Il caso Sofia Menjìvar Castillo:

I pericoli delle Honey Trap

Si prende in analisi un caso di phishing che ha utilizzato la tecnica delle honey trap per sottrarre il controllo di un crypto portafogli.

L’hacker ha impostato un profilo falso su vari social, curandolo per qualche mese al fine di renderlo più credibile possibile, il soggetto costruito si chiama Sofia Menjìvar Castillo, è una giovane donna nata in America Latina e cresciuta in Italia, il suo background ricopre discipline lontane da ciò che concerne le crypto e il mondo della cyber sicurezza, decisa a intraprendere una nuova strada, si iscrive a vari forum e gruppi telegram inerenti alle cryptovalute, trading e simili. In questo modo l’hacker può scandagliare gli

“Sofia Menjìvar Castillo” (Alias usato dall’Hacker)

elementi che popolano questi siti, individuando alla fine la vittima perfetta: John Tate (alias), giovane ragazzo benestante con un paio di anni d’esperienza nel settore. L’hacker ha scelto la vittima in base a delle prime informazioni raccolte sorvegliando il comportamento di Tate sui forum: eccessivamente fiducioso delle sue capacità, arrogante, sicuro di sé, caratteristiche che spianano terreno fertile per un attacco di ingegneria sociale tramite la tecnica della Honey Trap, ossia la raccolta di informazioni riservate sfruttando un comportamento provocante, una connessione romantica o una rapporto intimo. Storicamente utilizzatoa da spie donne per raccogliere informazioni da importanti cariche ricoperte da uomini, negli ultimi anni è stata dimostrata ampiamente la pericolosità di questa tecnica quando usata su internet attraverso la creazione di profili falsi.

Tornando al caso in analisi, Sofia ha approcciato John, dimostrandosi inesperta e ingenua, ma intrapendente e curiosa, anche se con scarsi risultati. Nel corso delle settimane Sofia ha posto varie domande a Tate inerenti alle cryptovalute, formulandole in modo da avere ovvie risposte, per far crescere il senso di sicurezza della vittima e facendogli abbassare la guardia, allo stesso tempo utilizzando un comportamento civettuolo per approfondire il rapporto intimo tra i due. Nel tempo, l’hacker ha acquisito alcune informazioni anagrafiche della vittima, come la data di nascita, il nome del suo primo cane, nome e data di nascita dei genitori, ma soprattuto la sua email, queste informazioni sono bastate all’hacker per eseguire la seconda fase del suo iter: tentare, senza intenzione di successo, a cambiare password o altre credenziale del profilo Crypto.com, così che, con frequenza alternante, il sito inviasse a John varie notifiche di emergenza per tentativi di accesso al suo profilo. Questo comportamento è stato fatto per far abituare la vittima alle varie richieste di autenticazione a due fattori e simili, sia per analizzare la sua risposta a questi warning, sia per fargli alzare la guardia, che, controintuitivamente, è stato ciò che ha sancito la perdita del suo portafogli.  
Prima di analizzare la fase finale del piano dell’hacker è bene specificare che il sito Crypto.com utilizza una tecnica di sicurezza chiamata Recovery Phrase o Root Phrase: una chiave composta da massimo 24 parole, leggibili da umano, prese da una pool di 2048 possibili. La Recovery Phrase è il dato più sensibile di un profilo Crypto.com, attraverso di essa si può cambiare qualsiasi credenziale senza passare per le altre autenticazioni.

Infine, nello stesso periodo in cui john riceveva i vari alert di tentato accesso, Sofia ne ha ricevuti alcuni a sua volta, condividendo le sue preoccupazioni con la vittima, chiedendogli aiuto. Il tutto è culminato quando l’hacker ha inviato a Tate una email di phishing accuratamente formata: essa infatti specificava che, visto i vari alert ricevuti nei giorni precedenti, crypto.com richiedeva l’inserimento della recovery phrase, (dato mai richiesto prima), per effettuare un ripristino totale del portafogli ed evitare futuri tentativi di accesso. Il successo dell'email di phishing è stato determinato dal rapporto di fiducia che la vittima credeva di avere con Sofia. Pochi minuti prima che John ricevesse la stessa email, Sofia gli aveva inviato uno screenshot, lamentandosi dell'ennesima richiesta di autenticazione dell'identità. Subito dopo, gli aveva comunicato di aver seguito le istruzioni della mail e di aver ripristinato il proprio wallet, sperando che questa fosse l'ultima verifica necessaria per risolvere definitivamente il problema delle frequenti richieste di autenticazione. Questa azione è stata ciò che ha tratto definitivamente in inganno John, il quale, credendo Sofia ingenua e inesperta, non ha mai dubitato delle sue parole, cosicché, quando anch’egli ha ricevuto la mail, ha inserito la sua recovery phrase, non sapendo di starlo facendo in un sito clonato dall’hacker per poter sottrare la frase a Tate e usarla in seguito per sottrargli tutti i fondi.

La Mail di Phishing era così composta:

From: help-centre@cry.pto.it

Caro **John Tate**

Il nostro sistema ha rilevato frequenti tentativi di accesso al suo portafogli da parte di terzi, per questo motivo è richiesta la conferma della sua *Recovery Phrase* e il successivo ripristino del suo portafogli al fine di evitare futuri tentativi di accesso.

Questa operazione richiede la massima urgenza e dev’essere obbligatoriamente eseguita entro **48** ore dall’emissione di questa notifica

**Passi per verificare il tuo portafogli**

1. Clicka il link sottostante per acceder al portale di ripristino di Crypto.com
2. Inserisci la tua *Recovery Phrase* esattamente come è stata generata..
3. Conferma la phrase per terminare il processo di autenticazione

**Conferma la tua frase di recupero**  
<a href="https://sitoclonatoperphishare.com">https:// crypto.com/it </a>

**Cosa succede in caso di mancata verifica ?**

La mancata verifica della *Recovery Phrase* comporterebbe:

* Accesso limitato al tuo portafogli
* Impossibilità di processare le transazioni
* Potenziale Perdita di fondi

Per qualsiasi domanda, può rispondere a questa email help-centre@cry.pto.it

La ringraziamo per la pronta risposta

**Cordiali saluti,**  
Il Team Sicurezza di Crypto.com  


Possiamo analizzare come la mail sembri perfettamente credibile, fa riferimento a cose successe che solo il sito crypto.com potrebbe sapere e fa leva sull’urgenza e la gravità della situazione. La vittima, non fosse stata offuscata dai comportamenti dell’hacker, avrebbe potuto accorgersi di alcune sbavature, come inconsistenza nella punteggiature o nella nomenclatura degli elementi sensibili. I due elementi più ovvi sono due: il primo è la mail del finto servizio clienti [help-centre@cry.pto.it](mailto:help-centre@cry.pto.it) innanzitutto è un dominio italiano, difficile per una multinazionale, inoltre, il dominio non è “crypto”, ma “cry.pto”, evidente tentativo di emulare il sito originale.

Il secondo campanello di allarme dovrebbe provenire dalla situazione generale: la recovery Phrase il dato più sensibile del profilo crypto.com, è impossibile che venga richiesta dall’azienda attraverso una Mail.