REPORT S5/L5

ANALISI ATTACCO PISHING TRAMITE I.A

Luca Tavani

SCENARIO

L’attaccante ha utilizzato tecniche OSINT (Open Source Intelligence) per raccogliere informazioni sulla vittima e rendere l'attacco di phishing più efficace.

- Tramite una semplice ricerca su Google Dorks, ha trovato il nome e l’email della vittima, Marco Rinaldi, in un vecchio documento online.
- Analizzando profili social e forum finanziari, ha scoperto che **Marco Rinaldi** è cliente di Unicredit.
- Ha individuato la filiale di riferimento della vittima in un PDF pubblico trovato tramite Google Dorks.

SCENARIO

Con queste informazioni, l’attaccante ha creato un’email altamente credibile, includendo il nome della filiale reale nella firma dell’email, aumentando così la probabilità che la vittima cada nell’inganno e inserisca le sue credenziali nel sito fasullo.

OBIETTIVI :

- ✓ Rubare credenziali bancarie della vittima.
- ✓ Prendere controllo del conto bancario.
- ✓ Effettuare bonifici fraudolenti o altre transazioni.

Email di phishing creata con I.A

📩 Oggetto: 🚨 [URGENTE] Pagamento sospetto sul tuo conto Unicredit

✉️ Mittente: Unicredit Servizio Clienti support@unicredit-secure.com

Gentile Marco Rinaldi,
abbiamo rilevato un pagamento sospetto dal tuo conto Unicredit dell'importo di 385,90€ verso un destinatario non riconosciuto.
Dettagli della transazione:

- Importo: 385,90€
- Destinatario: SHOPTECH S.R.L.
- Data: 28/02/2025
-

Se non hai autorizzato questa transazione, è necessario un intervento immediato per evitare l'addebito. Ti invitiamo a verificare il tuo account e bloccare il pagamento accedendo al nostro portale di sicurezza:

👉 Accedi al tuo account sicuro Clicca qui

Per garantire la sicurezza del tuo conto, ti consigliamo di completare la verifica entro 24 ore, altrimenti la transazione verrà processata automaticamente.
Per qualsiasi domanda, puoi contattare il nostro servizio clienti al numero 800-123-456.
Unicredit Servizio Clienti
Assistenza e Sicurezza Online - Filiale di Roma Centro

Analisi dell'Email di Phishing

✅ **Perché questa email è credibile?**

✓ **Mittente falso ma realistico** → L’email sembra provenire da Unicredit.

✓ **Uso di dettagli specifici** → Importo preciso, nome dell’azienda, data della transazione.

✓ **Tono professionale** → Simile a una comunicazione ufficiale.

✓ **Chiamata all’azione immediata** → La vittima è spinta a cliccare per evitare una perdita di denaro.

✓ **Firma personalizzata** → Il riferimento alla filiale locale aumenta la credibilità.

Analisi dell'Email di Phishing

❌ **Segnali di phishing evidenti**

❌ **URL malevolo** → Il dominio vero di Unicredit è unicredit.it, non unicredit-secure-login.com.

❌ **Pressione psicologica** → La frase "entro 24 ore" crea panico e spinge l'utente ad agire senza verificare.

❌ **Mittente sospetto** → Unicredit non usa email con domini diversi da @unicredit.it.

A.I PHISHING CONCLUSION

Questa simulazione dimostra come un attacco di phishing possa essere altamente mirato grazie all'uso di OSINT. I criminali informatici sfruttano dati pubblici per rendere i loro messaggi più credibilie difficili da identificare come falsi. Grazie anche all'uso dell' **artificial intelligence** come chatGPT.

Per proteggersi da questi attacchi, è essenziale:

- **Verificare sempre il mittente e il dominio dell'email.**
- **Non cliccare su link sospetti e accedere direttamente al sito ufficiale.**
- **Non farsi prendere dal panico e contattare la banca per confermare l'autenticità della comunicazione.**

GRAZIE PER L'ATTENZIONE

CYBERSECURITY SPECIALIST

Luca Tavani