U2W1L5 – Progetto settimanale

Ingegneria sociale

Sintesi:

Questo report analizza la creazione di un'email di phishing, mettendone in evidenza i campanelli d'allarme, segnalando qual è il modus d'azione corretto quando si ricevono email che fanno leva sull'urgenza e sul panico cognitivo.

Richieste:

- Creazione di uno scenario
  - Contesto realistico
  - Obiettivo dell'attacco
- Scrittura di un'email di phishing tramite IA
  - Convincente, ma con i campanelli d'allarme tipici del phishing
- Spiegazione
  - Dello scenario
  - Del perché la mail potrebbe risultare credibile
  - Quali elementi dovrebbero mettere in allarme l'utente

Introduzione:

La richiesta è quella di creare, mediante Intelligenza Artificiale, il corpo di un'email di phishing.

La scelta è ricaduta su qualcosa che possa toccare da vicino molti di noi: un'email da parte di amministrazione@eplcode.com che avvisa che un pagamento non è andato a buon fine e chiede di fare il login e re-inserire i dati per il pagamento.

Lo scopo di questa campagna di phishing è doppio: rubare le credenziali EPICODE degli studenti ed i loro dati bancari.

Punti chiave:

Per creare l'email, il focus è stato posto su alcuni punti chiave:

- Urgenza
- Uso di Typosquatting/Homoglyph
- Persistenza del danno
- Scarsa tracciabilità dell'attacco

Svolgimento:

Scenario:

Lo scenario scelto è ricaduto su uno di tipo amministrativo/finanziario, infatti nell'email vi è una comunicazione di una notifica amministrativa urgente in merito a una questione burocratica irrisolta e il tutto giunge da parte di quello che si presenta come un ente fidato: la scuola.

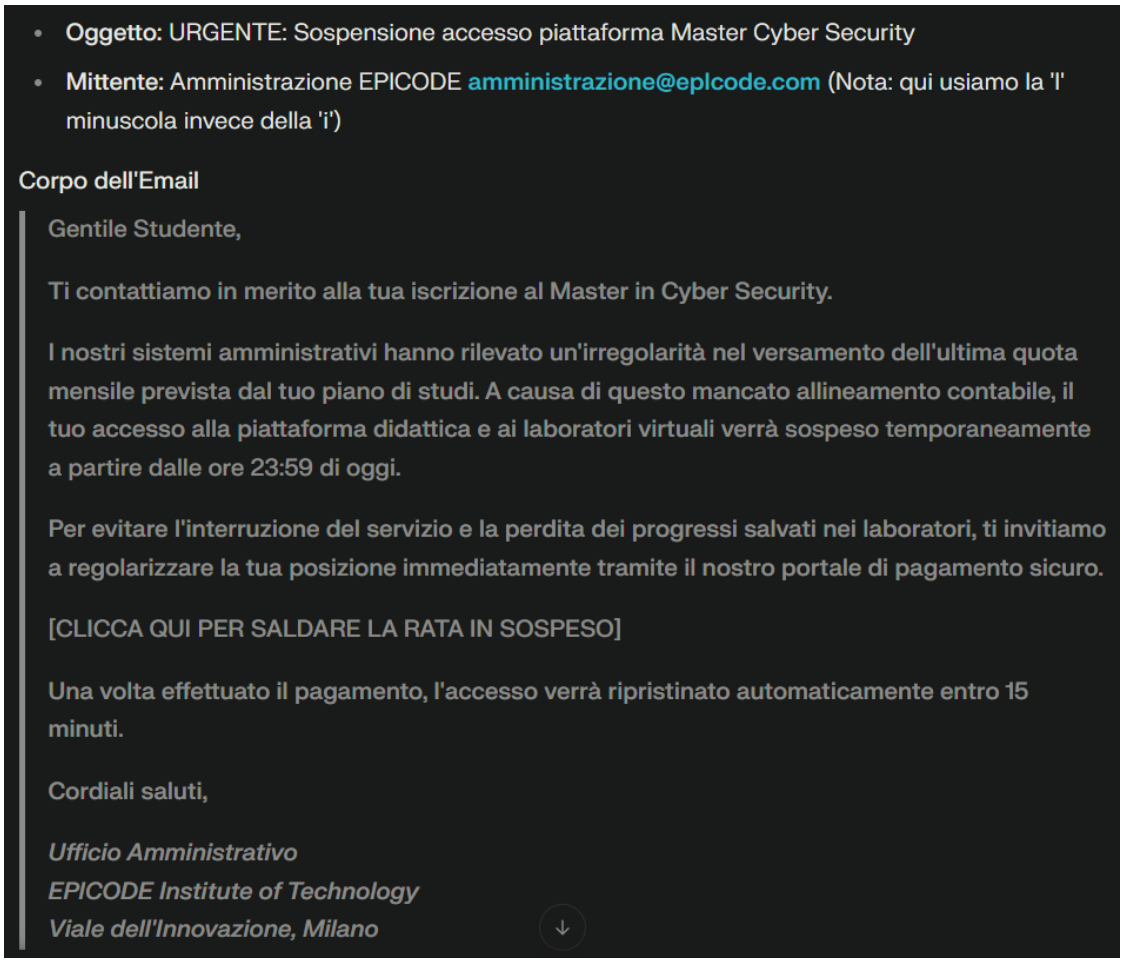
Il tipo di attacco scelto è uno Spray and Pray, ovvero un attacco generico, indirizzato a più utenti, nella speranza che alcuni di loro abbocchino. La scelta è quindi ricaduta su una campagna massiva con destinatario generico.

Si utilizza il principio di urgenza e scarsità che bypassa il procedimento logico a favore dell'istinto di sopravvivenza.

Il premio Nobel Kahneman ha infatti teorizzato che il nostro cervello opera secondo due sistemi, quello razionale (lento, analitico, che controlla i dettagli) e quello istintivo (veloce, emotivo, automatico). Di conseguenza, l'idea è quella di stimolare il sistema istintivo per indurre la vittima ad agire rapidamente, senza permettere al sistema razionale di entrare in gioco. L'istinto di sopravvivenza prende il sopravvento e spinge all'azione, invece che a notare i campanelli d'allarme.

Stesura della mail:

Deciso come strutturare l'attacco, tramite un prompt strutturato si è chiesto all'IA di generare un messaggio.



- **Oggetto:** URGENTE: Sospensione accesso piattaforma Master Cyber Security
- **Mittente:** Amministrazione EPICODE amministrazione@epicode.com (Nota: qui usiamo la 'l' minuscola invece della 'i')

Corpo dell'Email

> Gentile Studente,
>
> Ti contattiamo in merito alla tua iscrizione al Master in Cyber Security.
>
> I nostri sistemi amministrativi hanno rilevato un'irregolarità nel versamento dell'ultima quota mensile prevista dal tuo piano di studi. A causa di questo mancato allineamento contabile, il tuo accesso alla piattaforma didattica e ai laboratori virtuali verrà sospeso temporaneamente a partire dalle ore 23:59 di oggi.
>
> Per evitare l'interruzione del servizio e la perdita dei progressi salvati nei laboratori, ti invitiamo a regolarizzare la tua posizione immediatamente tramite il nostro portale di pagamento sicuro.
>
> [CLICCA QUI PER SALDARE LA RATA IN SOSPESO]
>
> Una volta effettuato il pagamento, l'accesso verrà ripristinato automaticamente entro 15 minuti.
>
> Cordiali saluti,
>
> *Ufficio Amministrativo*
> *EPICODE Institute of Technology*
> *Viale dell'Innovazione, Milano*

Figura 1 email di phishing generata dall'IA

Il messaggio è semplice, fa leva sulla parte istintiva del cervello e, tramite typosquatting, inganna il colpo d'occhio sul mittente facendolo sembrare affidabile. Oltretutto il messaggio presenta una Call To Action mirata: il pulsante che porta alla soluzione è messo in evidenza, senza fornire opzioni differenti quali "contattaci" o "leggi le F.A.Q.", indirizzando l'utente verso la trappola.

Eliminando le distrazioni, si porta la vittima ad agire per risolvere il problema nell'unico modo proposto.

Dietro al bottone si nasconde l'URL malevolo. In questo attacco, si è pensato a un doppio attacco, optando sia per il credential harvesting che per il Credit Card Grabbing, infatti il pulsante rosso o arancione (colori che segnalano allarme) porterà anzitutto a una landing page mirror di Epicode creata con un tool come SET (Social Engineering Toolkit) e che si presenta come una copia esatta della pagina originale.

Questo serve a un duplice scopo: la vittima pensa che il login sia un'ulteriore sicurezza, una verifica sull'identità da parte dell'ente, mentre per l'attaccante è un modo di intercettare le credenziali di accesso.

Una volta effettuato l'accesso, il reindirizzamento avverrà verso una pagina che chiede di inserire i dati della carta di credito per aggiornare il metodo di pagamento. Non vi è un addebito istantaneo o tracciabile, ma le informazioni finanziare della vittima vengono raccolte dall'attaccante per poterle usare per addebiti multipli in un secondo momento o per venderle a terzi.

Spiegazione:

Analisi dei fattori di credibilità:

L'efficacia di questa mail non risiede tanto nel payload quanto nella sua capacità di manipolazione psicologica e mimetismo visivo.

I fattori principali per cui risulta credibile sono tre:

1. Authority Bias: la comunicazione simula la provenienza da un ente noto e gerarchicamente superiore, in questo caso l'amministrazione scolastica, che detiene realmente il potere di revocare l'accesso. Gli studenti tendono istintivamente a fidarsi delle comunicazioni istituzionali, senza andare a sottoporle ad analisi critica.
2. Homoglyph Attack (Attacco Omografico): l'utilizzo del dominio eplcode.com sfrutta la somiglianza visiva in molti font standard per le caselle mail, tra la elle minuscola e la i, sia maiuscola che minuscola, permettendo quindi di superare il primo filtro visivo dell'utente.
3. Pretexting (Coerenza del Contesto): per uno studente attivo, la minaccia di interruzione del servizio è uno scenario possibile e temuto che rientra quindi nella Loss Aversion. Il contesto è coerente con le aspettative di chi utilizza un servizio a rate o un abbonamento.

Red Flags:

Nonostante l'apparenza legittima, il messaggio presenta diversi campanelli d'allarme rilevabili tramite un'analisi attenta (e quindi l'attivazione del sistema razionale del cervello):

1. Header Analysis: l'analisi del mittente, e quindi un controllo accurato sull'indirizzo email, rivela l'utilizzo di typosquatting: eplcode invece di epicode.
2. Saluto generico: l'utilizzo di un saluto generico come può essere, nel nostro caso, "Gentile Studente", invece dell'utilizzo del nome proprio è tipico delle campagne di Spray And Pray massive, in quanto spesso l'attaccante possiede solo una lista di mail e non i dati anagrafici completi.
3. Urgenza Artificiale: la necessità di agire entro un tempo prestabilito, nel nostro caso la mezzanotte del giorno successivo, è una tattica di pressione psicologica. Le mail ufficiali spesso offrono soluzioni tramite molteplici canali e finestre di risoluzione più ampie.

4. Hovering: passando il cursore sul pulsante “CLICCA QUI” la barra di stato del browser rivelerebbe il dominio differente da quello ufficiale della scuola
5. Testi Imperativi: l’utilizzo di verbi d’azione stimola la parte del cervello istintiva, aumentando la sensazione di urgenza
6. Urgenza Visiva: il bottone è spesso rosso o arancione, colori che segnalano allarme o allerta
7. Cognitive Tunneling: una mail ufficiale conterrebbe footer con privacy policy, link ai social o al sito istituzionale, etc, elementi assenti o resi non clickabili nelle mail di phishing. L’unico elemento interattivo è quello che spinge a effettuare il pagamento.

Comportamento corretto:

Di fronte a un’email di questo tipo, la procedura di sicurezza prevede:

1. Stop And Look: evitare di agire d’impulso, prendersi un attimo e verificare che l’urgenza sia giustificata.
2. Controllo del mittente e del dominio: verificare attentamente il dominio e la presenza di variazioni prima di fidarsi, fare attenziona a homoglyph e typosquatting
3. Controllo del link: senza clickare, passare il mouse sopra al pulsante per verificare la destinazione e la sua coerenza con il dominio ufficiale.
4. Verifica Out-Of-Band: non utilizzare contatti o link forniti dall’email sospetta, ma contattare l’amministrazione o visitare il sito tramite un canale ufficiale noto per richiedere le dovute conferme.
5. Segnalazione: inoltrare la mail al team IT o di sicurezza – senza clickare su nulla – inoltrandola come allegato per mantenere tutti gli header originali e permetterne quindi l’analisi.

Conclusioni:

L’esercizio dimostra come il phishing non si basi esclusivamente su vulnerabilità tecniche, ma faccia leva, tramite tecniche d’ingegneria sociale, sull’anello debole: le vulnerabilità umane. La combinazione di elementi tecnici e psicologici crea un attacco estremamente efficace anche contro utenti con una buona alfabetizzazione digitale.

L’analisi condotta evidenzia alcuni aspetti fondamentali per la difesa:

1. Consapevolezza del Dual-Process Theory: sapere che esiste un meccanismo decisionale del cervello suddiviso sistema razionale e sistema istintivo permette di riconoscere quando si sta agendo sotto pressione emotiva. L’urgenza artificiale è progettata per impedire l’attivazione del sistema razionale e del pensiero critico. Si rendono quindi fondamentali le procedure di verifica standardizzate anche sotto stress, come possono essere quelle presentate nella sezione “comportamento corretto”.
2. Rilevanza della Formazione Continua: le campagne di phishing si evolvono continuamente, adottando nuove tecniche e adattandosi ai nuovi contesti. La formazione deve includere simulazioni pratiche che espongano gli utenti al rischio in ambiente controllato.
3. Verifica Out-Of-Band: effettuare verifiche tramite i canali ufficiali, indipendenti dalla mail e fidati, è una regola fondamentale per qualsiasi operazione che richieda azioni urgenti su dati sensibili. È un principio semplice, ma estremamente efficace, contro buona parte degli attacchi di social engineering

Concludendo, la creazione di questo scenario di phishing, in ambiente controllato e consapevole, ha permesso l’analisi dall’interno delle dinamiche di un attacco che, statisticamente, resta uno dei più diffusi nel panorama della sicurezza informatica.

La comprensione delle tattiche offensive è un prerequisito essenziale allo sviluppo di strategie difensive efficaci e per contribuire allo sviluppo di una cultura della sicurezza informata.