S5 - L1
Information gathering

Emanuele Benedetti | 7 gennaio 2025

Consegna

La consegna di oggi richiede di effettuare una simulazione della fase di raccolta di informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i principali strumenti della fase di information gathering.

Strumenti Principali:

1. **Google**
    - Utilizzato per la raccolta iniziale di informazioni
        - Esempi di utilizzo: ricerca di dati pubblici, articoli, profili social, documenti aziendali
2. **Maltego**
    - Strumento per l'analisi e la visualizzazione di relazioni tra persone, gruppi, organizzazioni, domini, siti web e altre entità. Permette di costruire mappe di connessioni e scoprire informazioni nascoste.

Svolgimento

Selezione del target

Ho deciso di prendere in esame due distinti target: *Epicode*, una scuola di formazione online ed *Accenture*, multinazionale statunitense operante nel settore della consulenza strategica. La decisione nasce dalla volontà di provare a reperire informazioni su aziende di grandezza diversa.

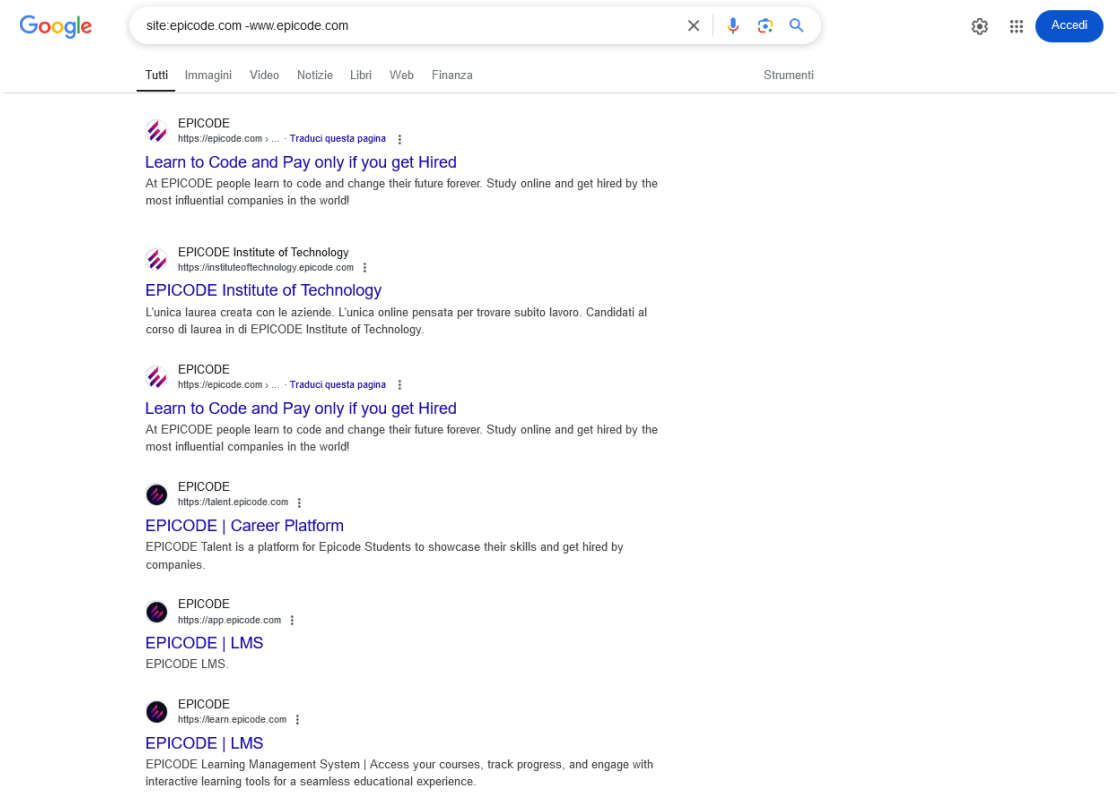
Raccolta di informazioni

Ho svolto la raccolta delle informazioni tramite *OSINT* (Open Source Intelligence).

In particolare, ho utilizzato il motore di ricerca Google attraverso l'utilizzo di operatori speciali che permettono di utilizzare Google al massimo delle proprie potenzialità per svolgere le ricerche.

Non avendo alcuna informazione sui target, ho cominciando cercando i siti web delle aziende.

Partendo da Epicode, ho cercato tutti i sottodomini indicizzati dal motore di ricerca tramite la tecnica del *Site Crawling*, utilizzando la query **site:epicode.com -www.epicode.com**. In questo modo il motore di ricerca filtra tutti i siti che contengono epicode.com omettendo i risultati che contengono www.epicode.com, in poche parole otteniamo informazioni circa i sottodomini di epicode.com escludendo ridondanze inutili.

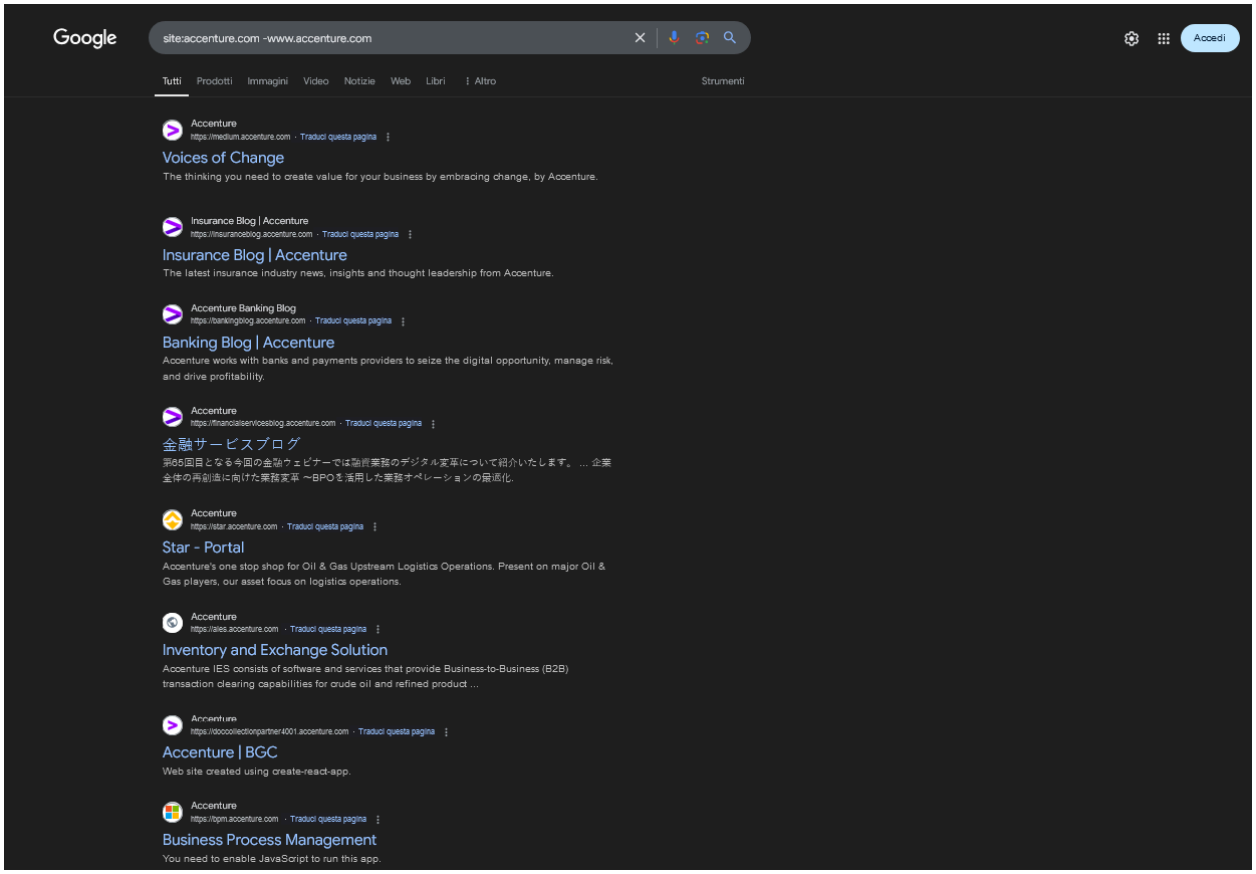


Come mostrato nell'immagine, sono venuto a conoscenza dei sottodomini di epicode.com, in particolare: instituteoftechnology.epicode.com, talent.epicode.com, app.epicode.com, ed infine learn.epicode.com.

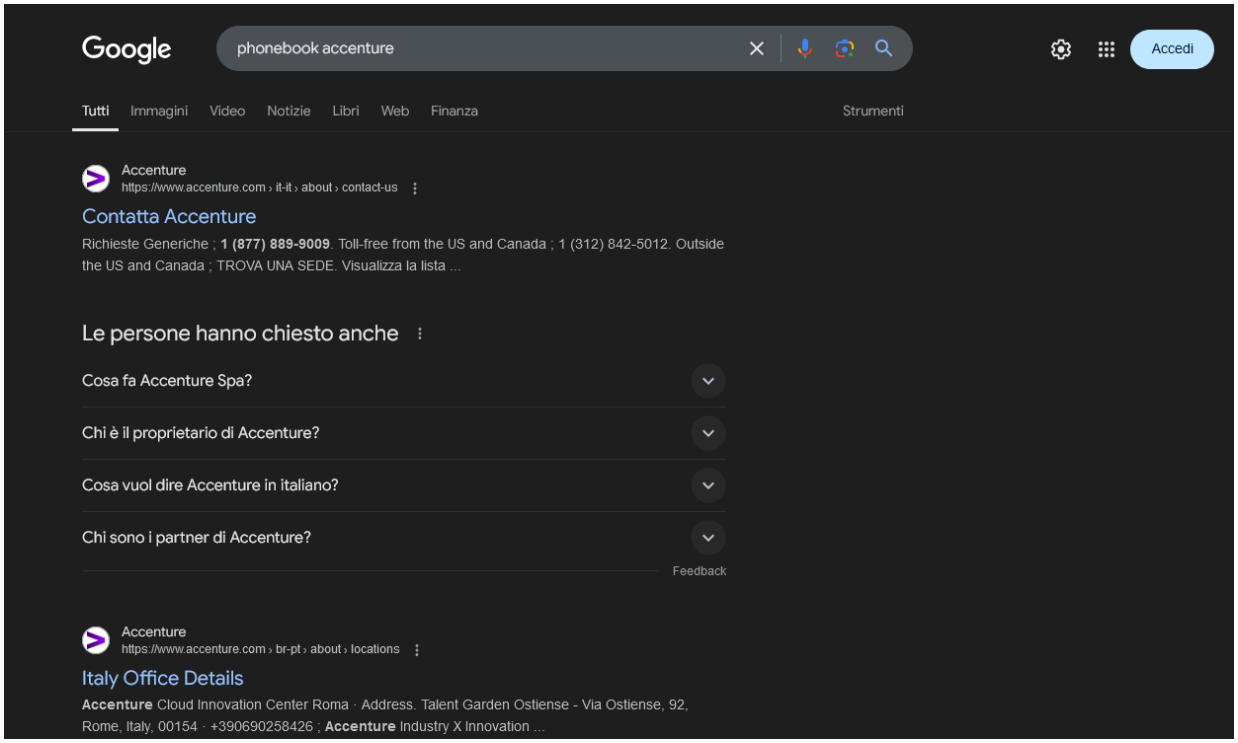
Ho provato a reperire ulteriori informazioni tramite google come numeri di telefono (utilizzando la keyword phonebook) senza tuttavia ottenere risultati.

Dopo aver raccolto le informazioni sulla prima azienda target, ho eseguito nuovamente i passaggi per ottenere le informazioni anche sul secondo obiettivo.

Ho cercato i sottodomini di Accenture tramite la query **site:accenture.com -www.accenture.com**, ottenendo: medium.accenture.com, insuranceblog.accenture.com, bankingblog.accenture.com, financialservicesblog.accenture.com, star.accenture.com e tanti altri domini di terzo livello.



Data la diversa grandezza del secondo target, ho cercato di ottenere i numeri di telefono dell'azienda e dei dipendenti. Tramite **phonebook accenture** sono riuscito a reperire diversi numeri di telefono di varie sedi dell'azienda e di alcuni dipendenti.



Raccolta informazioni ed analisi con Maltego

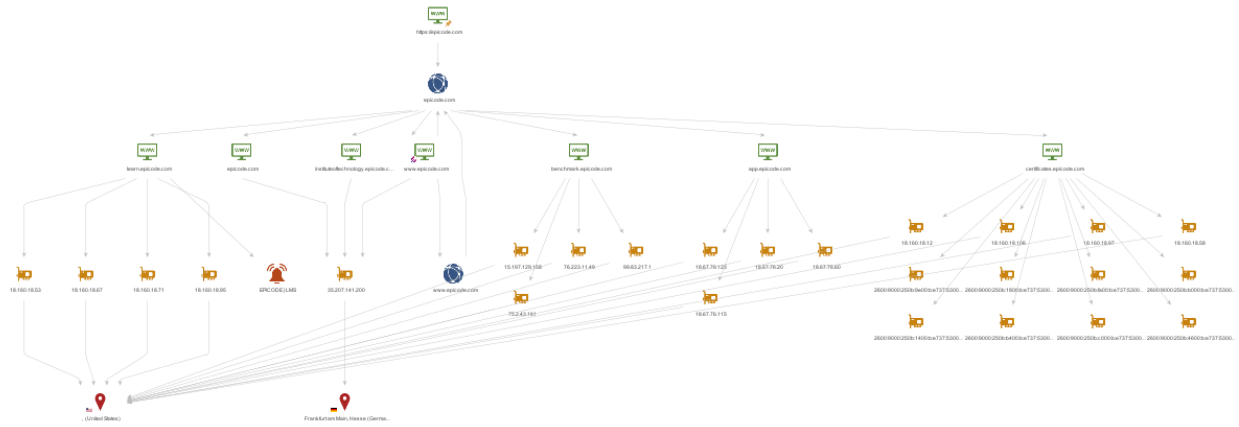
Dopo la raccolta di informazioni tramite motore di ricerca sono passato all'utilizzo dello strumento Maltego, strumento per la raccolta e l'analisi delle informazioni.

Il programma permette di integrare le informazioni già trovate e di trovarne di nuove non immediatamente visibili. Sempre partendo dal sito web ho incominciato a cercare nuove informazioni sul target Epicode. Date le medie dimensioni dell'azienda e le poco rilevanti informazioni reperibili online, mi sono concentrato soprattutto sull'ottenimento degli indirizzi IP e la localizzazione degli stessi.

Il grafico che segue, ottenuto tramite Maltego, mostra tutti gli indirizzi IP che il software è riuscito a trovare, partendo dai sottodomini ottenuti tramite ricerca su google.

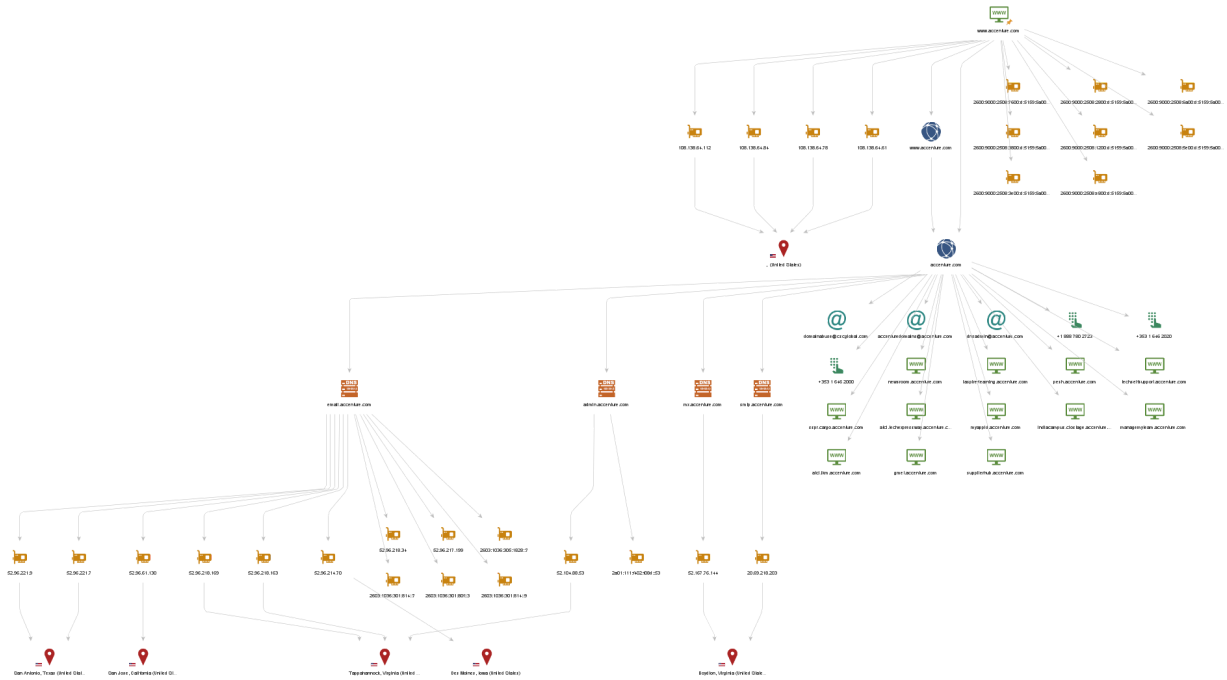
Il programma inoltre è stato in grado di individuare anche i sottodomini non indicizzati sui motori di ricerca (certificates.epicode.com e benchmark.epicode.com).

Tramite Maltego inoltre ho potuto visualizzare la localizzazione dei server che ospitano i siti web dell'azienda target (Frankfurt am Main in Germania e Dulles negli Stati Uniti).



Come da aspettative il secondo target ha mostrato molte più informazioni dovute alla maggiore grandezza dell'azienda. Dopo aver importato le informazioni ottenute precedentemente, ho ancora una volta cercato di ottenere ulteriori sottodomini non indicizzati e indirizzi IP dell'azienda come nel target precedente. Tuttavia per il secondo target mi aspettavo di ottenere maggiori informazioni come email aziendali numeri di telefono, oltre che alla localizzazione delle infrastrutture tramite indirizzi IPv4.

Come da aspettative il software Maltego è stato in grado di estrapolare tutte queste informazioni e fornirle sotto forma di grafico, come mostrato nell'immagine che segue.



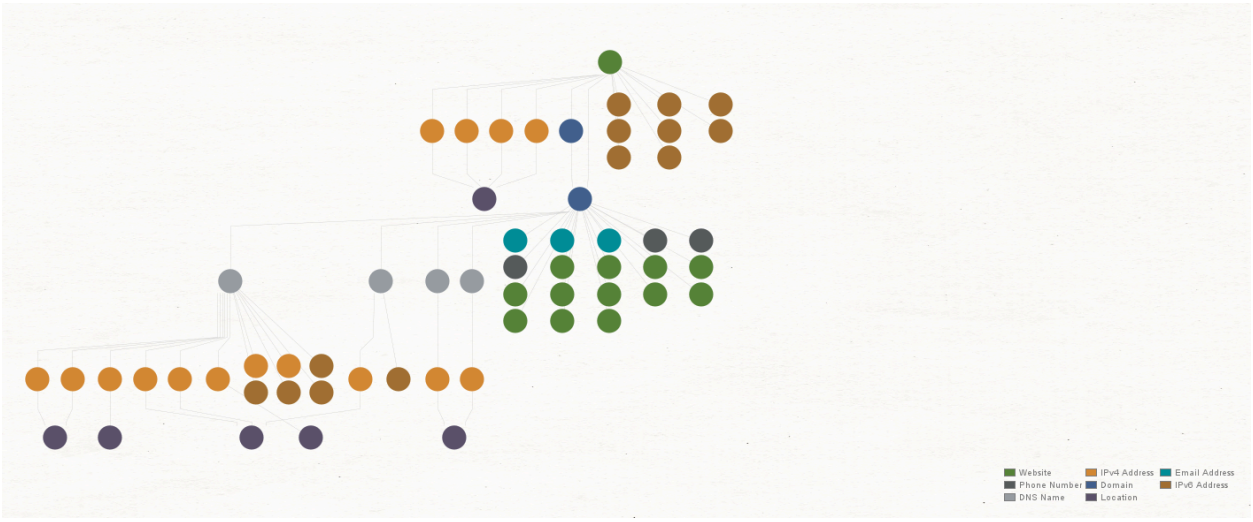
Come mostrato, si è stati in grado di reperire gli indirizzi dei server dell'azienda (ad esempio server mail) indirizzi email della società e numeri di telefono di varie sedi.

In questo caso invece i server si trovano tutti negli Stati Uniti, in particolare negli stati della California, Virginia ed Iowa.

Conclusione

Tramite motore di ricerca, utilizzando le opportune query e tecniche avanzate, è possibile ottenere informazioni importanti sui target scelti. Le tecniche passive di raccolta informazioni permettono di utilizzare fonti pubbliche senza interagire direttamente con il target e non richiedono l'utilizzo di alcun tool specifico.

Dopo una fase iniziale passiva è possibile approfondire la raccolta di informazioni tramite tool specializzati che permettono di analizzare e visualizzare tutti i dati collezionati. In particolare Maltego è uno strumento avanzato che mi ha permesso di realizzare questo report sulle aziende target scelte.



Le due immagini mostrano schematicamente, tramite una legenda, quali informazioni Maltego è stato in grado di raccogliere e collegare, per fornire un quadro completo dei target scelti.