PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5780 di Lunedì 03 febbraio 2025

Agli attacchi phishing si aggiungono ora gli attacchi vishing

Questi attacchi rappresentano l'evoluzione della precedente categoria di attacchi, e sono basati sull'invio di messaggi vocali, spesso creati da intelligenza artificiale.

Questo tipo di frode si basa sull'uso di canali telefonici per condurre degli attacchi contro ignari utenti. In questo caso il truffatore utilizza un messaggio vocale per indurre in inganno il suo bersaglio. Molto spesso questo messaggio vocale è addirittura creato da applicativi di intelligenza artificiale, che sono anche in grado di rispondere a possibili domande del soggetto attaccato, che desidera approfondire il tema sottoposto alla sua attenzione.

Ad esempio, l'attaccante può spacciarsi per un dipendente di un istituto bancario e cercare di ottenere dati personali del soggetto attaccato, avanzando varie motivazioni, come ad esempio un tentativo di frode sulla sua carta di credito ed attacchi similari.

Spesso questi attacchi sono assai difficili da individuare perché le chiamate, da parte di istituzioni finanziarie ed altre strutture pubbliche, possono essere relativamente frequenti.

Inoltre non dimentichiamo che vittime di questi attacchi sono per solito persone di una certa età, che possono essere più vulnerabili ad attacchi di questo tipo.

Sono state già pubblicati numerosi i documenti, che aiutano l'utente attaccato ad individuare tempestivamente questo tipo di truffa. Ad esempio, si raccomanda di non inviare mai dati personali in risposta a queste richieste o, prima di procedere, si raccomanda di effettuare una chiamata di controllo ad un numero sicuramente legittimo, come ad esempio il numero della propria agenzia bancaria. Non bisogna mai chiedere un numero telefonico di verifica al soggetto che chiama, perché egli potrebbe evidentemente dare un numero fasullo.

Si raccomanda inoltre all'utente chiamato di fare attenzione alle inflessioni vocali del chiamante, che, ove sia simulato da un applicativo di intelligenza artificiale, potrebbe generare una voce con riflessi vocali anomali. Esistono anche degli applicativi che sono in grado, meglio di un utente normale, di individuare una possibile chiamata fraudolenta.

È bene anche tener presente che l'utilizzo di applicativi, che effettuano automaticamente un gran numero di chiamate, fa sì che le persone prese a bersaglio dai malviventi informatici possano crescere in misura esponenziale, aumentando la probabilità che qualche soggetto chiamato possa abboccare.

Al proposito, raccomandiamo ai lettori anche di prendere contatto con il sito Internet dell'autorità garante italiana, che ha messo a disposizione una scheda informativa, che aiuta l'utente a proteggersi da questa particolare tipologia di attacco informatico.

Infine, ricordiamo ai lettori che per completare il panorama di queste particolari tipologie di attacco non bisogna dimenticare anche la terza forma di attacco, chiamata smishing. In questo caso lo strumento di attacco è un messaggio SMS inviato dal malvivente al soggetto preso a bersaglio.

Adalberto Biasiotti

Consigliamo la lettura degli articoli:

Vishing: come proteggersi dal phishing telefonico?

Smishing: cosa è e come difendersi

I suggerimenti del Garante per proteggersi dal phishing

www.puntosicuro.it