Pegasus: la lunga storia di processi e smentite del Gruppo NSO

Frank Andrews

20 luglio 2021 – Middle east eye

L'azienda israeliana afferma di non poter essere considerata responsabile per il modo in cui gli Stati, "clienti sovrani", utilizzano la sua tecnologia.

Il gruppo NSO non è nuovo agli scandali.

Le affermazioni fatte questa settimana secondo cui la tecnologia *spyware* del programma Pegasus dell'azienda israeliana è stata utilizzata per sorvegliare 50.000 telefoni – appartenenti a capi di stato, giornalisti, attivisti per i diritti umani, oppositori politici e altro – potrebbero rappresentare l'accusa più grave mossa contro l'azienda, ma non sarebbe la prima.

Pegasus, che in vari modi infetta i telefoni con *spyware*, ha rappresentato una manna per i regimi autoritari che usano le tecnologie per tracciare chiunque sia percepito come critico nei confronti del loro potere.

Il Gruppo è stato oggetto di numerose azioni legali e denunce.

Martedì i pubblici ministeri francesi hanno annunciato di aver aperto un'indagine con l'accusa secondo cui Pegasus è stato utilizzato dall'intelligence marocchina per spiare i giornalisti francesi, dopo che *F*orbidden Stories, organizzazione senza scopo di lucro [con la missione di "continuare e pubblicare il lavoro di giornalisti minacciati, incarcerati o assassinati", ndtr.] ha condotto un'inchiesta che ha rivelato come alcuni Stati, tra cui l'Arabia Saudita, gli Emirati Arabi Uniti, il Bahrain e il Marocco, starebbero

usando la tecnologia Pegasus per spiare cittadini e dissidenti, inclusi i collaboratori di *Middle East Eye* Madawi al-Rasheed e Azzam Tamimi.

I familiari, gli amici e i contatti più stretti del giornalista saudita assassinato Jamal Khashoggi erano tra le molte migliaia di persone sorvegliate.

Nel corso degli anni, NSO, fondata nel 2010, ha ripetutamente cercato di sottrarsi alle responsabilità riguardo a come gli Stati utilizzino la sua tecnologia per spiare giornalisti e difensori dei diritti umani.

NSO afferma di seguire tutte le normative israeliane che disciplinano l'esportazione dei suoi prodotti e di vendere solo agli alleati di Israele, mai ai suoi nemici. Afferma inoltre di vendere solo a governi e mai a individui o utenti non autorizzati e che Pegasus è destinato esclusivamente a combattere la criminalità e il terrorismo.

Sottolinea tuttavia che una volta venduto il prodotto, non c'è alcun controllo (o almeno così sostiene) su come venga utilizzata la tecnologia.

Middle East Eye ha indagato sulla lunga lista di accuse a cui NSO ha dovuto rispondere nel corso degli anni e su come l'azienda abbia reagito.

2016

Secondo un rapporto di Citizen Lab [laboratorio interdisciplinare dell'Università di Toronto per ricerca, sviluppo e politica strategica di alto livello, ndtr.] e Lookout Security [società californiana che produce software di sicurezza su cloud per dispositivi mobili, ndtr.], si è scoperto che nell'agosto 2016 gli Emirati Arabi Uniti stavano monitorando l'iPhone dell'attivista per i diritti umani negli Emirati Ahmed Mansoor utilizzando lo *spyware* Pegasus.

Mansoor ricevette un sms che gli chiedeva di aprire un link per

avere informazioni sui prigionieri torturati negli Emirati Arabi Uniti.

NSO non ha confermato di aver creato lo *spyware* utilizzato per raggiungere Mansoor. Tuttavia ha affermato in una dichiarazione di "vendere solo ad agenzie governative autorizzate e rispettare pienamente le rigorose leggi e regolamenti sul controllo delle esportazioni. Inoltre l'azienda non gestisce nessuno dei suoi sistemi: è un'azienda esclusivamente tecnologica".

Altri Paesi che il rapporto di Citizen Lab ha scoperto potrebbero aver utilizzato questa tecnologia includono Messico, Turchia, Israele, Thailandia, Qatar, Kenia, Uzbekistan, Mozambico, Marocco, Yemen, Ungheria, Arabia Saudita, Nigeria e Bahrein.

In un caso collegato a quello del 2016, anche le autorità degli Emirati Arabi Uniti avrebbero impiegato Pegasus in un tentativo di *phishing* [azione per ottenere con l'inganno dati riservati, ndtr.] contro il giornalista *MEE* Rori Donaghy, che parlava in modo critico degli abusi del regime autocratico del Paese.

Nel corso dell'indagine su questo attacco, Citizen Lab ha scoperto che 1.100 attivisti e giornalisti dell'Emirato erano stati presi di mira allo stesso modo e che per questi attacchi il governo aveva pagato al gruppo NSO 600.000 dollari.

2017

Nel febbraio 2017, Citizen Lab ha rivelato che Pegasus era stato utilizzato per colpire degli attivisti messicani che cercavano di contrastare l'obesità infantile. Il *malware* aveva accesso ai loro telefoni quando aprivano i link con testi che dicevano, ad esempio, "Mentre stai lavorando, sto fottendo la tua vecchia, ecco una foto" e "[tua figlia] ha appena avuto un grave incidente… ecco dove è ricoverata".

Nello stesso anno, il *New York Times* ha riferito che i telefoni di attivisti politici messicani per i diritti umani e anticorruzione, che stavano indagando su possibili crimini commessi dal governo e dai suoi agenti, erano stati infettati da Pegasus. Il *NYT* ha affermato che

le vittime hanno notato le intrusioni per la prima volta nell'estate del 2016.

Il governo messicano ha negato ogni responsabilità in merito allo spionaggio.

2018

Nell'agosto 2018 Amnesty International ha affermato che uno dei membri del suo personale, così come molti sauditi difensori dei diritti umani, erano stati presi di mira con il software Pegasus, utilizzando messaggi di testo con link che dicevano, ad esempio:

"Puoi per favore coprire [la protesta] davanti all'ambasciata saudita a Washington per i fratelli detenuti in Arabia Saudita? Mio fratello sta facendo il Ramadan e io sono qui con una borsa di studio, quindi per favore non taggarmi".

Quando Amnesty ha collegato lo spionaggio alla NSO, l'azienda ha risposto: "Il nostro prodotto è destinato esclusivamente alle indagini e alla prevenzione di crimini e terrorismo. Qualsiasi utilizzo della nostra tecnologia contrario a tale scopo costituisce una violazione delle nostre politiche, dei contratti legali e dei nostri valori come azienda".

In seguito Amnesty ha affermato che alla luce dell'attacco informatico stava considerando un'azione legale per costringere il ministero della Difesa israeliano a revocare la licenza di esportazione a NSO.

Nello stesso mese di agosto, il *New York Times* ha riferito che NSO stava affrontando due cause legali con l'accusa di aver partecipato attivamente allo spionaggio illegale.

Il giornale affermava che le cause, intentate da un cittadino del Qatar e da giornalisti e attivisti messicani, erano state depositate in Israele e a Cipro, e che i documenti presentati a sostegno delle accuse dimostravano che gli Emirati Arabi Uniti avevano utilizzato lo *spyware* Pegasus per almeno un anno.

Secondo il *NYT*, gli Emirati avevano intercettato i telefoni dell'emiro del Qatar, di un caporedattore di un giornale con sede a Londra e di un potente principe saudita. Gli Emirati Arabi Uniti, insieme al Bahrain e all'Arabia Saudita, erano a quel tempo coinvolti in una disputa con il Qatar che portò il trio a imporre un blocco terrestre e marittimo contro il loro vicino.

Nell'ottobre 2018 Citizen Lab ha dichiarato che il software Pegasus aveva attaccato il telefono di un caro amico di Jamal Khashoggi, Omar Abdulaziz, prima dell'omicidio del dissidente e che il software aveva preso di mira difensori dei diritti umani in Bahrain, negli Emirati Arabi Uniti e altrove.

Lo stesso mese l'informatore statunitense Edward Snowden aveva affermato che Pegasus era stato utilizzato dalle autorità saudite per sorvegliare Khashoggi prima della sua morte.

"Sono il peggio del peggio", ha detto Snowden dell'azienda. NSO nega che la sua tecnologia sia stata "in alcun modo" utilizzata per l'omicidio.

Sempre a ottobre, Citizen Lab ha affermato che i suoi stessi ricercatori erano stati presi di mira da agenti collegati alla NSO. La NSO ha negato le accuse.

A novembre *Haaretz* ha riferito che nell'estate del 2017 NSO aveva firmato un accordo con l'intelligence saudita.

Rispondendo ad *Haaretz*, NSO ha affermato che "ha operato e opera esclusivamente in conformità con le leggi sull'esportazione della difesa e secondo le linee guida e la stretta supervisione di tutti i componenti dell'establishment della Difesa [israeliana, ndtr.], comprese tutte le questioni relative alle politiche e alle licenze di esportazione. Le informazioni fornite da *Haaretz* sull'azienda, sui suoi prodotti e sul loro utilizzo sono errate, basate su voci e pettegolezzi di parte. Il quadro distorce la realtà".

Poi, secondo quanto riportato dal *New York Times*, a dicembre Abdulaziz ha intentato una causa contro NSO, sostenendo che la

società aveva aiutato i sauditi a spiare le sue comunicazioni con Khashoggi.

Il Gruppo NSO ha affermato ancora una volta che la sua tecnologia è stata “concessa su licenza al solo scopo di fornire ai governi e alle forze dell’ordine la capacità di combattere legalmente il terrorismo e la criminalità”.

I contratti per l’utilizzo del software, ha aggiunto, “vengono forniti solo dopo un completo controllo e previa autorizzazione da parte del governo israeliano”, ha affermato NSO.

“Non tolleriamo un uso improprio dei nostri prodotti. Se c’è il sospetto di un uso improprio, indaghiamo e intraprendiamo le azioni necessarie, inclusa la sospensione o la risoluzione del contratto”, ha aggiunto.

L’amministratore delegato della società, Shalev Hulio ha affermato in seguito che NSO non era stata coinvolta nel “terribile omicidio”, ma non ha risposto in merito alla segnalazione secondo cui Hulio era andato personalmente a Riyadh per vendere il software Pegasus ai sauditi.

2019

Nel febbraio 2019, una società di *private equity* [che apporta nuovi capitali a una società come investimento finanziario, ndtr.] ha acquistato lo *spyware* NSO e ha dichiarato a Citizen Lab di essere “impegnata ad aiutarla a diventare più trasparente in merito alla sua attività”.

E ad aprile, secondo quanto riferito, l’azienda ha congelato dei nuovi accordi con l’Arabia Saudita.

A maggio, Amnesty ha affermato che avrebbe presentato una petizione legale al tribunale distrettuale di Tel Aviv per bloccare le licenze di esportazione di NSO, e uno scrittore satirico saudita che vive in esilio a Londra ha intentato un’azione legale contro l’Arabia Saudita, accusando il Paese di aver utilizzato lo spyware Pegasus per

ottenere informazioni personali dal suo telefono.

Lo stesso mese un'indagine del *Financial Times* ha rivelato che dei malintenzionati stavano sfruttando la funzione di chiamata di WhatsApp telefonando alle vittime per diffondere Pegasus.

"In nessun caso NSO è stata coinvolta nell'operazione o nell'identificazione degli obiettivi della sua tecnologia, che è gestita esclusivamente da agenzie di intelligence e forze dell'ordine", ha risposto la società al *FT*. "NSO non avrebbe, o non potrebbe, utilizzare il software in proprio per prendere di mira qualsiasi persona o organizzazione".

Nell'ottobre dello stesso anno WhatsApp, di proprietà di Facebook, ha intentato una causa contro il gruppo NSO accusandolo di aver cercato illegalmente di sorvegliare giornalisti, attivisti per i diritti umani e altri in 20 Paesi tra cui Messico, Emirati Arabi Uniti e Bahrain.

L'azione legale, intentata in California presso un tribunale federale degli Stati Uniti, accusava il gruppo NSO di aver cercato di infettare circa 1.400 "dispositivi bersaglio" con *spyware* ostile che potrebbe essere utilizzato per rubare informazioni agli utenti di WhatsApp.

"Contestiamo recisamente le accuse odierne e le combatteremo con forza", ha affermato il gruppo NSO in una nota.

"L'unico scopo di NSO è fornire tecnologia all'intelligence governativa autorizzata e alle forze dell'ordine per aiutarli a combattere il terrorismo e gravi forme di criminalità".

Un mese prima, a settembre, NSO aveva messo a punto una politica dei diritti umani, affermando che avrebbe rispettato i principi guida delle Nazioni Unite.

A novembre, un gruppo di dipendenti di NSO ha intentato una causa contro Facebook, affermando che il gigante dei social media aveva bloccato ingiustamente i loro account privati quando aveva fatto causa a NSO il mese prima, accusando Facebook di "punizione

collettiva”.

Il giorno prima, intervenendo a una conferenza sulla tecnologia a Tel Aviv, il presidente della NSO Shiri Dolev aveva difeso la sua azienda, affermando che le tecnologie NSO hanno reso il mondo più sicuro.

Dolev ha anche affermato di auspicare che NSO possa parlare apertamente del ruolo che svolge nell’aiutare le forze dell’ordine a catturare i terroristi.

“Terroristi e criminali usano le piattaforme e le app dei social che usiamo tutti noi ogni giorno”, ha detto.

2020

Nel gennaio 2020 un giudice israeliano ha ordinato a NSO di affrontare la denuncia di pirateria informatica intentata contro il Gruppo dall’attivista saudita Omar Abdulaziz e di pagare le sue spese legali, e un tribunale ha stabilito che la causa legale di Amnesty per impedire a NSO di esportare il suo software si sarebbe dibattuta a porte chiuse.

Lo stesso mese Reuters ha riferito che almeno dal 2017 l’FBI stava indagando su NSO riguardo al suo possibile coinvolgimento in un attacco informatico contro cittadini e società statunitensi, nonché per una sospetta raccolta di informazioni nei confronti di governi.

La società ha affermato di non essere a conoscenza di alcuna inchiesta.

Secondo *The Guardian* ad aprile i documenti del tribunale relativi al caso WhatsApp dimostravano come NSO avesse negato ogni responsabilità per come era stata utilizzata la sua tecnologia, affermando che WhatsApp aveva “confuso” le azioni di NSO con quelle dei suoi “clienti sovrani”.

“I governi clienti agiscono prendendo tutte le decisioni su come utilizzare la tecnologia”, ha affermato la società. “Se qualcuno ha installato Pegasus su un qualche presunto ‘dispositivo bersaglio’

non sono stati gli imputati [Gruppo NSO] a farlo. Sarebbe stato un ente di un governo sovrano".

"Il Gruppo NSO non gestisce il software Pegasus per i suoi clienti", ha detto a *The Guardian*.

A giugno, un'indagine di Amnesty International ha rivelato che lo *spyware* della NSO era stato utilizzato contro il noto giornalista marocchino e difensore dei diritti umani Omar Radi.

Il rapporto di Amnesty afferma che l'attacco a Radi era avvenuto tre giorni dopo l'annuncio della nuova politica dei diritti umani della NSO.

In risposta, NSO ha dichiarato di essere "profondamente turbata" dalle accuse e che avrebbe immediatamente avviato un'indagine.

"Coerentemente con la propria politica dei diritti umani, il Gruppo NSO considera seriamente la responsabilità di rispettare i diritti umani ed è fortemente impegnata a evitare di causare, contribuire o essere direttamente collegata a effetti negativi sui diritti umani", ha affermato NSO in una nota.

Comunque la società ha preso le distanze dall'accusa di avere legami con le autorità marocchine e ha affermato che, per la natura della sua attività, deve salvaguardare la riservatezza dei suoi clienti.

"Siamo obbligati a rispettare gli interessi di riservatezza degli Stati e non possiamo rivelare l'identità dei clienti", ha affermato NSO.

Martedì Radi è stato condannato a sei anni di carcere per aggressione sessuale e spionaggio, accuse che lui nega.

Nel luglio 2020, un tribunale di Tel Aviv ha respinto la petizione di Amnesty e 30 attivisti per i diritti umani che chiedevano di revocare la licenza di esportazione al gruppo NSO, affermando che non avevano fornito prove del fatto che il software Pegasus fosse stato utilizzato per spiare gli attivisti della ONG britannica.

Le indagini di luglio e agosto hanno rivelato che il software Pegasus

era stato utilizzato per spiare politici catalani in Spagna e sacerdoti in Togo.

A dicembre Citizen Lab ha riferito che dozzine di giornalisti dell'agenzia di stampa *Al Jazeera*, finanziata dal Qatar, sono stati presi di mira con un attacco di Pegasus tramite iMessage, attacchi probabilmente collegati ai governi dell'Arabia Saudita e degli Emirati Arabi Uniti.

Un giornalista di *Al Jazeera* ha detto di aver ricevuto minacce di morte sul suo telefono: "Hanno minacciato di farmi diventare il nuovo Jamal Khashoggi".

In una dichiarazione il gruppo NSO ha messo in dubbio le accuse di Citizen Lab, ma ha affermato di "non essere in grado di commentare un rapporto che non abbiamo ancora visto".

L'azienda ha affermato di fornire software al solo scopo di consentire "alle forze dell'ordine governative di affrontare la criminalità organizzata e l'antiterrorismo".

All'inizio di quel mese, una conduttrice televisiva di *Al Jazeera* ha intentato un'altra causa negli Stati Uniti, sostenendo che il gruppo NSO ha hackerato il suo telefono tramite WhatsApp a causa delle sue critiche al potente principe ereditario dell'Arabia Saudita Mohammed bin Salman.

A dicembre, una coalizione di associazioni per i diritti umani, tra cui il gruppo per i diritti sulla rete Access Now, Amnesty International, il Comitato per la Protezione dei Giornalisti e Reporter senza Frontiere, si è unita alla lotta legale di Facebook contro NSO, sostenendo che la società dà la priorità ai profitti rispetto ai diritti umani, facendo seguito a un'azione simile promossa da una serie di grandi aziende tecnologiche tra cui Google e Microsoft.

2021

A marzo *The Guardian* ha riferito che il Dipartimento di Giustizia degli Stati Uniti ha ripreso le indagini sul gruppo NSO, dopo mesi in cui le

principali società tecnologiche statunitensi andavano affermando che l'azienda israeliana è "potente e pericolosa" e non dovrebbe avere l'immunità per il suo ruolo nelle operazioni di pirateria informatica.

Il *Guardian* ha riferito che all'inizio del 2020 il gruppo NSO era stato oggetto di un'indagine dell'FBI, che però sembrava essersi arenata e il Dipartimento di Giustizia stava ora mostrando un nuovo interesse per il caso.

A luglio, un'indagine condotta da Forbidden Stories e Amnesty International ha rivelato che i telefoni di migliaia di giornalisti, attivisti e funzionari sono stati presi di mira o violati utilizzando Pegasus.

In risposta, NSO ha respinto le "false affermazioni", ha definito le accuse "teorie non provate" e parte di una "narrazione oscena... strategicamente inventata da diversi gruppi di interessi specifici strettamente allineati".

"Le tecnologie vengono utilizzate ogni giorno anche per spezzare i circuiti di pedofilia, sesso e traffico di droga, individuare i bambini scomparsi e rapiti e i sopravvissuti intrappolati sotto edifici crollati e proteggere lo spazio aereo dalla dannosa penetrazione di pericolosi droni", ha aggiunto.

"In parole povere, NSO ha una missione salvavita e la società proseguirà imperterrita ad adempiere a questa missione, nonostante i continui tentativi di screditarla su false basi ".

"Nonostante quanto sopra", ha aggiunto, "NSO continuerà a indagare su tutte le affermazioni credibili di un uso scorretto e a intraprendere azioni appropriate in base ai risultati di quelle indagini".

(traduzione dall'inglese di Luciana Galliano)