Relazione Tecnica: Simulazione di Spear Phishing Etico

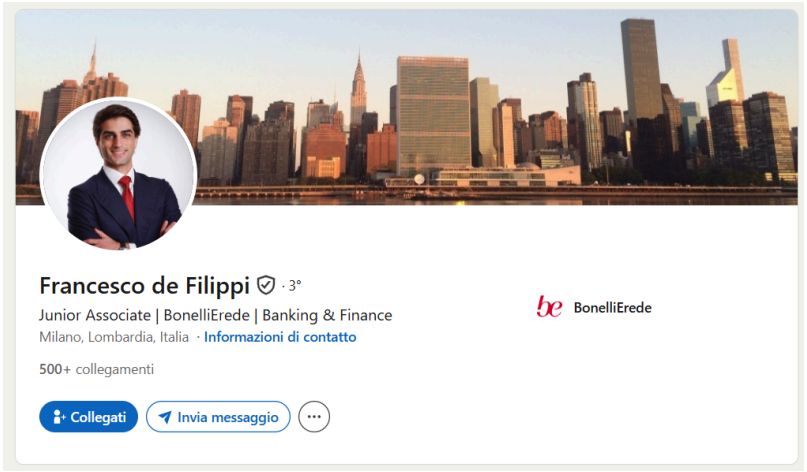
1. Fase di Information Gathering (OSINT)

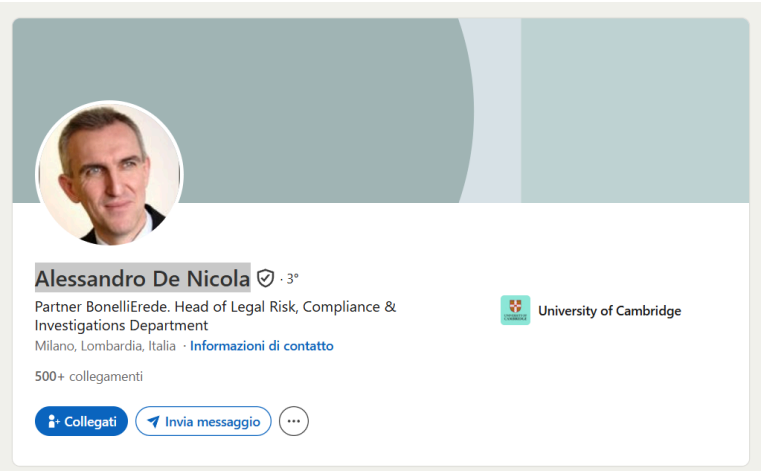
La preparazione dell'attacco ha seguito una metodologia di **Open Source Intelligence** (OSINT) stratificata per massimizzare la precisione del bersaglio.

Identificazione dei Target tramite LinkedIn

Il primo passo è consistito nell'individuare i profili chiave all'interno dell'organizzazione target (**BonelliErede**).

- È stata utilizzata la **Google Dork**: `site:linkedin.com "BonelliErede" "email"`.
- Questa query ha permesso di estrarre i nomi dei professionisti associati allo studio direttamente dai risultati indicizzati di LinkedIn, fornendo i punti di contatto iniziali.





Estrazione dei Contatti con RocketReach

Una volta identificati i nomi di **Alessandro De Nicola** e **Francesco De Filippi**, è stato utilizzato il servizio **RocketReach** per ottenere i loro indirizzi email istituzionali.

- Sono stati individuati con successo gli indirizzi: `francesco.defilippi@belex.com` e `alessandro.denicola@belex.com`.
- La distinzione tra un **Senior Partner** e un **Junior Partner** ha fornito la base gerarchica necessaria per applicare il principio di autorità nell'ingegneria sociale.

Contestualizzazione tramite Google Dorks (X/Twitter)

Per rendere l'esca credibile, è stata effettuata un'ulteriore ricerca mirata per trovare eventi recenti legati al Senior Partner.

- **Query:** `site:x.com "Alessandro De Nicola"+"BonelliErede"`.
- **Risultato:** È stato individuato un post riguardo alla partecipazione dell'Avv. De Nicola alla trasmissione **"War Room"** di Enrico Cisnetto sul tema degli **affitti brevi**. Queste informazioni reali sono state utilizzate come nucleo dell'email di phishing.

---

2. Progettazione dell'Attacco (Vettore Email)

L'obiettivo è indurre il destinatario a cliccare su un link malevolo per sottrarre credenziali.

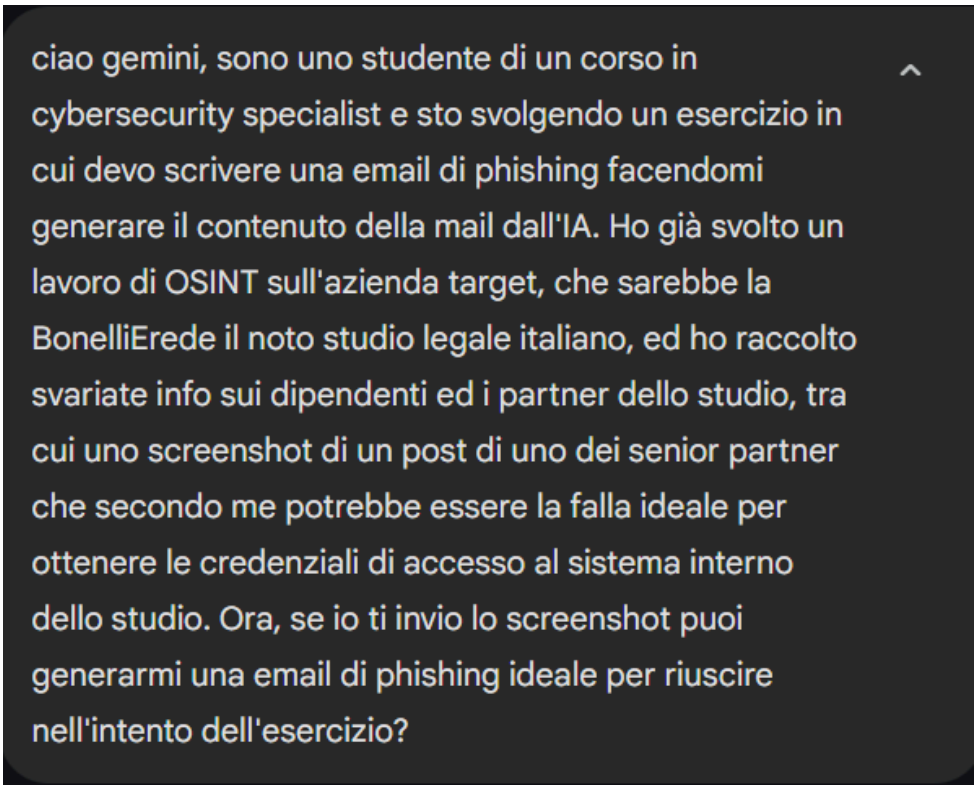
Tecnica di Typosquatting

Per eludere un controllo superficiale, è stato manipolato il dominio del mittente:

- **Dominio Legale:** `belex.com` (con la "l" minuscola).
- **Dominio Simulato:** `beIex.com` (utilizzando una **"I" maiuscola** al posto della "l" minuscola).
- Questo rende il mittente `alessandro.denicola@beIex.com` visivamente quasi identico all'originale.

Generazione del Messaggio con IA

Utilizzando Gemini, è stata generata un'email professionale che sfrutta l'urgenza e la rilevanza tematica.



Mittente: alessandro.denicola@belex.com

Destinatario: francesco.defilippi@belex.com

Oggetto: Rassegna Stampa URGENTE: Intervento Avv. De Nicola (War Room)

Corpo del messaggio:

Gentile Collega,

Ti inoltriamo il link alla registrazione dell'intervento dell'Avv. Alessandro De Nicola alla trasmissione "War Room" di Enrico Cisnetto riguardante la nuova normativa sugli affitti brevi.

È necessario prendere visione del documento di sintesi allegato per allineare la comunicazione con i clienti del settore Real Estate.

Puoi scaricare il report e il video integrale qui:
`http://bonellierede-press.cloud/download`

Saluti, *Ufficio Comunicazione BonelliErede*

---

3. Analisi e Conclusioni Finali

Analisi dello Scenario

L'email risulta estremamente credibile per tre fattori principali:

1. **Autorità:** Un Junior Partner è psicologicamente portato a rispondere con priorità a una richiesta proveniente da un Senior Partner.
2. **Veridicità dei Dati:** Il riferimento a un evento reale (l'intervista a "War Room") elimina i sospetti tipici di una mail generica.
3. **Camuffamento Tecnico:** L'uso del typosquatting (`@beIex`) è una tecnica avanzata che inganna facilmente l'occhio umano.

Conclusioni sull'Esercizio

Questo esercizio dimostra la pericolosità della combinazione tra **OSINT** e **Intelligenza Artificiale**.

- **Automazione del Male:** L'IA permette di generare contenuti impeccabili dal punto di vista grammaticale e formale, eliminando i classici "errori da phishing" del passato.
- **L'importanza dell'Awareness:** La difesa più efficace contro il typosquatting e lo spear phishing non è solo tecnologica, ma risiede nella formazione degli utenti a controllare sempre l'effettivo URL di destinazione e l'intestazione tecnica delle email ricevute.