Report Attività OSINT: Analisi Target "Matteo Salvini" & "Lega Online"

Analista: Bkm4ge

Data: 06 Gennaio 2026

Oggetto: Information Gathering tramite Maltego e Arricchimento AI

Classificazione: TLP: WHITE (Dati pubblici/OSINT)

1. Executive Summary

L'obiettivo di questa esercitazione è stato mappare la superficie digitale associata al soggetto "Matteo Salvini" e all'infrastruttura politica correlata ("Lega Online"). Utilizzando **Maltego** come strumento principale di link analysis, integrato con tecniche di Google Dorking e arricchimento tramite AI (Gemini), è stato possibile ricostruire la catena che lega l'identità fisica all'infrastruttura server, identificando punti di contatto critici come i servizi di Webmail.

2. Metodologia e Workflow

Il processo di raccolta informazioni è stato suddiviso in quattro fasi distinte, partendo dall'entità persona fino ad arrivare all'infrastruttura fisica dei server.

Fase 1: Identificazione Iniziale e Scraping Email

Input Entity: `Matteo Salvini` (Person), `Lega Online` (Phrase).

Sono state eseguite le trasformazioni standard per enumerare i contatti e le proprietà digitali associate al soggetto.

- **Transform:** `Utilities To Email Address`
- **Transform:** `To Email within Properties`
- **Transform:** `To Domain`

Risultato Grezzo: L'output ha generato un grafo complesso contenente numerosi indirizzi email e domini eterogenei. Molti di questi risultati erano "falsi positivi" dovuti a casi di omonimia o associazioni contestuali non rilevanti (articoli di giornale, blog esterni).

Fase 2: Filtraggio e Validazione (Google Dorks)

Per ripulire il dataset dai risultati non pertinenti (noise reduction), i domini emersi sono stati sottoposti a verifica manuale e automatizzata tramite **Google Dorks**.

- **Tecnica:** Cross-reference dei domini con query specifiche per confermare l'appartenenza ufficiale all'ecosistema politico del target.
- **Azione su Maltego:** I domini validati sono stati re-inseriti come entità `Domain` confermate. Su ogni dominio menzionante il target o appartenente alla struttura ufficiale è stato iterato il processo di discovery.

Fase 3: Discovery Infrastrutturale (Mail Servers)

Focalizzandosi sui domini validati, l'analisi si è spostata sulla ricerca dei sottodomini e dei servizi di posta, vettori critici per la sicurezza.

- **Transform:** `CTI Domain To Address`
- **Target:** Siti ufficiali filtrati.

Highlight Risultati:

L'operazione ha isolato con successo i record DNS associati alla gestione della posta elettronica, restituendo:

- `leganord.info`
- `mail.leganord.info` (Identificato come interfaccia Webmail attiva).

Una volta risolti i nomi a dominio in indirizzi IP, siamo passati dall'analisi logica a quella infrastrutturale.

Fase 4: Arricchimento Dati e Geolocalizzazione (AI Integration)

Ottenuti gli indirizzi IP dei Webserver, è stata utilizzata una trasformazione avanzata basata su Intelligenza Artificiale per ottenere un profilo contestuale dell'hardware e della location.

- **Transform:** `Utilities Search with AI [Gemini]`
- **Input:** Indirizzi IP dei Webserver identificati.

Esito dell'Analisi AI:

L'integrazione con Gemini ha restituito un profilo dettagliato dell'infrastruttura sottostante:

Dato Rilevato	Descrizione
Nome Server	Identificazione dell'hostname della macchina (es. server farm dedicate o hosting gestito).
Utilizzo	Conferma del ruolo del server (Web Server + Mail Exchanger).
Geolocalizzazione	Coordinate approssimative dei server fisici (Data Center). Arezzo, Tuscany, Italy
Network	Identificazione dell'IP di Broadcast della sottorete.

3. Analisi dei Risultati

L'attività di *Information Gathering* ha permesso di tracciare un percorso chiaro:

1. **Dall'Identità al Dominio:** È stato possibile scremare le omonimie e isolare i domini "Lega" effettivi.
2. **Dal Dominio al Servizio:** L'individuazione di `mail.leganord.info` espone l'interfaccia di accesso alla posta, che rappresenta un potenziale punto di ingresso per attacchi di *Brute Force* o *Phishing* mirato.
3. **Dal Servizio all'Infrastruttura:** Grazie all'AI, abbiamo ottenuto visibilità sulla posizione fisica e sulla configurazione di rete (Broadcast IP), dati utili per mappare il provider di hosting e le potenziali vulnerabilità di rete (es. vicini di server rumorosi o subnet non sicure).

4. Conclusioni e Note Etiche

L'analisi si è limitata a tecniche passive (OSINT). Nessun pacchetto offensivo è stato inviato verso i server target. Le informazioni raccolte, in uno scenario reale di *Red Teaming*, verrebbero utilizzate per definire la superficie di attacco. Dal punto di vista difensivo (*Blue Teaming*), si raccomanda di verificare l'esposizione del pannello di webmail e di monitorare i log di accesso sugli IP identificati.