PROGETTO S5/L5: Simulazione email phishing con ChatGPT

Simuliamo un'azione di email phishing da parte di un attaccante o hacker che è a conoscenza di persone che hanno un conto bancario online e delle loro relative email o che sia riuscito ad avere accesso alla banca dati delle email dei clienti che hanno un conto bancario online collegato ad esso.

Ci sono vari modi per cui l'hacker possa essere arrivato in possesso di questi dati che, per chi non ne da la giusta importanza, sono molto preziosi e importanti sia per i clienti, ma sopratutto per l'azienda che ha la loro fiducia.
Uno dei modi, potrebbe esserci stata una violazione di un servizio di terze parti, tipo una piattaforma di newsletter. Un secondo modo potrebbe esserci stato un altro attacco phishing mirato a dipendenti interni. Un altro modo potrebbe essere che l'attaccante tramite vulnerabilità software abbia avuto accesso a database interni dell'azienda.

In questa simulazione, nel nostro caso di Spear Phishing, attacchi phishing mirati personalizzati in base alle informazioni raccolte sulle vittime, il nostro target sarà Trade Republic, una banca tedesca e un broker online che anche dalla sua app per smartphone permette di comprare e vendere azioni, obbligazioni ed ETF. A gennaio 2025, Trade Republic è usata da 8 milioni di clienti e gestisce asset per circa 100 miliardi di euro. Quindi un target molto importante e appetibile da possibili attaccanti.

Nel file "Phishing Trade Republic.pdf" simula questo attacco phishing descritto poco fa. Grazie all'utilizzo del tool Gophish ho ricreato la stessa email che il nostro target invia a chi è già suo cliente. Infatti a partire dalla fine di Gennaio 2025 Trade Republic ha lanciato la sua succursale in Italia con l'attivazione di IBAN italiani e un conto corrente, anche per quelli già esistenti e quindi chi aveva attivato il servizio in Italia non può mantenere l'iban tedesco.

Questa email a prima vista potrebbe sembrare credibile alla vittima dato che è molto simile alla email che invia il nostro target, con grafica usata normalmente dall'azienda e una firma HTML simile sempre alla loro. L'inserimento di un linguaggio tecnico è un altro elemento per la sua credibilità, ad esempio "Beneficiare del Regime Amministrato", e tutte le indicazioni dell'azienda che si vedono sempre in fondo alla mail.

Gli elementi invece che dovrebbero destare sospetti a chi apre l'email sono gli errori di battitura, "Grazie per la COLABBORAZIONE" o l'inserimento di emoji per fare leva alla vittima sulla importanza della mail e attirare subito l'attenzione su di essa. Un altro è l'assenza del nome del cliente dopo "Ciao". Per far pressione alla vittima viene inserito anche un tempo limite per provvedere all'attivazione dell'iban sennò verrebbe temporaneamente sospesa. E infine la frase "L'attivazione è disponibile solo tramite sito desktop" è un alto campanello d'allarme poichè l'attaccante sta indirizzando di suo volere il cliente ad accedere tutto quanto dal sito desktop per riuscire a catturare tutte le informazioni, quali numero di telefono, codice di sblocco dell'app e impossessarsi dell'account ma non solo!