Rapporto: un sistema spionistico israeliano dietro al nuovo scandalo che ha preso di mira giornalisti russi

Redazione di Palestine Chronicle (PC, RT)

26 settembre 2023 – Palestine Chronicle

Il telefono del fondatore del sito di notizie lettone Meduza è stato hackerato prima di un incontro a Berlino tra giornalisti russi dell'opposizione.

Lunedì Galina Timchenko, una giornalista russa dell'opposizione che vive in Lettonia, ha raccontato a *The Guardian* che uno Stato europeo sconosciuto ha usato un programma di spionaggio israeliano per hackerare il suo telefonino.

Le autorità lettoni hanno negato qualsiasi ruolo nell'hackeraggio.

Timchenko, che ha fondato il sito di notizie *Meduza* contro il Cremlino, ha detto al giornale inglese *The Guardian* che all'inizio dell'anno ha ricevuto un messaggio da Apple che la informava che il suo telefono era stato hackerato prima di un incontro a Berlino tra giornalisti di opposizione russi.

Secondo il giornale, almeno quattro altri giornalisti russi – tre dei quali usavano SIM lettoni nei loro telefoni – sono stati colpiti allo stesso modo.

Timchenko ha affermato che inizialmente ha sospettato che ci fosse il Cremlino dietro all'hackeraggio, ma un'analisi della università di Toronto e di *Access Now* [associazione creata per difendere in diritti civili digitali, ndt.] hanno scoperto che probabilmente il responsabile è stato l'ente di uno Stato europeo che ha usato *Pegasus*, un programma di spionaggio sviluppato dall'israeliano NSO Group.

La Russia non usa *Pegasus*, mentre agenzie in molti Stati europei lo fanno – incluse Germania, Lettonia ed Estonia.

Pegasus può essere installato sul telefono della persona presa di mira indipendentemente dal fatto che l'utente clicchi o meno su un falso link. Una volta installato, Pegasus dà all'hacker la possibilità di leggere messaggi, guardare le foto, tracciare l'ubicazione della persona e anche accendere la videocamera e il microfono senza che il proprietario del telefono se ne accorga.

Secondo una lista di clienti di NSO che è trapelata nel 2021, più di 50.000 politici, giornalisti, attivisti ed esponenti del mondo degli affari sono stati spiati usando il programma di spionaggio.

È probabile che l'hackeraggio sia stato effettuato da qualche servizio di sicurezza europeo. Noi non sappiamo se sia stata la Lettonia o qualche altra Nazione, ma siamo più presenti in Lettonia" ha affermato Ivan Kolpakov, caporedattore di *Meduza*.

L'ambasciata lettone a Washington ha affermato che "non è a conoscenza di nessuna misura di sorveglianza elettronica presa contro la sig.ra Timchenko," mentre in Germania, dove è avvenuta la compromissione, la polizia federale si è rifiutata di commentare.

Timchenko e Kolpakov hanno detto a *The Guardian* di avere ragioni per sospettare il coinvolgimento di Riga, indicando una disputa lo scorso anno tra lo Stato lettone e *TV Dozhd* [televisione indipendente russa, ndt.], un altro mezzo di comunicazione dell'opposizione russa.

(traduzione dall'inglese di Gianluca Ramunno)

In tutto il mondo il gruppo NSO scosso dalle critiche e dalle cause legali.

Tamara Nassar

15 febbraio 2022 – The Electronic Intifada

Dopo un anno particolarmente negativo, la società di spyware israeliana NSO Group inizia il 2022 sempre più assediata da critiche e cause legali.

Dopo essere stata quasi portata alla rovina da cause legali e liste di esclusione nel 2021, la famigerata compagnia di spionaggio è coinvolta in uno scandalo nazionale secondo cui la sua tecnologia è stata utilizzata per spiare i cittadini israeliani.

La rivista economica israeliana *Calcalist* ha rivelato di recente che la polizia israeliana ha utilizzato Pegasus, il programma simbolo dell'azienda, per spiare alti funzionari del governo, giornalisti, personaggi pubblici e leader delle proteste.

Sindaci di diverse città israeliane, il personale di un importante quotidiano israeliano e funzionari di diversi ministeri erano fra gli hackerati dal malware.

Anche la cerchia ristretta dell'ex primo ministro israeliano Benjamin Netanyahu è stata presa di mira, inclusi due consiglieri e suo figlio Avner Netanyahu.

Anche Emi Palmor, l'ex direttore generale del ministero della giustizia, è stato spiato dal programma. In particolare, Palmor ha trascorso anni presso il ministero della giustizia israeliano a imporre la censura ai discorsi dei palestinesi prima di essere assunta dal consiglio di sorveglianza di Facebook.

Calcalist ha riferito che la polizia israeliana stava essenzialmente cercando attività di spionaggio anche prima che fosse stata aperta una indagine contro gli obiettivi e senza mandati giudiziari".

Lo spyware Pegasus è uno degli strumenti più sofisticati conosciuti nel settore della sorveglianza. Dopo averlo installato con successo sul telefono di un bersaglio, coloro che spiano possono estrarre una quantità impressionante di dati, incluse immagini, registrazioni, schermate, password oltre a e-mail e messaggi di testo.

Gli hacker possono anche accendere la fotocamera e registrare l'audio da remoto, controllando il dispositivo a piacimento. L'infezione può essere difficile o impossibile da rilevare per un utente medio e in genere richiede l'analisi di esperti.

Calcalist ha scritto: "L'uso di Pegasus non era locale o limitato a un piccolo numero di casi". Era "uno degli strumenti più efficaci" utilizzati dalla polizia israeliana. Il giornale ha descritto come la tecnologia sia stata utilizzata per ottenere informazioni private sulle attività sessuali di almeno un attivista al fine di ricatto.

Questo richiama alla mente che i membri del ramo dell'intelligence militare israeliana Unit 8200, da cui sono stati reclutati molti lavoratori del gruppo NSO, hanno precedentemente ammesso di aver spiato i dati privati più intimi di palestinesi, comprese le informazioni finanziarie e sessuali, al fine di ricattarli.

In Israele è scoppiata una vasta protesta pubblica e pare che il ministro degli interni, Omer Barlev, si sia mosso per istituire una commissione di indagine sulla questione.

Oltre a dichiarare di dover "capire esattamente cosa è successo", il primo ministro Naftali Bennett ha totalmente approvato l'uso della tecnologia del gruppo NSO da parte della polizia israeliana per spiare i cittadini palestinesi di Israele.

Bennett la scorsa settimana ha affermato: "Serve uno strumento come questo quando combatti contro famiglie criminali e gravi aggressioni".

"Non voglio eliminare lo strumento stesso, piuttosto regolarne l'uso." Bennett ha affermato che tali strumenti sono "molto importanti nella guerra contro il terrorismo", ma che "non erano destinati a un esteso spionaggio elettronico di cittadini israeliani o di personaggi pubblici nello Stato di Israele".

Se le auto-indagini di Israele sui suoi crimini contro i palestinesi sono indicative, il gruppo NSO riceverà nella migliore delle ipotesi un buffetto e l'indagine servirà da foglia di fico per rendere

accettabili altre faccende simili.

Sin dalla sua fondazione il gruppo NSO ha lavorato fianco a fianco con il ministero della Difesa israeliano e necessita della licenza di quest'ultimo per la vendita [dei suoi programmi all'estero, ndt]. Secondo quanto riferito, l'azienda si appresta a rafforzare gli interessi di Israele all'estero.

Il quotidiano di Tel Aviv *Haaretz* ha riferito domenica che l'agenzia internazionale di spionaggio e omicidi israeliana Mossad ha utilizzato la tecnologia Pegasus del gruppo NSO per spiare cellulari "in modo non ufficiale".

Il giornale ha affermato che ciò è avvenuto sotto l'ex capo del Mossad Yossi Cohen, citando anonimi dipendenti del gruppo NSO. Questi stessi impiegati hanno aggiunto che funzionari del Mossad hanno frequentato il quartier generale dell'azienda, Herzliya vicino a Tel Aviv, a volte portando "funzionari da paesi stranieri come parte degli sforzi per vendere loro il software", ha detto Haaretz.

L'FBI acquista Pegasus

Nel frattempo, il gruppo NSO ha anche fatto notizia sulla stampa statunitense per altre accuse di abusi.

Il *New York Times Magazine* ha rivelato il mese scorso che l'FBI ha acquistato la tecnologia spyware da NSO Group.

Pegasus è stato a lungo commercializzato come uno strumento in grado di hackerare tutti i telefoni tranne quelli americani. In questo modo, Israele ha assicurato agli Stati Uniti che i clienti stranieri di NSO Group non avrebbero spiato gli americani.

"Ma impediva anche agli americani di spiare gli americani", ha detto il *Times*.

Quindi il gruppo NSO ha fatto un'eccezione. Ha progettato un programma, chiamato Phantom, che poteva essere venduto esclusivamente alle agenzie governative statunitensi e può essere utilizzato per hackerare numeri di telefono statunitensi.

L’FBI ha acquistato questo programma, ma afferma di non averlo mai usato contro gli americani in attesa di capire se le leggi vigenti gli avrebbero consentito di farlo.

Non è chiaro se l’FBI abbia utilizzato il programma o meno, ma è da notare che anche mentre conduceva discussioni [sul possibile uso dello spyware, ndt] che hanno abbracciato “due amministrazioni presidenziali”, ha rinnovato gli accordi finanziari con NSO Group.

La rivista non sembra mettere in dubbio l’affermazione dell’FBI di aver deciso di “non utilizzare le armi della NSO”.

“Sacchi di soldi”

Nel frattempo, un ex vicepresidente di una società di telecomunicazioni con sede in California ha affermato che il gruppo NSO ha offerto alla sua azienda “sacchi di soldi” in cambio dell’accesso alle reti globali di cellulari.

Gary Miller, che all’epoca lavorava per Mobileum, afferma di essere stato coinvolto in una telefonata nel 2017 quando Shalev Hulio, co-fondatore di NSO Group, e un altro rappresentante del gruppo hanno fatto l’offerta.

Dal giugno scorso, Miller lavora per Citizen Lab, una organizzazione di ricerca con sede a Toronto, che ha pubblicato numerosi rapporti e rivelazioni sulla tecnologia del gruppo NSO. Gli analisti del Citizen Lab esaminano i telefoni per trovare tracce di Pegasus.

Curiosamente, Miller è un cliente di Whistleblower Aid, un’organizzazione guidata da figure losche con precedenti stretti legami con il Dipartimento di Stato degli Stati Uniti e l’apparato di intelligence.

Uno dei suoi ultimi maggiori clienti è stata Frances Haugen, l’ex product manager di Facebook che ha fatto trapelare documenti interni che accusavano l’azienda, tra le altre cose, di svilire l’immagine fisica delle ragazze.

Haugen è stata portata davanti al Congresso per fornire argomenti

a coloro che chiedono maggiore censura e controllo del discorso pubblico su Facebook con le viste di impedire a paesi come Cina e Iran di utilizzare la piattaforma per fini nefasti – una riproposizione della stessa vecchia narrativa del Russiagate.

È stata acclamata come un'eroica "whistleblower".

Non è chiaro perché uno come Miller, che ora lavora per una organizzazione che storicamente ha denunciato il NSO, sia il cliente di un tale gruppo.

Tutela e credibilità

In risposta alle cause legali e alle rivelazioni della stampa di come la sua tecnologia sia stata utilizzata in modo improprio per prendere di mira giornalisti, difensori dei diritti umani e politici, la difesa del gruppo NSO è rimasta coerente.

Il gruppo NSO ha ripetutamente affermato di vendere i suoi programmi solo a governi e agenzie governative e di mettere in atto rigide misure di protezione da usi impropri

I recenti scandali dell'azienda di spyware rivelano che l'uso improprio è più diffuso di quanto si pensasse.

Una fonte anonima ha detto a *Calcalist* che il gruppo NSO è più coinvolto nella gestione dello spyware di quanto affermino.

Secondo la fonte le informazioni più importanti sulle operazioni di spionaggio e le informazioni così ottenute vengono generate e conservate sull'infrastruttura cloud gestita da NSO Group, non dal cliente.

Quindi il gruppo NSO non può rivendicare in toto l'ignoranza o la mancanza di responsabilità per l'uso improprio dei suoi programmi. I suoi servizi non terminano alla fine della transazione, ma comportano un processo continuo in cui l'azienda fornisce costantemente assistenza.

Come ha recentemente dichiarato all'Electronic Intifada Podcast

l’economista e ricercatore Shir Hever, non si tratta di una transazione in cui il gruppo NSO invia un “CD ROM” ai suoi clienti e se ne lava le mani. Invece è una transazione basata su una forma di abbonamento che garantisce comunicazioni e assistenza continue da parte dell’azienda.

La stessa fonte ha detto a *Calcalist* che i “client” possono disabilitare i “log” e quindi nascondere alcune informazioni sugli obiettivi di spionaggio. Ciò suggerisce che il gruppo NSO concede ai suoi clienti la licenza di spiare chi vogliono nell’ombra, indipendentemente dal fatto che rispettino la affermazione di facciata di perseguire i “criminali”.

Se l’attuale scandalo nazionale di NSO Group può dirci qualcosa, è semplicemente che una tecnologia di questo tipo è pronta per gli abusi sia dell’inventore che del cliente. Gli attivisti per i diritti umani e altri attivisti sono destinati a subirne le conseguenze.

(traduzione dall’Inglese di Giuseppe Ponsetti)