Facebook OSINT: come ricavare informazioni tramite specifiche Query

Author : Sergio Caruso

Date : 12 dicembre 2018

Le tecniche OSINT permettono di ricavare informazioni da fonti pubbliche come:

- **Mezzi di comunicazione** — giornali, riviste, televisione, radio e siti web.
- **Dati pubblici** — rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi.
- **Motori di ricerca e community**

Anche sulle piattaforme Social è possibile ricavare informazioni senza per forza far riferimento a software del settore come Maltego e relativi Transform (es. SocialLinks).

Facebook è una di quelle piattaforme che meglio si presta alla raccolta d'informazioni.

Nell'articolo sarà illustrato un procedimento che potrà poi essere automatizzato in completa autonomia, scrivendo qualche riga di codice o semplicemente creandosi un form in HTML.

Il "Facebook OSINT" si avvale quindi di due grosse macro-categorie:

- Google Dork (solo tecnica)
- Manipolazione delle URL

Queste tecniche permettono di scoprire informazioni su persone, gusti, mi piace, recensioni, luoghi visitati e tutte quelle informazioni che non sono reperibili dal profilo dell'utente stesso.

Il primo passo è quello di cercare il codice numerico dell'utente Facebook, per poterlo poi inserire in specifiche posizioni di una URL.

Le URL che utilizzeremo sono così composte:

1. URL statica

2. ID Utente
3. Termine di ricerca

| URL statica | ID utente | Variabile di ricerca |

https://www.facebook.com/search/0000000/photos-liked

Seguendo questo piccolo schema, che sarà sempre identico nella struttura, possiamo utilizzare le variabili di ricerca.

Per ogni variabile di ricerca, ho specificato il corrispondente in italiano e la struttura della URL

- ***Places Visited / Luoghi visitati***
  https://facebook.com/search/[User ID]/places-visited
- ***Recent Places Visited / Luoghi visitati di recente***
  https://facebook.com/search/[User ID]/recent-places-visited
- ***Places Checked/In / Luoghi in cui ci si è registrati***
  https://facebook.com/search/[User ID]/places-checked-in
- ***Places Liked / "Mi Piace" ai luoghi***
  https://facebook.com/search/[User ID]/places-liked
- ***Pages Liked / "Mi Piace" alle pagine***
  https://facebook.com/search/[User ID]/pages-liked
- ***Photos By User / Foto dell'utente***
  https://facebook.com/search/[User ID]/photos-by
- ***Photos Liked / "Mi Piace" alle foto***
  https://facebook.com/search/[User ID]/photos-liked
- ***Photos Of /Tagged / Foto in cui l'utente è stato taggato***
  https://facebook.com/search/[User ID]/photos-of
- ***Photos Comments / Commenti alle foto***
  https://facebook.com/search/[User ID]/photos-commented
- ***Photos Interacted / Interazioni con foto***
  https://facebook.com/search/[User ID]/photos-interacted
- ***Photos Interested / Foto di interessi***
  https://facebook.com/search/[User ID]/photos-interested
- ***Photos Recommended / Foto raccomandate***
  https://facebook.com/search/[User ID]/photos-recommended-for
- ***Apps Used / App in uso***
  https://facebook.com/search/[User ID]/apps-used
- ***Videos / Video***
  https://facebook.com/search/[User ID]/videos
- ***Videos Of User / Video dell'utente***
  https://facebook.com/search/[User ID]/videos-of
- ***Videos Tagged / Video con Tag***
  https://facebook.com/search/[User ID]/videos-tagged
- ***Videos By User / Video per l'utente***
  https://facebook.com/search/[User ID]/videos-by

- ***Videos Liked / "Mi Piace" ai video***
  https://facebook.com/search/[User ID]/videos-liked
- ***Video Comments / Commenti ai video***
  https://facebook.com/search/[User ID]/videos-commented
- ***Future Event Invitations / Inviti agli eventi futuri***
  https://facebook.com/search/[User ID]/events
- ***Events Year / Eventi per anno (da specificare)***
  https://facebook.com/search/str/[User ID]/events/[Year]/date/events/intersect/
- ***Events Created Year / Eventi creati dall'utente in un anno specifico (da indicare)***
  https://facebook.com/search/str/[User ID]/events-created/[Year]/date/events/intersect/
- ***Events Invited Year / Inviti agli venti in un anno specifico (da indicare)***
  https://facebook.com/search/str/[User ID]/events-invited/[Year]/date/events/intersect/
- ***Events Joined Year / "Partecipo\Mi interessa" agli venti in un anno specifico (da indicare)***
  https://facebook.com/search/str/[User ID]/events-joined/[Year]/date/events/intersect/
- ***Posts by User / Post dell'utente***
  https://facebook.com/search/[User ID]/stories-by
- ***Posts by Year / Post dell'utente per anno (da specificare)***
  https://facebook.com/search/[User ID]/stories-by/[Year]/date/stories/intersec
- ***Posts Tagged / Post con Tag***
  https://facebook.com/search/[User ID]/stories-tagged
- ***Posts Liked / "Mi Piace" ai Post***
  https://facebook.com/search/[User ID]/stories-liked
- ***Posts Commented / Commenti ai post***
  https://facebook.com/search/[User ID]/stories-commented
- ***Employers / Luogo di lavoro\Datore di lavoro\Azienda***
  https://facebook.com/search/[User ID]/employers
- ***Reviews / Recensioni***
  https://facebook.com/[User ID]/reviews
- ***Groups / Gruppi***
  https://facebook.com/search/str/[User ID]/groups
- ***Co/Workers / Colleghi\Collaboratori***
  https://facebook.com/search/[User ID]/employees
- ***Friends / Amici***
  https://facebook.com/search/[User ID]/friends
- ***Followers / Followers***
  https://facebook.com/search/[User ID]/followers
- ***Relatives / Parenti***
  https://facebook.com/search/[User ID]/relatives
- ***Friends' Likes / "Mi Piace" degli amici alle pagine***
  https://facebook.com/search/[User ID]/friends/pages-liked

C’è da specificare che tutto ciò è normale, non si tratta di un bug o altro, ma è proprio Facebook che è strutturato in questa maniera; le limitazioni alla privacy sono decise da ogni singolo utente che interagisce con la piattaforma.

Un profilo che utilizza tutti gli accorgimenti di privacy possibili, interagendo con un altro utente che non le utilizza, deve “sottostare” alle impostazioni di quest’ultimo.

Riassumendo, nelle interazioni, chi ha il livello di privacy più basso, decide la visibilità o meno delle informazioni.

Di seguito, ho voluto effettuare degli esempi pratici proprio per constatare l'efficacia di una indagine OSINT condotta in questo modo:

Ho preso come esempio il profilo Facebook di Bill Gates (questa tecnica vale sia per i profili che per le pagine):

https://www.facebook.com/BillGates/

Fig1 – Pagina\Profilo di Bill Gates

Adesso occorre ricavare l'ID del profilo.

Per semplificare i passaggi ho utilizzato un tool online molto intuitivo

Find your Facebook ID
https://findmyfbid.com/

Fig2 – Inserimento del link al profilo nel form del servizio “Find your Facebook ID”

Inserendo la URL del profilo, come da immagine, ci viene immediatamente restituito l'ID **216311481960**

Fig3 – ID del profilo di Bill Gates

Adesso che abbiamo l'ID, possiamo svolgere tutte le ricerche che desideriamo, l’importante è che nello stesso browser, ci sia una sessione Facebook attiva, dato che la piattaforma blocca qualsiasi richiesta effettuata dall’esterno.

Non occorre essere amici del profilo o seguire la pagina oggetto di studio, può bastare anche un profilo TEST.

Vediamo che foto piacciano a Bill

| URL statica | ID utente | Variabile di ricerca |

https://www.facebook.com/search/216311481960/photos-liked

Fig4 – Dettaglio delle foto dove Bill ha messo un “Mi Piace”

Con lo stesso identico procedimento di prima, possiamo vedere tutti i commenti effettuati sotto le foto

https://www.facebook.com/search/216311481960/photos-commented

Fig5 – Dettaglio delle foto commentate

Fig6 – Il commento inserito sotto una foto

Qui invece abbiamo la lista delle pagine che Bill segue

https://www.facebook.com/search/216311481960/pages-liked

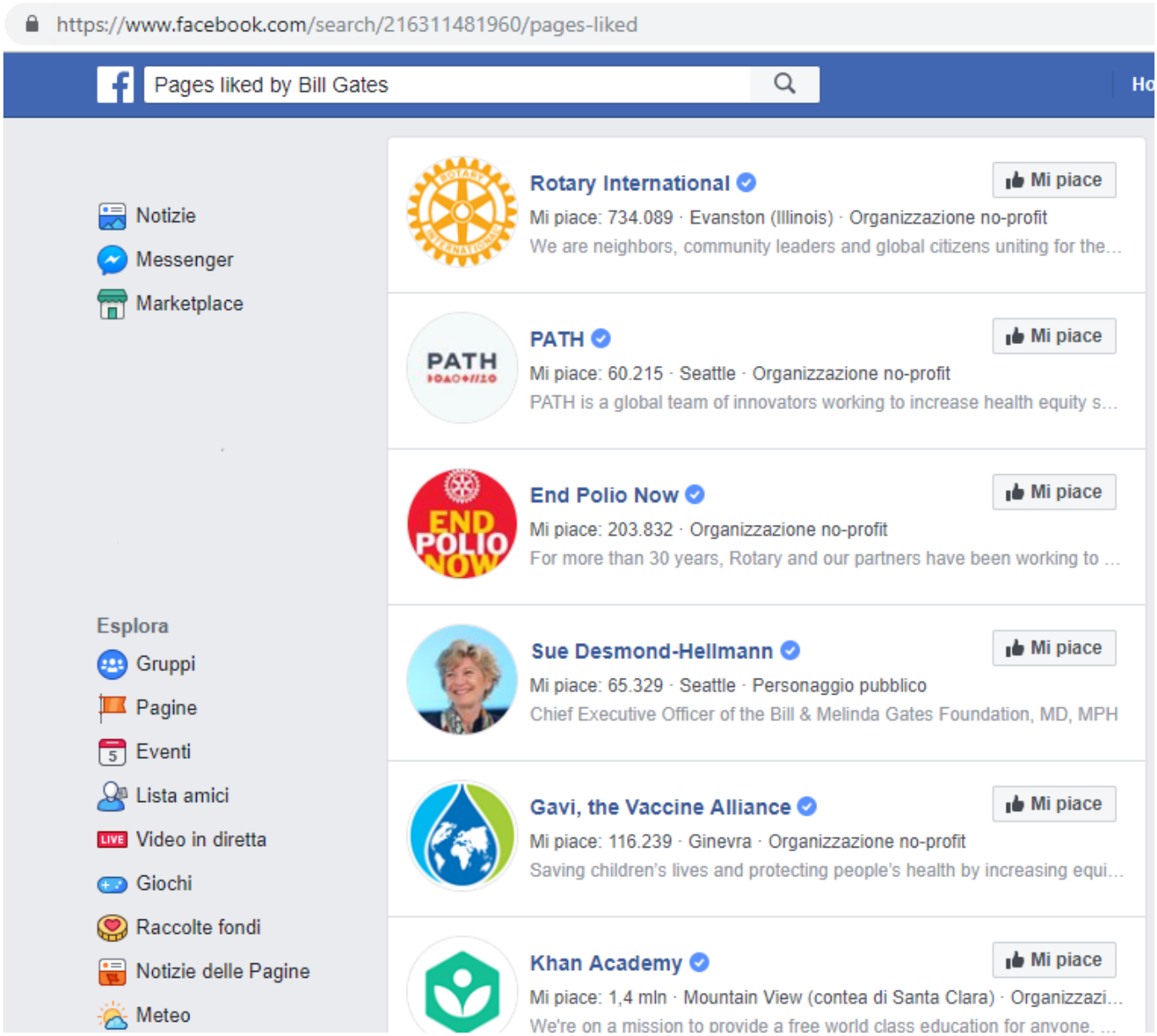

Fig7 – Lista delle pagine seguite

Abbiamo visto che, anche se si tratta di una pagina, lo stesso identico procedimento è possibile effettuarlo con il profilo personale di un utente

Effettuando la stessa prova con la pagina di Mark Zuckerberg, otteniamo altri risultati molto dettagliati

Il primo passo è sempre quello di ricavare l'ID utente partendo dal link del suo profilo:

https://www.facebook.com/zuck

Con lo stesso metodo di prima, utilizziamo il servizio “Find your Facebook ID”

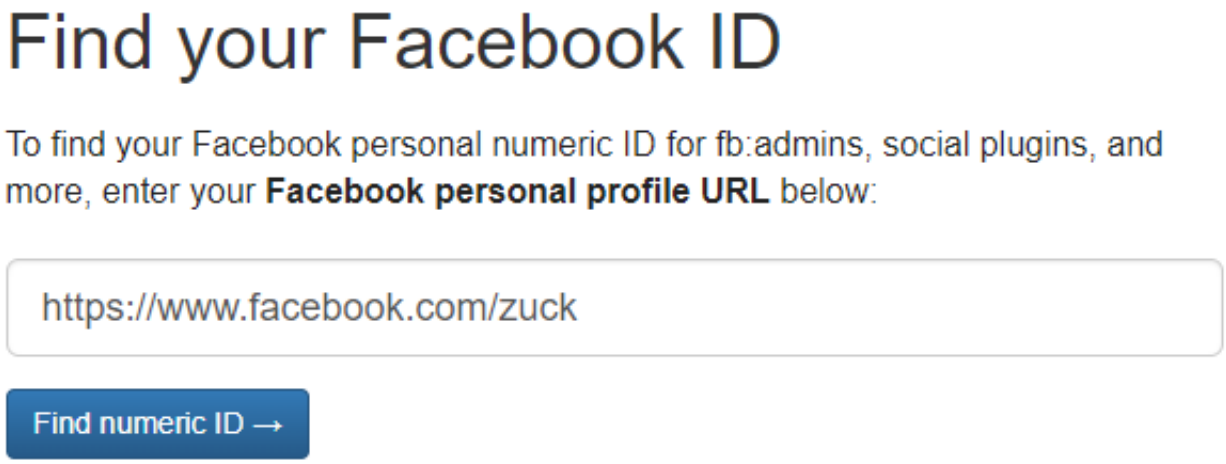

Fig8 – Inserimento del link utente nel form

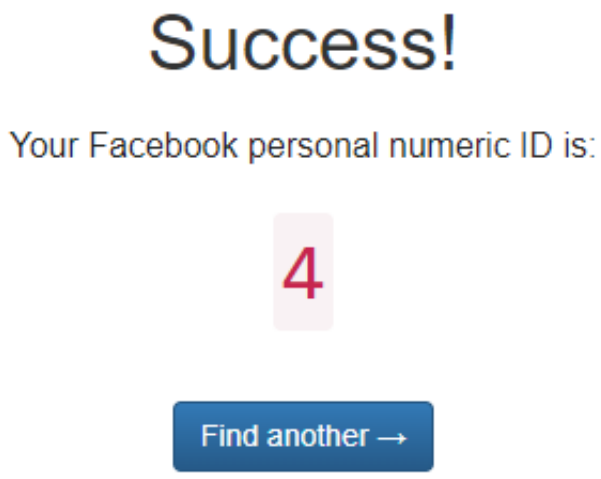

Fig9 – ID utente restituito dal servizio

Ricostruendo la URL, abbiamo i seguenti parametri

| URL statica | ID utente |

https://www.facebook.com/search/4/

Analizzando i risultati, riusciamo a trovare i vari commenti lasciati da Mark su varie foto

https://www.facebook.com/search/4/photos-commented

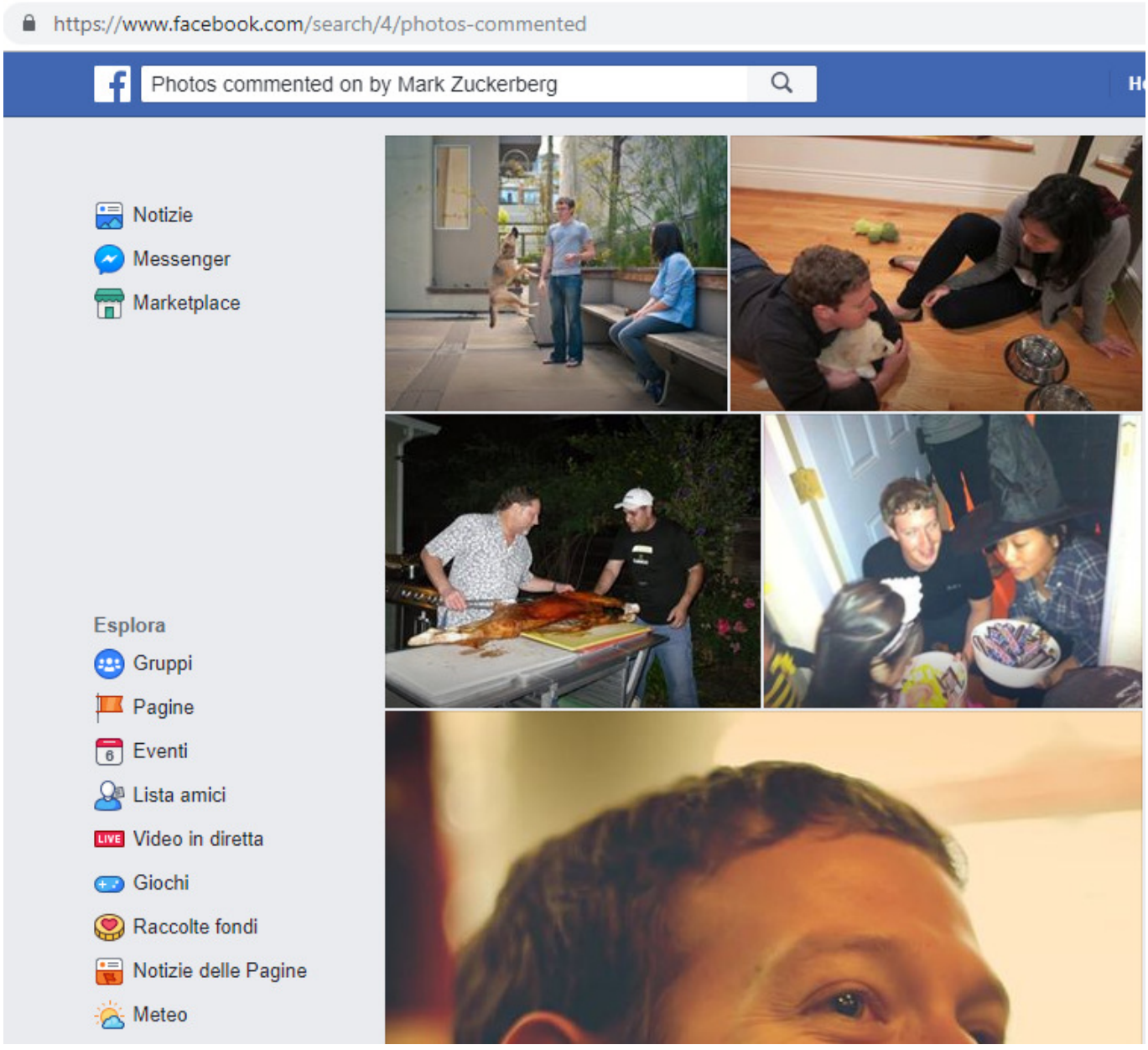

Fig10 – Varie foto commentate da Mark

Fig11 – Dettaglio di un commento

Si è parlato anche delle tecniche di “Dorking”, però possono essere utilizzate per ottenere informazioni a largo spetto.

Infatti, se utilizzassimo la query “Photos commented on by Bill Gates” come nell’esempio precedente, otterremmo dei risultati grossolani.

Se addirittura venisse utilizzata per un nome comune come ad esempio Mario Rossi, i risultati sarebbero numerosi, ma prenderebbe i dati di tutti gli utenti che hanno quel nome e cognome

Fig12 – Query di ricerca in Facebook

Difatti, inserendo la ricerca su Facebook nella relativa casella, otterremo anche una URL non attinente a quella in esame

https://www.facebook.com/search/top/?q=photos%20commented%20on%20by%20bill%20gates&epa=SEARCH_BOX

Per motivi di privacy sulla pubblicazione dell’articolo, ho evitato di analizzare profili personali, ma posso assicurare che le informazioni ottenute con questa tecnica sono molte e sui profili che adottano tutte le impostazioni di privacy al massimo, i risultati sono ottimi.

Articolo a cura di **Sergio Caruso**