Falso allarme Gmail: il data breach subito da Google non riguarda gli account personali

Descrizione

(Adnkronos) â?? Un'onda di panico si Ã¨ diffusa online dopo che la notizia di un presunto data breach che avrebbe colpito 2,5 miliardi di account Gmail ha iniziato a circolare sui social media. Tuttavia, un'analisi approfondita condotta da Google e da esperti di sicurezza ha smentito l'allarme, chiarendo che l'attacco, pur essendo significativo, non ha compromesso direttamente i singoli account utente di Gmail. L'incidente, gestito dai gruppi di hacker noti come UNC6040 e UNC6395, non ha violato i sistemi centrali di Google, ma ha sfruttato un punto debole nella catena di fornitura. Gli hacker hanno preso di mira gli ambienti Salesforce di diverse aziende, tra cui Google, utilizzando tecniche sofisticate di vishing (phishing vocale) e ingegneria sociale. Fingendosi membri del supporto IT, i criminali hanno indotto i dipendenti a concedere autorizzazioni a un'applicazione malevola, compromettendo cosÃ¬ i dati aziendali. L'indagine di Google Ã¨ condotta dal Google Threat Intelligence Group (GTIG), che collabora a stretto contatto con Salesforce, Salesloft e Mandiant (una societÃ di Google). Stanno tracciando un'attivitÃ criminale sofisticata e in evoluzione.
La finalitÃ di questi attacchi Ã¨ esclusivamente finanziaria. Una volta rubati grandi volumi di dati, che includono informazioni di contatto e credenziali sensibili (come le chiavi di accesso ad AWS e le password), i criminali ricattano le aziende vittime chiedendo il pagamento in Bitcoin entro 72 ore.
L'attacco non ha quindi colpito i dati personali degli utenti consumer di Gmail, ma informazioni relative a clienti e contatti aziendali, come nomi, email e numeri di telefono, gestiti da Google attraverso le sue piattaforme corporate. Il pericolo per i privati risiede nel fatto che le loro informazioni di contatto professionali (come indirizzi email di lavoro o numeri di telefono) potrebbero essere state parte dei dati aziendali rubati. Gli hacker potrebbero utilizzare queste informazioni per lanciare attacchi mirati di phishing o vishing, fingendosi un collega o un partner commerciale. L'obiettivo Ã¨ ingannare la persona per ottenere credenziali sensibili o per indurla a eseguire azioni dannose. In questo senso, i singoli utenti non sono le vittime primarie della violazione, ma possono diventare "vittime a valle", a causa della successiva manipolazione dei dati rubati. Nonostante il panico per i 2,5 miliardi di account Gmail si sia rivelato infondato, la vicenda rimane un importante monito. La minaccia principale non Ã¨ stata una falla nel sistema di Google, ma la capacitÃ degli hacker di sfruttare la fiducia e la disattenzione umana. I criminali hanno usato le informazioni rubate non solo per chiedere riscatti alle aziende, ma anche per lanciare attacchi mirati di phishing e vishing contro i dipendenti e i contatti aziendali, fingendosi operatori Google per rubare credenziali o codici di verifica.

Per proteggersi da attacchi simili, Ã¨ fondamentale adottare misure di sicurezza essenziali: Attivare l'autenticazione a piÃ¹ fattori (MFA): Ã¨ una delle difese piÃ¹ forti. Nonostante gli hacker possano provare a eludere il sistema, l'MFA aggiunge un livello di protezione fondamentale. Utilizzare le Passkey: dove possibile, usare le passkey. Offrono una difesa ancora piÃ¹ robusta e rendono quasi impossibile il furto delle credenziali. Essere vigili contro il phishing e il vishing: non fidarsi mai di chiamate o email inaspettate che chiedono dati personali o codici di accesso, anche se sembrano provenire da fonti autorevoli. Aziende come Google non chiederanno mai le credenziali al telefono. Eseguire il "Controllo sicurezza" di Google: questo strumento permette di verificare lo stato dell' account e ricevere suggerimenti su come rafforzare le protezioni. â??tecnologiawebinfo@adnkronos.com (Web Info)

Categoria

1. Tecnologia

Tag

1. adnkronos
2. Tecnologia

Data di creazione
Settembre 1, 2025
Autore
andreaperocchi_pdnrf3x8