**Report su Simulazione di un Attacco di Social Engineering Multicanale con Integrazione CVE**

**Data:** 2 Maggio 2025

**Luogo:** Roma, Lazio, Italia

**Obiettivo:** Analizzare un attacco di social engineering simulato che impiega una combinazione di e-mail di phishing (con errori linguistici) e pretexting telefonico, sfruttando la menzione di una vulnerabilità CVE per aumentare la credibilità.

**Introduzione:**

Il presente report documenta una simulazione concettuale di un attacco di social engineering multicanale mirato ai dipendenti di un'azienda che utilizza il software "SecureMail Pro". L'attacco combina una fase iniziale di phishing via e-mail con un successivo tentativo di pretexting telefonico. Un elemento chiave di questa simulazione è l'inclusione di errori di battitura e grammaticali nell'email, volti a emulare uno scenario in cui l'attaccante potrebbe non essere italiano, una tattica a volte utilizzata per filtrare le vittime meno sospettose. L'attacco fa inoltre riferimento a una vulnerabilità CVE (anche se ipotetica) per conferire un'apparente legittimità all'interazione.

**Fase 1: E-mail di Phishing (con errori di battitura):**

L'attacco inizia con l'invio di un’e-mail di phishing, redatta in un italiano imperfetto, che cerca di allarmare l'utente riguardo a un problema di sicurezza e prepara il terreno per un successivo contatto telefonico.

**OGGETTO: ATTENZIONE URGENTE:** Pericolo Securita al Suo SecureMail Pro - Azione Richiesta Subito!

Caro utente di SecureMail Pro,

Il nostro gruppo di securita ha trovato una cosa brutta, una vulnerabilità (CVE-2025-XXXX) che puo dare problemi alla versione 2.3.1 di SecureMail Pro che lei usa. Questa cosa cattiva puo far vedere a persone non autorizzate le informazioni segrete che sono nei file di log del programma.

Noi stiamo lavorando forte per aggiustare questo problema e presto faremo uscire una "pezza" per sistemare tutto. Nel frattempo, per tenere sicuri i suoi dati, un tecnico bravo del supporto di SecureMail Pro, uno di quelli di terzo livello, forse la chiamera al telefono nelle prossime ore per aiutarla a controllare i log e mettere una protezione temporanea.

Per favore, aiuti il tecnico quando la chiama e faccia quello che dice. E importante fare presto per non perdere le informazioni della ditta.

Se lei ha domande o non capisce qualcosa, puo rispondere a questa email.

Saluti,

Il Gruppo di Securita IT

**Analisi Dettagliata dell'Email di Phishing:**

Questa e-mail presenta diverse caratteristiche tipiche di un tentativo di phishing, aggravate dalla presenza di errori linguistici che simulano la scrittura di un non madrelingua:

- **Oggetto Allarmistico e con Errori:** L'uso di "ATTENZIONE URGENTE" e l'errore in "Securita" ("Pericolo Securita") creano un senso di allarme immediato ma allo stesso tempo minano la credibilità del mittente come comunicazione ufficiale.
- **Errori Grammaticali e di Sintassi:** Frasi come "trovato una cosa brutta, una vulnerabilità", "puo dare problemi alla versione", "far vedere a persone non autorizzate le informazioni segrete che sono nei file di log del programma" e "faremo uscire una 'pezza' per sistemare tutto" sono sintatticamente imprecise e contengono errori grammaticali che un'azienda seria raramente commetterebbe.
- **Scelta di Parole Inappropriata:** L'uso di espressioni come "cosa brutta" e "pezza" al posto di termini più tecnici e professionali ("vulnerabilità", "patch") contribuisce a un'impressione di scarsa professionalità.
- **Tono Urgente e Autorità Sfruttata:** L'email insiste sulla necessità di agire "subito" e introduce la figura di un "tecnico bravo del supporto di terzo livello" per indurre l'utente a fidarsi e a collaborare.
- **Riferimento a un CVE (anche se implicito):** La menzione di "CVE-2025-XXXX" (anche se non spiegato in dettaglio) cerca di aggiungere un livello di legittimità tecnica all'allarme di sicurezza.
- **Richiesta di Collaborazione Telefonica:** L'email prepara specificamente l'utente a ricevere una telefonata e chiede di seguire le istruzioni del tecnico, aprendo la strada alla fase di pretexting.

**Fase 2: Pretexting Telefonico (Role-Playing Concettuale):**

Dopo l'invio dell'e-mail, l'attaccante (fingendosi il "tecnico bravo del supporto di terzo livello") contatta telefonicamente i dipendenti.

**Esempio di Interazione Telefonica:**

**Attaccante:** "Buongiorno, sono [Nome Inventato], la chiamo dal supporto tecnico di SecureMail Pro. Ha ricevuto la nostra e-mail riguardo al problema di securita, la vulnerabilità CVE-2025-XXXX?" (Nota l'uso della parola "securita" con un probabile accento straniero).

**Vittima:** "Sì, l'ho ricevuta. Diceva che un tecnico mi avrebbe chiamato."

**Attaccante:** "Esatto. Io sono il tecnico. Dobbiamo controllare subito i suoi file di log per vedere se ci sono tracce di questa cosa brutta e mettere una protezione veloce prima che sia troppo tardi. Posso guidarla per fare questa verifica?"

L'attaccante potrebbe quindi cercare di convincere la vittima a:

- Fornire le proprie credenziali di accesso.
- Installare un software di accesso remoto con la scusa di applicare la "patch" o controllare i log.
- Rivelare informazioni sensibili sul sistema o sui dati aziendali.

**Analisi del Pretexting Telefonico:**

- **Coerenza con l'Email:** L'attaccante si riferisce all'email precedentemente inviata, aumentando la credibilità dell'interazione.
- **Sfruttamento della Paura e dell'Urgenza:** Il riferimento alla "cosa brutta" e alla necessità di agire "subito" mira a manipolare le emozioni della vittima.
- **Uso di un Termine Tecnico (CVE):** Anche se la vittima potrebbe non capire cos'è un CVE, la sua menzione può conferire un'aura di serietà e competenza all'attaccante.
- **Richiesta di Azioni Specifiche:** L'obiettivo finale è indurre la vittima a compiere azioni che compromettano la sicurezza (fornire credenziali, installare software malevolo).
- **Possibile Persistenza degli Errori Linguistici:** L'uso continuato di errori di pronuncia o grammatica ("securita") potrebbe essere un'arma a doppio taglio: potrebbe sembrare meno professionale, ma potrebbe anche filtrare le vittime più sospettose, lasciando solo quelle più vulnerabili.

**Segnali di Allarme Comuni (Sia nell'E-mail che nella Telefonata):**

- Errori grammaticali e di battitura evidenti.
- Richieste urgenti e inaspettate di informazioni sensibili o azioni immediate.
- Minacce di conseguenze negative se non si agisce rapidamente.
- Link o richieste di download da fonti non verificate.
- Chiamate o e-mail non richieste da "tecnici" che chiedono accesso remoto o credenziali.
- Incongruenze nell'indirizzo e-mail del mittente o nel numero di telefono del chiamante.
- Pressione a non verificare l'identità del richiedente tramite canali ufficiali.

**Contromisure Efficaci:**

- **Verifica Scettica:** Trattare con cautela tutte le comunicazioni inaspettate, specialmente quelle che richiedono azioni urgenti o la divulgazione di informazioni sensibili.
- **Verifica Indipendente:** Non utilizzare i contatti forniti nell'email o dalla persona che chiama. Verificare l'identità del mittente o del chiamante tramite canali ufficiali e

conosciuti (es. contattando direttamente il reparto IT tramite il numero di telefono interno).

- **Non Fornire Informazioni Sensibili:** Non condividere mai password, numeri di carta di credito o altre informazioni riservate tramite e-mail o telefono a meno che non si sia assolutamente certi dell'identità del destinatario.
- **Consapevolezza dei CVE (a livello utente):** Anche se non è necessario comprendere i dettagli tecnici, essere consapevoli che le aziende comunicheranno gli aggiornamenti di sicurezza tramite canali ufficiali (sito web, bollettini di sicurezza) può aiutare a diffidare di richieste non convenzionali.
- **Segnalazione Immediata:** Segnalare immediatamente qualsiasi e-mail o telefonata sospetta al reparto IT o al responsabile della sicurezza.

**Conclusione:**

Questa simulazione evidenzia come gli attacchi di social engineering possano essere sofisticati e sfruttare una combinazione di tecniche e canali per manipolare le vittime. L'inclusione di errori linguistici nell'email, pur potendo sembrare amatoriale, può paradossalmente aumentare il tasso di successo con utenti meno esperti o più inclini a fidarsi di comunicazioni che invocano urgenza e autorità. La menzione di una vulnerabilità CVE, anche se non compresa appieno dalla vittima, può aggiungere un velo di legittimità tecnica all'attacco. La difesa efficace contro tali minacce richiede una forte consapevolezza da parte degli utenti, procedure di verifica rigorose e una cultura aziendale orientata alla sicurezza.