S5-L1

MALTEGO

Maltego è uno strumento di analisi e intelligence dei dati progettato per scoprire e visualizzare relazioni tra informazioni provenienti da fonti diverse. È particolarmente utilizzato in ambiti come la sicurezza informatica, la criminalistica e l'analisi di dati aziendali.

Caratteristiche Principali

1. \*\*Visualizzazione Grafica\*\*: Maltego rappresenta i dati sotto forma di grafi, consentendo di vedere chiaramente le connessioni tra diverse entità, come persone, aziende, indirizzi IP e domini.

2. \*\*Raccolta di Dati\*\*: Lo strumento integra diverse fonti di dati, inclusi social media, registri di dominio e informazioni pubbliche, per raccogliere informazioni rilevanti su un soggetto specifico.

3. \*\*Trasformazioni\*\*: Maltego utilizza "trasformazioni", che sono funzioni che permettono di eseguire query sui dati per ottenere informazioni dettagliate. Ad esempio, si possono cercare tutte le menzioni di una persona su vari social network.

4. \*\*Collaborazione\*\*: Consente a team di lavoro di collaborare su progetti, condividendo scoperte e dati in tempo reale.

Applicazioni

- \*\*Sicurezza Informatica\*\*: Per analizzare minacce e vulnerabilità.

- \*\*Investigazioni Forensi\*\*: Tracciare reti criminali e relazioni tra soggetti coinvolti in crimini.

- \*\*Analisi Competitiva\*\*: Studiare le attività dei concorrenti e raccogliere informazioni strategiche.

- \*\*Intelligence Aziendale\*\*: Monitorare la reputazione del brand e analizzare il sentiment del mercato.

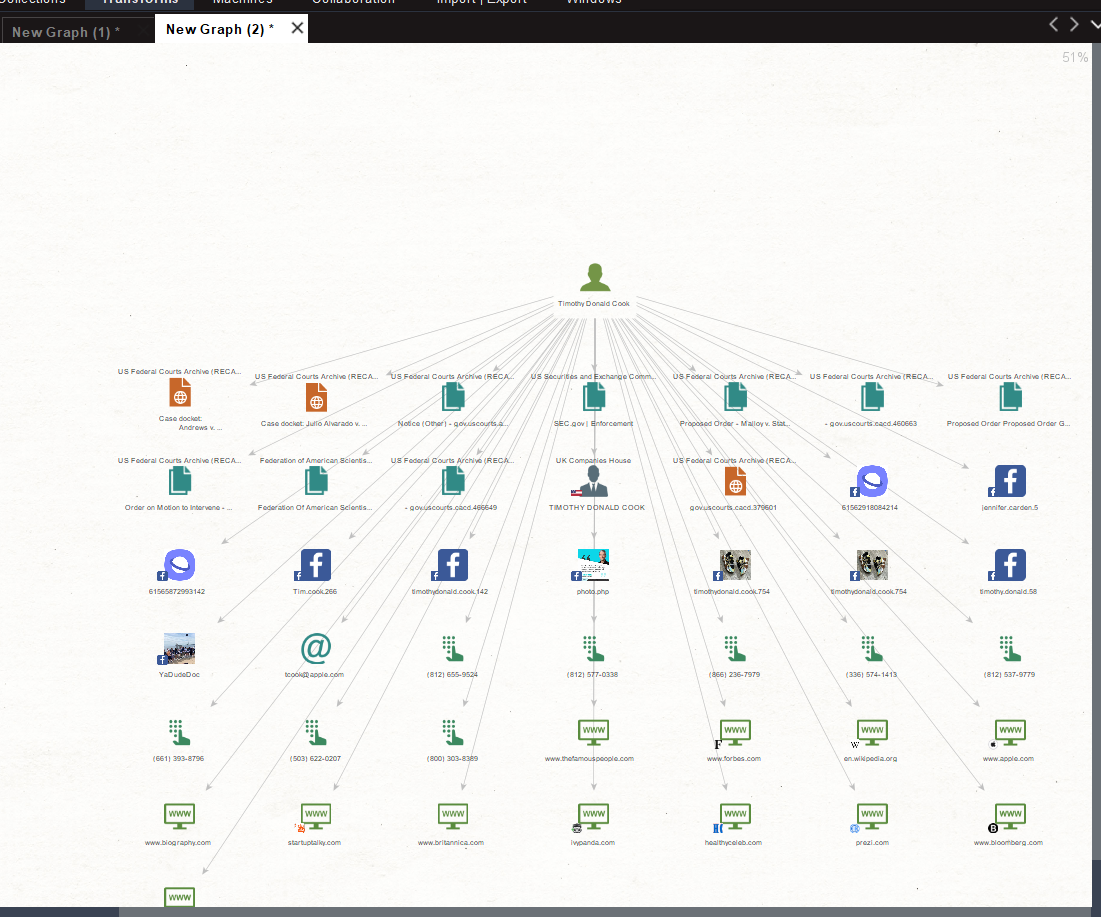
Conclusione

In sintesi, Maltego è uno strumento potente per l'analisi delle informazioni e la scoperta di relazioni complesse, utile per professionisti che operano in vari settori. La sua capacità di visualizzare dati in modo intuitivo e di raccogliere informazioni da fonti disparate lo rende un alleato prezioso nell'intelligence moderna.

Nella foto sotto abbiamo preso in esame “Timothy Donald Cook”, poniamoci infatti nei panni dell’azienda “apple” prima del suo arrivo.

L’azienda avrebbe dovuto fare a sua volta una ricerca su di lui, perché una società deve sempre avere la lungimiranza di prevenire un eventuale attacco e per farlo deve stare attenta anche alle persone che contatta per un colloquio ed un lavoro futuro.

Avremmo potuto usare questo programma nella fasi prima del colloquio, cosi avremo potuto sapere più informazioni su di lui.



Tra le varie cose che possiamo cercare troviamo:

* Email address
* Social media profile
* Domain e web presence

GOOGLE HACKING

Google Hacking, o "Google Dorking," è una tecnica che sfrutta operatori avanzati di ricerca di Google per trovare informazioni sensibili o vulnerabilità su siti web. Questa pratica permette di identificare informazioni come file non protetti, configurazioni di server, password esposte o anche interi database accessibili pubblicamente, utilizzando query specifiche.

Gli operatori utilizzati in Google Hacking includono:

- \*\*"filetype:"\*\* per cercare file di un certo tipo (es. PDF, DOC).

- \*\*"inurl:"\*\* per trovare URL contenenti parole specifiche (utile per individuare pagine di login, amministrazione, ecc.).

- \*\*"intitle:"\*\* per cercare titoli di pagine specifici (es. "Index of" per directory non protette).

- \*\*"site:"\*\* per restringere la ricerca a un dominio specifico.

Ad esempio, una query come `inurl:admin filetype:sql` potrebbe rivelare file SQL non protetti nelle directory di amministrazione, offrendo potenziali punti di accesso per gli hacker.

Sebbene Google Hacking sia legale, può diventare una pratica illecita se utilizzata per accedere a informazioni senza autorizzazione.

Esempio prendendo EPICODE

