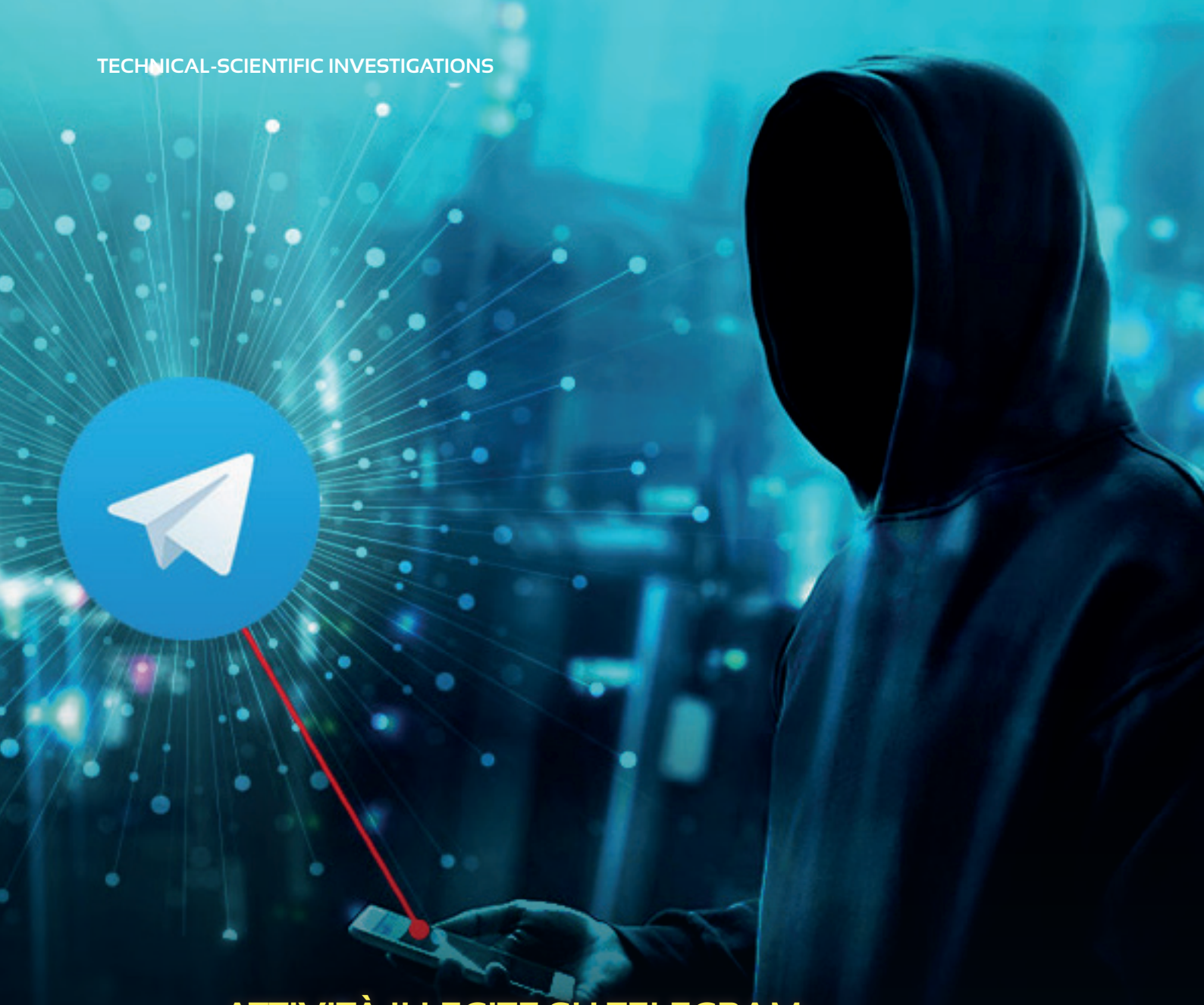

ATTIVITÀ ILLECITE SU TELEGRAM: LA SOCIAL MEDIA INTELLIGENCE A SUPPORTO DELLE INDAGINI

Nell'ambito dell'analisi del fenomeno del "falso documentale", sulla scia del precedente articolo che si sofferma sulla presenza di specifici canali sulla piattaforma Telegram dedicati alla vendita di documenti definibili come "buoni falsi", la società IPS ha fornito il proprio supporto per uno studio più approfondito all'interno di questi canali.
Mediante l'adozione di strumenti automatizzati, con gli indizi pubblici a disposizione, vediamo come sia stato possibile risalire ad alcune informazioni potenzialmente utili per scoprire la reale identità di chi si cela dietro questi canali.

Manuel GIARRUZZO, Product Specialist.

Nicola MARINI, Business Development.

Telegram è un servizio di messaggistica istantanea e broadcasting basato su cloud, fruibile in versione app e desktop, lanciato nel 2013 dall'imprenditore russo Pavel Durov, già noto per aver creato anche il Social Network VKontakte (servizio analogo a Facebook utilizzato prevalentemente in Russia).
Le caratteristiche principali del servizio sono la possibilità di scambiare messaggi di testo tra due utenti o tra gruppi fino a 200.000 partecipanti, effettuare chiamate vocali cifrate "punto-punto", scambiare messaggi vocali, videomessaggi, fotografie, video, sticker e altre tipologie di file.

A differenza di altri servizi di messaggistica, come ad esempio WhatsApp, Telegram si caratterizza per una connotazione più *social*. Infatti, è possibile eseguire ricerche all'interno dell'app per trovare gruppi, canali e addirittura utenti, senza necessariamente avere la loro utenza telefonica registrata nella rubrica del proprio terminale mobile.

Ad oggi, in tutto il mondo sono più di 400 milioni gli utenti attivi[1], 100 milioni in più rispetto allo stesso periodo dello scorso anno. Facendo riferimento al mercato italiano, sono 13 milioni gli utenti che utilizzano l'applicazione di messaggistica russa[2].

Come molte altre piattaforme social, anche Telegram è un terreno ideale in cui proliferano attività illecite, ma negli ultimi tempi la piattaforma si sta contraddistinguendo per volume e specificità di tali attività, grazie soprattutto ad alcuni aspetti precipui del mezzo stesso. È infatti possibile creare ed inviare messaggi e scambiare file multimediali di qualsiasi formato in maniera completamente anonima grazie alla cifratura end-to-end della piattaforma. Inoltre, la capacità di ricercare utenti, gruppi e canali tramite la barra di ricerca incorporata nell'applicazione, consente di raggiungere un numero incredibilmente elevato di utenti con estrema facilità.

In particolare, oltre alla comunicazione orizzontale tra due o più utenti, Telegram permette di comunicare attraverso le seguenti modalità:

- **Gruppi**: gli utenti possono iscriversi e comunicare tra loro su un determinato argomento di interesse;
- **Canali**: rispetto ai gruppi, i canali sono un mezzo di comunicazione unidirezionale. Solamente chi ha creato il canale – ed altri eventuali gestori – possono inviare messaggi, mentre gli iscritti ricevono tali messaggi senza la possibilità di effettuare commenti.

Ad oggi non sono disponibili dati ufficiali forniti da Telegram sulla quantità di gruppi e canali, ma alcune analisi attendibili stimano che siano stati creati nel tempo circa 6 milioni di gruppi e canali pubblici.
Una parte consistente di questi gruppi e canali sono regolarmente utilizzati per attività illecite dirette o indirette. La possibilità di fruizione dei contenuti è particolarmente agevole grazie alla facilità di ricerca offerta dallo strumento. Innanzitutto, è possibile ricercare un gruppo o canale tramite la barra di ricerca integrata nell'applicazione Telegram, ulteriormente attraverso siti web dove sono riportate *Directories* di gruppi e canali, oppure, infine, attraverso il passaparola.

Recentemente, l'utilizzo di Telegram per fini illeciti ha avuto risonanza internazionale, quando la Procura di Bari ha disposto il sequestro di numerosi canali[3] dove venivano regolarmente pubblicati quotidiani, riviste, ebook e serie tv. In quell'occasione, ma l'indagine è ancora in corso, sono stati chiusi 114 canali (in alcuni casi si tratta di canali già precedentemente chiusi e riaperti con altro nome).
Come facilmente intuibile, il fenomeno però non si limita a colpire il mondo dell'editoria, ma è più ramificato e diffuso di quanto si possa immaginare. Ad oggi, in particolare, si evidenzia la diffusione di molteplici tipologie di

1 https://telegram.org/blog/400-million/it.

2 https://www.wired.it/economia/business/2020/02/07/whatsapp-telegram-business/#:~:text=WhatsApp%20pu%C3%B2%20contare%20oltre%2031,ai%2013%20milioni%20di%20utenti.

3 ANSA, "Pdf pirata giornali e libri, stop a 114 canali Telegram. Inchiesta procura Bari, in alcuni casi sono canali già chiusi" https://www.ansa.it/puglia/notizie/2020/05/04/pdf-pirata-giornali-e-libri-stop-a-114-canali-telegram_44e80496-caab-45c0-b782-006f235e2a56.html

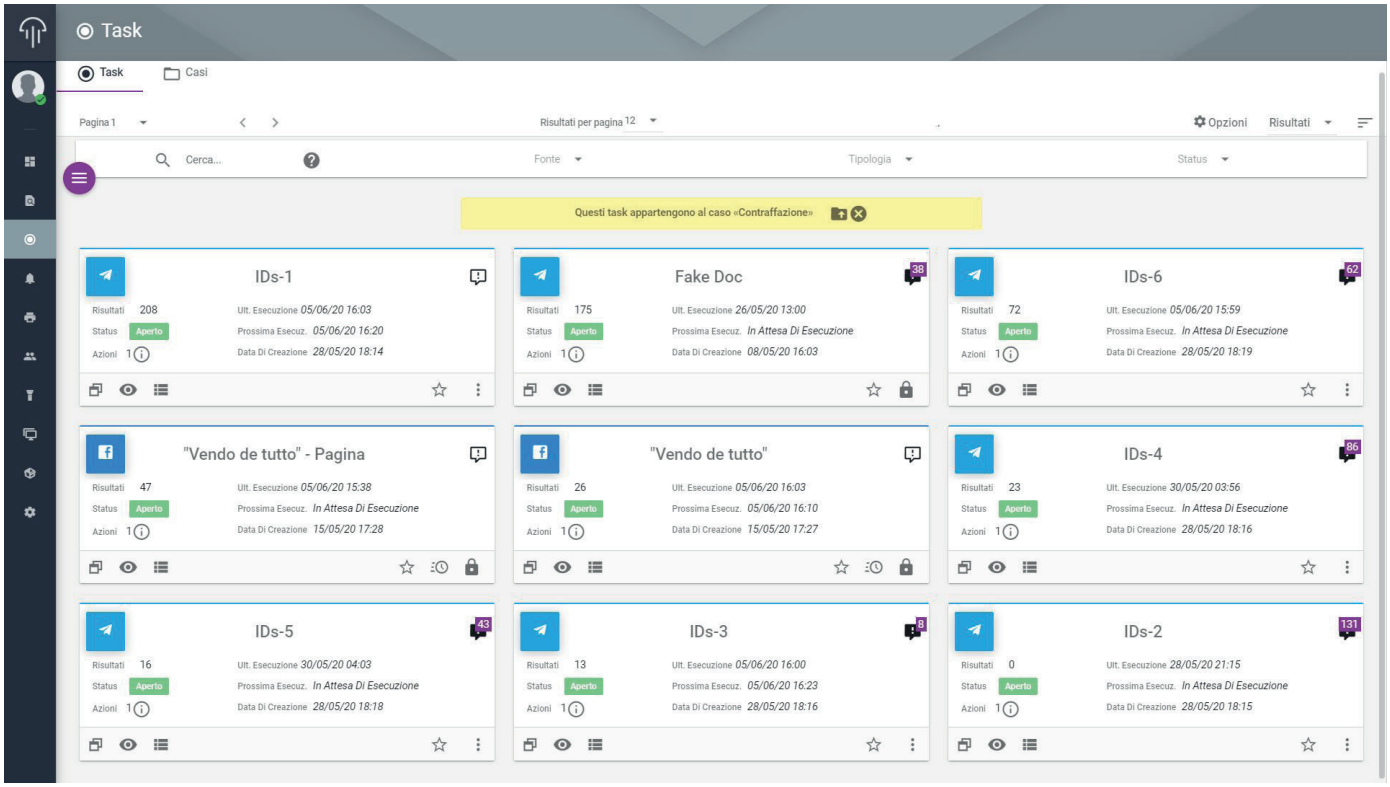

Figura 1 - Vista dei canali esaminati su Telegram.

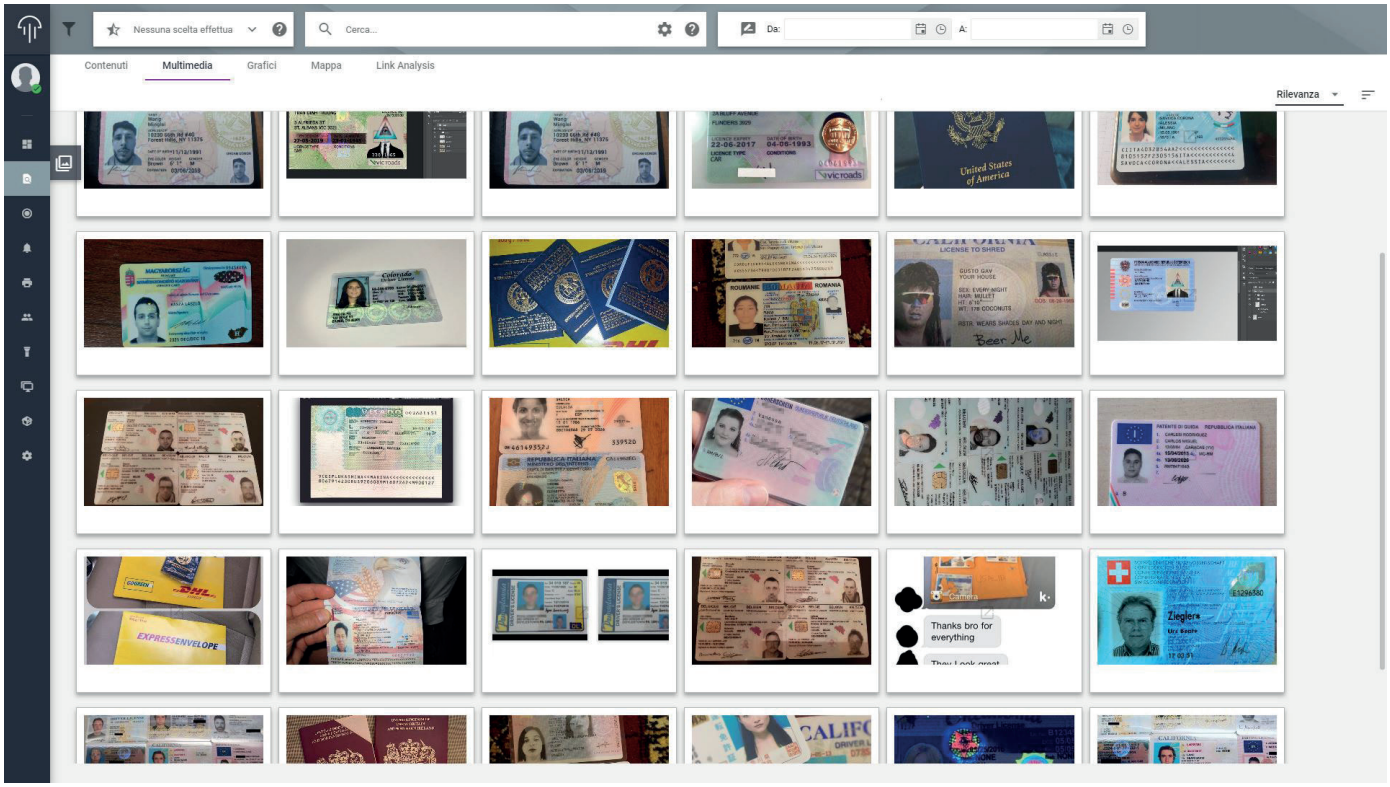

Figura 2 - immagini e video raccolti nei canali di Telegram esaminati.

illeciti, tra cui emergono nettamente il falso documentale e la contraffazione.

Al fine di analizzare il fenomeno si è provveduto ad effettuare una ricerca analizzando numerosi canali/gruppi di Telegram. Si è dunque provveduto ad avviare circa 40 diverse attività di monitoraggio su altrettanti canali e gruppi Telegram collegati a fenomeni illeciti, di cui si rappresenta di seguito una percentuale per tipologia:

- **55% Contraffazione**
- **45% Falso documentale**

L'attività di monitoraggio si è protratta per un periodo di quattro settimane. L'arco temporale limitato dell'indagine è dovuto alla natura stessa di questi raggruppamenti di utenti. Infatti, l'illiceità degli argomenti trattati, comporta una continua attività di chiusura e riapertura dei canali e dei gruppi.

L'attività di indagine ha utilizzato le capacità tecniche del sistema MEDUSA® di IPS S.p.A., una piattaforma integrata di Social Media e Open Source Intelligence in grado di raccogliere, analizzare e storicizzare dati da molteplici fonti di informazione, tra cui Social Network (Facebook, Twitter, Instagram, YouTube, LinkedIn, Snapchat, VKontakte, Reddit, Telegram, ecc.), Web, Forum, Dark Web, CDR (Call Detail Records - tabulati telefonici), identificando, in numerosi contesti, anche informazioni private. Durante le varie fasi dell'indagine sono stati raccolti e storicizzati oltre 12.000 elementi, comprensivi di contenuti testuali, file multimediali, elenco dei partecipanti ai gruppi e canali, arrivando ad individuare, in alcuni casi, informazioni relative all'identità degli utenti convolti nelle attività sospette.
L'analisi si è svolta seguendo un approccio di ricerca top-down, attraverso strumenti di occultamento propri del sistema MEDUSA®, come ad esempio le Sandbox, consentendo una ricerca automatizzata su gruppi e canali all'interno di Telegram. In questo modo l'attività preliminare di ricerca si è svolta in completa sicurezza, emulando su una macchina virtuale un dispositivo mobile, in modo tale da rendere il più possibile sicura l'attività di indagine.
Tutti i dati raccolti sono stati collezionati in maniera completamente anonima da parte del sistema e storicizzati nel database in modo tale da permettere un'eventuale analisi a posteriori dei dati raccolti, anche in caso di successiva cancellazione da Telegram.

Sono stati raccolti anche altri elementi quali ad esempio Item ID e User ID, identificativi univoci utili a riconoscere un utente o un determinato elemento.

La ricerca ha consentito di analizzare la tipologia e la quantità di utenti presenti in questi gruppi, il numero di messaggi, il numero di interazioni, oltre all'individuazione dei soggetti promotori di queste attività.

Attraverso l'analisi è stato possibile individuare i seguenti elementi:

- 7.462 file multimediali, tra cui:
  - 393 Documenti d'Identità
  - 141 Passaporti
  - 129 Patenti di guida
  - 67 Documenti personali di altro tipo
- 2.307 messaggi di testo:
  - 26 utenze telefoniche
  - 14 indirizzi di criptovalute
  - 7 indirizzi email
  - 63 luoghi
  - 4 indirizzi IP
- 21.912 utenti di gruppi e canali.

Si rappresenta di seguito un caso operativo che ha consentito di individuare una possibile identità collegata ad una attività di Falso Documentale.

Si è proceduto secondo le seguenti fasi:

1. **Focus su una specifica area geografica di provenienza dei documenti**
   Attraverso lo strumento di Media Monitoring di MEDUSA® è stato possibile elencare rapidamente i soli documenti di carattere nazionale.
2. **Filtraggio per identificativi univoci**
   Al fine di individuare i soggetti promotori di tali attività, è stato applicato un filtro per evidenziare elementi univoci ad essi collegati.
   Il risultato ha evidenziato la presenza di un numero di cellulare di possibile interesse poiché ripetuto più volte all'interno dei messaggi di testo e con chiaro intento promozionale.
3. **Profilatura del potenziale Target**
   Inserendo il numero di cellulare del punto precedente all'interno dello strumento Cerca Persone, che consente di ricercare informazioni di carattere privato presenti online, è stato individuato un nominativo ed il relativo indirizzo e-mail, oltre ad ul-

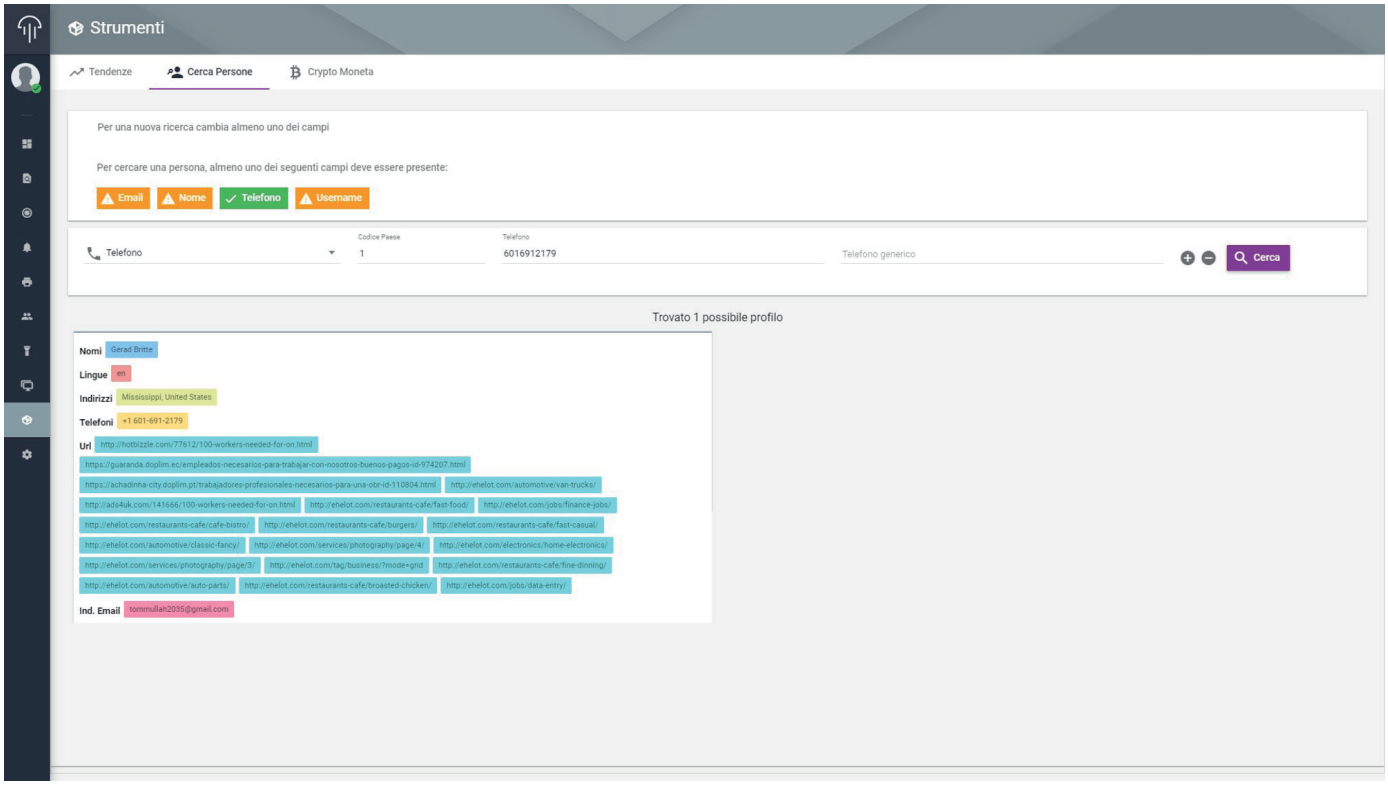

Figura 3 - Evidenza del potenziale soggetto promotore della vendita illecita.

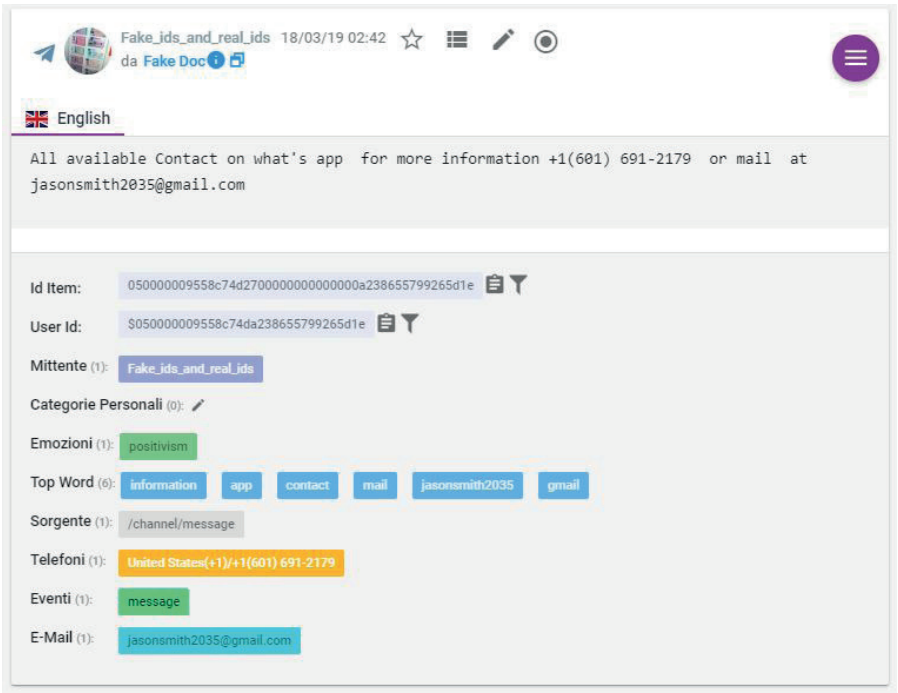

Figura 4 - Identificazione di un potenziale profilo attivo nella vendita dei documenti falsi su un canale di Telegram.

teriori risultati quali ad esempio la foto, le relazioni e numerose URL.

4. **Evidenza su fonti aperte**
   Tramite l'analisi delle URL individuate, utilizzando la navigazione assistita e sicura, agevolata dallo strumento delle Sandbox di cui sopra, sono emerse numerose pagine web con informazioni relative al Target come le attività lavorative, ulteriori messaggi di testo, il nome e l'indirizzo Web di un'azienda di proprietà dello stesso soggetto attenzionato.

I quattro rapidi passaggi sopra descritti hanno consentito, partendo da un'analisi generale di Telegram, di identificare un Target particolarmente attivo nella promozione, diffusione e vendita di Documenti Falsi. ©