from morning till night -

services

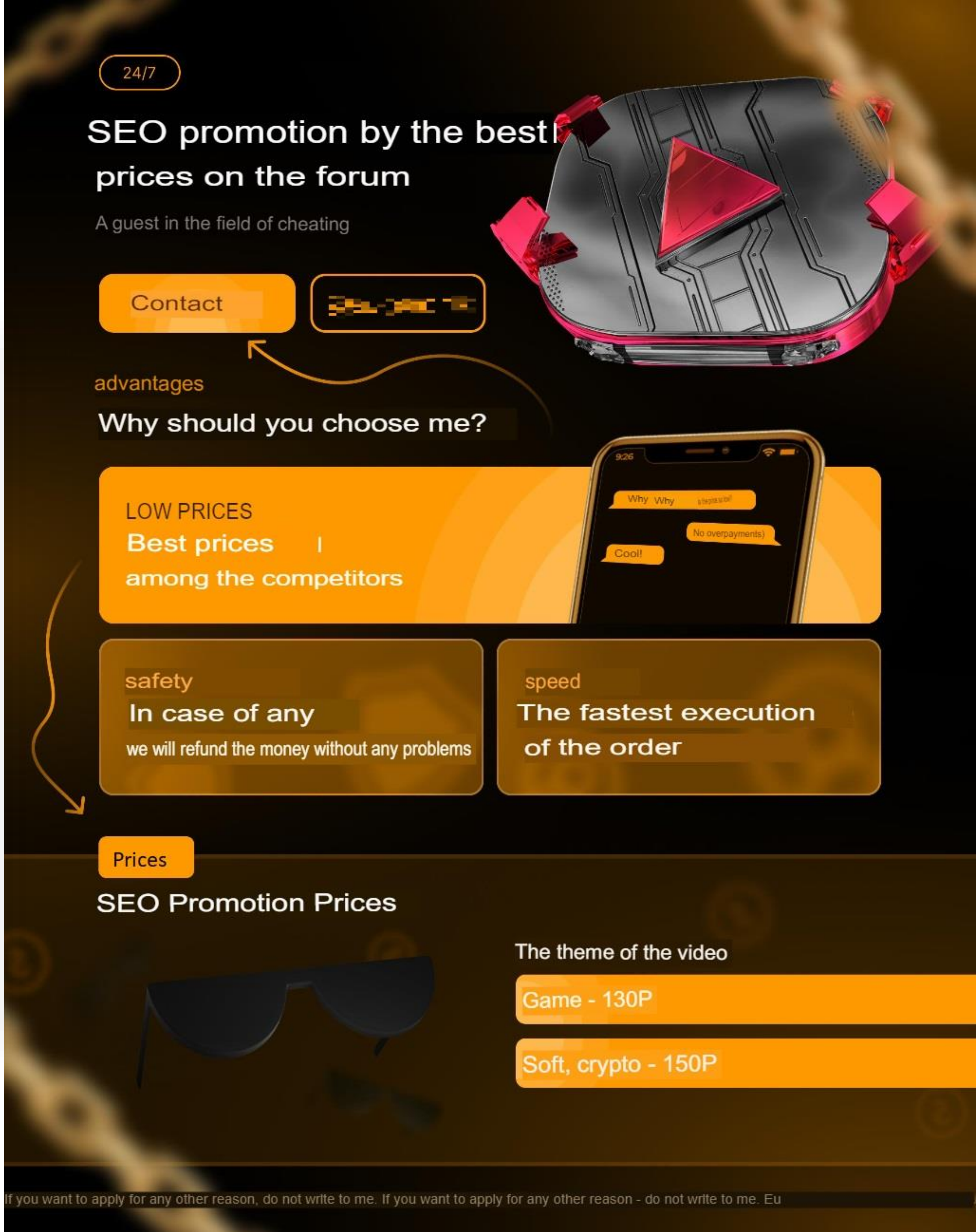
Video streaming via 911 - 60 rubles (+30 rubles for the next video on the same channel)

SEO 80+ | Game (200 rub), Crypto (350 rub)

Video Unicalization - 100 rubles

Archive for your Build - 100 rubles

A FULL PACKAGE OF ALL THE ABOVE - 400 rubles



24/7

SEO promotion by the best prices on the forum

A guest in the field of cheating

Contact [redacted]

advantages

Why should you choose me?

LOW PRICES

Best prices among the competitors

safety

In case of any

we will refund the money without any problems

speed

The fastest execution of the order

Prices

SEO Promotion Prices

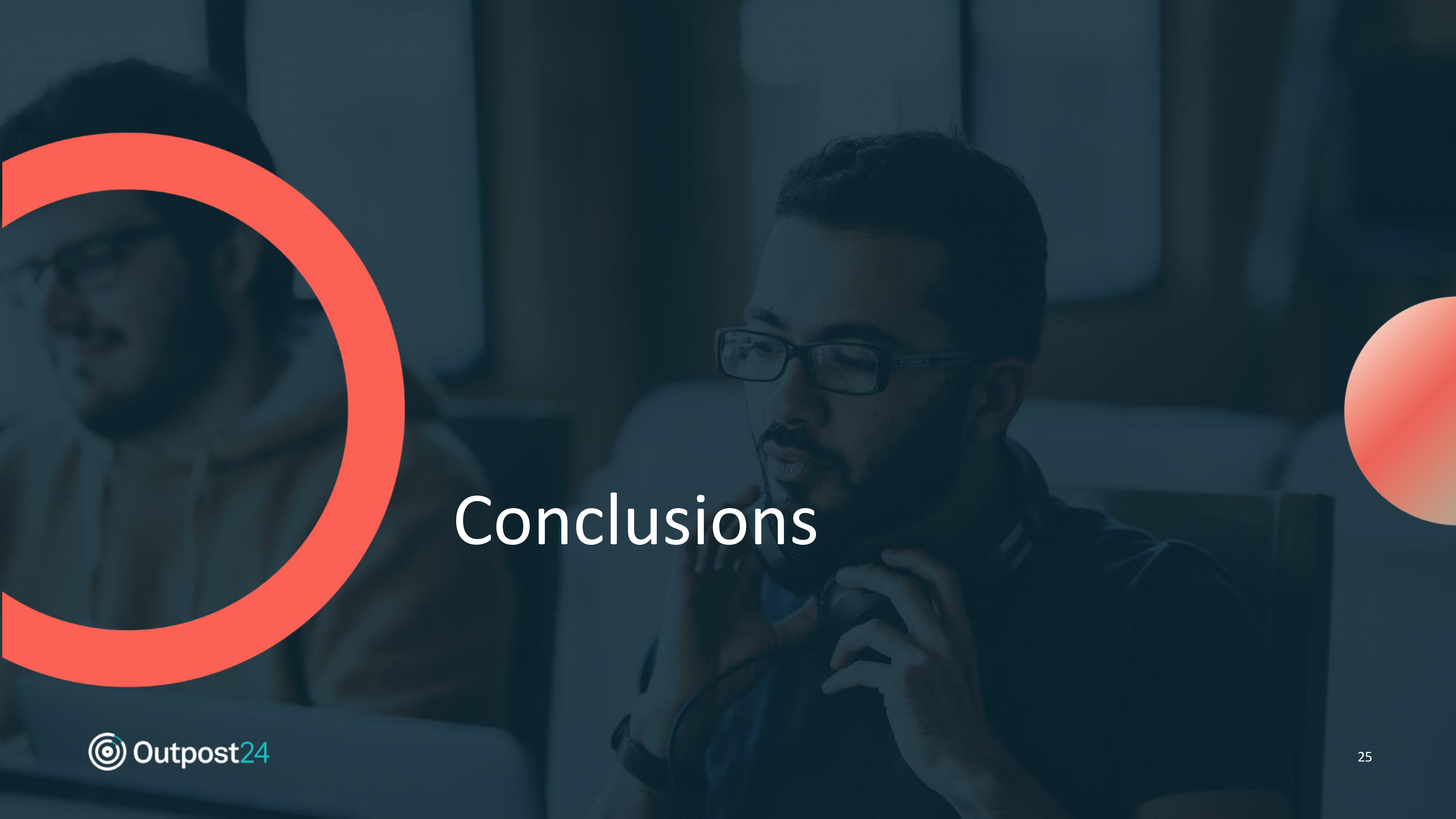
The theme of the video

Game - 130P

Soft, crypto - 150P

If you want to apply for any other reason, do not write to me. If you want to apply for any other reason - do not write to me. Eu

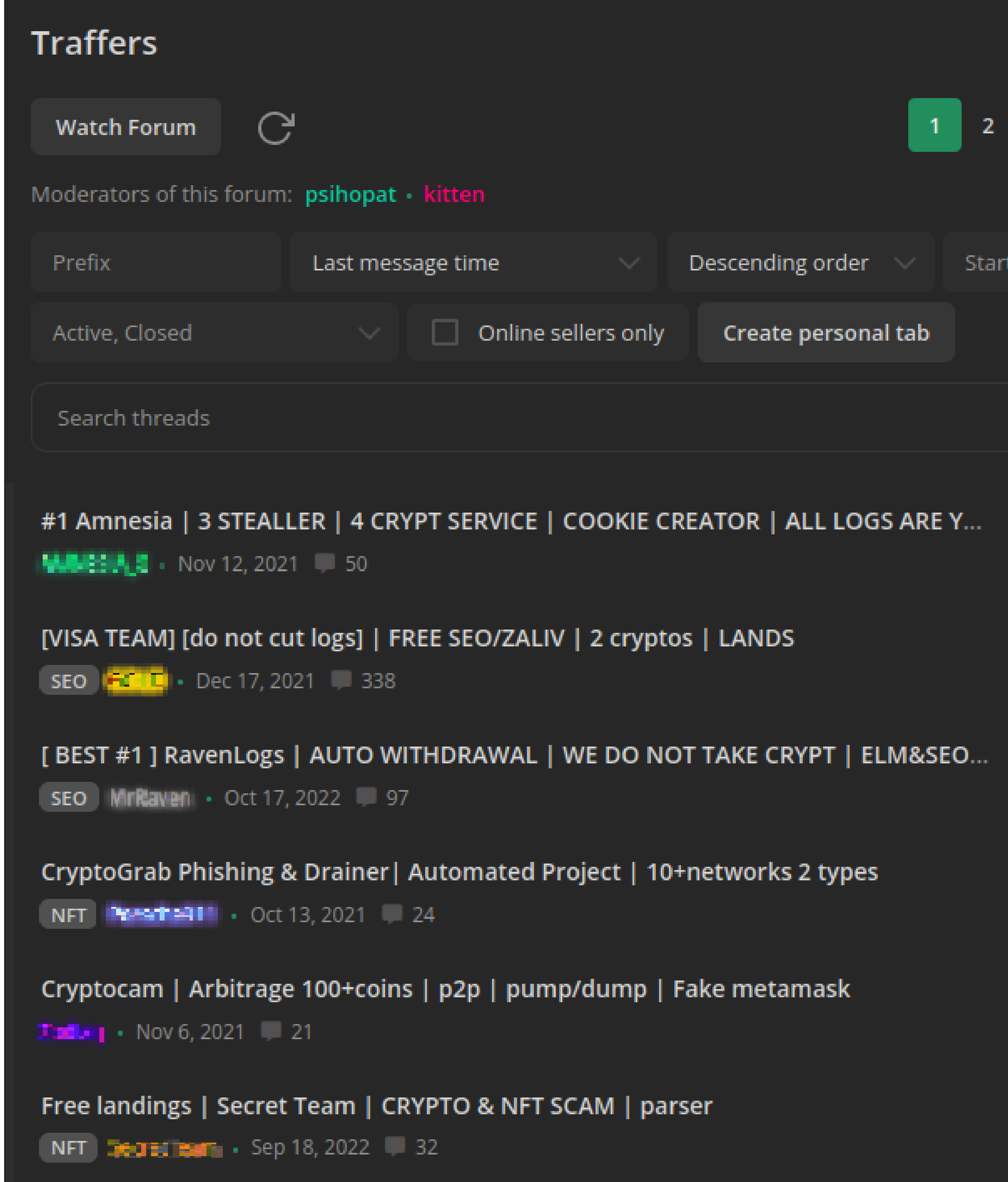
Outpost24



Conclusions

Conclusions – Impact on the ecosystem

- Proliferation of credential stealers
- Dedicated services for traffers
- Forums and platforms change to support this new business model
- Lower entry barrier for cybercriminals



Traffers

Moderators of this forum: psihopat • kitten

#1 Amnesia | 3 STEALLER | 4 CRYPT SERVICE | COOKIE CREATOR | ALL LOGS ARE Y...
[redacted] • Nov 12, 2021 50

[VISA TEAM] [do not cut logs] | FREE SEO/ZALIV | 2 cryptos | LANDS
SEO [redacted] • Dec 17, 2021 338

[BEST #1] RavenLogs | AUTO WITHDRAWAL | WE DO NOT TAKE CRYPT | ELM&SEO...
SEO [redacted] • Oct 17, 2022 97

CryptoGrab Phishing & Drainer| Automated Project | 10+networks 2 types
NFT [redacted] • Oct 13, 2021 24

Cryptocam | Arbitrage 100+coins | p2p | pump/dump | Fake metamask
[redacted] • Nov 6, 2021 21

Free landings | Secret Team | CRYPTO & NFT SCAM | parser
NFT [redacted] • Sep 18, 2022 32

Outpost24

Conclusions - Recommendations

Prevention

- Reinforce cyberhygene habits
- Device authentication

Mitigation

- 2FA
- Credential monitoring
- Password auditing
- Access audit

Thank you for listening in!

- contact: victor.acin@blueliv.com