Google identifica uno spyware “italiano” che prende di mira Android e iOS

https://www.mobileworld.it/wp-content/uploads/2021/01/spia-spy-sorveglianza-privacy-sicurezza-800×533.jpg,

Nel panorama attuale degli smartphone, che siano Android o iOS, si stanno producendo grandi sforzi nei confronti della salvaguardia della **privacy** e della **sicurezza** degli utenti. In questo contesto, il team *Threat Analysis Group* di Google ha scovato uno **spyware** che riguarda da vicino **l’Italia**.

Il nome identificativo dello spyware è **Hermit** e sarebbe stato sviluppato da ***RCS Lab***, un’azienda italiana che fornisce servizi alle forze dell’ordine nazionali e internazionali. Secondo quanto scovato dal team di Google, tale spyware è stato **attivo in Italia** e in Kazakistan, rubando dati personali a utenti senza il loro consenso.

Hermit è in grado di agire con la collaborazione di **fornitori di servizi di rete** locali, i quali avrebbero il ruolo di interrompere la connettività da e verso lo smartphone della vittima. Successivamente Hermit invia un messaggio contenente

un link, con lo scopo di **indurre l'utente** a installare **un'app** per ripristinare i servizi di connettività. Tale app in realtà contiene dei pacchetti per rendere **operativo lo spyware**.

In altri casi, Hermit si è servito di schermate relative ai **social network**, create ad arte per indurre l'utente a credere che l'accesso ai social risultava bloccata e che il ripristino sarebbe possibile **installando una specifica app**.

Agendo tramite un **sideload** dunque, ovvero senza la necessità di ospitare l'app dello spyware sul Play Store dove sarebbe stata più **facilmente riconoscibile** dagli strumenti di sicurezza di Google, i malintenzionati dietro Hermit riuscivano a entrare in possesso di informazioni personali dagli utenti tramite i loro smartphone.

Una volta operativo nel dispositivo, Hermit è in grado di **registrare telefonate**, leggere le **notifiche** e i testi annessi e accedere allo **storage interno** del dispositivo. Lo spyware sarebbe in grado di agire tanto su Android quanto su iOS.

Google ha menzionato esplicitamente RCS Lab come coloro che sarebbero dietro allo spyware. Questo sui dispsositivi Android sarebbe anche stato in grado di **camuffarsi da app ufficiale Samsung**.

Dopo la scoperta, Google ha riferito di aver **ulteriormente migliorato** i suoi strumenti di sicurezza integrati su Android, come Play Protect. Pertanto, possiamo aspettarci che, almeno i dispositivi Android siano meno vulnerabili a Hermit. D'altro canto, è interessante, e per certi versi **preoccupante**, notare come in questo caso lo spyware è stato concepito **non per sfruttare una vulnerabilità** software ma per **aggirare** gli attuali sistemi di sicurezza integrati, i quali si sono rivelati insufficienti.

Read More