CONSEGNA 20 FEBBRAIO S5L2

L'obbiettivo di oggi è quello di effettuare una simulazione di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo è quello di familiarizzare con i tool principali della fase di information gathering.

Il target scelto è un'indirizzo mail aziendale di una piccola azienda, nello specifico è l'indirizzo del Responsabile Direzione Tecnica. Per prima cosa ho inserito il target su Maltego e grazie alle varie Transform installate, come IPInfo, Etherscan, Shodan, ho cominciato la fase di raccolta dati.(vedi figura 1).

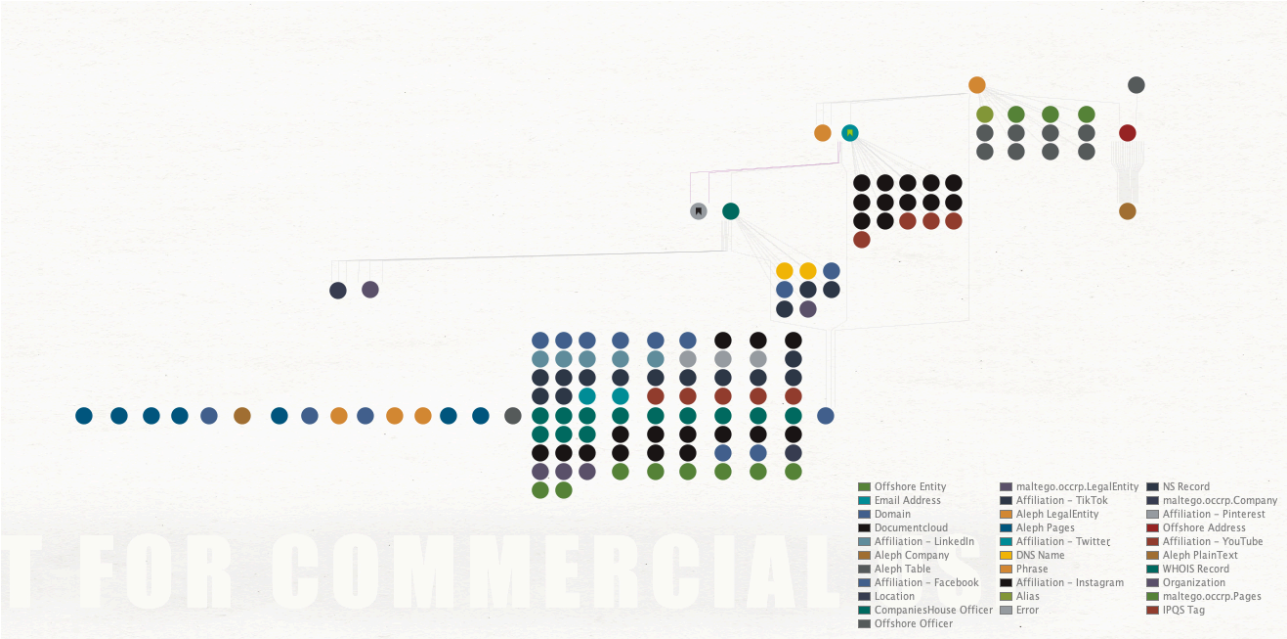

Fig 1 - Fase di ricerca, uso delle varie Transform

Durante la fase di ricerca, ho trovato il nome dell'amministratore delegato dell'azienda e tramite la Transform affilation ho avuto modo di ritrovare il nome in oggetto sui vari social da esso usato. Sicuramente in fase di analisi potremmo trovare delle vulnerabilità su tutto quello che riguarda il mondo dei social network e il modo in cui l'impiegato dell'azienda ne può usufruire in modo scorretto, aprendo le porte ad avventori malevoli.(Fig.2)

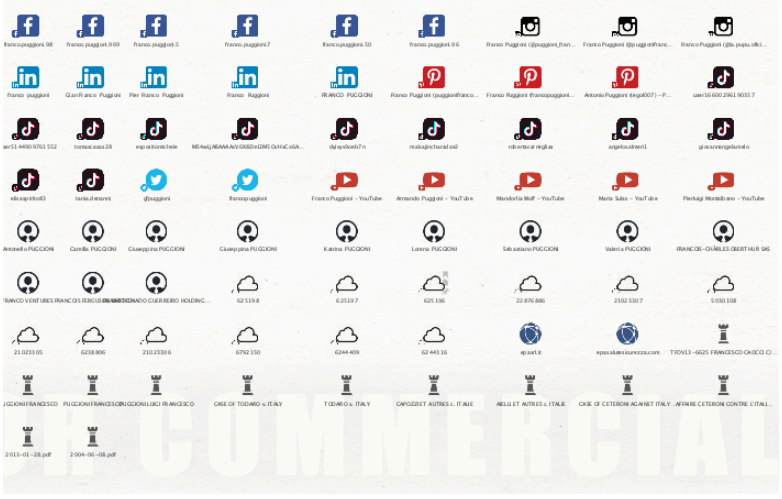

Fig. 2

In ultima istanza ho fatto un breve ricerca tramite i google doks, nello specifico ho usato intext, utile per localizzare pagine che contengono determinati caratteri o stringhe all'interno del proprio testo. Lo scopo era quello di vedere se l'indirizzo cercato potesse trovarsi in pagine, elenchi di siti "bucati" o elenchi SQL.(Fig.3) Nel risultato sono usciti pochi risultati riferiti unicamente all'azienda, dati i scarsi risultati, ho cercato l'indirizzo su haveibeenpwned.com per scoprire che l'indirizzo è stato esposto unicamente ad una violazione.

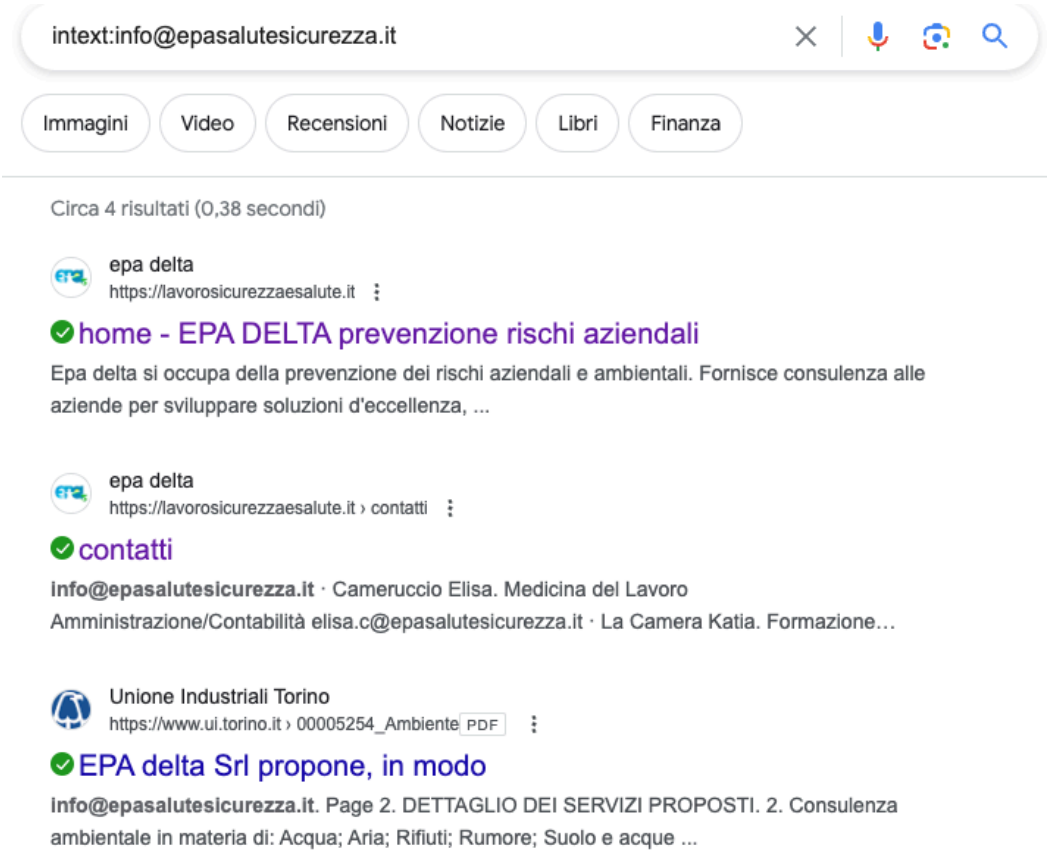

Fig.3