Ancora xHelper: il trojan per Android è immortale

Apr 08, 2020 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

Il malware è in circolazione dall'anno scorso e non sembra rallentare. Gli esperti: "gli utenti continuano a installare app da siti non affidabili".

La proliferazione di app malevole per Android non è una notizia e la continua comparsa di nuovi malware è qualcosa a cui ormai ci siamo abituati. Ne esiste, però, una categoria particolare: quelli che sembrano non avere nessuna intenzione di sparire anche dopo l'individuazione da parte delle società di sicurezza e l'estromissione dai market ufficiali.

Il caso di **xHelper**, illustrato dai ricercatori di **Kaspersky** in un post sul blog della società di sicurezza, è emblematico. Il trojan per Android, infatti, è in circolazione da quasi un anno.

La tecnica di distribuzione utilizzata dai pirati informatici è estremamente semplice: il malware è infatti proposto come un'app per la manutenzione del sistema e l'ottimizzazione delle prestazioni.

In realtà, tra le pieghe del codice si nascondono una serie di comandi che avviano il download e l'installazione di una serie di applicazioni malevole, compreso il trojan **Triada**.

SI tratta di una strategia che i ricercatori definiscono “a matriosca” e che sfrutta un trucchetto molto particolare: la cartella che contiene gli eseguibili viene collegata al file *install-recovery.sh* assegnando loro l’attributo “immutabile”. **In pratica, I file non possono essere cancellati attraverso le ordinarie procedure e, in alcuni casi, nemmeno con un reset alle condizioni di fabbrica**.

Molti esemplari di xHelper risultano infatti essere stati scaricati da malware preinstallati nei firmware dei telefoni, soprattutto di modelli a basso costo.

A parte questi casi limite come quelli citati, la persistenza di xHelper sembra però essere dovuta all’abitudine da parte degli utenti di ostinarsi a installare applicazioni “gratuite” offerte sulle pagine di siti di dubbia affidabilità.

Insomma, secondo i ricercatori Kaspersky siamo di fronte al solito meccanismo per cui il tentativo di risparmiare qualche euro (vista la diffusione geografica di xHelper sarebbe forse meglio parlare di rubli) si trasforma in un disastro.

Condividi l’articolo

Attacco a Email.it: 600.000 account in vendita sul Dark Web

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/04/08/ancora-xhelper-il-trojan-per-android-e-immortale/?utm_source=rss&utm_medium=rss&utm_campaign=ancora-xhelper-il-trojan-per-android-e-immortale