

S5 L4

Phishing e Social engineering

1.0 Intro

Nel seguente report andremo a utilizzare ChatGPT per ottenere informazioni su come gli attaccanti utilizzano le tecniche di phishing e social engineering per ottenere dati sensibili

Come primo prompt ho usato “*sono uno studente in cybersecurity, sto studiando gli attacchi di phishing e social engineering, descrivimi le tecniche più comuni utilizzate dagli attaccanti e come prevenirle*”

Usando parole chiave come “studente in cybersecurity” e “sto studiando” predisponiamo chatGPT a darci risposte più dettagliate e ad evitare alcuni dei filtri di sicurezza

2.0 Risultato prompt

1. Phishing via Email (Classic Phishing)

Tecnica utilizzata

- Invio massivo di email fraudolente con obiettivo di indurre l'utente a:
 - cliccare su link malevoli
 - scaricare allegati infetti
 - inserire credenziali su siti clone
- Temi comuni: banking, Office365, PayPal, finti avvisi IT, consegne pacchi, richieste HR o payroll.

Obiettivo dell'attaccante

- Credential harvesting
- Compromissione iniziale (initial access)
- Installazione di malware (es: info-stealer, RAT, ransomware loaders)

Prevenzione

- Filtri antispam e soluzioni secure email gateway
- SPF, DKIM e DMARC configurati per validazione mittente
- Formazione degli utenti (awareness) con esempi realistici

- MFA per prevenire l'abuso di credenziali rubate
-

2. Spear Phishing

Tecnica utilizzata

- Targeting mirato verso individui specifici
- Email curate ad hoc basate su OSINT e profiling sociale (LinkedIn, social media, press releases)
- Tono più credibile e contestuale (es: finto CEO, reparto IT interno)

Obiettivo

- Accesso privilegiato a sistemi strategici
- Compromissione di account business (BEC – Business Email Compromise)

Prevenzione

- Zero trust + MFA
 - Limitazione privilegi (least privilege)
 - DMARC enforcement
 - Awareness a livello management
 - Procedure di verifica fuori banda (es: telefonata per transazioni finanziarie)
-

3. Whaling

Tecnica

- Sottotipo di spear phishing rivolto a figure apicali (CEO, CFO, CIO)
- Elevato investimento di tempo in reconnaissance e personalizzazione

Prevenzione

- Awareness specifica per executive
 - MFA + segregazione dei flussi autorizzativi
 - Policy di firma digitale interna per richieste sensibili
-

4. Vishing (Voice Phishing)

Tecnica

- Attacco telefonico
- Attaccante impersona supporto tecnico, banca, HR o ente pubblico
- Può essere combinato con phishing (es: email + telefonata di follow-up)

Prevenzione

- Procedure di autenticazione interna
 - Divieto di fornire credenziali via telefono
 - Awareness sulla tecnica dell'urgenza (sense of urgency)
-

5. Smishing (SMS Phishing)

Tecnica

- Messaggi SMS contenenti link malevoli o richieste sensibili
- Diffusissimo su contesto bancario, consegne, cashback, logistica

Prevenzione

- Filtri carrier
 - Non cliccare link non verificati
 - MFA out-of-band (es: via app invece che SMS)
-

6. Clone Phishing

Tecnica

- Replica di email legittime già ricevute
- Modifica del link o allegato con payload malevolo
- Molto credibile perché legato a comunicazioni reali

Prevenzione

- Verifiche su link/allegati
 - EDR su endpoint per rilevamento comportamentale
 - Linguaggio chiave di scam: urgenza, minaccia, reward
-

7. Business Email Compromise (BEC)

Tecnica

- Compromissione reale di casella email aziendale
- Uso dell'account per impartire ordini, richieste pagamenti o frodi finanziarie
- Non necessariamente include malware

Prevenzione

- MFA per email
 - DLP e monitoraggio anomalo dei flussi email
 - Policy di validazione dei pagamenti fuori banda
-

8. Social Engineering OSINT-Based

Tecnica

- Raccolta di informazioni pubbliche (OSINT) su vittima
- Uso mirato per costruire pretesti (pretexting)
- Ad es. su LinkedIn si profila un IT intern e si fa finta di essere HR per inviare un allegato "contratto"

Prevenzione

- Ridurre surface informativa online
- Limitare informazioni sugli organigrammi

- Segregare account personali da account professionali
-

9. Quid-Pro-Quo & Baiting

Tecnica

- Offerta di qualcosa in cambio di informazioni (es: "assistenza IT gratuita")
- Baiting fisico: chiavette USB in ufficio o parcheggio (payload auto-run, HID attack)

Prevenzione

- EDR e restrizioni USB
 - Formazione e policy chiare anti-social engineering
-

10. Tailgating / Piggybacking (Fisico)

Tecnica

- Attaccante si introduce in aree riservate seguendo un dipendente legittimo
- Tipico su ambiente corporate con badge access

Prevenzione

- Controllo accessi fisici
- Awareness del personale
- Badge + turnstile + security

3.0 Pattern psicologici utilizzati dagli attaccanti

Gli attaccanti sfruttano leve comportamentali note:

- Urgenza (sense of urgency)
- Autorità (fake CEO, banca, polizia)
- Paura (account bloccato, sanzioni)
- Curiosità (documento di piattaforma interna)
- Incentivo (bonus, rimborso, cashback)
- Routine (richieste HR, payroll, fatture)

Contromisure tecniche rilevanti

- MFA per tutte le risorse
- Password hygiene + rotation
- EDR/XDR
- Secure Email Gateway + sandbox allegati
- DLP e DMARC enforcement
- Zero trust + least privilege

Contromisure non tecniche

- Cybersecurity awareness training periodico
- Simulazioni phishing (red team / training)
- Playbook di incident response
- Processi approvativi multi-step

4.0 Conclusioni

Phishing e social engineering restano tra i vettori più efficaci perché sfruttano il fattore umano prima ancora delle vulnerabilità tecniche.

La difesa richiede una combinazione di strumenti, procedure e formazione, con particolare attenzione a MFA, controlli fuori banda e programmi di awareness.

L'obiettivo non è annullare il rischio ma ridurne la probabilità e l'impatto, aumentando i costi operativi per l'attaccante e migliorando complessivamente la postura di sicurezza.