



Tra i principali tormentoni dell'estate 2016 un posto di primissimo piano spetta certamente a Pokemon Go, il gioco che utilizza la realtà aumentata e che spinge milioni di giovanissimi, giovani e non più giovani a girovagare per le strade, armati di smartphone, a caccia di Pokemon selvatici da catturare.

{loadposition user7}

Ma ogni grande successo nasconde grandi insidie in materia di sicurezza e Pokemon Go non fa eccezione.

Si chiamano infatti Pokemon Go Ultimate, Guide & Cheats for Pokemon Go e Install Pokemongo

le
tre

false app di Google Play appena scoperte dagli esperti di ESET, il più grande produttore di software per

la sicurezza digitale dell'Unione Europea, in grado di bloccare lo schermo dello smartphone per poi connettersi a siti porno o di attivare costosi servizi a pagamento all'insaputa degli utenti.

La prima delle tre app fake, Pokemon Go Ultimate, celandosi come una versione del famoso gioco di successo, è in grado di bloccare immediatamente lo schermo dello smartphone dopo il suo avvio. Dopo un riavvio forzato, possibile solo togliendo la batteria dallo smartphone o modificando le impostazioni dei dispositivi Android, il malware si esegue in background, quindi in modalità invisibile alla vittima, cliccando in maniera nascosta su pubblicità porno. Per eliminare questa minaccia l'utente deve andare su Impostazioni -> Gestione applicazioni -> PI Network e disinstallarla manualmente.

Le altre due applicazioni fake individuate dagli esperti di ESET su Google Play, Guide & Cheats for Pokemon Go e Install Pokemongo, appartengono alla famiglia degli scareware ed inducono le vittime a pagare per falsi servizi estremamente costosi, promettendo di generare Pokecoin, Pokeball o Lucky Egg.

Le app fake non sono rimaste a lungo su Google Play e sono state immediatamente rimosse dallo store dopo la segnalazione di ESET.

Pokémon GO è un gioco così accattivante che, nonostante tutti gli avvertimenti degli esperti di sicurezza, gli utenti tendono ad accettare i rischi e a scaricare qualsiasi cosa pur di catturare tutti i Pokémon. Coloro che davvero non possono resistere alla tentazione dovrebbero almeno seguire le regole base di sicurezza:

- scaricare le applicazioni solo da fonti attendibili
- verificare le recensioni degli altri utenti, concentrandosi sui commenti negativi e tenendo ben a mente che quelli positivi potrebbero essere stati inseriti appositamente
- leggere le condizioni e i termini d'uso delle app, focalizzandosi sui permessi richiesti
- utilizzare una soluzione di sicurezza mobile in grado di controllare tutte le app del dispositivo

Per ulteriori informazioni sull'argomento è possibile visitare la pagina del blog di ESET Welivesecurity al seguente link:

<http://www.welivesecurity.com/2016/07/15/pokemon-go-hype-first-lockscreen-tries-catch-trend/>

{jcomments on}

{loadposition user6}