Spionaggio di stato: i gruppi APT usano un malware per Android

Feb 12, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Gli obiettivi comprendono organizzazioni attiva nel settore militare, della produzione di energia nucleare e della gestione dei sistemi elettorali.

Smartphone nel mirino: anche i gruppi APT (Advanced Persistent Threat) non disdegnano i dispositivi mobile per portare i loro attacchi. Anzi: stando a quanto riportano i ricercatori di **Kaspersky**, gli hacker di stato starebbero utilizzando nuovi malware per **Android** allo scopo di sottrarre informazioni sensibili dai loro bersagli.

Gli attacchi avrebbero presa di mira sia il governo pakistano, sia quello indiano. Nel dettaglio, i pirati informatici avrebbero colpito in **Pakistan** bersagli tra l'esercito e le organizzazioni che si occupano di produzione di energia (e armamenti) nucleari, mentre in **India** i pirati avrebbero attaccato gli enti che gestiscono le elezioni nella regione del **Kashmir**.

I malware utilizzati, che i ricercatori hanno battezzato con i nomi di **Hornbill** e **SunBird**, sarebbero stati diffusi attraverso applicazioni per Android infette, che nel caso di Hornbill sono state pubblicate su store di terze parti, mentre per quanto riguarda SunBird sono state caricate direttamente su **Google Play**.

Il codice malevolo contenuto nelle app per Android avrebbe consentito ai pirati informatici di rubare informazioni sensibili dai dispositivi mobili delle vittime, compresi SMS; messaggi Whatsapp e dati sulla geolocalizzazione.

Insomma: tutto il necessario per sorvegliare a distanza le vittime e ottenere, in virtù dei rispettivi ambiti di attività, informazioni estremamente riservate.

Il malware più pericoloso, secondo i ricercatori, sarebbe SunBird, che rispetto al "collega" Hornbill utilizzerebbe strumenti più sofisticati e un sistema di comunicazione più efficiente con i server Command and Control utilizzati dai pirati.

L'attacco, spiegano gli esperti che hanno analizzato i malware, sarebbe opera di un soggetto (non identificato) che agirebbe con l'obiettivo di favorire il governo indiano nel confronto a livello geopolitico con il vicino Pakistan.

Condividi l'articolo

Boom di vendite online di accessi (hackerati) alle reti

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2021/02/12/spionaggio-di-stato-i-gruppi-apt-usano-un-malware-per-android/?utm_source=rss&utm_medium=rss&utm_campaign=spionaggio-di-stato-i-gruppi-apt-usano-un-malware-per-android