Report sulla Campagna di Phishing

Report sulla Campagna di Phishing

1. Scenario di Attacco

Contesto Aziendale:

Un’azienda di riferimento nell’ambito tecnologico, la TechCorp, che raccoglie e gestisce dati sensibili relativi alla clientela ed ai propri dipendenti. La TechCorp ha una rete articolata in cui sono attivi anche lavoratori esterni all’azienda. La cybersecurity è un grande problema e una seria preoccupazione per la TechCorp, ma in questo caso c’è stata una violazione: un dipendente, Giuseppe, ha venduto l’account aziendale a un truffatore.

Giuseppe, essendo un impiegato scontento, ha colto l’opportunità di vendere l’accesso all’email dell’account a un truffatore che ha tentato di realizzare uno schema di phishing.

L'Attacco:

Il **truffatore** che ha perpetrato l'atto aveva ottenuto accesso all'account email di Giuseppe e ha utilizzato le informazioni per inviare **un'email di phishing mirata** da un account email aziendale compromesso. Il messaggio intendeva ingannare il destinatario facendogli credere che fosse emesso dal **reparto IT** dell'azienda. Nell'email, l'account è stato segnalato come in procinto di essere sospeso se il destinatario non avesse cambiato le proprie credenziali entro il periodo fornito.

L'obiettivo principale di questo tipo di attacco era **raccogliere un'ID aziendale** e **password** e utilizzarle per penetrare nella rete senza permesso. L'attaccante si aspettava che, una volta che i dipendenti avessero cliccato sul collegamento fornito nell'email, avrebbero inserito le loro password su un sito web falso e gli attaccanti avrebbero ottenuto alcune informazioni aziendali e personali nel processo.

---

2. Email di Phishing

L'email inviata dallo scammer appariva come segue:

Oggetto: ⚠️ Urgente: Aggiornamento delle tue credenziali aziendali richiesto entro 24 ore!

Corpo del Messaggio:

Caro [Nome del Collega],

Sono **Giuseppe**, del dipartimento **IT Security**, e ti scrivo per informarti che stiamo implementando un **aggiornamento urgente di sicurezza** per rafforzare la protezione dei nostri sistemi aziendali. Questo è

un processo che riguarda tutti i dipendenti e deve essere completato immediatamente per evitare sospensioni di account e interruzioni nei servizi aziendali.

Azione richiesta:
Per garantire la continuità del tuo accesso alla rete aziendale, è fondamentale che tu **aggiorni le tue credenziali** il prima possibile. Ti chiediamo di farlo entro **le prossime 24 ore**, altrimenti il tuo account verrà **temporaneamente sospeso** per motivi di sicurezza.

Fai clic sul link sottostante per procedere con l'aggiornamento delle tue credenziali:
http://intranet-securelogin[.]com/update-credentials

⚠️ **Attenzione:** Se non completi l'aggiornamento entro il termine indicato, il tuo account sarà **sospeso** fino a nuove istruzioni dal dipartimento IT.

Se hai bisogno di assistenza, non esitare a rispondere a questa email o a contattarci direttamente tramite il nostro supporto IT.

Grazie per la tua collaborazione.
Cordiali saluti,
Giuseppe
IT Security Team

---

3. Analisi dell'Email di Phishing

Cosa rende l'email credibile:

1. **Provenienza dall'email aziendale compromessa:**
   Dato che l'email proviene da un legittimo account aziendale, la maggior parte dei destinatari potrebbe non avere motivo di dubitare che sia falsa. Il semplice fatto che l'email sembri essere stata inviata dal dipartimento IT dell'azienda rende il messaggio ancora più convincente.
2. **Minaccia di sospensione dell'account:**
   L'email dà un'impressione di urgenza, facendo credere che l'aggiornamento non possa attendere altrimenti l'account aziendale così com'è verrà presto sospeso. Le persone sono più propense a prendere provvedimenti quando sentono che il tempo è essenziale, specialmente quando c'è un'indicazione di interruzione dei servizi aziendali.
3. **Tono ufficiale e professionale:**
   L'email è stata scritta in un tono formale, sottolineando il dipartimento IT e l'esistenza di supporto tecnico che contribuisce a far sì che l'email non sembrasse spam.
4. **Chiarezza della richiesta:**
   Qualsiasi email rende possibile per gli utenti aggiornare i propri dati di accesso fornendo un link, qualcosa che la maggior parte delle persone potrebbe considerare normale da parte di un datore di lavoro.

Elementi sospetti nell'email:

1. **Link sospetto:**
   Il link contenuto nell'email, pur apparendo legittimo, punta a un dominio esterno non associato all'azienda. Un'analisi attenta avrebbe rivelato che il dominio "intranet-securelogin[.]com" non corrisponde al dominio dell'azienda, un chiaro segnale di phishing.
2. **Mancanza di dettagli di contatto:**
   L'email non fornisce informazioni concrete come un numero di telefono o un indirizzo email diretto per contattare il dipartimento IT. Questo è un campanello d'allarme, poiché un'email legittima includerebbe sempre un modo per verificare direttamente la richiesta.
3. **Urgenza senza verifica:**
   La richiesta di agire entro 24 ore, senza alcuna forma di verifica (come una telefonata o un altro mezzo), è una tecnica tipica del phishing. Le comunicazioni ufficiali solitamente offrono più tempo per prendere decisioni e non impongono termini così stretti.

---

4. Conclusioni e Raccomandazioni

Conclusioni sull'Attacco:

Questo attacco sfrutta una **compromissione dell'account aziendale** per inviare un'email di phishing estremamente mirata, che sembra provenire da una fonte ufficiale e che crea un senso di urgenza. La richiesta di aggiornamento delle credenziali è progettata per sembrare legittima, ma nasconde l'intento di rubare le credenziali di accesso. Sebbene l'email sembri credibile, presenta diversi segnali di allarme, come il link sospetto e la mancanza di informazioni di contatto chiare.
