CRESCONO GLI ATTACCHI IN ITALIA
ALLARME HACKER 2025 ARRIVA IL VIDEO CHE TI RUBA LA FACCIA

Fonte: Rapporto Clusit Sicurezza in Italia - dati primo semestre 2024. Milano, 20 gennaio 2025

S. A.

I deepfake sono filmati, foto e audio generati dall'intelligenza artificiale sulla base di contenuti reali: sostituiscono voce e volto di una persona per colpire in rete. Sono una delle maggiori minacce attese quest'anno. L'ultima indagine Trend Micro

di **UMBERTO TORELLI**

Nell'eterna lotta tra pirati informatici e cyberpoliziotti, quest'anno si inserisce un terzo attore. Parliamo dei sistemi di intelligenza artificiale, usati dai primi per scovare nuove modalità di incursioni nel web, dai secondi per difendersi. L'Italia è uno degli obiettivi degli attacchi informatici, sempre più sofisticati e intensi: una tendenza in crescita.

Lo segnala il Rapporto annuale sulla situazione della sicurezza informatica, rilasciato da Check Point Software a fine novembre. Ebbene nei sei mesi fra maggio e ottobre 2024 il nostro Paese è stato sottoposto in media a 1.896 attacchi settimanali, oltre 200 in più rispetto alla media mondiale.

Le previsioni

L'utilizzo dell'intelligenza artificiale non è una novità, ma oggi ciò che spaventa di più sono i deepfake: video, foto e audio falsi generati dall'intelligenza artificiale partendo da contenuti reali, con la tecnica per la sintesi dell'immagine e della voce umana. Sempre più convincenti — qualcuno li ha chiamati «il falso che ti ruba la faccia» —, sono stati inseriti tra le principali minacce nel 2025 dal report di Trend Micro «The easy way in-out, securing the artificial future». L'indagine, che anticipiamo, è prevista essere presentata a Milano il 24 gennaio.

Secondo gli esperti, quest'anno dei deepfake verrà fatto largo uso. Se la nuova tecnologia consente di creare immagini e filmati manipolati in modo digitale grazie all'Ai, l'obiettivo dei cybercriminali è generare soggetti artificiali che svolgono azioni mai accadute nella realtà. Di fatto vengono sostituiti voce e volto di una persona, realizzando filmati falsi, ma del tutto realistici. Basta guardare la precisione nel sincronismo labiale delle parole pronunciate dal soggetto preso di mira.

Nel dark web si trovano le tabelle con i prezzi: 100 euro per una sincronizzazione labiale, 150 euro per sostituire l'intero viso

Il listino

Nel dark web si possono trovare le tabelle con i prezzi richiesti dai pirati informatici per vendere i deepfake: un listino variabile in funzione del grado di precisione. Una sincronizzazione labiale, per esempio, costa circa 100 euro per trenta secondi di contenuti. Il prezzo sale a 150 euro per la sostituzione dell'intera faccia.

Ma non è finita. Quest'anno sono anche attesi i «gemelli digitali cattivi», «malicious digital twins», una versione avanzata dei deep fake, per mettere a segno nuove truffe. Spiega Alessandro Fontana, country manager di Trend Micro Italia: «Sono addestrati per imitare lo stile di scrittura e la personalità, con lo scopo di costruire video convincenti che prenderanno di mira vittime inconsapevoli».

Come valutare, dunque, la veridicità dei contenuti creati con l'intelligenza artificiale? Esistono piattaforme online che offrono funzionalità di rilevamento dei falsi video. Tra queste c'è DeepFake-o-Meter: sviluppata con software open source dall'Università di Buffalo, scansiona video, audio e immagini, valutando alla fine dell'analisi le probabilità che il contenuto sia vero o falso.

Ma basta seguire qualche avvertenza perché anche un non addetto ai lavori possa valutare la veridicità di un filmato. «Ad esempio, bisogna osservare le espressioni facciali, spesso poco naturali o rigide —dice Fontana —, e cercare incongruenze tra audio e movenze: il corpo potrebbe non risultare sincronizzato con il volto durante i movimenti».

Attenzione anche a dettagli come le ombre, i riflessi e i movimenti innaturali degli occhi (per esempio, i battiti delle ciglia).

Nel corso dei prossimi mesi dovremo difenderci peerò anche da altri attacchi: quelli basati sull'«ingegneria sociale», che con l' inganno mirano a ottenere dagli stessi utenti informazioni e dati sensibili.

«Arriveranno gli access broker, gruppi criminali specializzati nel rubare credenziali private per cederle al mercato nero», dice Luca Nilo Livrieri, direttore area prevendita Sud Europa di CrowdStrike. Vengono presi di mira password, dati anagrafici e biometrici, credenziali bancarie. Il meccanismo è simile al lavoro dei broker finanziari: si tratta infatti di intermediari che si muovono tra i criminali e chi compera accessi falsi su larga scala, per rivenderli al dettaglio sul darkweb. Un mercato illegale con domanda e offerta, basato sul tipo di dati disponibili.

Secondo il Global Threat Report 2024 di CrowdStrike, gli access broker continuano a guadagnare vendendo ad altri gruppi cybercriminali l'accesso ai sistemi informatici delle aziende. Il numero di intrusioni messe in vendita risulta essere aumentato di quasi il 20% rispetto all'anno precedente.

Alla fine tutto questo incrementa anche gli attacchi ransomware, dove viene richiesto un riscatto per restituire le informazioni catturate.

Un rimedio è ricorrere a una protezione personale che si avvalga non solo di password, adottando il controllo multifattoriale della propria identità digitale.

«È bene usare metodi di autenticazione che contengano informazioni multilivello — dice Livrieri —, ad esempio qualcosa che hai, qualcosa che sai e qualcosa che sei».

+20

Per cento

Gli accessi ai sistemi informatici delle aziende messi in vendita nel 2024 rispetto al 2023