

Facebook scopre 400 app truffa: a rischio i dati di un milione di utenti



I dati di un milione di utenti di Facebook potrebbero essere stati compromessi da 400 app di terze parti scaricabili sul Play Store di Google (355) e nell'App Store di Apple (47). Di che parliamo? Di **malware, categoria spyware, software progettati per carpire le informazioni all'utente**. App "truffaldine" le ha definite Meta, la società madre del social network blu, in un report stilato dai ricercatori della sicurezza di Facebook e che è stato reso noto appena ieri.

App progettate, si spiega, per dirottare le credenziali dell'account Facebook degli utenti, mascherate da servizi "divertenti o utili", come falsi editor di foto (circa il 40%), app per fotocamere, servizi VPN, reti private virtuali che affermavano di aumentare la velocità di navigazione e di ottenere l'accesso a siti Web bloccati, app per oroscopo, strumenti di monitoraggio del fitness. Alcune app promettevano

anche di trasformare la faccia dell'utente in un cartone animato.

Un guaio che ha spinto la società di Palo Alto ha inviare avvisi a 1 milione di persone che potrebbero aver utilizzato le app, in cui si informano gli utenti che le informazioni sull'account potrebbero essere state compromesse da un'app (la società non ha indicato quale), consigliando di reimpostare le password.

Una vicenda questa che ripropone in modo drammatico quanto siano fragili le misure messe a punto dalle pur grandi compagnie a tutela della privacy. Le app truffaldine di cui si parla hanno superato le misure di sicurezza di Apple e Google per essere chiari. Sullo sfondo l'ombra della vicenda Cambridge Analytica, società che ha avuto accesso impropriamente ai dati personali di milioni di utenti di Facebook. Caso per il quale Facebook ha dovuto sborsare 5 miliardi di dollari e che ha cambiato per sempre la società di Zuckerberg.

Meta ha rimosso queste app

Sul caso ieri ha fatto il punto il direttore di Threat Disruption di Meta, David Agranovich. Il manager ha detto che Meta ha condiviso i suoi risultati sia con Apple che con Google: entrambe le società hanno confermato che le app identificate da Meta sono state rimosse dai rispettivi app store. "Tutte le app identificate nel rapporto non sono più disponibili su Google Play", ha detto un portavoce di Google.

"Gli utenti sono anche protetti da Google Play Protect, che blocca queste app su Android". Meta ha trovato app dannose sia nel Play Store di Google che nell'App Store di Apple. Mentre le app Android dannose erano per lo più app di consumo, come i filtri fotografici, le 47 app iOS erano quasi esclusivamente quelle che Meta chiama app di "utilità aziendale".

Questi servizi, con nomi come “Very Business Manager”, “Meta Business”, “FB Analytic” e “Ads Business Knowledge”, sembravano essere mirati specificamente alle persone che utilizzavano gli strumenti aziendali di Facebook. “I criminali informatici sanno quanto siano popolari questo tipi di app e le usano per ingannare le persone e rubare i loro account e informazioni” ha detto Agranovich. “Se un’app promette qualcosa di troppo bello per essere vero, come funzionalità inedite per un’altra piattaforma o sito di social media, è probabile che abbia secondi fini”.

Come funziona il traffico di informazioni via app

Come funzionava il traffico truffaldino di informazioni? Semplice il meccanismo. Le app spesso richiedono agli utenti di “Accedere con Facebook” prima di poter accedere alle funzionalità promesse. Ma queste funzionalità di accesso sono semplicemente un mezzo per rubare le informazioni sull’account degli utenti di Facebook.

Il direttore di Threat Disruption di Meta, David Agranovich, ha notato che molte delle app identificate da Meta erano a malapena funzionanti. “Molte delle app fornivano poche o nessuna funzionalità prima dell’accesso e la maggior parte non forniva alcuna funzionalità anche dopo che una persona ha accettato di accedere” ha sottolineato sempre Agranovich.