APP ANDROID MALEVOLE – UN CASO RECENTE

Quasi tutti abbiamo installato sui nostri dispositivi mobili le app dei principali istituti di credito: consentono di gestire i propri conti correnti, e in generale fare **online banking**.

Vista la grande diffusione delle app per l'accesso ai conti correnti, i criminali informatici stanno quindi utilizzando strategie sempre più articolate ed efficaci per **sottrarre denaro** altrui superando anche le più moderne soluzioni per l'autenticazione a due fattori.

I ricercatori di Threat Fabric, società di sicurezza, a febbraio 2022, avevano lanciato l'allarme dopo l'individuazione di una app (Fast Cleaner) ospitata sul Play Store, presentata come uno strumento utile a risparmiare batteria e ottimizzare il funzionamento del dispositivo mobile e scaricata più di 50.000 volte che provocava l'installazione del malware **Xenomorph**.

Tra le **app italiane** aggredite da Xenomorph citiamo ad esempio quelle di ING, Intesa Sanpaolo, Banca Sella, BCC, BNL, Carige, Banca MPS, Bancaperta, UBI Banca, Unicredit, Scrigno, Banco Posta-Postepay e altre ancora.

Il malware può intercettare le notifiche, registrare gli SMS e utilizzare tecniche per sottrarre le credenziali di autenticazione che consistono nel sovrapporre dei campi per l'inserimento di dati a quelli mostrati nelle app originali.

È essenziale evitare l'installazione di app Android che richiedano permessi troppo ampi o non giustificati sulla base delle funzioni offerte dall'applicazione stessa, e controllare se sia presente la frase “Acquisti in-app”: significa che molte delle funzionalità offerte potrebbero non essere accessibili gratis, ed in questi casi è sempre bene elevare il livello di attenzione.

Si consiglia inoltre di diffidare di quelle applicazioni che propongono il download di componenti aggiuntivi da server di terze parti senza passare per il Play Store.