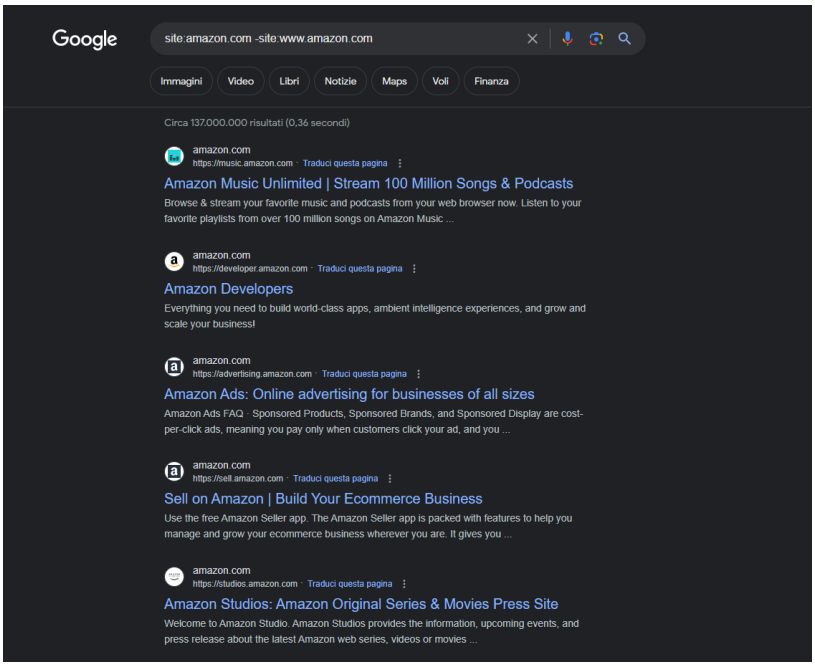
[CONSEGNA SETTIMANA 5 LEZIONE 2]

Raccolta di informazioni

Una delle prime fasi di un pentesting è la cosiddetta fase di raccolta delle informazioni. Tra i vari strumenti a nostra disposizione oggi utilizzeremo *le query di google e Maltego*.

Il nostro target è la società ***Amazon***, cerchiamo di raccogliere alcune informazioni di base tramite le ricerche su google.



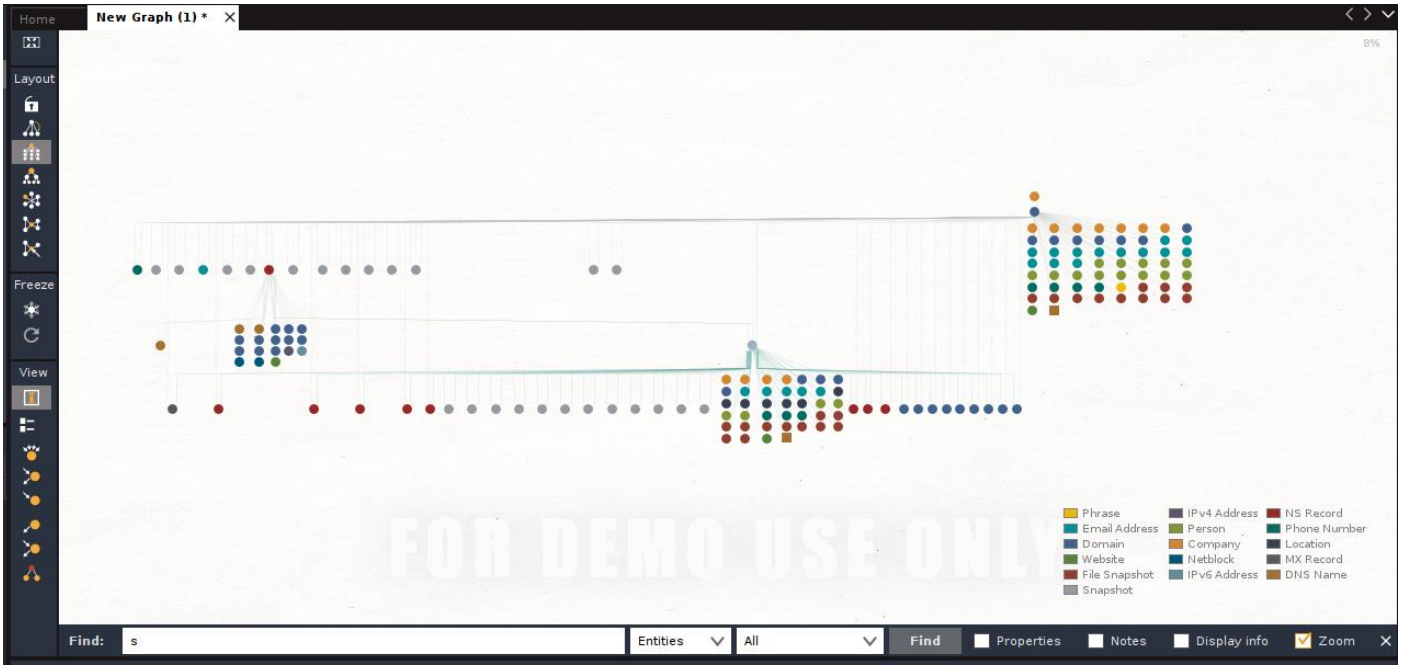
Possiamo notare da una prima ricerca tramite google che al URL amazon.com sono associati numerosi sottodomini che spaziano da siti web per la riproduzione della musica, a advertisement e produzione di film e serie tv originali dell'azienda.

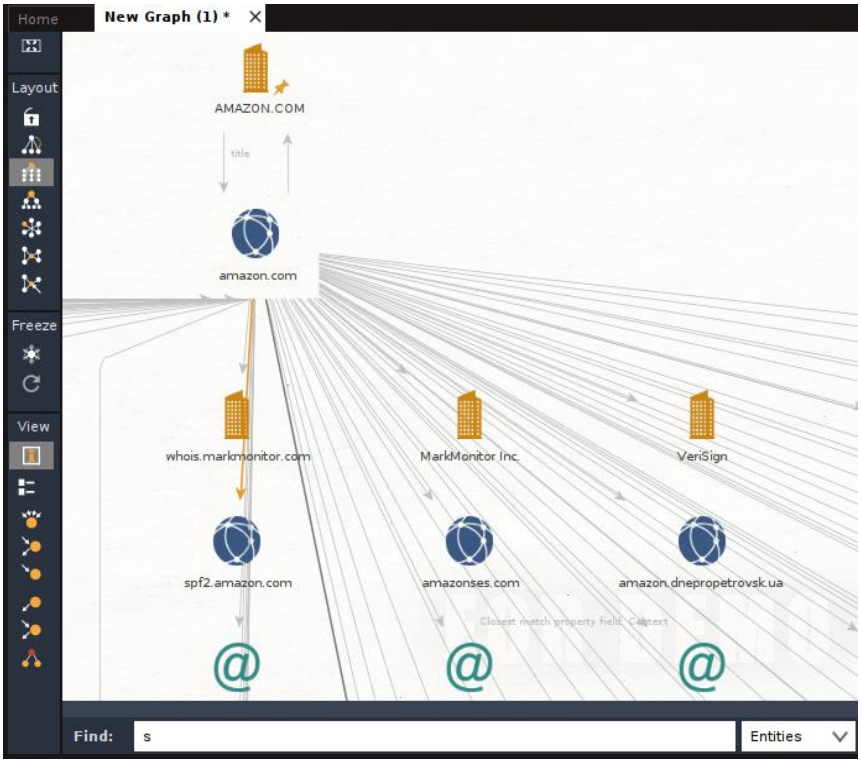
TARGET : Amazon.com

QUERY : site: -site:

RISULTATI: numerosi sottodomini che denotano una società di ampie dimensioni e che spazia in numerosi ambiti.

Possiamo quindi passare all utilizzo del software Maltego, per una ricerca più approfondita.





Partendo da una ricerca sulla società Amazon abbiamo riscontrato la presenza di un dominio principale, ovvero amazon.com, da qui, estendendo la ricerca abbiamo riscontrato la presenza di numerose informazioni tra cui:

- DNS
- Indirizzi email
- URL
- Persone (possibilmente dipendenti dell'azienda)
- File di snapshot
- Numeri di telefono
- Locazioni geografiche

La presenza di un così vasto numero di informazioni può risultare dispersivo ad una prima occhiata ma è sicuramente un grande passo avanti nella ricerca di informazioni riguardo l'azienda e di conseguenza ,dovessimo ragionare in termini malevoli, sarebbe un grande aiuto per un eventuale attacco.

Ci sono altri strumenti che si potrebbero utilizzare per la raccolta di informazioni, tra i più noti possiamo citare *Shodan, Whois* oppure *WaybackMachine*.