Rapporto sicurezza VMware: in aumento gli attacchi alle API e l’uso di deep fake. Troppo lavoro per i team di sicurezza, che soffrono il burnout

https://www.hwupgrade.it/i/n/vmware_logonew_720.jpg,

Il numero di esperti di sicurezza a rischio burnout è diminuito rispetto allo scorso anno, ma risulta ancora elevato: due esperti su tre valutano, o hanno valutato, di lasciare il lavoro per questo motivo

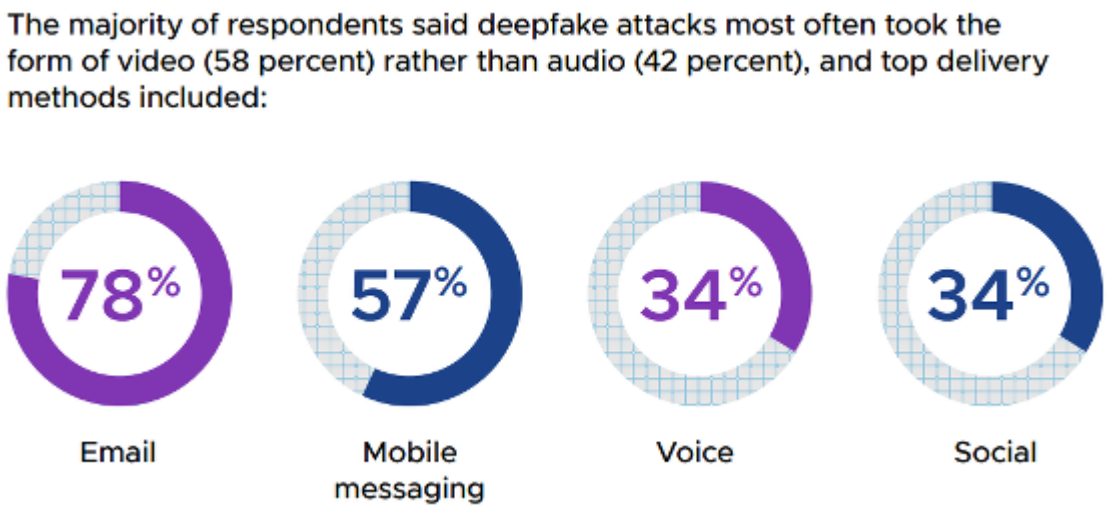
di Alberto Falchi pubblicata il **09 Settembre 2022**, alle **18:31** nel canale Security

VMwareCloud Security

VMware ha pubblicato in questi giorni, in concomitanza con la conferenza dedicata alla sicurezza informatica Black Hat USA 2022, il suo ottavo report annuale sullo stato della cybersecurity, il **Global Incident Response Threat Report**.

Fra i punti salienti, il crescente uso di deepfake nelle campagne di attacco e la crescita degli attacchi verso le API, considerate la prossima frontiera per il crimine informatico. A complicare lo scenario **il sovraccarico di lavoro dei team di sicurezza, che accusano pesantemente lo stress**.

I criminali informatici si evolvono: cresce l'uso dei deepfake

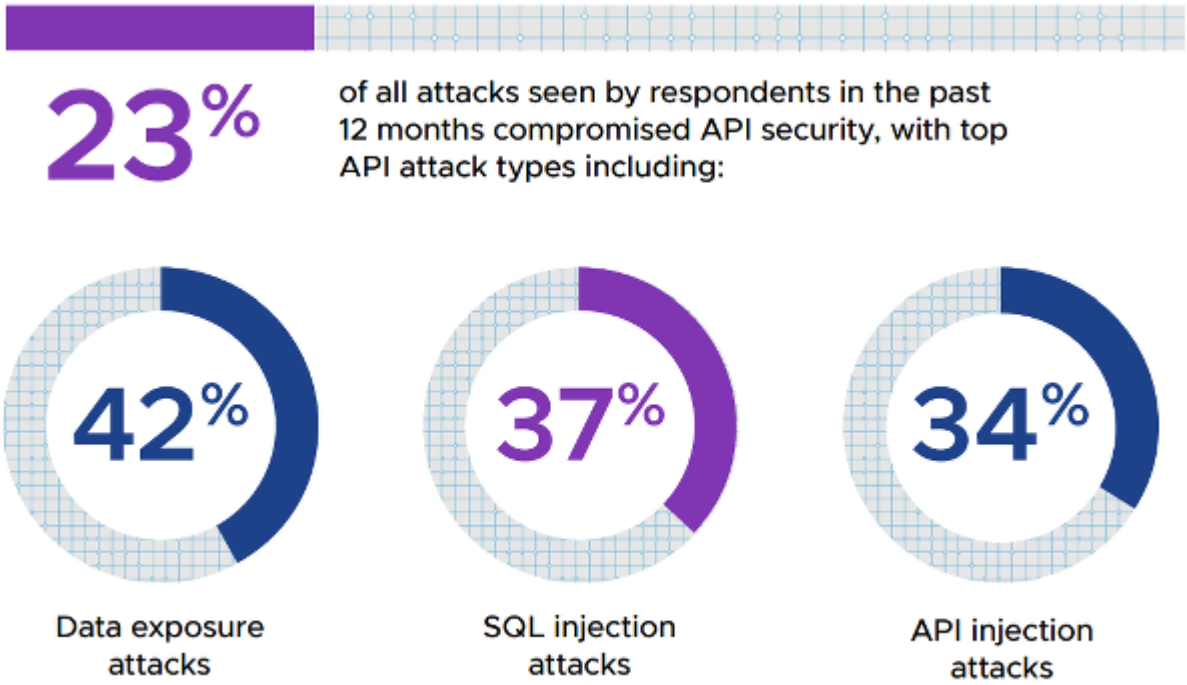


L'intelligenza artificiale ha fatto passi da gigante negli ultimi mesi, e oggi i software per generare testi, immagini e video interamente al computer sono evolutissimi. Così tanto che ormai creare un deepfake è relativamente semplice, e i criminali informatici se ne sono resi conto.

Il report di VMware evidenzia come la tecnica del deepfake sia sempre più utilizzata, per esempio per impersonare l'amministratore delegato o qualche altro manager e convincere i dipendenti a effettuare trasferimenti bancari. Secondo VMware, questa modalità di attacco è cresciuta del 13%, e due persone su tre del campione preso come riferimento (66%) sostengono di essere stati testimoni di un tentativo di violazione di questo tipo.

"*Per eludere i controlli di sicurezza, oggi i criminali informatici stanno introducendo nei loro metodi di attacco anche i deepfake*", ha dichiarato **Rick McElroy**, principal cybersecurity strategist di VMware. "*Secondo il nostro report, due intervistati su tre hanno rilevato l'utilizzo di deepfake dannosi come parte di un attacco, con un aumento del 13% rispetto allo scorso anno e l'e-mail a rappresentare il metodo di trasmissione più comune. Oggi i criminali informatici non si limitano più a utilizzare video e audio manipolati nelle*

campagne di disinformazione o nelle influence operations. Il loro nuovo obiettivo è sfruttare la tecnologia deepfake per ottenere l'accesso e compromettere le organizzazioni".



Un altro dato molto interessante è che praticamente **un attacco su quattro (23%) prende di mira le Application Programming Interface (API)**, e secondo la multinazionale questo trend è destinato a crescere.

Il problema del burnout dei team di sicurezza

Si parla di burnout quando si lavora troppo per prolungati periodi, fatto che può portare a stanchezza, demotivazione, distrazione. Ad accusare maggiormente queste problematiche sono i team di sicurezza, che hanno grandi responsabilità e ogni giorno sono chiamati a stare dietro a un numero elevatissimo di allarmi e verificare che nulla sia stato compromesso e che l'infrastruttura sia al sicuro.

Non si tratta di una novità: questo problema è messo in evidenza da qualche anno. **Rispetto allo scorso, sono calata di qualche misura le percentuali di chi sosteneva di aver sofferti di burnout**, ma questo non basta a tranquillizzare. Più della metà degli esperti di sicurezza (57%) ha infatti dichiarato di aver sperimentato livelli molto elevati di stress negli ultimi 12 mesi. Il 69% di questi ne ha sofferto tanto da aver valutato di lasciare il lavoro. C'è però un dato positivo: le aziende si stanno rendendo conto del problema e in due casi su tre hanno attivato programmi di benessere per ridurre il rischio di burnout.

"*Per difendersi dalla progressiva estensione della superficie di attacco, i team di sicurezza hanno bisogno di un livello adeguato di visibilità su carichi di lavoro, dispositivi, utenti e reti per rilevare, proteggere e rispondere alle minacce informatiche*", ha dichiarato **Chad Skipper**, global security technologist di VMware. "*Se i team di sicurezza prendono decisioni basate su dati incompleti e imprecisi, viene inibita loro anche la capacità di implementare una strategia di sicurezza granulare e i loro sforzi per rilevare e bloccare gli attacchi laterali sono ostacolati da un contesto limitato dei loro sistemi*".

Read More