Un report forense suggerisce che il caso Paragon sia più grave del previsto

A fine gennaio, è emerso che giornalisti e attivisti italiani sono stati intercettati illecitamente con uno **spyware noto come Graphite**, prodotto dall'azienda di natali israeliani **Paragon**. Il Governo italiano, cliente dell'impresa in questione, non ha ancora comunicato al pubblico gli esiti della sua indagine interna. Chi ha espresso un'opinione è invece il **The Citizen Lab**, gruppo dell'Università di Toronto che ha analizzato la situazione dal lato tecnico. Secondo il suo primo report, la situazione potrebbe essere **più grave di quanto fino a oggi noto**.

Il rapporto, pubblicato il 19 marzo, si è focalizzato sul verificare due scenari: quello canadese, vicino alla realtà dell'accademia, e quello **italiano**, contesto che è stato malauguratamente in grado di fornire numerosi elementi di ricerca. Gli accademici hanno riscontrato un possibile legame tra Graphite e le Forze di polizia dell'Ontario, tuttavia gli elementi più interessanti emergono proprio dallo scenario nostrano.

Grazie all'intervento di Meta, sappiamo da tempo che almeno **sette italiani sono stati monitorati** su WhatsApp attraverso il software di spionaggio. Tra questi Francesco Cancellato, direttore del giornale *Fanpage*, Luca Casarini, fondatore di Ong Mediterranea, Giuseppe Caccia e don Mattia Ferrari, rispettivamente co-fondatore e cappellano di bordo di Mediterranea Saving Humans. Indiscrezioni intercettate da *The Guardian* e discussioni politiche hanno dunque rivelato che **Roma ha contratti in essere con Paragon** e che questi siano stati sospesi dopo l'esplosione dello scandalo.

L'indagine forense di The Citizen Lab, effettuata in collaborazione con Meta, aggiunge ulteriori tasselli. Gli apparecchi **Android** infetti analizzati hanno rivelato la **presenza di un artefatto** che è stato battezzato per l'occasione BIGPRETZEL, il quale si ritiene sia connesso all'azienda israeliana. Partendo dalla traccia digitale, è emerso dunque che lo spyware non si sia limitato a infettare Whatsapp: lo smartphone di Caccia evidenzia per esempio almeno altre due app infette, tra cui una non meglio definita "popolare app di messaggistica".

Il gruppo canadese ha quindi scandagliato l'**iPhone** di David Yambio, rifugiato libico e fondatore di Refugees in Libya, il quale non figura tra i famosi sette identificati da Meta, ma ha comunque ricevuto una notifica omologa da parte di Apple. Il telefono ha evidenziato delle attività anomale il 13 giugno 2024, fenomeni che l'azienda produttrice dell'apparecchio non esita a identificare come **"attacchi spyware molto sofisticati"**. La falla che ha consentito il monitoraggio di Yambio pare sia stata colmata con l'aggiornamento a iOS 18, tuttavia è probabile che i dati dell'attivista siano stati compromessi.

The Citizen Labs **sospetta che l'Italia sia un *cluster*** di fenomeni di spionaggio, un polo di sorveglianza che viene motivato dal posizionamento strategico nel Mediterraneo e dal ruolo

che le ONG manifestano nei confronti dell'accoglienza e dell'**assistenza a migranti e rifugiati**. La verifica effettuata dai ricercatori si limita agli avvenimenti più recenti, tuttavia si sospetta che la presenza di spyware sia antecedente al caso Paragon, che possa aver coinvolto altre imprese di spionaggio.

I ricercatori hanno inoltrato i loro risultati a Paragon stessa, la quale ritiene che contengano **"diverse imprecisioni"**, sostenendo però di non poter commentare più approfonditamente in assenza di dettagli tecnici più precisi. The Citizen Labs nota inoltre che l'azienda israeliana custodisca un "registro dettagliato" delle attività dello spyware Graphite e suggerisce alle autorità italiane di richiederne accesso, così da verificarne gli eventuali impieghi illeciti. "Anche se gli spyware mercenari sono stati acquistati con uno scopo primario, come per esempio investigare gruppi criminali, l'esperienza ci rivela che, con il tempo, la tentazione di usare queste potenti tecnologie per scopi politici è considerevole", conclude amaramente il report.

[di Walter Ferri]