PRATICA S5L1

L’esercizio di oggi prevede una simulazione della fase di raccolta informazioni utilizzando dati pubblici su un target a scelta.
Lo scopo dell’esercizio è familiarizzare con i principali strumenti della fase di information gathering.

1. SELEZIONE DEL TARGET

Ho scelto come target Spotify, azienda innovativa nell’ambito audio-streaming.

2. RACCOLTA DELLE INFORMAZIONI CON GOOGLE

Per questa fase, ho utilizzato ricerche Google avanzate (query), applicando operatori specifici per ottenere informazioni mirate.

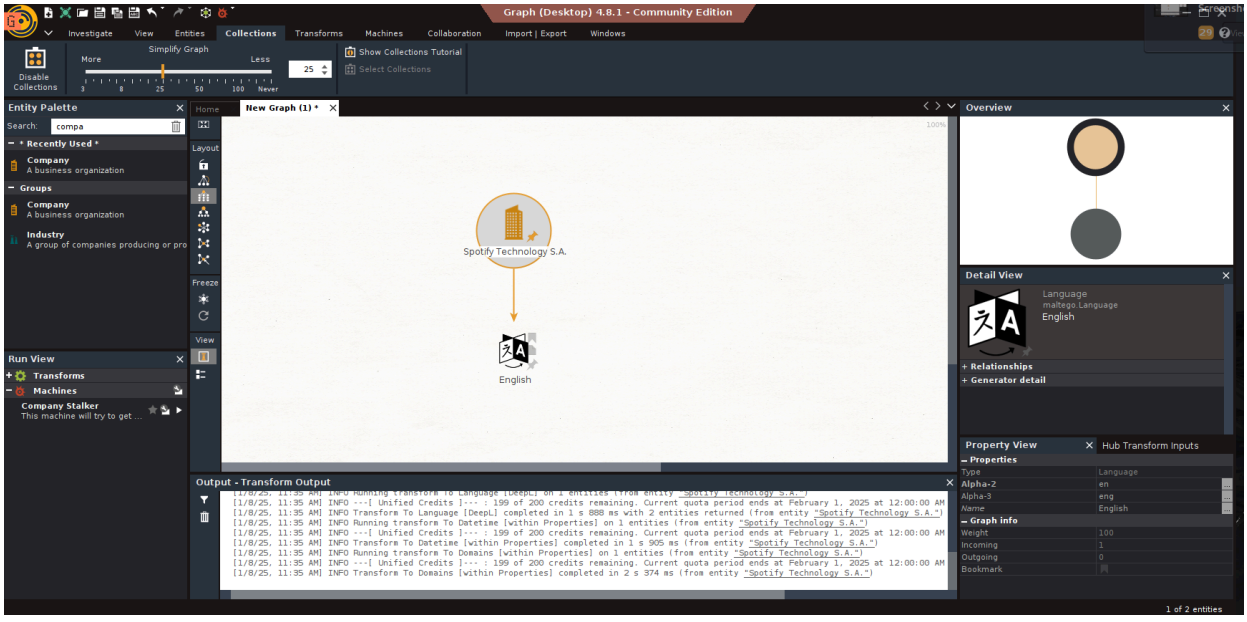
1. site:spotify.com per trovare informazioni di base sull’azienda.
2. site:spotify.com “contacts” per trovare informazioni sui contatti.
3. filetype:pdf site:spotify.com financial report per individuare report annuali finanziari e ottenere informazioni sul flusso di lavoro e di
crescita.
4. inurl:”privacy” site:spotify.com per ottenere informazioni sulle politiche di sicurezza vigenti.
5. site:spotify.com intext:”password” per verificare la presenza di informazioni sensibili in chiaro.
6. spotify “vulnerability report” per ottenere informazioni su vulnerabilità esistenti o modalità di segnalazione.
7. site:github.com spotify per ottenere eventuale codice sorgente o bug individuati dagli utenti.
8. spotify site:shodan.io per verificare eventuali dispositivi o sistemi
esposti.
9. spotify site:pastebin.com per evidenziare fughe di dati.
10. spotify feedback OR spotify “negative reviews” per ottenere informazioni sulla reputazione e sui problemi degli utenti.

3. RISULTATI

• Ho ottenuto diversi risultati per ognuna delle ricerche elencate sopra:
1. Informazioni di base sull’azienda come:
- CEO, Daniel EK.
- Fondazione, 23 Aprile 2006.
- Dipendenti, 7242.
- Fatturato, 13,25 mld.
- Sede principale, Stoccolma, Svezia
- Sede fiscale, Lussemburgo

2. Non espongono numeri di telefono ma si affidano principalmente all’assistenza via chatbot e mail.
3. Diversi PDF contenenti report annuali dove si espongono diverse figure interne in ruoli importanti dell’azienda, come analisi dei rischi. Comunicazioni sulla gestione dei flussi di lavoro per i vari dipartimenti.
4. Informativa sulla privacy appena aggiornata al 10 Ottobre 2024, che modifica la gestione dei dati degli utenti.
5. Nessuna password di account esposta, ma diverse lamentele da parte di utenti sul fatto che spotify continui a resettare le loro password, che potrebbe suggerire un uso imprudente degli ultimi.
6. Spotify utilizza un sistema basato su ricompense per ottenere informazioni sulle proprie vulnerabilità o bug da parte degli utenti
esterni, una di queste è stata scoperta da Umar Farooqui che ha ricevuto ben 200 dollari di ricompensa.
7. Sulla piattaforma Github nessun codice debole esposto
8. shodan.io manifesta la presenza di diversi server, alcuni di questi lavorano con porta 80 aperta.
9. Uno script per rimuovere i brani in eccesso dalle proprie playlist, e l'apk di spotify
10. Recensioni negative dai motivi più disparati, tra cui il prezzo del piano premium, bug nella piattaforma web, e tanti altri

Ho inserito le informazioni ottenute su Maltego e ho ottenuto delle nuove informazioni come si vede dalla mappa:



CONCLUSIONI:

Un esercizio davvero interessante che dimostra quanto sia a volte facile reperire delle informazioni, anche molto gravi come nel caso
delle carte di credito rubate, sul web. Maltego è uno strumento davvero potente che facilita enormemente il processo di Information
Gathering e aiuta a creare una mappa visiva e mentale che aiuta a seguire investigazioni molto vaste.