

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 Whatsapp 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 infettate 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, ndr.] 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, ndr.] 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, ndr.] 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)

Il processo contro il software di sorveglianza israeliano si svolge a

porte chiuse

Pegasus è collegato allo spionaggio politico in Messico, Emirati Arabi e Arabia Saudita: Citizen Lab dell'università di Toronto.

16 gennaio 2020 - Al Jazeera

Giovedì un tribunale israeliano ha disposto le udienze a porte chiuse del processo intentato da Amnesty International per bloccare le esportazioni del gruppo NSO [dalle iniziali dei fondatori dell'azienda: Niv, Shalev e Omri, è una società tecnologica israeliana, ndr.] di software di spionaggio, che le associazioni per i diritti affermano vengano usati per spiare giornalisti e dissidenti in tutto il mondo.

Una giudice della Corte Distrettuale di Tel Aviv ha citato preoccupazioni relative alla sicurezza nazionale quando ha escluso il pubblico e i media dalle udienze. L'iniziativa ha comportato un'immediata condanna da parte dell'associazione di attivisti.

“È vergognoso che veniamo costretti al silenzio”, ha detto ai giornalisti Gil Naveh, un portavoce di Amnesty.

Il Ministero della Difesa di Israele - che ha richiesto il divieto della Corte - e NSO hanno rifiutato di commentare la causa intentata da Amnesty. La causa potrebbe stabilire se il governo debba inasprire i controlli sulle esportazioni di strumenti informatici - un settore in cui Israele è leader mondiale.

Amnesty afferma che i governi hanno usato il software di hackeraggio dei cellulari della società israeliana per reprimere gli attivisti in tutto il mondo. Uno studio di Citizen Lab [Laboratorio dei Cittadini, associazione che difende i cittadini dallo spionaggio illecito dei governi, ndr.] dell'università di Toronto ha collegato Pegasus allo spionaggio politico in Messico, Emirati Arabi e Arabia Saudita.

NSO ha affermato di vendere la propria tecnologia solo ad enti statali e alle forze dell'ordine per “aiutarle nella lotta al terrorismo e alla criminalità organizzata.”

La giudice Rachel Barkai inizialmente aveva detto che avrebbe permesso che le argomentazioni di Amnesty fossero ascoltate dal pubblico, ma gli avvocati del governo hanno sostenuto che sarebbe parso che lo Stato stesse accettando le accuse di Amnesty e Barkai ha cambiato idea.

NSO è finita sotto esame quando un dissidente saudita legato al giornalista assassinato Jamal Khashoggi ha intentato causa sostenendo che NSO aveva aiutato la corte reale ad entrare nel suo cellulare e a spiare le sue comunicazioni con Khashoggi.

NSO ha negato che la sua tecnologia sia stata utilizzata nell'omicidio di Khashoggi.

In ottobre WhatsApp, che è di proprietà di Facebook Inc., ha fatto causa a NSO presso la corte federale degli Stati Uniti a San Francisco. WhatsApp ha accusato NSO di aiutare le spie governative ad entrare nei telefoni di circa 1.400 utenti in quattro continenti.

Nella causa di Amnesty, intentata da membri e sostenitori del suo ufficio di Israele, l'organizzazione ha affermato che NSO continua a trarre profitti dal suo programma spia che viene usato per commettere violazioni contro attivisti in tutto il mondo e che il governo israeliano "è rimasto a guardare senza fare niente."

"Il modo migliore per impedire che i potenti prodotti di spionaggio di NSO arrivino ai governi repressivi è revocare la licenza di esportazione della società, e questo è esattamente ciò che questa causa legale intende fare", ha detto Danna Ingleton, vicedirettrice di Amnesty Tech.

Amnesty Tech è descritta sul sito web di Amnesty International come una collettività globale di avvocati, esperti di informatica, ricercatori e tecnologie che sfidano "la sistematica minaccia ai nostri diritti" da parte delle imprese di spionaggio.

NSO, che l'anno scorso è stata acquisita dalla società privata Novalpina Capital con sede a Londra, a settembre ha annunciato che avrebbe iniziato ad attenersi alle linee guida dell'ONU sulle violazioni dei diritti umani.

FONTE: Agenzia di informazioni Reuters

(Traduzione dall'inglese di Cristiana Cavagna)