WhatsApp: azienda israeliana ‘pesantemente coinvolta’ nello spionaggio dei nostri utenti

Stephanie Kirchgaessner da **Washington**

29 aprile 2020 – The Guardian

La NSO Group accusata di aver hackerato 1400 persone, inclusi attivisti per i diritti umani

Nuove deposizioni processuali presentate da WhatsApp rivelerebbero che una azienda israeliana specializzata in spyware usava server con sede negli USA e che era “pesantemente coinvolta” nell’hackeraggio di telefonini di 1.400 utenti di WhatsApp, inclusi funzionari governativi di alto livello, giornalisti e attivisti per i diritti umani.

Le nuove affermazioni sul NSO Group sostengono che l’azienda israeliana sarebbe responsabile di serie violazioni dei diritti umani, incluso l’hackeraggio di oltre una decina di giornalisti indiani e dissidenti del Rwanda.

Per anni, NSO Group ha detto che il suo software di sorveglianza è acquistato dai governi per rintracciare terroristi e altri criminali e di non avere a disposizione informazioni indipendenti riguardo a come tali clienti, che in passato avrebbero incluso l’Arabia Saudita e il Messico, usino il suo software.

Ma la causa intentata l’anno scorso da Whatsupp contro NSO, la prima nel suo genere intentata da una grande azienda tecnologica, sta rivelando altri dettagli su come lo spyware Pegasus verrebbe utilizzato contro obiettivi precisi.

La scorsa settimana WhatsApp ha rivelato come le proprie indagini su come Pegasus sia stato usato l’anno scorso contro 1.400 utenti mostrerebbero che i server controllati da NSO Group, non i governi suoi clienti, erano parte integrante di come si effettuavano gli hackeraggi.

WhatsApp ha detto che le vittime ricevevano telefonate tramite l’app di

messaggistica ed erano infettatate da Pegasus. Ha poi aggiunto: “NSO usava una rete di computer per monitorare e aggiornare Pegasus dopo che era stato impiantato sui dispositivi degli utenti. Tali computer erano controllati da NSO e servivano come centro nevralgico attraverso cui controllava le operazioni dei propri clienti e l’uso di Pegasus.”

Secondo l’accusa di WhatsApp, NSO otteneva un “accesso non autorizzato” ai suoi server tramite il processo di reverse engineering dell’app di messaggistica e poi eludeva le funzioni di sicurezza che impediscono la manomissione delle funzioni di chiamata della compagnia. Un tecnico di WhatsApp che aveva indagato sugli hackeraggi ha dichiarato in una deposizione giurata presentata al tribunale che in 720 casi l’indirizzo IP di un server in remoto era stato incluso nel codice malevolo usato negli attacchi. Secondo il tecnico, il server remoto con sede a Los Angeles era di proprietà di una azienda il cui data centre era usato da NSO.

NSO ha sostenuto nella sua deposizione di non avere informazioni su come i governi suoi clienti usino i suoi strumenti di hackeraggio e perciò non può sapere chi siano i loro bersagli.

Ma John Scott-Railton, un esperto che lavora per Citizen Lab [centro canadese che si occupa della difesa dei diritti dei cittadini contro l’uso improprio delle informazioni, ndtr.] e ha collaborato al caso con WhatsApp, ha detto che il controllo dei server coinvolti da parte di NSO suggerisce che l’azienda avrebbe avuto i log, inclusi gli indirizzi IP [etichetta numerica dei dispositivi informatici, ndtr.] che identificavano gli utenti oggetto della sorveglianza.

“Chi può sapere se NSO guarda quei log? Ma il semplice fatto che potrebbe avvenire smentisce quello che dicono,” fa notare Scott-Railton.

In una dichiarazione al *Guardian* NSO conferma quelle che aveva fatto in precedenza. “I nostri prodotti sono utilizzati per porre fine al terrorismo, limitare il crimine violento e salvare vite. NSO Group non gestisce il software Pegasus per i propri clienti,” afferma l’azienda. “Le nostre affermazioni precedenti sulle nostre attività, e la portata delle nostre interazioni con la nostra intelligence governativa e i clienti appartenenti alle forze dell’ordine sono corrette.”

L’azienda ha detto che avrebbe presentato la propria replica al tribunale nei prossimi giorni.

I nuovi sviluppi del caso arrivano nello stesso momento in cui NSO deve rispondere a domande, in sede separata, sull'accuratezza di un prodotto di tracciamento lanciato in seguito all'insorgere del Covid-19. Si chiama Fleming e usa i dati dei telefonini e le informazioni sulla salute pubblica per identificare con quali individui infettati si è venuti in contatto. Lo scorso finesettimana, un reportage dell'emittente NBC [rete televisiva US, ndtr.] ha affermato che la nuova app di tracciamento di NSO era commercializzata negli USA.

Ma in un thread su Twitter Scott-Railton ha sostenuto che la sua analisi rivelava che essa si basa su dati che sembrano molto imprecisi.

"Quando stai lavorando con dati che incorporano tante imprecisioni, sarebbe molto laborioso lanciare un allarme ogni volta che ciò accade. O chiedere la quarantena. O un test. La percentuale di falsi positivi esploderebbe. Ma … anche quella dei falsi negativi," ha aggiunto.

Interrogato sui tweet, NSO ha detto che le "accuse infondate" erano basate su "supposizioni e schermate non aggiornate e non su fatti".

"Fleming, il nostro prodotto contro il Covid-19, si è nel frattempo rivelato fondamentale per governi in tutto il mondo, contribuendo a contenere la pandemia. Stimati giornalisti di vari Paesi l'hanno esaminato, hanno capito come funziona la tecnologia e hanno riconosciuto che si tratta della più recente evoluzione dei software di analisi e che non mette in pericolo la privacy," ha concluso l'azienda.

(traduzione dall'inglese di Mirella Alessio)