PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5563 di Mercoledì 21 febbraio 2024

Sottratti 25 milioni di dollari con l'aiuto di sei controfigure deep fake

Con un certo ritardo, molti quotidiani, in varie parti del mondo, hanno dato notizia di una frode informatica che rappresenta un vero stato dell'arte e merita di essere descritta in profondità.

Colgo l'occasione per illustrare questa truffa, chiarendo il significato dell'espressione inglese "deep fake". Questa espressione, che si legge sempre più spesso, deve essere chiaramente compresa: in inglese la parola fake può essere sia aggettivo, sia sostantivo. Come aggettivo significa contraffatto, come sostantivo significa contraffazione.

L'aggiunta dell'aggettivo "deep", cioè profondo oppure accurato, fa riferimento alla qualità e credibilità della contraffazione.

Ciò premesso, vediamo che cosa è successo nella metà di gennaio 2024.

Un dipendente di un'azienda di consulenza finanziaria è stato invitato dal suo chief financial officer- CFO ad un incontro zoom, cui hanno partecipato altri cinque suoi colleghi. Durante l'incontro zoom, il CFO ha dato istruzioni a questo dipendente di provvedere ad effettuare cinque bonifici, su cinque diversi conti correnti, per un totale di 25 milioni di dollari.

Il dipendente in questione ha avuto alcune perplessità, circa la correttezza di quest'operazione, ma il fatto che alla conference call fossero presenti cinque suoi colleghi, che gli conosceva benissimo, lo ha tranquillizzato e di conseguenza egli ha provveduto ad effettuare i bonifici.

Solo dopo qualche giorno sono rinati i suoi sospetti ed ha effettuato un approfondimento, venendo a conoscenza del fatto che nessuno dirigente o dipendente aziendale era mai stato coinvolto in questo collegamento.

Evidentemente un criminale informatico, con ottime conoscenze dei profili personali dei sei soggetti coinvolti, ha creato dei "deep fake", talmente credibili, sia da un punto di vista di immagine, sia di eloquio, da convincere l'unico dipendente "vero" a prendere per buone le istruzioni ricevute durante il colloquio a distanza.

Appare evidente come una situazione del genere possa essere estremamente preoccupante, per gli esperti di sicurezza, in quanto oggi i collegamenti a distanza sono sempre più frequenti e quindi le opportunità per mettere a punto queste tipologie di piani criminosi crescono in maniera esponenziale.

Oggi sappiamo tutti come esistano applicativi che permettono di creare immagini perfettamente corrispondenti alle immagini reali, nonché applicativi in grado di colloquiare, con una pressoché perfetta simulazione della voce e delle espressioni del soggetto contraffatto. Chi scrive ha avuto occasione di utilizzare per qualche tempo uno specifico applicativo di Adobe, rendendosi conto che, dopo un breve periodo di addestramento, l'applicativo era in grado di leggere un testo con un tale perfezione di intonazione ed eloquio, da ingannare perfino la persona stessa, di cui l'eloquio veniva contraffatto.

Si tratta di un tema di estrema preoccupazione anche per gli specialisti criminologici, in quanto potrebbe diventare estremamente difficoltoso, a fronte di un'intercettazione telefonica, poter comprendere se i soggetti coinvolti nella conversazione erano deepfake o persone reali.

È un argomento di meditazione sul quale esortiamo tutti i lettori a prestare attenzione, cominciando a mettere a punto alcune tecnologie e procedure, che potrebbero aiutare a mettere in evidenza la reale consistenza fisica o meno di una controparte, con la quale si dialoga.

Adalberto Biasiotti

---

www.puntosicuro.it