La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per te

Truffe targettizzate

Panoramica

I cyber criminali continuano a inventare strategie nuove e creative per ingannare gli utenti. Un nuovo tipo di truffe sta guadagnando popolarità: le truffe targettizzate. I cyber criminali trovano o acquistano informazioni su milioni di utenti, successivamente utilizzano tali informazioni per personalizzare ("targettizzare", appunto) i loro attacchi. Di seguito ti mostreremo come si svolgono queste truffe e ti guideremo attraverso un esempio comune. Quanto più sai di queste truffe, tanto più facile è per te individuarle e non caderne vittima.

Come funziona?

Le truffe via e-mail o telefoniche non sono novità, i cyber criminali hanno tentato di ingannare gli utenti per anni. Alcuni esempi sono "Hai vinto la lotteria" o le infami truffe "alla nigeriana". Tuttavia, queste truffe sono generiche, i cyber criminali non le indirizzano miratamente a specifici utenti. Semplicemente creano un messaggio standard e lo inviano a milioni di persone. Per questo motivo, queste truffe sono di solito facili da individuare. Una truffa targettizzata è diversa, i cyber criminali fanno una ricerca su ogni vittima designata e la sua utenza e creano un messaggio personalizzato. Le ricerche sono svolte in prima persona o acquistando database contenenti informazioni (nomi di persone, password, numeri di telefono o altri dettagli). Tali informazioni sono facilmente disponibili a causa dei numerosi i siti Web violati quotidianamente. Spesso non vi è nemmeno bisogno di cercare tra i siti violati, molte informazioni sono infatti reperibili attraverso i profili nei social media e nei registri governativi pubblici, consultabili liberamente. Questa tipologia di cyber criminali prende quindi di mira solo i soggetti dei quali dispone di informazioni utili alla truffa.

In questa tipologia di truffa, altro trucco comune utilizzato dai cyber criminali è lo sfruttamento della paura per costringere l'utente a pagare. L'attacco si svolge così: vengono reperite o acquistate informazioni su accessi e password di utenti, provenienti da siti Web compromessi. Tra queste, le credenziali degli account sono utili per accedervi e carpire dettagli personali che sono poi dettagliatamente citati in una email inviata allo stesso utente. Tale email, comprende a volte la stessa password utilizzata nel sito compromesso, data come "prova" dell'aver hackerato il computer o il dispositivo (il che ovviamente non è vero). A volte, il cyber criminale arriva persino a sostenere di aver sorpreso l'utente a visualizzare pornografia online. Segue quindi una e-mail di richiesta di denaro e la minaccia, in caso di mancato pagamento, di vedersi condivise con familiari e amici le prove imbarazzanti delle proprie attività online.

La verità è che in quasi tutte le situazioni come questa, il cyber criminale non ha mai violato il sistema. Non sa nemmeno chi sia l'utente o quali siti web abbia visitato. Il truffatore sta semplicemente tentando di utilizzare i pochi dettagli personali che possiede

per spaventare e convincere di aver hackerato il computer o dispositivo, per indurre a pagare. Ricorda, i malfattori possono usare le stesse tecniche anche per una truffa telefonica.

Cosa posso fare?

Riconoscere che le e-mail o le telefonate come queste sono una truffa. È naturale sentirsi spaventati quando qualcuno dimostra di possedere alcune tue informazioni personali, tuttavia, ricorda che il mittente sta mentendo. L'attacco fa parte di una campagna su larga scala, non un'azione esplicitamente rivolta a te. Oggigiorno sta diventando molto più facile per i cyber criminali trovare o acquistare informazioni personali, quindi bisogna aspettarsi truffe sempre più targettizzate in futuro. Alcuni trucchi:

- **Ogni volta che ricevi un'e-mail, un messaggio o una telefonata, se queste denotano estrema urgenza, guardale con molto sospetto. Se qualcuno cerca di indurre o sfruttare emozioni come la paura, sicuramente sta provando a farti cadere in errore.**
- **Quando è presente una richiesta di pagamento in BitCoin, carte regalo o altri metodi non rintracciabili, sicuramente vi si nasconde una truffa.**
- **Quando ricevi un'e-mail sospetta, fai una ricerca su Google per controllare se altre persone hanno segnalato attacchi dello stesso tipo.**

In definitiva, il buon senso è la tua migliore difesa. Tuttavia, ti consigliamo anche di utilizzare sempre una password lunga, sempre diversa per ciascuno dei tuoi account online. Non riesci a ricordare tutte le tue password? Utilizza un programma per la gestione sicura delle password. Inoltre, abilita la verifica in due passaggi ogni volta che è possibile.

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

Lenny Zeltser *è un veterano della sicurezza informatica. Realizza soluzioni anti-malware presso i laboratori Minerva e insegna corsi di sicurezza presso il SANS Institute. La sua esperienza include anche managed security services e consulenza. Seguilo su* zeltser.com/blog *e su Twitter* @lennyzeltser.

Risorse

Social Engineering:	https://www.sans.org/u/MUU
Stop That Phish:	https://www.sans.org/u/MUZ
Search Yourself Online:	https://www.sans.org/u/MV4
Password Manager:	https://www.sans.org/u/MV9