OSINT, LinkedIn

Maria Ausilia Napoli Spatafora¹

Sommario

OSINT è l'acronimo di Open Source Intelligence ed indica quell'insieme di tecniche di intelligence atte a raccogliere informazioni pubbliche, gratuite e legali al fine di costruire dossier su soggetti, aziende e/o prodotti. Non è difficile comprendere come i social network siano diventati una fonte di notevolissima importanza per le ricerche OSINT: la quantità di dati al minuto che questi ultimi immagazzinano nei propri database è immensa e, non a caso, si parla di big data. Il trattamento dei big data non è semplice e così sono stati creati dei tool gratuiti e non che consentono di effettuare ricerche focalizzate e automatizzate. Lo scopo di questo report è di fornire un esempio di ciò con il social network LinkedIn molto utilizzato da aziende e professionisti che, per mezzo dei tool gratuiti che verranno esaminati, possono conoscere informazioni importanti per le proprie ricerche di mercato e non solo.

¹Dipartimento di Matematica e Informatica, Università degli Studi di Catania, ausilianapoli@gmail.com - X81000442

Indice							
	Introduzione						
1	LinkedIn						
2	The Endorser						
3	Linkedint						
4	Linkedin2username	;					
	Conclusioni						
	Riferimenti bibliografici						

Introduzione

Il termine OSINT sta per "Open Source Intelligence" e si tratta di uno degli aspetti chiave per comprendere la cybersecurity che regola il web dei nostri giorni.

Il termine OSINT è stato impiegato molti decenni fa: le agenzie militari statunitensi usano questo termine dal lontano 1980. Con questo termine ci riferiamo ad informazioni collezionate da risorse pubbliche disponibili su internet e non [1].

La keyword dietro il concetto di OSINT è "informazione" e - cosa molto importante - tale informazione deve essere ottenuta gratuitamente. Inoltre non importa che essa si trovi su giornali, blog, pagine web, tweets, social network, immagini, podcast o video, bensì importa che sia pubblica, gratuita e legale.

Conoscere le giuste informazioni, fa ottenere anche notevoli vantaggi sul proprio competitor a livello aziendale e non solo. Ogni organizzazione, infatti, dovrebbe sapere quali informazioni riguardanti le proprie attività "girano sul web" per affrontare con azioni mirate e concrete uno scenario di potenziale minaccia o per cogliere un vantaggio competitivo [2]. Con il loro diffondersi capillare e uso costante, i social network sono diventati una delle fonti principali per le tecniche OSINT: per mezzo di essi le aziende monitorano il sentiment

(le emozioni che gli utenti provano nei confronti di un oggetto e/o tema: es. rabbia, gioia, indifferenza...), uso improprio del marchio, spionaggio industriale, contraffazione, informazioni riservate... Ma monitorare il web significa lavorare direttamente sui Big Data e ciò comporta molteplici problemi: troppe informazioni da gestire, limitata disponibilità di informazioni per focalizzare la ricerca, lavoro manuale ripetitivo e frustrante, difficoltà nell'ottenere informazioni in tempo e nell'assegnare priorità ai risultati ottenuti. Esistono, tuttavia, vari tool che aiutano ad ottenere dati da centinai di siti in pochi

Questo report analizzerà le risorse disponibili per "fare" OSINT su LinkedIn in maniera rapida e comoda.

1. LinkedIn

Cos'è? LinkedIn è una piattaforma social impiegata principalmente nello sviluppo di contatti professionali (tramite pubblicazione e diffusione del proprio curriculum vitae) e nella diffusione di contenuti specifici relativi al mercato del lavoro (es. motore di ricerca del lavoro, pubblicità aziende, ecc.)[3]. Nel marzo del 2019 la rete ha superato 575 milioni di utenti[4].

Come funziona? A differenza di altri noti social network che sono finalizzati esclusivamente alla conoscenza di nuove persone, LinkedIn non è solo un social network dove possono essere postate foto, stati o dei semplici like come su Facebook. Su LinkedIn la cosa fondamentale è creare una "rete di contatti professionali"[5]. Oltre ad inserire il proprio curriculum, LinkedIn consente di mettere in risalto le proprie competenze e i propri punti di forza in ambito professionale e/o relazionale (le cosiddette skills) che potranno essere confermate dagli altri utenti (i cosiddetti riconoscimenti): se ne riporta un esempio 1.

Competenze e conferme	Aggiungi una nuova competenza
Rispondi al quiz di valutazione delle co	mpetenze
Audiometry - 2	
Giuseppe Petralia e 1 collegamento hanno cor	nfermato questa competenza
C++	
Python	
Strumenti e tecnologie	
Microsoft Office 7	Blogger - 4
с	
Competenze interpersonali	
Assistenza clienti - 3	
Lingue	
Lingua inglese . 2	
Altre competenze ®	
fitting protesi acustica 1	impedenzometria - 2
Article Creation -4	Biblioteca - 3
audiometria tonale	audiometria vocale - 1
mascheramento - 1	acufenometria - 1
otoscopia - 1	impronta auricolare - 1
processing-language	

Figura 1. La sezione competenze e conferme di un profilo LinkedIn

2. The Endorser

The Endorser[6] è un tool OSINT che permette di ottenere graficamente le relazioni tra utenti LinkedIn sulla base delle skills e dei riconoscimenti.

Esempio d'uso Per utilizzare questo tool occorre aprire il terminale e scrivere:

```
python3 the-endorser.py https://www.
linkedin.com/in/user1 https://www.
linkedin.com/in/user2
```

La figura 2 mostra il terminale con l'esecuzione del comando citato. L'output è un file che mostra le relazioni tra gli utenti selezionati. La figura 3 mostra la struttura del grafico fornito

```
ausilia@ausilia-VirtualBox:-/Documenti/the-endorser$ python3.6 the-endorser.py https://it.linkedir.com/in/maria-ausilia-napoli-spatafora-b5290836/en https://it.linkedin.com/in/siki-lembo-98485587 https://it.linked
```

Figura 2. Il terminale con il comando lanciato

in output e la figura 4 ne è un dettaglio.

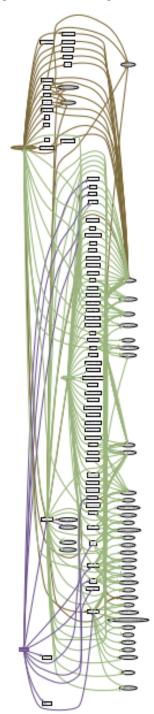


Figura 3. Il grafo di skills e riconoscimenti generato dal tool The Endorser

3. Linkedint

Linkedint[7] è un tool che consente di ottenere in csv o html la lista degli utenti afferenti ad una parola chiave che può essere il nome di una società; inoltre, è possibile filtrare anche tramite il dominio e/o dei prefissi della mail.

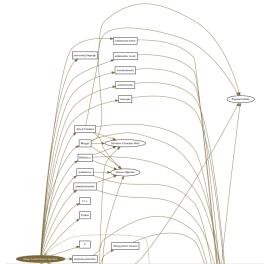


Figura 4. Un dettaglio del grafico mostrato in figura 3

Esempio d'uso Per utilizzare questo tool occorre digitare sul terminale:

python linkedint.py

Le figure 5, 6 e 7 mostrano rispettivamente il terminale e i due file forniti in output.



Figura 5. Il terminale con il comando lanciato

Photo	Name	Possible Email:	Job	Location
	Spendoon Settl	Clarifool.Catti@grv.com	HT Process Conclinator presso Ceneral Maters Outdat Propolaton Systems - Turko	Turin Area, Raly
	Sections Di Verdi	Gaetano Versili) gm.com	Curbet System Engineer	Turin Area, Italy
	Service MASHKOV	SergeyMASH0CV@gm.com	Curbol Systems Engineer (Functional Analysis) () General Motors - Cabol Propolation Systems	Turin Area, Italy
	Sectors Southern	Geverni Spadero gigm.com	Cornolland Engineer presso Altern	Turin Area, Italy

Figura 6. Una parte del file html generato in output con la keyword "General Motors" e dominio di email "gm.com"

4. Linkedin2username

Questo tool [8] richiede il nome dell'azienda della quale si vogliono conoscere i dipendenti connessi modulando la richiesta con dei parametri opzionali come –n per indicare un dominio

	A	В	C	D	E
	Circles	Getti	Giantuca Gata	Giantica Gattitions com	HR Process Coordinator presso General Motors Global Propulsion Systems - Torino
,	Gaetano	Di Venti	Gaetano Di Venti	Gaetano Ventidion com	Control System Engineer
	Sergery	MASHKOV	Serpey MASHKOY	Serpey MASHKOV/Bem.com	Control Systems Engineer (Functional Analyst) (D General Motors - Global Propulsion Systems
	Giovanni	Spedaro	Giovanni Spadaro	Govern Seedwolfen.com	Consultant Engineer presso Altran
	Eggg	He	Forg He	Ferg.Hedlan.com	Algorithm Design Development Engineer presso General Motors
	Agnese	Portora	Agnese Portera	Agress Porteradigm.com	Lab Engineer at General Motors Global Propulsion Systems
	Claudia	Crots	Clauda Crpti	Cleude Crott@grs.com	HR Coordinator at General Notice Powertrain Europe
	Costorgo	Principroduce	Costanzo Princiandero	Costaszo Princiandero (Egra com	Design Engineer presso General Motors
	giovanni	transport	piovenni franconi	giovarni franconi digra com	Development and Validation System manager presso GM Global Propulsion Systems - Torino SRL
0	Maria	Carrugia	Maria Carrugia	Maria Carrugholdigm.com	Technology System Engineer at General Motors
1	Simone	Alpe	Sirrore Aipe	Sirrore Apeglon, com	Lead ASIC Design Responsible Engineer at General Motors
	Francesco C.	Pesce	Francesco C. Pesce	FrancescoC.Pescedigm.com	Cirling. Technology Area Leader at General Motors Global Propulsion Systems
	Roberto	Bianchi	Roberto Bianchi	Roberts Swischighger.com	Base Collibration Engineer & System Hardware & Development Engineer presso General Motors
4	Davide	Mercuri	Davide Mercusi	Davide Mercurighans com	Controls Total Integration Engineer at General Motors
	Ivan Flaminio	Cozza	Ivan Plaminio Cozza	hvarFlorrinio,Cozzagbgm.com	presso
6	Lorenzo	Vendes	Lorenzo Venditi	Lorenzo Venditighan, com	Basic Sobware Engineer
7	Roffaele	Esposão	Raffaele Esposito	Raffaele Espositogbam com	Controls System Engineer presso General Motors
8	Luca	Garzocela	Luca Garzarella	Luca Gaczarelaghgru com	Development Validation System Manager at General Motors
	Giacomo	Ercole	Giacomo Ercole	Giocomo Ercoleghars.com	Supplier Quality Engineer presso General Motors
0	Daniele	Carvee	Daniele Carușo	Daniele Caruso@gm.com	System Development and Base Calibration Engineer
	Simone	D'Amico	Simone D'Amico	Simone DAnicostigm.com	Personal Banker presso Destsche Bank Italia
	Riccardo	Caramassi	Riccardo Caramassi	Riccardo Caramassidago com	Assistant Program Manager - Small Diesel Engine (1.36 presso General Motors
	Fabrizio	Above	Fabricio Abrate	Fabrigio Abratedigm.com	Controls Development Workgroup Leader at General Mators
	GALLERIA MAZZII	◆ 6M LÉCCE	GALLERIA MAZZINI GM LECCE	GALLERSAMAZZINLLECCE@grs.com	
Σ	Pegg	Cocegza	Pietro Cocazza	Pietro Coccezza@gm.com	Senior Total Validation Engineer presso General Mators Powertrain Europe
	Tomasz	Szczepankiewicz	Torsasz Szczepankiewicz	Tomasz Szczegonkiewicz@gm.com	ModelYear Manager at General Mators
		Figliotic	Recco Figliusis	Rocco, Figliusin digns, com	Disperte presso Ceneral Mators
	Gievenni	Matrici	Ciovanni Matrici	Ciovanni Matricigligni com	Serior Total Validation Engineer at General Motors
9	Alessandro	Zanoni	Alessandro Zanoni	Alessandro Zononidigra.com	Development & Validation System Manager presso GENERAL MOTORS POWERTRAIN - EUROPE SRL
	Stefano	Crassi	Stefano Grassi	Stefano Grassidium com	Global Program Management at GENERAL MOTORS
	Decie	Russe	Decio Russo	Decio,Russodign.com	Engine Handware Development Engineer presso GENERAL MOTORS GLOBAL PROPULSION SYSTEM
	Matteo	Presot	Moties Presot	Mattee Presot@gm.com	Supplier Quality Engineer presso General Motors
3	Disabella	Baletto	Disabetta Saletto	Elisabetta Saletio (Barn.com	DSE (Design System Engineer) for Small Diesel Engines for General Motors
	Glulla	Lombordo	Ciula Lombardo	Galla.Lombardo@gm.com	Supplier Quality Engineer at General Motors
5	Martina	Clorel	Martina Giorni	Martina Giornidians com	Control System Engineer presso GENERAL MOTORS POWERTRAIN - EUROPE SRIL
6	Vincence	Gena	Vincenzo Gesa	Vincenzo, Gesallion, com	Controller Integration Engineer (CIE)
7	Doniele	Zocco	Daniele Zocco	Daniele Zoccodigm.com	Control Integration Engineer presso GM Powerhain Europe
В.	Andrea			Andrea Mollanitions.com	Technology System Engineer (IIGM GPS - Toring

Figura 7. Una parte del file csv generato in output con la keyword "General Motors" e dominio di email "gm.com"

(es. "uber.com"); per ognuno dei dipendenti vengono trovate varie combinazioni di contatto e-mail. L'output consiste nei seguenti files di testo:

- nomeazienda-first.last.txt contiene l'elenco dei dipendenti nel formato nome.cognome ed eventualmente viene aggiunto il dominio (@nome.dominio) inserito come parametro (esempio 9);
- nomeazienda-first.txt contiene la lista del solo nome degli impiegati (esempio 10);
- nomeazienda-firstl.txt elenca i dipendenti per nome e la prima lettera del cognome (esempio 11);
- nomeazienda-flast.txt crea l'elenco degli impiegati con la prima lettera del nome seguita dal cognome per intero (esempio 12);
- nomeazienda-lastf.txt fornisce la lista del cognome seguito dalla prima lettera del nome per ogni dipendente (esempio 13);
- nomeazienda-rawnames.txt consiste nell'elenco di nome e cognome di ogni impiegato dell'azienda (esempio 14).

Esempio d'uso Sul terminale occorre scrivere il seguente comando per poter eseguire il tool:

```
python3 linkedin2username.py -u
   username -c azienda
```

Di seguito lo screen del terminale lanciato 8 e dei files di output (figure 9, 10, 11, 12, 13, 14).



Figura 8. Il terminale con il comando lanciato

gianluca.gatti@gm.com
giovanni.spadaro@gm.com
gaetano.di@gm.com
gaetano.venti@gm.com
sergey.mashkov@gm.com
feng.he@gm.com
agnese.portera@gm.com
claudia.crotti@gm.com
costanzo.prisciandaro@gm.com
giovanni.franconi@gm.com
maria.camuqlia@gm.com

Figura 9. Screen del file

general-motors-first.last.txt

gianluca@gm.com giovanni@gm.com gaetano@gm.com sergey@gm.com feng@gm.com agnese@gm.com claudia@gm.com costanzo@gm.com giovanni@gm.com

Figura 10. Screen del file

general-motors-first.txt

gianlucag@gm.com giovannis@gm.com gaetanod@gm.com gaetanov@gm.com sergeym@gm.com fengh@gm.com agnesep@gm.com claudiac@gm.com costanzop@gm.com giovannif@gm.com

Figura 11. Screen del file

general-motors-firstl.txt

ggatti@gm.com gspadaro@gm.com gdi@gm.com gventi@gm.com smashkov@gm.com fhe@gm.com aportera@gm.com ccrotti@gm.com cprisciandaro@gm.com gfranconi@gm.com

Figura 12. Screen del file

general-motors-flast.txt

gattig@gm.com spadarog@gm.com dig@gm.com ventig@gm.com mashkovs@gm.com hef@gm.com porteraa@gm.com crottic@gm.com prisciandaroc@gm.com franconig@gm.com

Figura 13. Screen del file

general-motors-lastf.txt

gianluca gatti
giovanni spadaro
gaetano di venti
sergey mashkov
feng he
agnese portera
claudia crotti
costanzo prisciandaro
giovanni franconi

Figura 14. Screen del file

general-motors-rawnames.txt

Conclusioni

Qualunque account LinkedIn può ottenere le stesse informazioni ricavate dai tool citati pur non usando questi ultimi; l'uso dei tool ha, però, consentito di passare da un processo di ricerca manuale generalizzato (costoso, inefficiente, con ritardo) ad un servizio più focalizzato (automatico, economico, intelligente, in tempo) utile alla scoperta di benefici e rischi per il business personale e/o dell'azienda. Questi tool gratuiti (esistenti non solo per LinkedIn, ma anche per gli altri social network) permettono di passare da "big data" a "small data" e i dati risultati, opportunatamente filtrati, aggregati, resi ordinabili, sono focalizzati, analizzabili con facilità e qualitativamente migliori.

Riferimenti bibliografici

- [1] Security Trails, What is OSINT? How can I make use of it? https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it.
- [2] P. Gasperi, L. Sbriz, and M. Tomazzoni. Monitoraggio Web: dai big data all'analisi di small data tramite OSINT. Un'implementazione pratica ed economica mediante web crawler. *Isaca Journal*, (1), 2018.
- [3] Wikipedia, LinkedIn. https://it.wikipedia.org/wiki/LinkedIn.
- [4] Kinsta, Mind-Blowing LinkedIn Statistics and Facts (2019). https://kinsta.com/blog/linkedin-statistics/.
- [5] Monetizzando, Linkedin: Cosa è, Come Funziona, Come Trovare Lavoro. https://www.monetizzando.com/linkedin/.
- [6] Github, The Endorser. https://github.com/eth0izzle/the-endorser.
- [7] Github, Linkedint. https://github.com/vysecurity/LinkedInt.
- [8] Github, Linkedin2Username. https://github.com/initstring/linkedin2username.