Progetto S5 – L5

Simulazione Real-Time
Phishing a tema Ransomware

Executive Summary

Questo report analizza una **simulazione di email di phishing ad alta credibilità** a tema ransomware, rivolta a personale tecnico.
L'attacco utilizza **impersonificazione di un vendor noto** tramite dominio typosquatted e linguaggio operativo tipico dei team IT.

L'email induce l'utente a effettuare una verifica di sicurezza tramite link esterno.
In caso di interazione, il rischio principale è il **furto di credenziali** e il **compromesso dell'account cloud**.

Il documento evidenzia indicatori di phishing, impatto potenziale e misure di contenimento, con l'obiettivo di migliorare prevenzione e consapevolezza.
Il rischio complessivo è classificabile come Alto in caso di interazione dell'utente.

Introduzione

Il presente report descrive una **simulazione di phishing a tema ransomware.**
Lo scenario riproduce un contesto realistico di **Security Operations**, in cui un'email fraudolenta si presenta come una notifica tecnica urgente.

L'analisi si concentra su **contenuto, contesto e indicatori di compromissione**, evidenziando come anche utenti tecnici possano essere esposti a questo tipo di minaccia.

Obiettivo del Report

L'obiettivo del report è:

- analizzare una email di phishing credibile in ambito IT;
- identificare le tecniche di ingegneria sociale utilizzate;
- evidenziare i principali indicatori di phishing;
- valutare il rischio in caso di interazione dell'utente.

La finalità è supportare attività di **awareness e miglioramento della postura di sicurezza**.

Email di phishing simulata – (collega IT)

Oggetto

[URGENTE][SOC] Tentativo di cifratura ransomware bloccato – verifica tenant necessaria

---

Mittente e Dominio

Security Notifications – IT Security
`alerts@microsft-security[.]example`

> *Indicatore chiave:* ***dominio typosquatted (microsft ≠ microsoft)***.

Corpo dell’email:

Buongiorno Henry,

ti scrivo perché **questa mattina il SOC ha bloccato un tentativo di cifratura ransomware** legato al tuo tenant cloud.

L’evento è stato **contenuto automaticamente**, ma dai primi controlli risulta **un’anomalia sugli identity logs** che va verificata subito per escludere ulteriori movimenti laterali o tentativi di riattivazione.

Dettagli rapidi:
• Stato: **Bloccato**
• Servizi coinvolti: **Identity Protection / Cloud Apps**
• Origine: accesso sospetto in fase di validazione

⚠ **Appena puoi, entra nel Security Center e conferma lo stato del tenant:**
👉 https://security-center-cloud[.]example/tenant-review

Serve solo una verifica, **non verranno applicate azioni automatiche** finché non viene confermato lo stato di sicurezza.

Se non riusciamo a chiudere la verifica in tempi brevi, il tenant potrebbe restare esposto a nuovi tentativi.

Grazie,
Paul R.
IT Security / SOC

Messaggio generato dal sistema di monitoraggio sicurezza

Nota metodologica:

Il link presente nel corpo dell’email è non operativo ed è utilizzato esclusivamente a scopo dimostrativo all’interno della simulazione.
Non conduce a una reale pagina di autenticazione né a servizi effettivi, ed **è stato inserito per riprodurre in modo realistico il vettore di attacco tipico delle campagne di phishing, senza esporre sistemi o utenti a rischi reali.**
L’analisi si concentra quindi sul comportamento dell’utente e sugli indicatori di phishing, non sull’effettiva esecuzione dell’accesso.

- Contesto Operativo

- **Audience:** Team tecnico / IT Manager
- **Canale:** Email aziendale
- **Minaccia:** Phishing (impersonificazione vendor)
- **Tema:** Ransomware
- **Stato:** Contenimento

- Oggetto dell’email:

[Ransomware Alert] Attività di cifratura bloccata su tenant – intervento richiesto

> **Nota tecnica:** Oggetto coerente con alert SOC/SIEM; segnala evento **già bloccato** (credibile per team IT).

- Mittente e dominio:

- **Mittente visualizzato:** Security Notifications
- **Dominio:** `alerts@microsft-security[.]example`

Indicatore chiave: typosquatting (`microsft` ≠ `microsoft`).

- Timeline operativa:

09:17 – Ricezione
Sul PC del reparto IT arriva un’email con oggetto ransomware. Il messaggio segnala attività di cifratura bloccata sul tenant.
09:18 – Valutazione iniziale
Il contenuto è tecnico, conciso, senza richieste dirette di password. L’evento appare **plausibile** per ambienti cloud.

09:19 – Verifica mittente
Il dominio del mittente contiene una **variazione ortografica** del vendor.
Conclusione: indicatore di phishing confermato.

09:20 – Verifica link (senza clic)
Il link “Security Center” **non** punta al portale ufficiale.
Conclusione: probabile **credential harvesting** con pretest ransomware.

09:21 – Classificazione
Phishing avanzato – impersonificazione vendor / tema ransomware.

09:22 – Contenimento
Segnalazione phishing, allerta al team, ricerca occorrenze, richiesta blocco dominio/URL.

- Estratto contenuto email (simulazione, non operativa)

- **Evento:** Tentativo di cifratura rilevato
- **Stato:** Bloccato
- **Servizio indicato:** Identity / Cloud Apps
- **Azione richiesta:** “Verifica stato di sicurezza” tramite link

  Linguaggio coerente con alert automatici; **assenza di richiesta esplicita di credenziali** aumenta la credibilità.

- Findings:

Cosa
Email che impersona un vendor noto usando **typosquatting** e pretest ransomware.

Quindi (Impatto)
Inserimento credenziali → **Account takeover**, possibile MFA-fatigue, accesso a posta e dati cloud.

Come (Evidenza)

- Dominio non autorizzato con errore ortografico (`microsft`).
- URL esterno non conforme ai portali ufficiali.

- Indicatori d’allarme (chiari e coerenti)

- Dominio **typosquatted** del vendor
- Link esterno per “Security Center”
- Oggetto ransomware che induce urgenza operativa
- Mancanza di riferimenti a canali ufficiali interni

- Raccomandazioni

Tattiche (immediate)

- Blocco dominio/URL sospetti su mail gateway e DNS
- Ricerca e quarantena messaggi simili
- Verifica log identity per click/approvazioni MFA

Strategiche

- Regole anti-typosquatting (vendor look-alike)
- Awareness mirata: “Il vendor non invia link di verifica via email”
- Conditional Access più restrittive per accessi anomali

In breve:

La simulazione evidenzia come una campagna di phishing ad alta credibilità, basata su pretest ransomware e typosquatting, rappresenti una minaccia concreta anche in ambienti IT strutturati. L’uso di terminologia enterprise aumenta la fiducia del destinatario e riduce la capacità critica.
L’interazione con l’email può portare a compromissione delle credenziali e account takeover, confermando il phishing come vettore iniziale chiave della kill chain. La mitigazione efficace richiede verifiche tempestive e un approccio strutturato che includa monitoraggio dei domini, policy restrittive e formazione mirata.

Conclusione

La simulazione conferma che la sicurezza efficace richiede l’integrazione di tecnologia, processi e formazione del personale, affinché anche messaggi apparentemente legittimi vengano analizzati criticamente prima dell’interazione, riducendo l’impatto delle campagne di phishing avanzate.