Scenario

La mail sarà di tipologia spear phishing, ovvero email indirizzata a un individuo ben scelto. Il target scelto è Paola Garifi per 3 principali motivi… in passato la sua email è gia stata hackerata, viaggia molto ed è il massimo esponente in EPRcomunicazione

Titolo mail:
EPRcomunicazione… Paola Garifi è davvero chi dice di essere?

Corpo mail:

LinkedIn

Paola Garifi

ecco cosa **nasconde**...

Vedi post

Scarica la nuova app LinkedIn per desktop

Scaricalo da Microsoft

Disponibile anche su dispositivo mobile

Scarica su App Store | DISPONIBILE SU Google Play

Il destinatario di questa email è Paola Garifi

Scopri perché queste informazioni sono incluse.

Stai ricevendo notifiche email sulle altre persone che potresti conoscere.

Annulla l'iscrizione · Guida

LinkedIn

Obiettivo:

L’obiettivo di questa email spear phishing è ottenere le credenziali di Paola Garifi, la presidente di EPRcomunicazione. Una volta ottenute le credenziali sarà possibile diffondere un ransomware interno (dipendenti dell’azienda) ed esterno (partner dell’azienda).

SCENARIO COMPLETO

Paola Garifi - Pt 1

Paola Garifi si trova a New York città che voleva visitare da ormai tanti anni.
Improvvisamente arriva una mail sul suo telefono che colpisce la sua attenzione: “**EPRcomunicazione… Paola Garifi è davvero chi dice di essere**?”. Paola incuriosita e al tempo stesso spaventata per cosa potrebbero aver detto sul suo conto apre senza pensare la mail e preme sul bottone **Vedi Post** … digita le credenziali ma non succede nulla… allora digita nuovamente le credenziali pensando di aver sbagliato password… ma questa volta la fa entrare su linkedin. Una volta entrata su Linkedin Paola non trova nessun post: “Lo avranno già cancellato o segnalato, meglio così" pensa Paola.

Criminale - Pt 2

Il Malintenzionato ora ha le credenziali, deve solo aspettare che Paola Garifi vada a dormire per poter mandare il ransomware al CEO dell’azienda EPRcomunicazione.

CEO - Pt 3

Il CEO riceve un messaggio da Paola Garifi che dice questo:
“Ciao Daniele, spero di non disturbarti, volevo informarti che mi sono appena arrivati i nuovi documenti per rimanere in conformità con le legislazioni, ti prego di mandare tutti gli allegati al personale e leggerli insieme domani durante le ore lavorative.
Ora che sono in viaggio almeno per un po’ vorrei rimanere tranquilla il più possibile.
Ci sentiamo quando torno”

Ransomware - Pt 4

Ora ti spiegherò le caratteristiche del ransomware.
Il ransomware funzionerà solamente se il documento verrà aperto su un PC e si attiverà con un delay di 10 minuti.

In caso non fossero passati 10 minuti o fosse aperto su dispositivi mobili, verrà mostrato solamente il testo del documento.

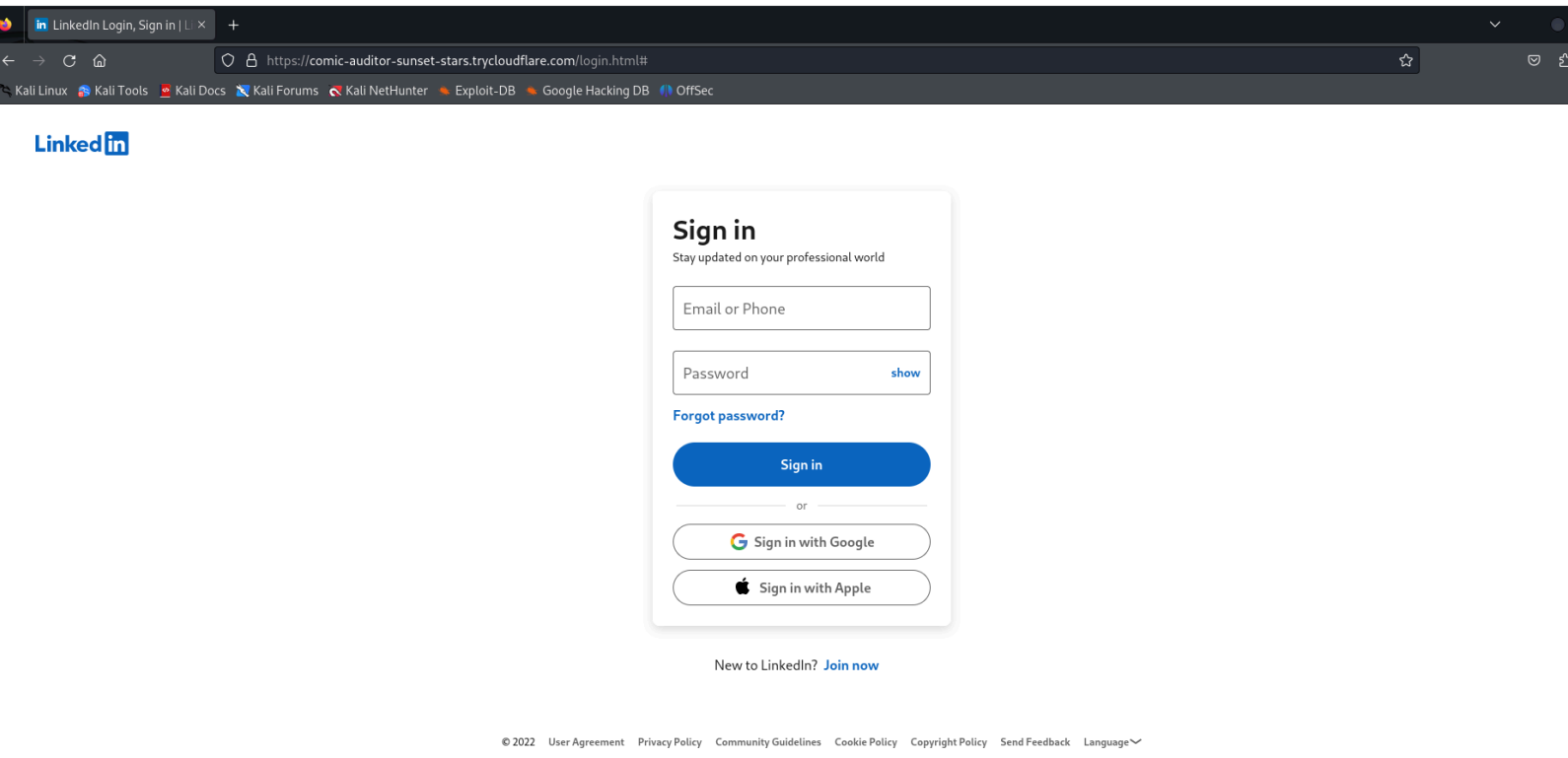
Sono importanti i dieci minuti di delay per assicurarsi che tutti i dipendenti aprano l’allegato sul proprio pc ed è anche di grande importanza che non si attivi su dispositivi mobili perché una volta letto il messaggio su linkedin è importante che il telefono non si infetti subito alla lettura perché creerebbe uno stato di allarme ancor prima di raggiungere i PC dell’azienda

Infezione - Pt 5

Daniele aspetta che tutti i dipendenti e lo staff entrino in azienda e si siedano ai loro PC.
Daniele avverte tutti che ha mandato una mail con l’allegato da leggere. I dipendenti e l’intero staff aprono l’allegato e una volta passati 10 minuti….
BTC WALLET: 1FakeBTCAddressForExample1234567890qwerty Tempo: 2 ore
Pagare entro la scadenza o tutti i file verranno distrutti e divulgati a fonti esterne

Prevenzione

- Nella mail andando al footer si può vedere che Paola Garifi è scritto in modo diverso
- Ispezionando il corpo della mail o guardando la mail mittente vicino al titolo si vedrà che non combacia con la mail originale di Linkedin
- Una volta digitate le credenziali nella pagina Linkedin non da nessun messaggio di errore per le credenziali, questo è un'altro grosso campanello d'allarme
- L'url del sito aperto non combacia con quello della login page di Linkedin
- Ispezionando la mail vera (il codice) ci sono moltissime informazioni diverse dalle mail originali di Linkedin
- Google suggerisce che il sito è non sicuro



Questa è una pagina creata da me, come ben si vede l'URL è completamente diverso dall'originale