Un sistema di spionaggio del gruppo NSO sarebbe stato utilizzato in attacchi informatici contro avvocati e giornalisti

Nick Hopkins *e* **Stephanie Kirchgaessner**

Martedì 29 ottobre 2019 – The Guardian

WhatsApp denuncia un'impresa israeliana accusandola di aver violato i telefoni di attivisti

WhatsApp ha iniziato un'azione legale senza precedenti contro un'impresa di armi informatiche accusata di essere dietro attacchi segreti contro più di 100 attivisti per i diritti umani, avvocati, giornalisti e docenti universitari in sole due settimane all'inizio dell'anno.

L'impresa di social media ha presentato una denuncia contro NSO Group, una compagnia israeliana della sorveglianza, affermando che essa è responsabile di una serie di attacchi informatici molto complessi che a suo parere hanno violato le leggi americane con una "inconfondibile modalità di uso illecito".

WhatsApp afferma di ritenere che durante il periodo di due settimane tra la fine di aprile e metà maggio questa tecnologia venduta da NSO sia stata usata per prendere di mira i telefonini di oltre 1.400 suoi utenti in 20 diversi Paesi.

WhatsApp pensa che in questo breve periodo tra quanti sono stati sottoposti agli attacchi informatici ci siano importanti difensori ed avvocati per i diritti umani, illustri personalità religiose, famosi giornalisti e funzionari di organizzazioni umanitarie.

Secondo quanto ritiene la compagnia, sono state vittime di attacchi anche un certo numero di donne precedentemente prese di mira dalla violenza informatica e personalità che hanno subito tentativi di assassinio e minacce di violenza, così come i loro parenti.

La denuncia di WhatsApp, presentata martedì a un tribunale californiano, chiede un'ingiunzione permanente che vieti a NSO di tentare di accedere ai sistemi su computer WhatsApp e Facebook, ad esso legato.

Ha anche chiesto al tribunale di sentenziare che NSO ha violato le leggi federali USA e della California contro frodi informatiche, ha violato i suoi contratti con WhatsApp ed ha "indebitamente abusato" di proprietà di Facebook.

"Questa è la prima volta che un fornitore di messaggistica criptata ha preso un'iniziativa legale contro un ente privato che ha perpetrato questo tipo di attacchi contro i suoi utenti," ha affermato un portavoce di WhatsApp. "Nella nostra denuncia spieghiamo come NSO abbia messo in atto il suo attacco, compresa l'ammissione di un dipendente di NSO che le nostre iniziative per porre rimedio all'attacco sono state efficaci."

La compagnia sta anche appoggiando richieste del relatore speciale ONU per il diritto di espressione, David Kaye, per una moratoria di questo tipo di programmi di spionaggio invasivo.

"Ci deve essere un deciso controllo giudiziario su armi informatiche come quella usata in questo attacco, per garantire che non vengano usate per violare i diritti individuali e le libertà a cui le persone hanno diritto ovunque nel mondo," ha affermato WhatsApp.

"Gruppi per i diritti umani hanno documentato una preoccupante tendenza in base alla quale tali strumenti sono stati usati per attaccare giornalisti e difensori dei diritti umani."

WhatsApp ha sostenuto di aver lavorato con "Citizen Lab", un gruppo di ricerca universitario con sede presso la Munk School di Toronto, per identificare le vittime degli attacchi e la tecnologia utilizzata contro di loro. L'organizzazione ha iniziato a contattare membri della società civile che siano stati colpiti dai presunti hacker.

John Scott-Railton, un ricercatore esperto di "Citizen Lab", ha detto che l'azione legale di WhatsApp è stata "un importante passo positivo per la protezione dei diritti umani in rete e rappresenterà sicuramente un precedente." Egli ha accusato NSO di agire con spregio nei confronti delle persone prese di mira. "Mentre dice all'opinione pubblica di essere preoccupata dei diritti umani, la

società privata di sistemi di spionaggio ha cercato di ritagliarsi una nicchia di impunità, per cui, in virtù della sua vicinanza ad alcuni governi, sostiene di agire in modo legale, ma quando le fa comodo preferisce disconoscere qualunque responsabilità per questo comportamento.

L'annuncio di WhatsApp giunge sei mesi dopo che ha comunicato di aver scoperto un punto debole che ha consentito ad aggressori informatici di installare programmi di spionaggio sui telefoni con il programma sia iPhone che Android, chiamando destinatari che usano la funzionalità telefonica dell'applicazione. In quel momento non era ancora chiaro come molti degli 1,5 miliardi di utenti di WhatsApp siano stati colpiti.

Da allora WhatsApp, in collaborazione con "Citizen Lab", nei giorni prima che la vulnerabilità venisse bloccata, ha cercato di capire come siano stati lanciati molti attacchi. Si ritiene che l'azienda sia rimasta scioccata da quello che ha scoperto.

Nella sua azione legale ha accusato NSO di "accesso e uso illegali dei computer di WhatsApp, molti dei quali si trovano in California."

Sostiene anche che NSO "ha preso una serie di iniziative, utilizzando senza autorizzazione server di WhatsApp e il suo servizio, per spedire singoli componenti del programma ostile ('codice dannoso') per prendere di mira dispositivi elettronici" – e che ciò è stato fatto in modo da "occultare l'identità e il coinvolgimento degli accusati."

La denuncia di WhatsApp non è l'unica rivolta contro NSO. L'impresa è stata accusata di aver preso di mira Omar Abdulaziz, uno stretto collaboratore di Jamal Khashoggi prima che il giornalista del Washington Post venisse assassinato l'anno scorso nel consolato saudita di Istanbul.

NSO ha affermato di prendere in esame le accuse nei confronti dei propri clienti e di riservarsi il diritto di ritirare agli utenti i permessi di utilizzo.

All'inizio di quest'anno l'azienda è stata acquistata da un'impresa privata con sede a Londra denominata "Novalpina Capital", che in giugno ha affermato che avrebbe svelato nuove regole di governo dell'azienda. Nel passato NSO ha tenacemente difeso l'utilizzo della sua tecnologia e del sistema informatico di sorveglianza, noto come "Pegasus", in quanto strumento di messa in pratica della legge che potrebbe contribuire a prevenire attacchi criminali e terroristici.

“Novalpina” ha attribuito alla tecnologia di NSO il merito di aver bloccato piani di un attacco terroristico in uno stadio affollato in Europa e, citando il governo messicano, ha affermato che nel 2011 ha contribuito all’arresto del boss della droga noto come “El Chapo”.

In novembre l’impresa israeliana ha reso nota una “nuova politica per i diritti umani”, che a suo dire è fondata su un “rispetto incondizionato per i diritti umani”. Tra le altre iniziative, si è impegnata a inserire nuove procedure corrette di controllo per identificare, prevenire e mitigare “effetti contrari ai diritti umani” a causa del possibile abuso della sua tecnologia.

Ha anche affermato che avrebbe condotto una valutazione del “potenziale di effetti contrari ai diritti umani” dovuti ad un uso scorretto dei prodotti di NSO, così come avrebbe imposto “obblighi contrattuali” che impedirebbero ai clienti di NSO di utilizzare i suoi prodotti per qualcosa di diverso da un’inchiesta su gravi delitti.

Ma la nuova politica è stata criticata da alcuni esperti dei diritti umani e della sorveglianza informatica, compreso Kaye dell’ONU.

In una lettera del 18 ottobre a Shalev Hulio, uno dei fondatori di NSO, Kaye ha sollevato dubbi sull’efficacia di queste nuove linee guida sui i diritti umani e delle procedure basate sulla necessaria attenzione, ed ha suggerito che [NSO] sembrava affidarsi totalmente ai suoi stessi clienti per l’autocertificazione sull’uso scorretto dei suoi prodotti.

NSO Group ha affermato: “Contestiamo con la massima fermezza le attuali accuse e ci opporremo fortemente ad esse. L’unico scopo di NSO è fornire una tecnologia ad agenzie di intelligence e forze dell’ordine governative per aiutarle a combattere il terrorismo e la grande criminalità. La nostra tecnologia non è destinata o autorizzata ad essere usata contro gli attivisti per i diritti umani e i giornalisti. Negli ultimi anni ha contribuito a salvare migliaia di vite.

“La verità è che piattaforme fortemente criptate sono spesso utilizzate da circoli di pedofili, boss della droga e terroristi per proteggere le proprie attività criminali. Senza tecnologie sofisticate, gli organi di polizia che devono garantire la nostra sicurezza devono affrontare ostacoli insormontabili. Le tecnologie di NSO forniscono soluzioni adeguate e legali a questo problema.

“Noi consideriamo ogni uso dei nostri prodotti diverso dalla prevenzione della grande criminalità e del terrorismo una misura vietata dai termini contrattuali. Se lo individuiamo, interveniamo. Questa tecnologia è radicata nella protezione dei diritti umani – compresi il diritto alla vita, alla sicurezza ed all’integrità fisica – ed è per questo che abbiamo cercato di adeguarci ai principi delle linee guida dell’ONU su attività economiche e diritti umani, per garantire che i nostri prodotti rispettino *tutti* i diritti umani fondamentali.”

Se siete stati colpiti da presunto hackeraggio di WhatsApp o avete informazioni su di esso contattate *Nick.Hopkins@theguardian.com oppure Stephanie.Kirchgaessner@theguardian.com*

(traduzione dall’inglese di Amedeo Rossi)