Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 1 / 10
www.datastampa.it

29 apr/5 mag 2022
n. 1458 · anno 29
internazionale.it
4,00 €

Ogni settimana il meglio dei giornali di tutto il mondo

Ivan Krastev
La Russia può ancora cambiare

Visti dagli altri
La 'ndrangheta in Costa Azzurra

Economia
Come Elon Musk ha conquistato Twitter

Internazionale

Pegasus
Chi controlla il software di spionaggio più potente del mondo

La lotta tra Stati Uniti e Israele per l'arma informatica che può entrare nei nostri telefoni

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 2 / 10
www.datastampa.it

In copertina

Il mondo sotto controllo

Ronen Bergman e Mark Mazzetti, The New York Times Magazine, Stati Uniti

Un'inchiesta del New York Times rivela in che modo Israele ha usato il software di spionaggio Pegasus per ottenere vantaggi diplomatici. E perché gli Stati Uniti prima lo hanno comprato e poi hanno cercato di vietarlo

ZIV KOREN (POLARIS/KARMA PRESS PHOTO)

Shalev Hulio, al centro, nella sede dell'Nso a Herzliya, in Israele, il 13 aprile 2019

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 3 / 10
www.datastampa.it

Nel giugno 2019 tre ingegneri informatici israeliani si sono presentati in un edificio del New Jersey usato dall'Fbi e hanno preso dagli scatoloni decine di server. Dopo averli sistemati in una stanza isolata, li hanno accesi e hanno fatto una serie di telefonate ai loro capi a Herzliya, un quartiere nella periferia di Tel Aviv in cui si trova la sede dell'Nso Group, l'azienda più conosciuta al mondo tra quelle che producono *spyware*, software che permettono di spiare telefoni e computer per rubare dati e informazioni. Poi, una volta sistemate le apparecchiature, hanno cominciato i test.

L'Fbi (Federal bureau of investigation, l'agenzia statunitense per la sicurezza interna) aveva appena comprato una versione di Pegasus, il principale strumento di spionaggio dell'Nso. Già da una decina d'anni l'azienda israeliana vendeva il suo sistema di sorveglianza ai servizi di sicurezza di tutto il mondo, promettendo risultati che nessun altro era in grado di garantire: intercettare le comunicazioni cifrate di tutti gli smartphone iPhone e Android in modo sistematico e affidabile. Sembrava che i prodotti dell'Nso fossero la soluzione a uno dei più grandi problemi dei servizi di sicurezza nel ventunesimo secolo: e cioè che criminali e terroristi usavano tecnologie di cifratura migliori di quelle a disposizione degli investigatori per decifrarle. Il mondo del crimine era riuscito a restare nell'oscurità anche mentre diventava sempre più globale.

Nel 2019, però, anche i numerosi abusi di Pegasus erano ormai ben documentati. Il governo messicano aveva usato il software non solo contro i criminali, ma anche contro giornalisti e oppositori. Gli Emirati Arabi Uniti se n'erano serviti per accedere al telefono di un attivista per i diritti civili, poi incarcerato. L'Arabia Saudita l'aveva usato contro le militanti per i diritti delle donne e, secondo la denuncia di un dissidente saudita, per spiare le comunicazioni di Jamal Khashoggi, editorialista del Washington Post ucciso e fatto a pezzi da agenti sauditi a Istanbul nel 2018.

Nulla di tutto questo, però, aveva impedito ai nuovi potenziali clienti, Stati Uniti compresi, di contattare l'Nso. I particolari dell'acquisto e della sperimentazione di Pegasus da parte dell'Fbi non sono mai stati resi pubblici. Inoltre, lo stesso anno in cui Khashoggi è stato ucciso, la Cia (Central intelligence agency, l'agenzia statunitense per la sicurezza esterna) aveva organizzato e finanziato la vendita di Pegasus al governo di Gibuti per aiutare l'alleato statunitense nella lotta al terrorismo, nonostante le preoccupazioni sulle violazioni dei diritti umani nel paese africano, tra cui la persecuzione dei giornalisti e il ricorso alla tortura contro gli oppositori. La Dea, l'agenzia impegnata nella lotta contro il traffico di droga, il Secret service, incaricato della sicurezza del presidente e della sua famiglia, e l'Africa command dell'esercito statunitense avevano già parlato con l'Nso. Ora era il turno dell'Fbi.

Durante i corsi di formazione, ad alcuni agenti dell'Fbi è stato chiesto di comprare degli smartphone e registrarli con account fittizi, usando schede sim di altri paesi (Pegasus è stato progettato in modo da non attaccare numeri statunitensi). A quel punto gli ingegneri, come già in altre dimostrazioni in giro per il mondo, hanno aperto l'interfaccia e, dopo aver inserito i numeri di telefono, hanno fatto partire l'attacco informatico.

La versione di Pegasus era "zero clic" – a differenza dei software di hackeraggio più comuni non richiedeva che l'utente

AMIR LEVY (GETTY IMAGES)

Una sede dell'Nso nel deserto di Arava, in Israele, l'11 novembre 2021

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 4 / 10
www.datastampa.it

cliccasse su un allegato o un link dannoso – perciò gli agenti statunitensi non hanno visto tracce di violazioni in corso sui telefoni. E non si sono accorti che i computer di Pegasus si collegavano a una rete di server in tutto il mondo, entravano nei telefoni e poi si ricollegavano alle attrezzature in New Jersey. Ma pochi minuti dopo hanno visto tutti i dati conservati nei dispositivi usati per la simulazione comparire sui grandi monitor dei computer di Pegasus: le email, le foto, i messaggi, i contatti personali. Si poteva risalire alla posizione di ogni dispositivo e perfino prendere il controllo della videocamera e del microfono. Grazie a Pegasus gli agenti dell'Fbi erano in grado di trasformare all'istante i telefoni di tutto il mondo in potenti strumenti di sorveglianza. Ovunque, tranne che negli Stati Uniti. Israele non voleva farli arrabbiare consentendo le attività di spionaggio di altri paesi sul loro territorio. Impedire all'Nso di programmare Pegasus per attaccare utenze statunitensi evitava ai clienti stranieri dell'azienda di spiare gli americani; ma impediva anche agli statunitensi di spiare altri statunitensi.

Miniera d'oro

Negli ultimi tempi l'Nso ha proposto all'Fbi una soluzione per aggirare il problema. Durante una dimostrazione alle autorità a Washington, l'azienda ha presentato un nuovo sistema, chiamato Phantom, capace di violare qualsiasi numero l'Fbi decida di mettere sotto sorveglianza negli Stati Uniti. In pratica, Israele ha concesso all'Nso una licenza speciale che permette a Phantom di attaccare anche utenze statunitensi. La licenza è disponibile solo per un unico tipo di clienti: le agenzie governative degli Stati Uniti. In un elegante volantino, stampato dalla sede statunitense dell'Nso e pubblicato per la prima volta dal sito d'informazione Vice, si legge che grazie a Phantom i servizi di sicurezza statunitensi possono raccogliere dati "estraendo e monitorando informazioni cruciali sui dispositivi mobili". È una "soluzione indipendente" che non richiede la collaborazione delle aziende di telecomunicazioni At&t e Verizon, né della Apple o di Google. Il sistema, si legge, "trasformerà il telefono del vostro bersaglio in una miniera d'oro d'informazioni".

Molti titoli di giornale si sono concentrati sullo spauracchio di un'azienda privata fuori controllo, che ha sede in Israele ma è finanziata all'estero

La presentazione di Phanton ha scatenato una discussione durata due anni tra i legali del dipartimento di giustizia e l'Fbi, a cavallo tra due amministrazioni presidenziali. La questione fondamentale era se l'uso di Phantom negli Stati Uniti fosse in contrasto con le leggi sulle intercettazioni. Il dibattito è continuato fino all'estate 2021, quando l'Fbi ha deciso di non usare gli strumenti dell'Nso. È stato più o meno allora che un consorzio di mezzi d'informazione chiamato Forbidden Stories ha pubblicato nuove rivelazioni sulle armi informatiche dell'Nso e sul loro uso contro giornalisti e dissidenti. Oggi il sistema Pegasus si trova, spento, nell'edificio del New Jersey. A novembre del 2021 gli Stati Uniti hanno annunciato quello che è sembrato – almeno a chi era a conoscenza dei rapporti precedenti – un voltafaccia nei confronti dell'Nso. Il dipartimento del commercio ha inserito l'azienda israeliana nella sua lista nera per attività "contrarie alla sicurezza nazionale o agli interessi di politica estera degli Stati Uniti". Nella lista, chiamata *entity list* e creata per impedire alle aziende statunitensi di avere rapporti commerciali con nazioni o altri soggetti potenzialmente impegnati a fabbricare armi di distruzione di massa, negli ultimi anni sono finiti vari produttori di armi informatiche. L'Nso non poteva più comprare dagli statunitensi componenti fondamentali per i suoi sistemi.

È stato uno schiaffo pubblico a un'azienda che sotto molti aspetti è il fiore all'occhiello dell'industria della difesa israeliana. Senza più accesso alle tecnologie statunitensi – tra cui i computer Dell e i server online di Amazon – l'Nso rischia di non riuscire ad andare avanti. Gli Stati Uniti hanno comunicato la notizia al ministro della difesa israeliano meno di un'ora prima che fosse resa pubblica. I funzionari israeliani erano furiosi. Molti titoli di giornale si sono concentrati sullo spauracchio di un'azienda privata fuori controllo, che ha sede in Israele ma è finanziata quasi completamente all'estero. Le autorità israeliane, però, hanno reagito come se si trattasse di un attacco allo stato. "Chi si lancia contro l'Nso in realtà punta alla bandiera bianca e azzurra che sventola alle sue spalle", ha detto Yigal Unna, fino al 5 gennaio di quest'anno direttore generale della direzione nazionale informatica di Israele.

La rabbia degli israeliani era in parte motivata dall'ipocrisia statunitense: il divieto è arrivato dopo anni di sperimentazioni segrete dei prodotti dell'Nso all'interno dei confini statunitensi e dopo che la Cia li ha messi in mano ad almeno un paese, il Gibuti, con precedenti per violazioni dei diritti umani. Ma Israele aveva anche i suoi interessi da tutelare. Grazie al sistema di concessione delle licenze per l'esportazione, il governo ha l'ultima parola sui soggetti a cui l'Nso può vendere il suo *spyware*. Da anni, quindi, l'azienda è un elemento centrale della strategia di sicurezza nazionale israeliana, che l'ha usata, insieme ad altre imprese del settore, per promuovere i suoi interessi nel mondo.

La combinazione tra il desiderio di

Da sapere Vicino alla Russia

◆ Alla fine di marzo del 2022 un'inchiesta congiunta del quotidiano britannico **The Guardian** e dello statunitense **The Washington Post** ha rivelato che Israele ha impedito all'Ucraina di comprare il software di spionaggio Pegasus dell'azienda Nso per timore di irritare la Russia. "La rivelazione permette di capire il modo in cui le relazioni tra Israele e la Russia a volte hanno compromesso le capacità offensive dell'Ucraina, andando contro le priorità degli Stati Uniti", scrive il Guardian. Il presidente ucraino Volodymyr Zelenskyj ha criticato la posizione assunta da Israele in seguito all'invasione russa dell'Ucraina cominciata il 24 febbraio. In un videomessaggio trasmesso al parlamento israeliano il 19 marzo ha detto che Tel Aviv avrebbe dovuto "dare risposte" sul perché non ha fornito armi all'Ucraina né applicato sanzioni alla Russia. Alcune persone che conoscono direttamente la vicenda sostengono che almeno fin dal 2019 i funzionari israeliani avevano fatto pressione sul loro governo per convincerlo a concedere la licenza all'Ucraina per l'uso del software di spionaggio. Ma le richieste sono state respinte e l'Nso non ha mai ricevuto il permesso di vendere Pegasus a Kiev.

"Secondo gli esperti, Israele ha motivi politici per restare vicino alla Russia", scrive ancora il Guardian. "Tra questi ci sono la sua dipendenza dalla Russia per lanciare attacchi alle postazioni iraniane in Siria e le speranze che Mosca si astenga dal firmare il ripristino dell'accordo quasi raggiunto a Vienna sul nucleare iraniano".

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 5 / 10
www.datastampa.it

ODED BALILTY (AP)/GETTY IMAGES)

L'ex premier israeliano Benjamin Netanyahu insieme al primo ministro indiano Narendra Modi a Tel Aviv. Israele, 6 luglio 2017

Israele di far valere la sua influenza e la fame di profitti dell'Nso ha avuto anche l'effetto di mettere Pegasus nelle mani di una nuova generazione di leader nazionalisti in tutto il mondo. Anche se la supervisione del governo israeliano avrebbe dovuto impedire che fosse usato dai governi contro dissidenti e oppositori, Pegasus è stato venduto a Polonia, Ungheria e India, nonostante i loro precedenti discutibili sui diritti umani.

Una nuova industria

Gli Stati Uniti hanno fatto i loro calcoli, comprando, testando e usando in segreto la tecnologia dell'Nso, anche se pubblicamente la denunciavano e cercavano di limitare il suo accesso alle aziende statunitensi. L'attuale resa dei conti tra gli Stati Uniti e Israele dimostra come i governi considerino sempre di più le armi informatiche allo stesso modo in cui in passato consideravano i mezzi militari come gli aerei caccia e le centrifughe per il nucleare: non solo strumenti fondamentali per la difesa nazionale ma anche moneta di scambio con cui conquistare influenza nel mondo.

Vendere armi è sempre stato uno strumento della diplomazia dei governi. I funzionari delle ambasciate statunitensi nel mondo hanno fatto per anni da intermediari tra le aziende della difesa americane e gli altri paesi, come dimostrano migliaia di documenti diffusi da WikiLeaks nel 2010. Quando i segretari della difesa degli Stati Uniti incontrano i colleghi stranieri nelle capitali alleate, spesso il risultato è l'annuncio di un accordo sulla fornitura di armi che aumenta i profitti di aziende come la Lockheed Martin o la Raytheon.

Dopo la bomba atomica, le armi informatiche sono la tecnologia che ha cambiato in modo più profondo le relazioni internazionali. Per certi versi sono ancora più destabilizzanti del nucleare: sono relativamente economiche, facili da comprare e possono essere usate senza conseguenze per chi attacca. La loro diffusione sta cambiando radicalmente la natura delle relazioni tra stati, come Israele ha scoperto da tempo e il resto del mondo comincia a capire ora.

Tel Aviv ha sempre considerato il traffico di armi fondamentale per la sopravvivenza della nazione. È stato un fattore centrale di crescita economica, che a sua volta ha finanziato attività di ricerca e sviluppo in campo militare e ha avuto un ruolo importante nel costruire nuove alleanze in un mondo pieno di pericoli. Dalla metà degli anni ottanta Israele si è imposto come uno dei primi esportatori di armi al mondo, con circa un lavoratore su dieci impegnato a vario titolo nel settore. Questo ha permesso al governo israeliano di avere il sostegno di alcuni leader stranieri che consideravano gli aiuti militari essenziali per mantenere il loro potere. In cambio, questi paesi hanno spesso votato a favore di Israele all'assemblea generale e al Consiglio di sicurezza delle Nazioni Unite e in altre organizzazioni internazionali, oltre a permettere al Mossad (l'agenzia per la sicurezza esterna) e alle forze armate israeliane di usare i loro territori come base per lanciare operazioni contro gli stati arabi.

Quando negli schemi degli strateghi militari le armi informatiche hanno cominciato a oscurare gli aerei, in Israele è nata una nuova industria delle armi. I reduci dell'unità 8200 – che, all'interno delle forze armate israeliane, si occupa di spionaggio – sono entrati in misteriose

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 6 / 10
www.datastampa.it

JESUS HELLIN (EUROPA PRESS/AP/LAPRESSE)

Il presidente della Catalogna Pere Aragonès parla ai giornalisti a Madrid. Spagna, 21 aprile 2022

startup private, alimentando un'industria multimiliardaria della sicurezza informatica. Come con le armi convenzionali, però, i produttori di quelle informatiche devono ottenere la licenza dal ministero della difesa per vendere i prodotti all'estero. Così il governo ha una leva fondamentale per influenzare le aziende e, in alcuni casi, i paesi compratori.

Senza permesso

Nessuna di queste aziende è stata commercialmente fortunata o strategicamente utile al governo israeliano come l'Nso. La sede è stata aperta in un ex allevamento avicolo a Bnai Zion, una cooperativa agricola alle porte di Tel Aviv. A metà degli anni duemila il proprietario dello stabile, rendendosi conto che gli sviluppatori informatici avrebbero reso più delle galline, ristrutturò lo spazio e cominciò ad affittarlo ad aziende tecnologiche in cerca di uffici a buon mercato. Tra i fondatori di startup si distingueva Shalev Hulio: carismatico e affabile, dava l'impressione – almeno all'inizio – di essere un po' ingenuo. Lui e il socio Omri Lavie, un ex compagno di scuola, avevano svolto il servizio militare obbligatorio in un'unità di combattimento e per anni avevano avuto difficoltà a creare un prodotto vincente. Avevano sviluppato un sistema per il video marketing che era partito bene ma si era schiantato con la recessione del 2008. Poi avevano fondato la CommuniTake, un'azienda che produceva strumenti in grado di consentire agli addetti all'assistenza di prendere il controllo a distanza dei telefoni dei clienti, con il loro permesso.

Visto lo scarso entusiasmo con cui fu accolta l'idea, i due amici decisero di rivolgersi a un mercato molto diverso. "Un'agenzia d'intelligence europea mi contattò", racconta Hulio in un'intervista. Presto si scoprì che il loro prodotto era in grado di risolvere un problema ben più grande di quelli affrontati dal servizio clienti.

Per anni i servizi di sicurezza erano stati in grado d'intercettare e leggere le comunicazioni, ma con la diffusione dei sistemi avanzati di crittografia non ci riuscivano più. Anche quando intercettavano un messaggio, non erano in grado di decifrare il contenuto. Ma se avessero controllato telefoni e computer, avrebbero potuto raccogliere i dati prima che fossero criptati. La CommuniTake aveva già scoperto come farlo. Quello che serviva ai due soci era trovare il modo per riuscirci senza il permesso del proprietario del dispositivo.

Così è nata l'Nso. Hulio e Lavi, non avendo i contatti necessari per provare il prodotto sul mercato, hanno coinvolto un terzo socio, Niv Karmi, che aveva lavorato nell'intelligence militare e nel Mossad. Hanno chiamato l'azienda Nso usando le iniziali dei loro nomi – il fatto che suonasse un po' come l'agenzia per la sicurezza nazionale statunitense Nsa era una fortunata coincidenza – e hanno cominciato ad assumere personale. La selezione era un punto fondamentale del piano aziendale. Oggi l'Nso ha più di settecento dipendenti nel mondo e una gigantesca sede centrale a Herzliya, dove i laboratori dedicati ai sistemi operativi Apple e Android sono pieni di smarphone che gli hacker testano costantemente per cercare e sfruttare nuovi punti deboli.

Quasi tutti i componenti della squadra di ricerca dell'Nso sono veterani dei servizi di sicurezza. La maggior parte ha fatto parte dell'Aman, la più grande agenzia d'intelligence israeliana, e molti dell'unità 8200, interna all'Aman. I più qualificati

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 7 / 10
www.datastampa.it

hanno frequentato corsi di formazione di alto livello, tra cui un riservato e prestigioso programma dell'unità 8200 chiamato Aram, che accetta solo poche reclute e le forma con i metodi più avanzati per programmare armi informatiche. Tutti questi ingegneri lavorano ogni giorno alla ricerca dei cosiddetti *zero days*, punti deboli ancora sconosciuti nei software dei telefoni che possono essere sfruttati per installare Pegasus.

Come una magia

Nel 2011 gli ingegneri dell'Nso hanno finito di programmare la prima versione di Pegasus. Con il nuovo strumento, l'azienda sperava di costruirsi rapidamente una base di clienti in occidente. Molti paesi, però, soprattutto in Europa, erano contrari a comprare prodotti d'intelligence stranieri. Le preoccupazioni riguardavano soprattutto le aziende israeliane, in cui erano impiegati molti ex alti funzionari dei servizi di sicurezza: i potenziali clienti temevano che i loro software potessero contenere *spyware* nascosti, dando così al Mossad l'accesso ai loro sistemi.

La reputazione era importante, per le vendite e per non farsi sfuggire i programmatori più preparati. Hulio nominò presidente dell'Nso il generale Avigdor Ben-Gal, sopravvissuto all'olocausto e stimato ufficiale delle forze di combattimento, e fissò quelli che sarebbero stati i quattro capisaldi dell'azienda: l'Nso si sarebbe limitata a vendere il prodotto senza mai incaricarsi della sua gestione; lo avrebbe venduto solo a governi e non a individui o aziende; avrebbe selezionato i governi a cui concedere l'uso del software; e avrebbe collaborato con la Deca, l'agenzia del ministero della difesa israeliano incaricata di rilasciare le licenze di vendita.

Quest'ultima decisione ha fatto dell'Nso un alleato stretto, se non addirittura un'appendice, della politica estera israeliana. Per Ben-Gal era una condizione fondamentale per la crescita dell'azienda: avrebbe ristretto il numero di paesi a cui vendere, ma l'avrebbe anche tutelata da eventuali contraccolpi negativi causati alle azioni dei suoi clienti. Quando informò il ministero della difesa che l'Nso si sarebbe volontariamente sottoposta a vigilanza, le autorità sembravano contente. Un ex consulente militare di Benjamin Netanyahu, all'epoca primo ministro israeliano, spiegò chiaramente i vantaggi della situazione: "Con il ministro della difesa seduto al posto di comando potremo controllare i movimenti di questi sistemi, sfruttarli a nostro beneficio e trarne vantaggi diplomatici".

Tra i fondatori di startup si distingueva Shalev Hulio: carismatico e affabile, dava l'impressione – almeno all'inizio – di essere un po' ingenuo

Poco dopo l'azienda ottenne la sua prima grande commessa. Il Messico, impegnato in una decennale battaglia contro i cartelli della droga, stava cercando il modo di intercettare messaggi cifrati dei telefoni BlackBerry usati dai narcotrafficanti. La Nsa era riuscita a entrare nei dispositivi, ma poteva garantire al Messico solo un accesso sporadico. Hulio e Ben-Gal organizzarono un incontro con il presidente messicano, che all'epoca era Felipe Calderón: Pegasus poteva fare la stessa cosa dell'Nsa, assicurando il controllo totale alle autorità messicane. Calderón era interessato.

Il ministero della difesa israeliano informò l'Nso che poteva vendere Pegasus al governo messicano e l'accordo fu concluso. Poco dopo gli agenti del Centro per l'investigazione e la sicurezza nazionale messicano (Cisen, ora chiamato Centro per l'investigazione nazionale) cominciarono a lavorare con una delle macchine Pegasus. Inserirono nel sistema il numero di telefono di una persona collegata al cartello di Sinaloa di Joaquín Guzmán e riuscirono a entrare nel BlackBerry. Gli investigatori potevano vedere il contenuto dei messaggi e la posizione di vari telefoni. "Improvvisamente abbiamo ricominciato a vedere e a sentire", racconta un ex responsabile del Cisen, "sembrava una magia". Il nuovo strumento aveva rilanciato l'intera operazione: "Per la prima volta sentivamo di poter vincere".

Opportunità e rischi

Era una vittoria anche per Israele. Il Messico è una delle principali potenze in America Latina, una regione in cui Israele ha combattuto per anni una specie di guerra di trincea diplomatica contro i gruppi anti-israeliani sostenuti dai suoi avversari in Medio Oriente. Non ci sono prove dirette che i contratti del Messico con l'Nso abbiano fatto cambiare la politica estera del paese nei confronti d'Israele, ma c'è sicuramente una correlazione. Dopo una lunga tradizione di voti contrari a Israele alle conferenze dell'Onu, il Messico ha cominciato ad astenersi. Nel 2016 Enrique Peña Nieto, subentrato a Calderón nel 2012, è andato in Israele, che non riceveva una visita ufficiale da un presidente messicano dal 2000. L'anno dopo Netanyahu è andato a Città del Messico, la prima volta di un premier israeliano. Poco dopo il Messico ha annunciato che si sarebbe astenuto su varie risoluzioni a favore della Palestina esaminate dall'Onu.

In una dichiarazione il portavoce di Netanyahu ha precisato che l'ex primo ministro non ha mai cercato contropartite dai paesi che avevano comprato Pegasus.

L'esempio del Messico mette in luce le opportunità e i rischi di lavorare con l'Nso. Nel 2017 i ricercatori di Citizen Lab, un gruppo che si occupa di sicurezza informatica e diritti umani all'università di Toronto, in Canada, hanno rivelato che le autorità messicane, impegnate in una campagna contro gli attivisti, i movimenti e i giornalisti di opposizione, avevano usato Pegasus per violare gli account dei promotori di una tassa sulle bevande gassate. Cosa ancora più inquietante, alcuni fun-

Da sapere Dalla Spagna al Regno Unito

◆ Un rapporto pubblicato il 18 aprile 2022 da **Citizen Lab**, un centro di ricerca che si occupa di sicurezza informatica e diritti umani all'università di Toronto, in Canada, ha rivelato che almeno 63 politici e personalità della società civile legate al movimento indipendentista catalano sono state spiate attraverso il software Pegasus tra il 2017 e il 2020. Il presidente catalano Pere Aragonès, tra le persone prese di mira, ha annunciato la sospensione di ogni collaborazione con il governo spagnolo finché non avrà fornito chiarimenti. Madrid ha negato ogni accusa. Citizen Lab ha svelato anche che tra il 2020 e il 2021 ha avvertito il governo britannico che Pegasus potrebbe essere stato usato per controllare utenze nell'ufficio del primo ministro e in quello degli affari esteri. Nel primo caso la sospetta intrusione sarebbe riconducibile a qualcuno legato agli Emirati Arabi Uniti. Nel secondo, oltre ad Abu Dhabi, sono stati indicati come paesi coinvolti anche India, Cipro e Giordania. Il 19 aprile il parlamento europeo ha annunciato che sarà costituita una commissione d'inchiesta per scoprire se l'uso di strumenti di spionaggio ha violato le normative e i diritti fondamentali dell'Unione. **The Guardian, Citizen Lab**

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 8 / 10
www.datastampa.it

zionari del governo avrebbero usato Pegasus per spiare gli avvocati che indagavano sull'uccisione di 43 studenti avvenuta a Iguala nel 2014.

Tomás Zerón de Lucio, il capo dell'agenzia messicana per la sicurezza interna, è stato tra gli autori dell'inchiesta del governo sul massacro, che ne attribuisce la responsabilità a una gang locale. Nel 2016, però, Zerón è stato indagato perché sospettato di aver coperto il coinvolgimento del governo nella vicenda. Per farlo si sarebbe servito di Pegasus: uno dei suoi compiti, infatti, era autorizzare l'acquisto di armi informatiche e altri materiali. Nel marzo 2019, poco dopo la vittoria del progressista Andrés Manuel López Obrador alle elezioni presidenziali, gli inquirenti hanno accusato Zerón di tortura, sequestro e inquinamento delle prove in relazione al massacro di Iguala. Zerón è scappato in Canada e poi in Israele, dov'è entrato con un visto turistico e ancora risiede nonostante la richiesta di estradizione del Messico, che ora lo accusa anche di appropriazione indebita.

Cordialità e alleanze

L'Nso ha raddoppiato i ricavi ogni anno: quindici milioni di dollari, trenta milioni, sessanta milioni. Questa crescita ha attirato l'attenzione degli investitori. Nel 2014 la Francisco Partners, una società internazionale di investimenti con sede negli Stati Uniti, ha comprato il 70 per cento delle azioni dell'Nso per 130 milioni di dollari e poi ha permesso la fusione con un'altra azienda di armi informatiche israeliana chiamata Circles. Fondata da un ex alto funzionario dell'Aman, la Circles produceva un software capace d'identificare la posizione di qualsiasi telefono nel mondo, sfruttando un punto debole scoperto dieci anni prima dall'intelligence israeliana. Dopo la fusione, quindi, l'azienda era in grado di offrire una gamma di servizi ancora più grande a un numero sempre maggiore di clienti.

Attraverso una serie di nuovi accordi commerciali, Pegasus ha contribuito a unire una nuova generazione di leader di destra in tutto il mondo.

Nel luglio 2017 Narendra Modi, eletto in India sulla base di un programma nazionalista hindu, è stato il primo capo di governo indiano a visitare Israele. Per decenni l'India aveva avuto una politica di sostegno alla causa palestinese e i rapporti con Israele erano gelidi. La visita di Modi, invece, è stata particolarmente cordiale, con tanto di passeggiata sulla spiaggia con Netanyahu a favore di telecamera. Dietro alla gentilezza c'era un motivo. I due paesi avevano appena concluso un accordo per la vendita di un pacchetto di armi e sistemi d'intelligence per un valore di circa due miliardi di dollari, il cui pezzo forte erano Pegasus e un sistema missilistico. Qualche mese dopo Netanyahu è andato in India per una rara visita di stato. Nel giugno 2019 l'India ha votato per la prima volta a sostegno d'Israele al consiglio economico e sociale dell'Onu, negando lo status di osservatore a un'organizzazione palestinese per i diritti umani.

Il ministero della difesa israeliano ha concesso all'Nso la licenza per vendere Pegasus anche in Ungheria, nonostante la campagna del primo ministro Viktor Orbán contro gli oppositori politici. Nel 2020 l'Ungheria è stata tra i pochi paesi a non condannare pubblicamente il piano israeliano di annessione unilaterale di parti della Cisgiordania. Nel maggio di quell'anno i ministri degli esteri dell'Unione europea hanno provato a raggiungere l'unanimità su un cessate il fuoco tra Israele e il gruppo islamico palestinese Hamas, e su un aumento degli aiuti umanitari a Gaza. L'Ungheria si è rifiutata di allinearsi agli altri ventisei paesi.

Probabilmente, però, le alleanze più preziose favorite da Pegasus sono state quelle tra Israele e i vicini arabi. Tel Aviv ha autorizzato la vendita del sistema agli Emirati Arabi Uniti come una sorta di ramoscello di ulivo dopo che nel 2010 il Mossad aveva avvelenato un dirigente di Hamas in un albergo a Dubai. Nel 2013 è stata offerta a Mohammed bin Zayed, il principe ereditario e leader di fatto del paese, detto Mbz, l'opportunità di comprare Pegasus. Mbz ha subito accettato. Gli Emirati non hanno esitato a usarlo contro i nemici interni.

Ahmed Mansoor, un blogger critico verso il governo, si è lamentato pubblicamente dopo che Citizen Lab aveva accertato che Pegasus era stato usato per violare il suo telefono. La sua email era stata violata, i suoi spostamenti sorvegliati. Inoltre, gli avevano ritirato il passaporto e rubato la macchina e 140mila dollari dal conto in banca, era stato licenziato e picchiato varie volte da sconosciuti per strada. "Cominci a pensare di essere osservato appena ti muovi", ha detto all'epoca. "Anche i tuoi familiari vanno nel panico". Nel 2018 Mansoor è stato condannato a dieci anni di carcere per dei post pubblicati su Facebook e Twitter.

Attraverso una serie di nuovi accordi commerciali, Pegasus ha contribuito a unire una nuova generazione di leader di destra

Dietro le quinte

Israele e gli Emirati si stavano avvicinando da anni. Le ostilità storiche tra Tel Aviv e il mondo arabo, che avevano influenzato a lungo la politica mediorientale, avevano ceduto il passo a una nuova precaria alleanza nella regione: Israele e gli stati sunniti del Golfo si erano allineati contro il loro acerrimo nemico, l'Iran a maggioranza sciita.

Nessun leader rappresenta meglio questa situazione di Mohammed bin Salman, detto Mbs, principe ereditario dell'Arabia Saudita, figlio del re Salman bin Abdulaziz e sovrano di fatto del regno. Nel 2017 le autorità israeliane hanno deciso di autorizzare la vendita di Pegasus a un servizio di sicurezza sotto la supervisione del principe. Un gruppo ristretto di alti funzionari della difesa israeliana, in contatto diretto con Netanyahu, ha assunto un ruolo chiave negli scambi con i sauditi, "prendendo molte precauzioni", secondo un esponente del governo israeliano coinvolto nella vicenda. L'obiettivo era assicurarsi il sostegno e la gratitudine del principe. Il contratto, che prevedeva una commissione iniziale per l'installazione di 55 milioni di dollari, è stato firmato nel 2017.

Anni prima, l'Nso aveva istituito un comitato etico composto da un gruppo bipartisan di ex funzionari del ministero degli esteri degli Stati Uniti incaricati di fare verifiche sui potenziali clienti. Dopo l'omicidio di Khashoggi nel 2018, il comitato si è riunito d'urgenza per decidere come rispondere alle voci di un coinvolgimento dell'Nso. Hulio ha negato che Pegasus fosse stato usato per spiare l'editorialista del Washington Post. I sistemi di Pegasus tengono traccia di tutte le operazioni nel caso in cui ci sia un reclamo e l'Nso, con il consenso del cliente, può esaminarle. Hulio sostiene che il suo personale ha analizzato i registri sauditi e ha riscontrato che nessun prodotto della Nso è

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 9 / 10
www.datastampa.it

TOM BRENNER (REUTERS/CONTRASTO)

Benjamin Netanyahu e Donald Trump, all'epoca in cui erano primo ministro d'Israele e presidente degli Stati Uniti, con i ministri degli esteri del Bahrein e degli Emirati. Washington, Stati Uniti, 15 settembre 2020

stato usato contro Khashoggi. Su indicazione del comitato, l'azienda ha comunque deciso di bloccare il sistema Pegasus in Arabia Saudita. Successivamente il governo israeliano ne ha chiesto la riattivazione, ma l'Nso, sempre su indicazione del comitato, l'ha negata.

Nel 2019, però, l'azienda è tornata sui suoi passi. D'accordo con Hulio, il fondo d'investimento privato britannico Novalpina ha rilevato le quote della Nso in possesso della Francisco Partners per un miliardo di dollari, una cifra cinque volte più grande di quella pagata dal fondo statunitense nel 2014. All'inizio del 2019 l'Nso ha accettato di riattivare il sistema Pegasus in Arabia Saudita. Accontentare i sauditi era importante per Netanyahu. Il primo ministro stava conducendo un'iniziativa diplomatica segreta che avrebbe dovuto rafforzare la sua immagine di statista: un riavvicinamento ufficiale tra Israele e diversi stati arabi. Nel settembre 2020 Netanyahau, Donald Trump (all'epoca presidente degli Stati Uniti) e i ministri degli esteri degli Emirati e del Bahrein hanno sottoscritto gli accordi di Abramo, salutati da tutti i firmatari come l'inizio di una nuova epoca di pace nella regione.

Dietro le quinte, però, c'era un bazar delle armi. L'amministrazione Trump aveva accettato di ribaltare le precedenti strategie politiche statunitensi e vendere caccia F-35 e droni armati Reaper agli Emirati e da settimane cercava di rassicurare Israele, preoccupato di non essere più l'unico stato dotato di F-35 nella regione. In un'intervista successiva, Mike Pompeo ha definito l'accordo sugli aerei da guerra "cruciale" per ottenere il consenso di Mbz. Al momento dell'annuncio degli accordi, Israele aveva già concesso la licenza per vendere Pegasus in quasi tutti i paesi firmatari. Un mese dopo c'è stato il primo intoppo: la licenza per l'esportazione in Arabia Saudita era scaduta e il ministero della difesa israeliano doveva decidere se rinnovarla. Citando l'uso improprio di Pegasus, il governo ha deciso di no. Senza la licenza, l'Nso non poteva più garantire la manutenzione ordinaria del software e il sistema si stava inceppando. Una serie di chiamate tra i collaboratori di Mbs, i dirigenti dell'Nso, il Mossad e il ministero della difesa israeliano non ha risolto il problema.

Allora Mbs ha chiesto di poter parlare al telefono con Netanyahu, dicono persone vicine alla vicenda. Mbs aveva argomenti convincenti. Suo padre, re Salman, non aveva firmato ufficialmente gli accordi di Abramo, ma aveva dato la tacita benedizione agli altri firmatari. Aveva anche acconsentito a una parte cruciale dell'accordo: l'uso dello spazio aereo saudita, per la prima volta nella storia, agli aerei israeliani diretti a est verso il golfo Persico. Se i sauditi avessero cambiato idea su questo punto, una parte fondamentale dell'accordo rischiava di saltare.

Netanyahu, a quanto pare, non era stato aggiornato sulla crisi in corso, ma dopo la conversazione con Mbs il suo ufficio ha subito ordinato al ministero della difesa di risolvere il problema. Quella sera un funzionario del ministero ha chiamato la sala operativa dell'Nso chiedendo di riattivare il sistema saudita, ma in mancanza di una licenza firmata, il responsabile ha respinto la richiesta. Saputo che l'ordine arrivava da Netanyahu, il dipendente dell'Nso si è fatto bastare un'email del ministero della difesa. Poco dopo Pegasus è tornato in

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 05/2020: 160.000
Diffusione: n.d.
Lettori: n.d.
Settimanale - Ed. nazionale

Internazionale

Dir. Resp.: Giovanni De Mauro

29-APR-2022
da pag. 1-50 /
foglio 10 / 10
www.datastampa.it

funzione. La mattina seguente un corriere del ministero è andato alla sede dell'Nso per consegnare una licenza con timbro e sigillo.

Nel dicembre 2021, quando l'Nso era da poco finita sulla lista nera statunitense, il consigliere per la sicurezza nazionale statunitense Jake Sullivan è arrivato in Israele per un incontro con le autorità su una delle grandi priorità della politica estera dell'amministrazione Biden: un nuovo patto sul nucleare con l'Iran a tre anni dal ritiro dall'accordo deciso da Trump. C'era però un'altra questione di cui le autorità israeliane – compresi il premier, il ministro della difesa e quello degli esteri – volevano discutere: il futuro dell'Nso. Gli israeliani hanno chiesto a Sullivan quali fossero i motivi della decisione di mettere l'azienda nella lista nera. L'hanno anche avvertito che in caso di fallimento dell'Nso, la Russia e la Cina avrebbero riempito il vuoto per aumentare la loro influenza, vendendo i loro sistemi di hackeraggio ai paesi che non potevano più comprare da Israele.

Yigal Unna, ex capo della direzione nazionale informatica di Israele, è convinto che il provvedimento contro le aziende israeliane, seguito da uno simile preso da Facebook, sia parte di un piano per neutralizzare il vantaggio di Israele sulle armi informatiche: "Dobbiamo prepararci a una battaglia per difendere il buon nome che ci siamo guadagnati onestamente". I funzionari dell'amministrazione Biden smentiscono questa ipotesi complottistica, spiegando che la decisione sull'Nso è stata presa unicamente per tenere a freno un'azienda ritenuta pericolosa e non ha niente a che fare con le relazioni tra Stati Uniti e Israele. Nell'alleanza decennale tra i due paesi, dicono, ci sono in ballo cose più importanti delle sorti di un'azienda informatica.

Mantenere il controllo

Ora però il futuro dell'Nso è a rischio, non solo perché i suoi sistemi dipendono dalle tecnologie statunitensi, ma anche perché la presenza nella lista nera rischia di scoraggiare potenziali clienti (e dipendenti). Un esperto israeliano del settore dice che "gli squali in acqua sentono l'odore del sangue" e secondo diversi funzionari e manager israeliani ci sono varie aziende statunitensi, alcune legate ai servizi di sicurezza, interessate a comprare l'Nso. Se così fosse, la nuova proprietà potrebbe rimettere l'azienda in linea con le normative statunitensi e vendere i prodotti alla Cia, all'Fbi e ad altre agenzie statunitensi disposte a pagare per il potere offerto da quest'arma.

Facebook sostiene di avere le prove che almeno un numero di telefono con un prefisso dell'area di Washington è stato attaccato

Le autorità israeliane temono una scalata strategica all'Nso che metta qualche altra azienda – o paese – nella condizione di decidere come e dove l'arma sia usata. "Lo stato d'Israele non può permettersi di perdere il controllo di questo tipo di aziende", ha detto un alto funzionario israeliano, spiegando perché ritiene improbabile una soluzione simile. "Pensiamo alla manodopera, alle competenze sviluppate". Una proprietà straniera può andar bene, ma Israele deve poter mantenere il controllo. Una cessione è possibile "solo a condizione che siano salvaguardati gli interessi e la libertà d'azione d'Israele".

Ma i giorni del quasi-monopolio israeliano sono finiti o lo saranno presto. La fame di armi informatiche di Washington non è passata inosservata ai potenziali concorrenti statunitensi dell'Nso. Nel gennaio 2021 la Boldend, un'azienda del settore, ha fatto una proposta commerciale al colosso della difesa Raytheon. Secondo una presentazione vista dal New York Times, l'azienda ha già sviluppato per diverse agenzie governative statunitensi un arsenale di armi capaci di attaccare telefoni e altri dispositivi.

Una schermata della presentazione in particolare evidenzia la natura contorta del commercio delle armi informatiche. La Boldend, si legge, aveva trovato un modo per hackerare WhatsApp, il popolare servizio di messaggistica di proprietà di Facebook, ma non ci riusciva più dopo un aggiornamento dell'app. È un particolare interessante perché, secondo un'altra schermata, uno dei principali investitori della Boldend è il Founders Fund, di proprietà del miliardario Peter Thiel, uno dei primi investitori di Facebook e ancora oggi un suo consigliere d'amministrazione. Il governo degli Stati Uniti "non dispone attualmente delle capacità" di violare WhatsApp, sostiene la presentazione, e i servizi di sicurezza sono interessati a comprare gli strumenti per farlo.

Nell'ottobre 2019 WhatsApp ha fatto causa all'Nso, sostenendo che l'azienda aveva sfruttato un punto debole presente nel suo sistema per attaccare 1.400 telefoni nel mondo. Oltre a chi controlla il sistema, al centro del procedimento c'è la questione di chi è responsabile dei danni causati. L'Nso si è sempre difesa dicendo che si limita a vendere la sua tecnologia a governi stranieri e che non ha alcun ruolo – né responsabilità – negli attacchi a soggetti specifici. Questa è stata a lungo la classica linea difensiva dei produttori di armi.

Facebook è determinata a dimostrare che queste affermazioni, almeno nel caso dell'Nso, sono false. Il colosso tecnologico sostiene che l'Nso è stata parte attiva in alcuni degli attacchi informatici, tanto da aver noleggiato alcuni dei server usati per violare gli account di WhatsApp. La tesi di Facebook è che senza il coinvolgimento dell'Nso, molti dei suoi clienti non sarebbero stati in grado di prenderla di mira.

I legali di Facebook pensavano di avere le prove per confutare una delle tradizionali linee di difesa dell'azienda israeliana, e cioè che il governo d'Israele vieta all'azienda di mettere sotto attacco qualsiasi utenza telefonica in territorio statunitense. Secondo gli atti processuali, Facebook ha affermato di avere le prove che almeno un numero di telefono con un prefisso dell'area di Washington era stato attaccato. Chiaramente qualcuno stava usando il software dell'Nso per spiare un numero di telefono statunitense.

Ma il colosso tecnologico non aveva il quadro completo. Evidentemente non sapeva che l'attacco al numero di telefono statunitense non era un'aggressione di una potenza straniera ma parte della dimostrazione all'Fbi di Phantom, il sistema progettato dall'Nso per i servizi di sicurezza statunitensi che avrebbe dovuto trasformare i telefoni degli americani in una "miniera d'oro d'informazioni". ◆ *fs*

GLI AUTORI

Ronen Bergman scrive per il New York Times Magazine da Tel Aviv, è l'autore di *Rise and kill first: the secret history of Israel's targeted assassinations* (Random House 2018). **Mark Mazzetti** è il corrispondente da Washington del New York Times, ha vinto due volte il premio Pulitzer per le inchieste a cui ha partecipato.