Acquirente fai attenzione: l'impresa israeliana che aiuta i governi a spiare i loro stessi cittadini

Richard Silverstein ,martedì 22 agosto 2017, Middle East Eye

Consentendo ai governi di violare i telefoni dei loro cittadini, un'azienda israeliana di sicurezza informatica ha presumibilmente reso il mondo più pericoloso per gli attivisti a favore dei diritti umani che lottano contro l'impunità delle imprese e degli Stati.

Dato che negli ultimi anni gli smartphone si sono moltiplicati e sono diventati un mezzo di comunicazione indispensabile per tutti noi, si sono moltiplicate anche le nuove aziende che si dedicano a violare questi telefoni a favore di governi – compresi i servizi militari, dello spionaggio e della polizia.

I clienti di queste imprese innovative utilizzano la nuova tecnologia per sorvegliare criminali e terroristi, per individuare e far fallire i loro piani. Questo è un uso legittimo. Ma ce ne sono altri che sono molto più redditizi per le imprese – e molto meno accettabili per le società democratiche.

Prendiamo per esempio l'attivista per i diritti umani degli Emirati [Arabi Uniti] Ahmed Mansoor. Nell'agosto 2016 ha ricevuto un messaggio ingannevole [phishing message] che sembrava provenire da una fonte fidata. Ma si è insospettito ed ha immediatamente inviato il suo telefono a "Citizen's Lab" [Laboratorio del Cittadino, centro studi interdisciplinare che si occupa del controllo sulle informazioni, ndt.] dell'università di Toronto per un'analisi forense.

Da questa verifica è risultato che le autorità degli Emirati si erano procurate "Pegasus", il più potente programma di malware [sistemi usati per apportare modifiche indesiderate ad un apparecchio informatico, ndt.] mai creato che si possa trovare sul mercato e venduto dall'azienda israeliana "NSO Group".

Se Mansoor avesse aperto il link, esso avrebbe preso il controllo del suo telefono

e consentito alla polizia di accedere non solo a tutto quanto vi si trovava (email, contatti e messaggi di testo, per esempio), ma anche alla macchina fotografica, al video e all'audio. La polizia avrebbe sentito e visto tutto quello che faceva e sarebbe stata in grado di prevenire ogni sua azione.

1. Attacchi di "Pegasus"

In un caso collegato del 2016, le autorità degli EAU hanno anche utilizzato "Pegasus" in un tentativo di intrusione che ha preso di mira il giornalista di MEE Rory Donaghy, che informava in modo critico sui soprusi del regime autocratico del Paese. Nel pieno di un'inchiesta su questo attacco, il "Citizen's Lab" ha scoperto che 1.100 attivisti e giornalisti del regno erano stati presi di mira allo stesso modo e che il governo aveva pagato a "NSO Group" 600.000 dollari per questi tentativi [di intercettazione].

Anche se è un prodotto commerciale, "Pegasus" – come molti altri strumenti simili per lo spionaggio ora sul mercato – è chiaramente anche un mezzo politico che consente a regimi autoritari di spiare i propri cittadini.

Infatti potrei andare anche oltre e dire che "Pegasus" è spesso utilizzato come arma informatica offensiva usata dall'élite mondiale per proteggere i propri interessi e contrastare il legittimo controllo da parte delle Ong e di altre associazioni di attivisti.

"Il governo compra (la tecnologia) e può usarla come vuole," ha detto a "HuffPost" Bill Marczak, un ricercatore di "Citizen's Lab" che ha analizzato molte campagne di controllo che secondo lui sono state condotte con "Pegasus".

"Sono praticamente dei mercanti di armi digitali."

Nelle ultime settimane il gruppo finanziario privato che possiede "NSO Group", valutato oggi 1 miliardo di dollari, ha cercato di vendere la compagnia, sollevando grandi questioni tra gli attivisti dei diritti digitali in merito a se un nuovo investitore ridurrà il sospetto uso del sistema di spionaggio dell'azienda contro dissidenti politici ed attivisti da parte di alcuni governi.

2. Dall’esercito alla tecnologia

Ci sono parecchie imprese che creano questo tipo di software maligni in vari Paesi, ma alcune di quelle di maggior successo sono israeliane.

Ciò è principalmente un risultato della “SIGINT-Unità 8200”, la più numerosa dell’esercito israeliano, che spia i segnali elettromagnetici, monitora, intercetta e sorveglia i nemici di Israele in Medio Oriente e in tutto il mondo.

I suoi ufficiali ricevono l’addestramento più sofisticato nello spionaggio ed uso dei segnali e creano la tecnologia più avanzata per farlo. Quando lasciano il servizio attivo trovano le porte aperte nel mondo tecnologico. Possono avere un lavoro molto ben remunerato nelle grandi imprese o utilizzare le competenze che hanno acquisito nell’esercito per fondare un’azienda innovativa propria.

Alcune delle aziende di maggiore successo includono Waze, Wix, Taboola, NICE Systems, Amdocs, Onavo (acquistata da Facebook per 150 milioni di dollari), Checkpoint, Mirabilis e Verint.

Molti dei progetti riguardano la sicurezza informatica, che è quello che l’ “Unità 8200” è stata costituita per debellare nei suoi tentativi di intercettare le comunicazioni delle forze nemiche di Israele. Alcune iniziative sono concentrate sulla protezione della sicurezza informatica. Questi sono i bravi, o i “cappelli bianchi” nella terminologia degli hacker.

Ma altri continuano lungo la direzione che gli hacker dell’”Unità 8200” perseguono durante il servizio militare: sono destinati ad aggirare le funzioni di sicurezza di vari sistemi.

Forse quella che ha avuto più successo tra queste imprese è “NSO Group” che si trova a Herziliya [importante università privata israeliana in stretti rapporti con i servizi di sicurezza, ndt.], il cui motto è “rendi il mondo un posto più sicuro.” Ma l’azienda ha reso sicuramente il mondo molto più pericoloso per un gran numero di attivisti politici e per i diritti umani che lottano contro l’impunità di imprese e governi.

3. Vulnerabilità da miliardi di dollari

“NSO” è stata fondata nel 2010 da due veterani dell’esercito israeliano, Shalev Hulio and Omri Lavie, che non erano stati nell’“Unità 8200” (nonostante informazioni in contrario). Secondo la rivista israeliana “Globes” [quotidiano di informazioni finanziarie, ndt], Lavie ha fatto il militare nei corpi di artiglieria e Hulio nel servizio di ricerca e soccorso.

Alle scuole superiori né Hulio né Lavie erano studenti particolarmente brillanti e, secondo le informazioni del “Globes”, hanno passato un sacco di tempo insieme sulla spiaggia. Dopo aver lasciato l’IDF, hanno deciso di diventare imprenditori di servizi in rete.

“NSO” è la loro terza e di gran lunga più importante iniziativa imprenditoriale di successo. Secondo i fondatori, la sua nascita è avvenuta per puro caso. Vari clienti avevano chiesto loro se ci fosse un modo per prendere il controllo di un cellulare senza avere accesso fisico all’apparecchio reale.

Benché avessero sentito dire che c’era [questa possibilità], non riuscivano a trovare nessun ingegnere informatico che avesse idea di come farlo, finché un giorno, seduti in un caffè, i due udirono per caso parlarne veterani dell’“Unità 8200”. Così nel 2010, proprio quando gli smartphone stavano per essere trasformati da oggetti per un solo uso in apparecchi quotidiani potenti, multiuso e indispensabili, fondarono “NSO”.

Iniziarono a farsi una clientela tra le forze di polizia di vari Paesi, offrendo la possibilità di spiare criminali sospetti in modi che nessuno aveva mai previsto. Fondarono una succursale per le vendite negli USA, “WestBridge Technologies”, per incentivare la penetrazione commerciale in uno dei loro maggiori mercati potenziali.

Attraverso la “Francisco Partners”, la società di capitale di rischio che nel 2015 ha comprato “NSO”, questa è finita sotto l’egida di un’impresa che possiede una serie di altre compagnie di telecomunicazioni che hanno fornito informazioni sensibili per fare passi avanti nelle possibilità di hackeraggio. Per esempio, “Intelligence Online” [rivista informativa nel campo dell’informatica, ndt.] riporta che Boaz Goldman è presidente del consiglio di amministrazione di “Inno Networks”, che installa reti di comunicazione mobile (3G e 4G). E’ appena entrato nel consiglio di amministrazione di una holding con sede in Lussemburgo che include “NSO Group” in un complicato rapporto finanziario. Questo accordo

d’affari fornisce all’azienda di armi informatiche un accesso diretto a grandi reti (SS7 – Signal System 7) utilizzate per trasmettere testi, email, chiamate telefoniche, dati di geo-localizzazione e chiavi di cifratura.

“NSO” ha anche iniziato a crearsi fonti che gli forniscono accesso a prototipi di modelli di cellulari prima che vengano immessi sul mercato, il che gli permette di fare analisi scientifiche in modo che gli ingegneri di “NSO” possano cercare falle di vulnerabilità che consentano un accesso totale ai telefoni che i loro clienti desiderano prendere di mira.

4. Zona grigia

Si potrebbe pensare che i produttori di telefonini intendano proteggere i propri prodotti come Fort Knox [area militare in cui sono conservate le riserve auree e monetarie degli USA, ndt.] e vietarli agli sguardi loschi di hacker come “NSO”. Ma l’impresa opera in una zona grigia e cerca di garantirsi quello di cui ha bisogno da varie fonti sia all’interno che all’esterno delle industrie produttrici.

Prima dei portatili, i criminali comunicavano nel modo in cui lo facevano tutti: con telefoni fissi, mail o di persona. La tecnologia per intercettare o controllare queste comunicazioni era semplice e primitiva: per i telefoni si usava una “cimice” [microspie per l’ascolto di conversazioni private, ndt.] su una linea telefonica.

La cimice avrebbe dovuto presumibilmente essere approvata da un giudice ed essere messa in funzione con l’aiuto di una compagnia telefonica. C’era un processo di controllo e questo veniva in genere rispettato, almeno nelle società democratiche.

La comunicazione elettronica ha cambiato tutte le regole, aprendo nuove modalità per spiare le singole persone. Si possono intercettare dall’esterno i segnali di comunicazione tra chi parla. “NSO” ne ha approfittato, sviluppando un programma che, una volta scaricato, prenderà il controllo del telefonino di chi lo utilizza.

Così non c’è più bisogno di intercettare telefonate, perché il cliente di “NSO” è effettivamente all’interno dello stesso telefono. Le forze di polizia ed i governi possono distruggere i piani per commettere reati o attacchi terroristici prima che avvengano e preservare l’ordine pubblico.

5. Una breccia delle dimensioni di un camion

Ma c'è un aspetto problematico in questa tecnologia per altri versi benefica: "NSO Group" controlla solo quelli che l'hanno comprata, non l'utilizzatore finale. Il primo cliente può offrirla ad altri individui o enti nel suo governo, o creare un'identità commerciale fittizia per celare l'uso finale che farà di "Pegasus".

"NSO" sostiene di seguire tutte le regole israeliane che governano l'esportazione dei suoi prodotti e vende solo agli alleati di Israele e mai ai suoi nemici. Sostiene anche di vendere solo a governi e mai a singoli individui o ad utilizzatori non autorizzati. Afferma che "Pegasus" è previsto solo per lottare contro criminali e terroristi e mai per essere usato a fini politici.

Tuttavia sottolinea che, una volta che ha venduto il prodotto, non ha il controllo (o per lo meno questo sostiene) su chi usa la tecnologia o sul come. Questa è una breccia abbastanza grande da farci passare un camion Mack [marca che produce negli USA camion enormi, ndt.], e consente ad "NSO" – e a decine di altre imprese di spionaggio informatico che offrono programmi simili – di evitare la responsabilità sui modi ripugnanti in cui la loro tecnologia viene usata.

Nel caso di Mansoor l'hackeraggio è stato diretto contro un cittadino considerato un criminale dallo Stato. Ma egli non lo è da nessun punto di vista riconosciuto da una società democratica. Non è stato imputato di nessun reato, di aver rapinato qualcuno o di aver messo una bomba. Nel 2011 è stato condannato a tre anni con l'accusa di oltraggio allo Stato (in seguito è stato amnistiato e liberato) – e ciò a quanto pare è stato sufficiente in un regime autocratico come quello degli EAU per considerarlo sospetto.

La tecnologia dell'"NSO" è caduta in cattive mani anche in Messico. Come ha informato il "New York Times", i telefoni di attivisti politici, per i diritti umani e contro la corruzione messicani che stavano facendo un'inchiesta su possibili delitti commessi dal governo e dai suoi agenti sono stati infettati da "Pegasus". Il "Times" afferma che le vittime se ne sono accorte per la prima volta nell'estate 2016.

Una di queste era l'avvocato che rappresenta i genitori di 43 studenti medi uccisi dalla polizia messicana in un caso per cui non è mai stata perseguita. Altri

stavano facendo un'inchiesta sulla corruzione di dirigenti d'azienda collusi con rappresentanti eletti.

Secondo mail interne della "NSO" datate a partire dal 2013 e lette dal "New York Times", il governo messicano ha pagato alla "NSO" più di 15 milioni di dollari per tre progetti. Funzionari messicani hanno negato di essere coinvolti nello spionaggio ed hanno aperto un'inchiesta.

Questi usi violano le disposizioni della licenza di esportazione israeliana in base alla quale "NSO" vende i propri prodotti. Ma ci sono scarse possibilità che i funzionari israeliani intervengano in questo caso. Sono interessati a promuovere le esportazioni israeliane, non a limitarle. Né vedono il proprio ruolo come un servizio di censori nei confronti del comportamento delle imprese israeliane.

"Middle East Eye" ha contattato l'agenzia di controllo dell'esportazione per la difesa del Ministero della Difesa israeliano per chiedere di commentare i suoi rapporti con "NSO". Non ha risposto prima che questo articolo venisse pubblicato. Abbiamo anche posto delle domande all'ufficio stampa del Ministero della Difesa, e neppure questo ha risposto a tempo per la pubblicazione.

Per esempio, molti esportatori di armi israeliani sono sospettati di essere impegnati in truffe e altre pratiche corruttive per ottenere contratti per la vendita di armamenti con eserciti stranieri. Poche tra queste imprese sono state messe sotto inchiesta dalle autorità israeliane, benché a parecchie sia stato vietato di fare affari in vari Paesi.

"Citizen Lab" ha detto a "Forbes" che "NSO" ha registrato domini in Israele, Kenya, Mozambico, Yemen, Qatar, Turchia, Arabia Saudita, Uzbekistan, Thailandia, Marocco, Ungheria, Nigeria e Bahrain, suggerendo che "Pegasus" potrebbe essere stato usato in questi Paesi, anche se non ci sono prove evidenti.

Secondo email interne, contratti e proposte di "NSO" visionate dal "New York Times", "NSO" fa pagare ai clienti 650.000 dollari per spiare i proprietari di 10 iPhone, più 500.000 dollari di commissione per la configurazione.

E' evidente quanto questo affare possa essere una miniera d'oro – ed anche perché "NSO" potrebbe essere tentata di allentare le considerazioni etiche per massimizzare il suo profitto potenziale. "Middle East Eye" ha cercato un cofondatore di "NSO" e l'addetto stampa dell'impresa per un

commento. Nessuno ha risposto.

Da imprenditori astuti quali sono, Lavie e Hulio hanno deciso di poter giocare da entrambi i lati. E' così che nel 2013 hanno fondato "Kaymera", un'altra azienda tecnologica con sede nell'università di Herzilya destinata a proteggere i clienti contro intrusioni informatiche indesiderate.

Nella maggior parte delle iniziative imprenditoriali, questo passaggio del confine avrebbe fatto scattare l'allarme. Ci potrebbero essere dei vantaggi nel condividere informazioni: non appena un ingegnere dell' "NSO" ha individuato il punto debole di un'impresa, potrebbe condividerlo con "Kaymera" per risolverlo.

Ma con la stessa facilità potrebbe succedere il contrario: "Kaymera" potrebbe informare "NSO" dei punti deboli che ha scoperto nei sistemi informatici o di comunicazione di un cliente. Questa informazione potrebbe effettivamente essere monetizzata a favore di entrambe le aziende. Middle East Eye ha contattato "Kaymera" per avere un commento e l'impresa non ha risposto.

Il problema è che, in uno Stato di sicurezza nazionale come Israele, considerazioni etiche come queste passano in secondo piano rispetto ai benefici per la sicurezza *e* finanziari.

6. Unicorni e galline dalle uova d'oro

La crescente clientela di "NSO" e i profitti che genera hanno attirato l'attenzione di società di capitale di rischio alla ricerca di opportunità di investimenti lucrosi. Una di queste è stata la società privata di investimenti "Francisco Partners" con sede negli USA.

Nel 2014 la società ha comprato una quota di maggioranza in "NSO" per 120 milioni di dollari. Le migliori società finanziarie investono in un'impresa per un lungo periodo, offrendo non solo un investimento di capitale, ma anche consulenza strategica e gestionale. Ma altre investono a breve termine. "Francisco" è una di queste.

Cosa interessante, "Francisco Partners" e un ramo di "NSO" hanno un passato di rapporti con l'ex consigliere per la sicurezza nazionale dell'amministrazione Trump Michael Flynn, che ha dato le dimissioni in febbraio dopo indiscrezioni sui

suoi rapporti con la Russia.

Secondo moduli informativi finanziari, una controllata di "NSO" con sede in Lussemburgo, "OSY Group", ha pagato a Flynn 40.280 dollari per il suo ruolo come membro del consiglio di amministrazione dal maggio 2016 al gennaio scorso. Flynn – che avrebbe lavorato per molte imprese di sicurezza informatica – è stato anche consulente del socio proprietario di "NSO", "Francisco Partners", ma non ha mai rivelato quanto lo hanno pagato.

Un mese prima che Flynn entrasse nel consiglio di amministrazione di "OSY", "NSO Group" ha aperto una nuova branca nella zona di Washington chiamata "WestBridge Technologies" che, secondo l' "Huffington Post", è "in lizza per contratti con il governo federale per prodotti del gruppo "NSO". Assumere Flynn avrebbe messo a disposizione di "NSO Group" una figura con ottimi contatti a Washington, per aiutarla a inserirsi nel mondo notoriamente esclusivo della destinazione dei fondi dei servizi segreti."

"Francisco Partners" ha tenuto "NSO" solo per un anno prima di iniziare a venderla con una valutazione di un miliardo di dollari. Nelle scorse settimane "Blackstone Group", una delle più grandi società finanziarie di Wall Street, avrebbe accettato di acquistare una quota del 40% in "NSO".

Un investimento di 400 milioni di dollari da parte di "Blackstone" avrebbe fatto diventare "NSO" un "unicorno" (una startup che ha raggiunto il valore di un miliardo di dollari o più) ed offerto ai suoi fondatori – e a "Francisco Partners" – un enorme guadagno.

Data la maggiore penetrazione nel mercato mondiale che l'investitore "Blackstone" avrebbe fornito a "NSO", le notizie hanno preoccupato gli attivisti per la libertà nella rete.

"Access Now", una Ong statunitense che sostiene un internet libero e democratico, ha dato vita ad una petizione on line ed a una campagna con l'intenzione di informare l'opinione pubblica sul modello di attività di "NSO". "Citizen Lab" si è unito al progetto scrivendo una lettera aperta al consiglio di amministrazione di "Blackstone", invitandolo a "considerare con attenzione le implicazioni etiche e per i diritti umani" del loro potenziale investimento.

7. “Blackstone” si ritira

Questa settimana sono comparse notizie secondo cui “Blackstone” è uscita dalle trattative con “NSO” senza arrivare ad un accordo. Rispondendo ad una richiesta di commento da parte di “Middle East Eye” nel giorno in cui è stata annunciata la fine dei colloqui, un rappresentante di “Blackstone” ha rifiutato di commentare l’affare. Un’altra società di investimenti, “ClearSky Technologies”, avrebbe accettato di acquistare una quota del 10% in “NSO”. Ma anch’essa ha confermato a “Middle East Eye” che non investirà nell’azienda.

Un portavoce di “NSO” ha rifiutato di discutere con la Reuters [agenzia di stampa inglese, ndt.] dei colloqui o del perché sono saltati.

Ma pare probabile che la polemica generata da “Access Now” e le questioni sollevate dai giornalisti abbiano reso prudente la società sulla responsabilità che si sarebbe accollata.

“Finché ‘Blackstone’ non parla,” ha detto Peter Micek, consulente legale di ‘Access Now’, “non sapremo se hanno ascoltato le voci di difensori dei diritti umani, giornalisti e vittime di reati le cui vite sono state sconvolte dagli strumenti di ‘NSO Group’”.

“Ma questo accordo defunto dimostrerà ad altri investitori, compreso l’attuale proprietario di ‘NSO’, ‘Francisco Partners’, che non c’è niente da guadagnare – e tutto da perdere – nell’investire nelle violazioni dei diritti umani.”

Tutto ciò mette in luce nuove domande su come “NSO” fa affari e sull’inconsistenza del suo modello etico. Perché, per esempio, “Pegasus” perde il simbolo e il controllo di “NSO” una volta che viene concessa la licenza ad un cliente? Perché l’azienda non può fissare condizioni esplicite nei suoi contratti stabilendo da chi e come sarà utilizzato?

8. Condizioni di utilizzo

Sembra ridicolo che un’impresa, la cui tecnologia è destinata a infiltrarsi e controllare le attività di singole persone prese di mira, non sia in grado di monitorare gli usi a cui vengono destinati i suoi prodotti.

Ovviamente, se “NSO” potesse controllare come i clienti utilizzano i suoi prodotti, potrebbe essere ritenuta responsabile se violano le condizioni di utilizzo. Gli attivisti per i diritti umani presi di mira o imprigionati a causa di “Pegasus” potrebbero forse fare causa per le proprie sofferenze a “NSO” in qualche sede giurisdizionale. Questa sarebbe un’ulteriore ragione per cui “NSO” preferisce non sapere quello che succede una volta che il suo malware lascia i suoi server.

E’ indispensabile che il futuro acquirente ne sia consapevole e risponda a queste preoccupazioni in modo costruttivo. Inoltre gli Stati che sono già clienti di “NSO” devono fare un lavoro molto migliore per monitorare come la tecnologia per la sorveglianza viene utilizzata nelle zone di loro competenza.

Gli Stati che stanno pensando di diventare clienti di “NSO” devono anche fornire tutele per garantire che “Pegasus” venga usato unicamente contro i veri cattivi, ma non contro civili, fautori del benessere pubblico, avvocati, giornalisti o attivisti politici.

Richard Silverstein *scrive sul blog “Tikun Olam”, dedicato a smascherare gli eccessi dello Stato della sicurezza nazionale israeliano. Il suo lavoro è comparso su “Haaretz”, “Forward”, “Seattle Times” e “Los Angeles Times”. Ha contribuito alla raccolta di saggi dedicata alla guerra in Libano del 2006, “A Time to Speak Out” [Il momento di far sentire la propria voce] (Verso), e a un altro saggio nella raccolta di prossima pubblicazione “Israel and Palestine: Alternative Perspectives on Statehood” [Israele e Palestina: prospettive alternative di sovranità nazionale] (Rowman & Littlefield).*

Le opinioni espresse in questo articolo sono dell’autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione di Amedeo Rossi)