Apple contro NSO, e le sue ricadute sull’industria della sorveglianza

Attorneys for Plaintiff Apple Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

APPLE INC.,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED, and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No.

COMPLAINT

DEMAND FOR JURY TRIAL

Apple ha fatto causa a NSO Group, l’azienda israeliana produttrice dello spyware Pegasus al centro di una serie di inchieste giornalistiche che hanno denunciato come questo strumento (ufficialmente venduto ai governi per indagare criminalità e terrorismo) fosse usato anche per spiare gli smartphone di giornalisti, funzionari governativi e attivisti. L’azione legale ritiene l’azienda israeliana responsabile di aver attaccato e sorvegliato utenti Apple e si aggiunge a quella intentata da Facebook nel 2019 dopo che lo spyware Pegasus era stato usato contro utenti Whatsapp. E, per prevenire ulteriori abusi, la società di Cupertino cerca anche un’ingiunzione permanente per impedire a NSO Group di utilizzare qualsiasi software, servizio o device Apple in futuro.

Il gancio degli ID Apple e i termini di servizio

La denuncia rivela anche nuovi dettagli su come l'azienda di spyware infetti i device delle vittime. Sappiamo infatti che NSO Group ha utilizzato un exploit, dei codici di attacco che sfruttano una vulnerabilità, noto come FORCEDENTRY, per violare i device Apple delle vittime e installare il software spia. La vulnerabilità è stata chiusa da Apple. Che però ora dice qualcosa in più: per usare l'exploit sugli apparecchi della Mela morsicata, "gli attaccanti hanno creato degli ID Apple per inviare dati malevoli ai dispositivi delle vittime, permettendo a NSO Group o i suoi clienti di inviare e installare Pegasus all'insaputa della vittima. Sebbene abusati per inviare FORCEDENTRY, i server Apple non sono stati hackerati o compromessi", ci tiene a specificare l'azienda californiana (qui il suo comunicato). Su questa parte ci torniamo più sotto.

Secondo la denuncia, gli ingegneri di NSO hanno creato oltre 100 Apple ID per eseguire gli attacchi. Nel creare questi account hanno però dovuto sottoscrivere i termini di servizio e le condizioni di iCloud, che pongono la relazione degli utenti con Apple sotto il cappello delle leggi della California. È proprio questo aspetto, scrive il New York Times, che avrebbe permesso all'azienda di iPhone di fare causa a NSO nel distretto settentrionale della California. "È stata una palese violazione dei nostri termini di servizio e della privacy dei nostri clienti", ha dichiarato Heather Grenier, direttrice senior dei contenziosi commerciali di Apple.

La denuncia di Apple in dettaglio

Guerre di Rete ha letto la denuncia. Notevole come esordisce. "Gli accusati sono famigerati hacker – amorali cyber mercenari del 21esimo secolo che hanno creato un sofisticato apparato di

cyber sorveglianza che invita a palesi e continui abusi. Progettano, sviluppano, vendono, distribuiscono, operano, e mantengono un malware offensivo e distruttivo e prodotti e servizi spyware che sono stati usati per prendere di mira, attaccare e danneggiare utenti Apple, prodotti Apple e Apple. Per il loro guadagno commerciale, mettono i clienti nelle condizioni di poter abusare dei loro prodotti e servizi per colpire singoli individui, inclusi funzionari governativi, giornalisti, imprenditori, attivisti, accademici e anche cittadini americani."

La denuncia prosegue spiegando come Apple abbia investito e puntato su privacy e sicurezza per i propri servizi e utenti. Si toglie anche qualche sassolino dalle scarpe, dicendo che i suoi prodotti sarebbero ancora più sicuri della concorrenza, citando uno studio secondo il quale il 98 per cento dei malware per apparecchi mobile colpirebbero dispositivi Android.

> *"NSO è l'antitesi di quello che Apple rappresenta in termini di sicurezza e privacy",*
>
> *scrivono gli avvocati della Mela morsicata.*

La denuncia ricorda un dato importante: questo genere di malware sofisticati interessano ancora un numero limitato di persone (persone che sono indagate nell'ambito di un'inchiesta della magistratura, e questo sarebbe l'uso legittimo e ufficiale, ma anche persone che sono nel mirino di governi per ragioni politiche).
La denuncia prosegue ricordando alcuni dei maggiori casi di cronaca che hanno riguardato l'uso e abuso di Pegasus: dal Pegasus Project, le inchieste coordinate dal consorzio giornalistico Forbidden Stories con altre 17 testate insieme al supporto tecnico del Security Lab di Amnesty International, fino al recente caso del ritrovamento dello spyware sui dispositivi di sei attivisti palestinesi (di cui ho scritto

due settimane fa, facendo notare come uno di questi avesse cittadinanza americana, un dato che viene sottolineato anche da Apple).

Infine si addentra nell'attacco che ha utilizzato il già citato exploit FORCEDENTRY. Cerco di mantenere la traduzione fedele, quindi il linguaggio risente del gergo legale. "Gli accusati hanno eseguito l'exploit prima usando i loro computer per contattare i server Apple negli Stati Uniti e all'estero in modo da identificare altri apparecchi Apple. Gli accusati hanno contattato i server Apple usando i loro ID Apple per confermare che il target stesse usando un device Apple. Poi avrebbero inviato dati malevoli creati dagli accusati per questo attacco attraverso i server Apple negli Usa e altrove. I dati malevoli sono stati inviati al telefono della vittima attraverso il servizio iMessage di Apple, disabilitando il logging sul device preso di mira così da poter mandare di nascosto il payload (il codice malevolo vero e proprio, ndr) di Pegasus attraverso un file più grande. Tale file era temporaneamente salvato in forma cifrata e illeggibile ad Apple su uno dei server iCloud di Apple negli Usa o altrove per la consegna (delivery) al target".

Apple prosegue sottolineando anche i costi che avrebbe dovuto sostenere per identificare e investigare l'attacco e sviluppare le relative protezioni e correzioni (patches). E aggiunge di non aver individuato attacchi contro iOS 15, invitando gli utenti ad aggiornare i propri iPhone.

Il riferimento alla entity list e alle inchieste giornalistiche

Uno degli aspetti che colpiscono della denuncia sono i riferimenti agli ultimi fatti di cronaca. È chiaro che il testo è stato aggiornato nelle ultime ore prima di essere depositato, e che alcuni di questi fatti costituiscono, quanto meno agli occhi dei legali Apple, un volano. Come se fosse da

tempo tutto pronto ma si aspettasse che succedessero alcune cose. Ad esempio, ed è un dato fondamentale, l'inclusione di NSO nella entity list del Dipartimento del Commercio americano (di cui avevo scritto qua), citata più volte. "Come conseguenza della sanzione del governo – scrive la denuncia – alle aziende Usa è fatto divieto di esportare certi prodotti e servizi a NSO senza una speciale licenza (su cui il governo Usa applicherà una presunzione di rifiuto per qualsiasi richiesta da parte di aziende americane [significa che la richiesta è automaticamente negata a meno di dimostrare specifiche circostanze da parte di chi la presenta, ndr]).

10 milioni per i ricercatori anti-malware governativi

Nel comunicato stampa, Apple dice anche un'altra cosa importante. Dopo aver lodato il lavoro di Citizen Lab e Amnesty Tech (i due gruppi di ricercatori che più di altri hanno fatto emergere l'uso e abuso di spyware governativi contro giornalisti e attivisti), dice che donerà 10 milioni di dollari alle organizzazioni che si occupano di questo genere di ricerca, oltre ai risarcimenti ottenuti con l'azione legale. E che sosterrà anche gli altri ricercatori su questi temi con assistenza tecnica e threat intelligence pro-bono (va detto che su Twitter alcuni noti ricercatori di sicurezza hanno mostrato una certa dose di incredulità rispetto alla promessa di collaborazione di Apple).

Nondimeno, un giorno dopo l'annuncio, Apple ha anche inviato delle notifiche ad alcuni suoi utenti, in quanto presi di mira da "attaccanti sponsorizzati da Stati, che avrebbero cercato di compromettere da remoto gli iPhone associati al tuo Apple ID". Tra questi utenti ci sono sei attivisti e ricercatori thailandesi; dodici dipendenti salvadoregni della testata online El Faro, critica del governo, oltre a due leader della società civile e due politici dell'opposizione in Salvador; e il presidente del

partito democratico in Uganda, Norbert Mao.

Che succede ora a NSO?

Nel giro di pochi mesi l'azienda di spyware si è trovata al centro delle rivelazioni del Progetto Pegasus, con 17 testate che hanno mostrato casi in cui lo spwyare era usato contro giornalisti e attivisti (anche in Europa). Il governo Usa l'ha messa nella sua entity list. Ha due cause legali mosse da due delle più grandi aziende tech, Facebook (Whatsapp) e Apple. E a tal proposito, a novembre, un tribunale americano (nella causa Whatsapp contro NSO Group) ha stabilito che NSO e Q Cyber (società madre menzionata e accusata anche nella denuncia di Apple) non godono di "immunità sovrana" per il fatto di vendere spyware ai governi. Inoltre Moody ha appena declassato NSO di due livelli. E, a detta di alcuni osservatori, l'azienda rischierebbe il default su un prestito da 500 milioni di dollari. Inoltre la Francia, ha rivelato giorni fa la MIT Technology Review, avrebbe cancellato una commessa che aveva in ballo con NSO dopo le rivelazioni del Pegasus Project che hanno raccontato come perfino dei politici francesi, e lo stesso presidente Macron, fossero tra i target di chi usava Pegasus (i sospetti in questo caso ricadono sul Marocco). Il morale fra i dipendenti dell'azienda israeliana è basso, rivela sempre MIT Technology Review. E il nuovo CEO ha subito mollato poco dopo essersi insediato.

La mossa (tardiva?) di Israele

Non solo. In questi giorni è emerso che a novembre Israele avrebbe ridotto da 102 a 37 il numero di Paesi a cui è permesso esportare strumenti di cybersicurezza da parte delle aziende locali. In pratica la nuova lista di Stati a cui è possibile vendere da parte di società israeliane include perlopiù nazioni europee, Stati Uniti, Canada, UK, India, Giappone, Corea del Sud, Australia, Nuova Zelanda. Non è

menzionata l'Ungheria, dove Pegasus è stato trovato sui dispositivi di giornalisti. L'Italia è nella lista. Probabilmente la mossa è stata presa per convincere il governo americano a indietreggiare sull'inclusione di NSO e Candiru nella sua lista nera sull'export, l'entity list. Il settore della cybersicurezza in Israele produce 10 miliardi di dollari di ricavi annuali, con il comparto offensivo che copre il 10 per cento delle vendite, scrive Calcalistech.

n punto di svolta nell'industria degli spyware?

Dunque per la prima volta dopo anni, l'industria degli spyware – che è cresciuta senza limiti nell'ultimo decennio, come ho raccontato a settembre in questo lungo approfondimento in 3 parti – sembra essere arrivata a un punto di svolta. Le mancanze della politica in questo settore, l'assenza di trasparenza e accountability sono state colmate dalle iniziative sparse della società civile (i ricercatori che hanno lavorato sui malware governativi, primi fra tutti Citizen Lab e Amnesty Tech, ma non solo loro, e poi i giornalisti che se ne sono occupati), dagli interessi e dalla discesa in campo di colossi tech, dalla nuova amministrazione americana che ha deciso di includere NSO nella sua entity list.
Il clima sta cambiando per tutto il settore. Anche se ancora manca un quadro regolatorio certo e anche se latitano i dati dettagliati sulle esportazioni di questi prodotti (l'Ue ci sta provando, ma col freno a mano tirato da alcuni Stati membri), esportare strumenti di sorveglianza in qualsiasi Paese senza controlli e remore è una scelta che alla lunga può diventare un boomerang, anche per le aziende che li producono.