

# Report Info Gathering

In questo report sono presenti i risultati di un'attività di raccolta di informazioni condotta sul target **Elon Musk**. L'analisi mira a delineare il profilo pubblico dell'entità investigata, mappandone la presenza digitale e le connessioni note.

## Obiettivi

- **Mappare la presenza digitale:** Identificare e documentare i principali profili social, siti web e domini associati a Elon Musk.
- **Raccogliere dati pubblici:** Reperire informazioni quali notizie, articoli, documenti aziendali e contatti resi pubblici.
- **Visualizzare le connessioni:** Analizzare e rappresentare graficamente le relazioni tra il target e altre entità come persone, organizzazioni e gruppi.

## Strumenti Principali

Strumento	Funzione
Google	Utilizzato per la raccolta iniziale per le informazioni pubbliche. Ha permesso di aggregare una vasta base di dati, includendo articoli di stampa, profili social, documenti aziendali e altre menzioni pubbliche associate al target.
Maltego	Piattaforma per l'analisi e la visualizzazione delle connessioni. Ha consentito di mappare in modo grafico le relazioni tra entità (persone, organizzazioni, domini), scoprendo collegamenti non immediatamente evidenti dalla semplice analisi dei dati grezzi.

## Raccolta di Informazioni con Google

Questa **fase iniziale** è stata strategica per costruire una base di conoscenza sul target. **Google** ci ha permesso di indicizzare e raccogliere un grande quantitativo di dati pubblici che costituiscono l'impronta digitale di **Elon Musk**.

## Query di Ricerca Utilizzate

Per ottimizzare la raccolta, sono state impiegate query di ricerca avanzate e parole chiave specifiche, tra cui:

## Ricerca documenti

- **Query:** `site:spacex.com filetype:pdf` -> Per estrazione metadati e nomi dipendenti.

I documenti PDF spesso contengono metadati (autore del file, software utilizzato per crearlo). Sono stati trovati manuali operativi (es. "Starship User Guide"). Questo rivela agli attaccanti quali tecnologie specifiche usa l'azienda, permettendo di preparare malware specifici per quei sistemi.

## Ricerca di Portali di Accesso (Login)

- **Query:** `site:tesla.com -www inurl:login`

Abbiamo cercato nel sito Tesla, escludendo il sito pubblico principale (`-www`) e cercando pagine che avessero la parola "login" nell'indirizzo (`inurl:`).

Il sito principale (`www.tesla.com`) risulta molto sicuro, mentre i sottodomini (es. `partner.tesla.com` o `toolbox.tesla.com`) sono usati dai fornitori o dai meccanici. Spesso questi portali secondari hanno misure di sicurezza inferiori e sono il punto di ingresso ideale per un attacco.

## Profilazione

- **Query:** `site:x.com/elonmusk` --> Ricerca mirata sui suoi profili social .

Ci permette di capire gli orari in cui è attivo online. Capire il suo stile di scrittura per creare email di **Phishing** credibili. Dall'analisi svolta risulta altamente vulnerabile al **"Baiting"**. Spesso risponde d'impulso a utenti sconosciuti, un attaccante potrebbe creare un account falso che tocca un argomento a lui caro (es. "Ho trovato un errore nel codice di Starlink") per indurlo a cliccare su un link malevolo o a rispondere rivelando dettagli tecnici.

## Ricerca Contatti Telefonici

- **Query:** `site:tesla.com "contact" OR "phone"`

Sono stati identificati i numeri diretti per l'Assistenza Clienti e le Relazioni con gli Investitori. Sebbene non siano numeri personali del target, rappresentano un canale di comunicazione che si potrebbero sfruttare per contattare l'azienda.

## Analisi delle Relazioni con Maltego

La prima fase ha permesso di raccogliere i dati, in questa seconda fase li andiamo a trasformare in Intelligenza operativa. Utilizzando **Maltego**, è stato possibile visualizzare le connessioni tra le singole informazioni, scoprendo relazioni e pattern che non sarebbero emersi da una semplice ricerca su google.

## Importazione dei Dati e Mappatura

I dati raccolti tramite Google (nomi, domini, profili social, organizzazioni) sono stati importati in Maltego. La piattaforma ha poi permesso di lanciare trasformazioni automatiche e di mappare manualmente le connessioni, creando un grafo visivo delle relazioni che legano il target al suo ecosistema digitale e professionale.

