30.04.2024

Truffa del CEO 2.0

Nella truffa del CEO classica, il personale di un'azienda riceve da chi si pensa essere il capo un'e-mail con l'ordine di eseguire immediatamente un certo pagamento. All'Ufficio federale della cibersicurezza è stato segnalato un caso che si spinge ancora oltre.

Il caso segnalato all'Ufficio federale della cibersicurezza (UFCS) è diverso dagli attacchi di cui si era a conoscenza finora. Diversamente dalla procedura abituale, alla vittima (un collaboratore autorizzato a effettuare pagamenti direttamente) non è stato impedito di contattare il suo superiore, anzi, con una telefonata un sedicente avvocato lo invitava proprio a partecipare a una videoconferenza con il capo. Quando il collaboratore si è collegato alla riunione online, effettivamente vedeva sullo schermo il presunto capo e poteva parlargli. Quest'ultimo ha poi cercato, durante la conversazione, di convincerlo a effettuare transazioni finanziarie.

Il video falsificato del capo è stato realizzato con l'aiuto dell'intelligenza artificiale. Non è chiaro da dove i criminali abbiano ottenuto il materiale necessario per generare il deep fake, ma si sospetta che abbiano utilizzato materiale video disponibile pubblicamente.

Un'altra possibilità per acquisire i dati, soprattutto per copiare la voce, è quella di effettuare delle telefonate in precedenza. Diverse aziende hanno infatti segnalato che recentemente hanno ricevuto chiamate da parte di persone sconosciute che chiedevano tutta una serie di informazioni sull'azienda, le quali potrebbero essere utilizzate per sferrare attacchi mirati. Con la voce registrata del capo è possibile realizzarne una copia tramite intelligenza artificiale e deepfake.

Questo episodio dimostra che i criminali sfruttano sempre più spesso gli strumenti dell'intelligenza artificiale, sebbene il suo uso non sia ancora perfetto. Nel caso in questione, la truffa è stata smascherata: i truffatori si erano limitati a manipolare solo il volto del capo, mentre l'abbigliamento non corrispondeva al suo stile e anche la voce non era imitata particolarmente bene.

Come riconoscere un deepfake:

- I movimenti delle labbra non sono sincronizzati con le parole pronunciate
- Errori di pronuncia
- Formulazioni strane
- Scarsa qualità video
- Utilizzo di materiale da altri contesti

Maggiori informazioni sulla truffa del CEO e in particolare su come proteggersi sono disponibili all'indirizzo: www.ebas.ch/ceofraud (http://www.ebas.ch/ceofraud)

L'articolo originale dell'UFCS è disponibile qui (https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/2024/wochenrueckblick_14.html) .