La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

La truffa del CEO / BEC

Cos'è la truffa del CEO / BEC?

Gli hacker informatici continuano a sviluppare un tipo di attacco e-mail chiamato Frode del CEO o Business Email Compromise (BEC). Questi tipi di attacchi consistono in e-mail mirate che ingannano la loro vittima e la spingono a compiere un'azione che non dovrebbero intraprendere. Nella maggior parte dei casi questi attacchi mirano al denaro. Ciò che rende questi attacchi particolarmente pericolosi è che gli hacker informatici ricercano con attenzione le loro vittime prima di lanciare il loro attacco. Le tecnologie di sicurezza informatiche attualmente impiegate non sono in grado di fermare questi attacchi perché non ci sono allegati e-mail infetti o collegamenti dannosi da rilevare. Ecco in sintesi come funziona l'attacco.

L'hacker cibernetico utilizza Internet per ricercare la vittima designata e le persone con cui interagisce la vittima. Ad esempio, se ti prendono di mira, cercheranno di capire chi è il tuo capo al lavoro oppure un agente immobiliare con cui sei in contatto. L'utente malintenzionato crea quindi una email, fingendo di essere una persona a te nota e ti invia l'email. L'e-mail è urgente e generalmente richiede di agire immediatamente, ad esempio chiedendo che venga rielaborata una fattura, che venga modificato il destinatario di un pagamento oppure convincendo la vittima a condividere documenti sensibili. L'email ha lo scopo di spingerti a fare quello che vogliono. Ecco due esempi di come un simile attacco potrebbe funzionare.

Bonifico Bancario: I cyber crimnali sono sempre a caccia di soldi. Eseguono ricerche sull'azienda per cui lavori, ad esempio identificando chi lavora nell'ambito dei pagamenti o chiunque sia responsabile del trasferimento di fondi. I criminali quindi creano e inviano un'email a queste persone fingendo di essere il loro capo o un dirigente di alto livello. L'email all'interno del testo riporta un'emergenza per la quale si rende necessario un trasferimento immediato di denaro su un nuovo conto bancario. L'e-mail li spinge quindi a commettere un errore pressati dall'urgenza inviando inconsciamente denaro al criminale informatico.

Frode Fiscale: I criminali informatici cercano informazioni personali da utilizzare per frodi fiscali. Uno dei modi più veloci per ottenere questo è rubare le informazioni di tutti i dipendenti di un'azienda. I criminali informatici ricercano e identificano coloro che lavorano nelle risorse umane. Quindi inviano email false a queste persone, facendo finta di essere un dirigente di alto livello oppure qualcuno che lavora nell'ambito legale. Le e-mail fanno riferimento a delle situazioni urgenti che richiedono informazioni fiscali su tutti i dipendenti. Le vittime delle Risorse Umane pensano di inviare i documenti sensibili al dirigente, mentre in realtà li stanno mandando a un cybercriminale.

Proteggi te stesso

Quindi cosa puoi fare per proteggerti? Il buon senso è la tua migliore difesa. Ecco gli indizi più comuni da cercare.

- **L'e-mail di solito è molto breve e urgente (spesso solo un paio di frasi) e la firma dice che l'e-mail è stata inviata da un dispositivo mobile.**
- **L'e-mail trasmette un senso di urgenza, ti spinge a ignorare o aggirare le politiche imposte dalla tua azienda. Segui sempre le politiche e le procedure standard, anche se l'email sembra provenire dal tuo capo o persino dal CEO.**
- **L'email è correlata al lavoro, ma utilizza un indirizzo email personale, come @gmail.com o @hotmail.com.**
- **L'e-mail sembra provenire da un senior manager, un collega o un commerciale che conosci o con cui lavori, ma il tono del messaggio non è coerente con il profilo della persona.**
- **Le istruzioni di pagamento sono dettagliate e differiscono da quelle tipicamente effettuate, ad esempio fanno spesso riferimento ad un pagamento immediato a un altro conto bancario.**

Se sospetti di essere stato preso di mira al lavoro, interrompi tutte le interazioni con il mittente e riferiscilo al tuo supervisore. Se sei stato preso di mira a casa e sei caduto vittima di una frode di questo tipo effettuando un bonifico bancario, segnalalo immediatamente alla tua banca, e poi alle forze dell'ordine.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

L'autore di questo articolo

***Don Cavender** è un ex agente speciale dell'FBI, con oltre 22 anni di esperienza nell'analisi forense digitale e cybercrimine. Di recente ha preso di mira le organizzazioni di criminalità informatica come coordinatore del BEC di Washington DC. Don Cavender eroga corsi di formazione e svolge attività di ricerca in informatica forense digitale e indagini informatiche.* @don_cavender
https://www.linkedin.com/in/donald-cavender

Risorse

Social Engineering:	https://www.sans.org/u/HE3
Stop That Phish:	https://www.sans.org/u/GEG
Stop That Malware:	https://www.sans.org/u/HEd
SLock Down Your Login:	https://www.sans.org/u/HEi