Report – Simulazione di Phishing: Progetto “MC-Must” 🍔

1. Premessa

L’obiettivo dell’attività è simulare un attacco di phishing verosimile e strutturato, sfruttando l’immagine di un brand noto per attirare la vittima e indurla a fornire i propri dati.
La simulazione ha incluso: creazione del contesto, progettazione dell’email, costruzione del funnel, e raccolta della mail list tramite una falsa campagna social.

2. Considerazioni Personali

Un attacco di phishing ben riuscito non inizia con l’email.
Inizia **molto prima**, con l’inganno psicologico e con la costruzione di una mailing list credibile e mirata.
Il funnel e la lista sono il vero “cuore nascosto” di ogni operazione malevola.

Il **funnel** è un modello strategico che rappresenta il processo con cui si guida una persona da semplice "curiosa" a cliente effettivo (e potenzialmente fedele). Il termine deriva dalla forma **a imbuto**, perché molte persone entrano nella fase iniziale, ma solo una parte continua fino all'obiettivo finale (come un acquisto o una registrazione).

Cos’è il funnel in un attacco di phishing:

Nel contesto della cybersecurity e dell’ingegneria sociale, il termine **funnel** indica il **percorso graduale e strategico** attraverso il quale un attaccante guida una vittima dall’interesse iniziale fino all’azione finale desiderata, come cliccare su un link, fornire dati personali o inserire credenziali.

Questo approccio, mutuato dal marketing digitale, è particolarmente efficace perché sfrutta meccanismi psicologici progressivi, come fiducia, desiderio, urgenza e ricompensa.

Struttura tipica di un funnel di phishing:

Fase	Descrizione
1. Adescamento (Attenzione)	L'utente viene attirato da un contenuto interessante o vantaggioso: una pubblicità, un post sui social, un messaggio sponsorizzato o un annuncio accattivante.
2. Interesse e interazione (Coinvolgimento)	La vittima viene invitata a lasciare una mail, cliccare un bottone o accedere a un modulo. In questa fase l'utente *collabora volontariamente* fornendo un primo dato.
3. Personalizzazione (Conferma)	Dopo aver ottenuto l'indirizzo email o altre informazioni, l'attaccante invia un'email credibile, in linea con la comunicazione precedente. Questo rafforza la fiducia dell'utente.
4. Compromissione (Azione finale)	L'utente clicca su un link e inserisce i propri dati su una pagina falsa, credendo sia legittima. In questa fase si realizza l'obiettivo del phishing: furto d'identità o accesso non autorizzato.

Creare una mailing list. Perché è necessario:

La mailing list serve a **raggiungere persone reali** con comunicazioni mirate. Più è curata, più l'attacco ha probabilità di riuscire.
Una lista costruita in modo mirato (es. raccogliendo utenti interessati a promozioni fast food) aumenta la **credibilità percepita** dell'email e riduce il rischio che venga ignorata o classificata come spam.

Gli hacker impiegano diverse tecniche per creare mailing list da utilizzare in campagne di phishing. Queste strategie mirano a raccogliere un ampio numero di indirizzi email validi, spesso sfruttando l'ingegneria sociale e strumenti automatizzati.

Ecco i metodi principali:

- Acquisto o scambio di liste di email

Gli hacker possono acquistare o scambiare elenchi di indirizzi email da altri cybercriminali. Queste liste spesso provengono da precedenti violazioni di dati o campagne di phishing.

- Raccolta automatizzata tramite bot (Email Harvesting)

Utilizzando software chiamati "harvester" o "spider", gli hacker scansionano automaticamente pagine web, forum, archivi di mailing list e altre fonti online alla ricerca di indirizzi email pubblicamente accessibili.

- Attacchi di tipo Directory Harvest Attack (DHA)

In un attacco DHA, gli hacker inviano email a una vasta gamma di possibili combinazioni di nomi utente presso un dominio specifico (es. nome.cognome@azienda.com) per identificare quali indirizzi sono validi. Se il server di posta non rifiuta l'email, l'indirizzo viene considerato valido e aggiunto alla lista.

- Creazione di campagne false per raccogliere email

Gli hacker possono creare siti web o campagne promozionali fasulle che offrono incentivi, come buoni sconto o premi, in cambio dell'iscrizione con un indirizzo email. Queste campagne possono essere pubblicizzate tramite social media o annunci online, attirando utenti ignari a fornire volontariamente i propri dati.

- Utilizzo di strumenti di ingegneria sociale

Strumenti come il Social Engineering Toolkit (SEToolkit) permettono agli hacker di creare pagine di phishing, inviare email o SMS falsificati e generare payload sotto forma di file apparentemente innocui. Questi strumenti facilitano la raccolta di indirizzi email e altre informazioni sensibili.

- Estrazione da fonti pubbliche e social media

Gli hacker possono raccogliere indirizzi email da fonti pubbliche come WHOIS, profili LinkedIn, forum e altri siti web dove gli utenti pubblicano volontariamente i propri contatti. Queste informazioni vengono poi utilizzate per creare mailing list mirate.

- False campagne sui social media

Una tecnica sempre più diffusa consiste nella creazione di profili o pagine sui social media che imitano marchi noti o promuovono eventi inesistenti.

Gli hacker lanciano campagne pubblicitarie fasulle che offrono incentivi, come buoni sconto o premi, in cambio dell'iscrizione con un indirizzo email. Queste campagne possono essere pubblicizzate tramite social media o annunci online, attirando utenti ignari a fornire volontariamente i propri dati.

- Tecniche avanzate con l'uso dell'IA

Recentemente, gli hacker hanno iniziato a utilizzare l'intelligenza artificiale per generare email di phishing altamente personalizzate. L'IA può analizzare profili online e comportamenti degli utenti per creare messaggi convincenti, aumentando l'efficacia delle campagne di phishing.

3. Creare uno scenario

Contesto realistico:

Abbiamo immaginato un attacco di phishing basato su un finto profilo Instagram chiamato @mc.lovers.official, collegato al marchio fittizio **MC Lovers**, che promuove l'uscita misteriosa di un nuovo panino esclusivo. Il post recita:

"🍔 Vuoi essere tra i **primi 1000 in tutta Italia** ad assaggiarlo GRATIS? Scrivi 'LO VOGLIO' in DM e partecipa all'estrazione."

Chi invia il messaggio riceve una risposta automatica che chiede:

"Per completare l'iscrizione, scrivici il tuo nome e l'indirizzo email."

Questo genera una mailing list reale e qualificata, che verrà poi usata per inviare l'email di phishing personalizzata.

Obiettivo del phishing:
Rubare le credenziali personali degli utenti, spacciando la truffa per un'iniziativa promozionale ufficiale. Il link incluso nell'email porta a un finto portale "MC Lovers" dove viene chiesto l'accesso tramite Google o Apple ID.

4. Scrivere l'email di phishing

Oggetto: 🍔 Sei tra i 1000 selezionati per provare il nuovo MC Lovers – Attiva il tuo assaggio gratuito

Da: premi@mc-lovers.cloud
A: [utente@email.com]

MC Lovers Italia – Ufficio Promozioni 2025

Ciao [Nome],

Grazie per averci scritto! Sei ufficialmente tra i **1000 utenti selezionati in tutta Italia** per partecipare all'anteprima esclusiva del nostro **nuovo panino segreto**.

🎁 Il tuo buono digitale per l'assaggio gratuito è pronto!

👉 **Attivalo subito qui:**
Riscatta il tuo panino ———> **rimanda al sito "finto portale".**

⏳ Hai 24 ore per completare la registrazione.

Il nuovo panino sarà disponibile **solo per chi riceve questo invito**.

Grazie per essere un vero Lover.

Team MC Lovers

Questa email è generata automaticamente.

Per assistenza, visita www.mc-lovers.it -—> **rimanda al sito "originale mc".**

5. Spiegare lo scenario

Perché l'email potrebbe sembrare credibile:

- L'utente ha **avviato volontariamente** il contatto tramite DM su Instagram
- Il tono è coerente con lo stile di comunicazione "giovane" dei brand fast food
- Non ci sono errori ortografici
- Il link sembra plausibile
- L'email è **personalizzata con il nome dato in chat**

Campanelli d'allarme che dovrebbero far riflettere la vittima:

- Dominio non ufficiale (mc-lovers.cloud)
- L'urgenza forzata ("solo 24 ore")
- Mancanza di verifica attraverso canali ufficiali
- Richiesta di accedere tramite account Google o Apple senza motivazione chiara

6. Conclusioni

L'intera campagna fa leva sulla percezione di autorevolezza del marchio e sull'abitudine degli utenti a interagire quotidianamente con contenuti promozionali simili. Questo rende l'attacco ancora più efficace.

Questa simulazione ha permesso di analizzare in modo concreto come si costruisce un attacco di phishing credibile, partendo da una semplice interazione su Instagram e arrivando alla compromissione potenziale della vittima.

Abbiamo dimostrato che:

- Il phishing non è più solo “email strane con errori”, ma campagne **studiate nei minimi dettagli** e **visivamente coerenti** con la comunicazione reale di un brand.
- L’elemento chiave è il **funnel di attacco**, che sfrutta fiducia, curiosità e urgenza per condurre l’utente, passo dopo passo, fino alla trappola finale.
- La **mailing list** non viene “raccolta per caso”, ma costruita attraverso l’inganno, facendo credere all’utente di partecipare a una vera promozione.

Attraverso questo esercizio abbiamo preso consapevolezza non solo dei **segnali di allarme**, ma anche delle strategie psicologiche usate dai criminali per **colpire in modo credibile, mirato e silenzioso**.

7. Considerazioni aggiuntive

Questa simulazione ha mostrato che oggi **un attacco di phishing efficace si costruisce prima dell’email**, attraverso canali e contenuti familiari per l’utente, come i social.

- **Instagram è diventato un terreno fertile per truffe silenziose**: sfruttando la grafica curata, la logica degli influencer e l’urgenza delle promozioni, è possibile creare un contatto credibile senza destare sospetti.
- La raccolta delle email tramite messaggi diretti (*DM*) appare naturale. L’utente non si sente ingannato: è lui a cercare di “entrare” in qualcosa di esclusivo.
- È sufficiente **un’immagine accattivante, una promessa semplice e una risposta automatica ben scritta** per convincere decine o centinaia di persone a fornire i propri dati.
- **Il vero rischio non è l’email in sé, ma il contesto che la rende plausibile.**

Per questo motivo, esercitazioni come questa non sono solo utili: sono **necessarie**. Aiutano a capire **come si costruisce il phishing moderno** e dove bisogna imparare a riconoscerlo: *non più solo nella posta in arrivo, ma anche nel feed di Instagram*.

Spinazzola (BT) 02/05/2025