https://www-insider.com
data mancante

I fondatori di una startup israeliana di spyware da un miliardo di dollari accusata di aiutare l'Arabia Saudita ad attaccare i dissidenti stanno finanziando una rete di nuove società che hackerano altoparlanti, router e altri dispositivi intelligenti

di Becky Peterson

La società israeliana di sicurezza informatica NSO Group è stata accusata di aver venduto sofisticate tecnologie di sorveglianza digitale all'Arabia Saudita e ad altri paesi sospettati di utilizzarle per attaccare dissidenti e giornalisti.

Nonostante le polemiche, la società è estremamente redditizia, guadagnando circa 125 milioni di dollari l'anno scorso, secondo una fonte che ha visto i suoi dati finanziari.

I fondatori e gli ex studenti di NSO Group hanno generato una rete di oltre una dozzina di startup simili, molte delle quali operano in segreto, che vendono attacchi contro router, computer, altoparlanti intelligenti e altri dispositivi digitali.

Per ora, la maggior parte delle società di capitale di rischio tradizionali sta alla larga dalle società che vendono "capacità informatiche offensive", citando rischi legali e reputazionali. Per affrontare i suoi critici, NSO Group rilascerà un nuovo "codice dei diritti umani" la prossima settimana.

Trascorri un po' di tempo nell'oscuro mondo delle aziende che vendono "capacità informatiche offensive" - strumenti segreti che ti consentono di hackerare telefoni, computer e altri dispositivi digitali per spiare i loro utenti - e un gruppo si profila.

Si trova al centro di un vivace ma discreto ecosistema di startup con sede in Israele specializzate nell'aggirare, indebolire e contrastare le

caratteristiche di sicurezza del nostro ambiente digitale, garantendo ai clienti, in alcuni casi, un accesso quasi illimitato a messaggi, chiamate e conversazioni di quasi chiunque scelgano.

Ci sono più di una dozzina di società di questo tipo in Israele, secondo investitori e dipendenti nello spazio, sebbene molte di esse siano gestite di nascosto da fondatori che hanno lasciato miracolosamente poche tracce della loro esistenza su Internet.

E il principale tra questi è NSO Group, la più grande azienda all'avanguardia della sicurezza informatica offensiva, secondo coloro che investono e lavorano nel settore.
I fondatori di NSO Group affermano che la sua tecnologia, incentrata sulla compromissione degli smartphone, è progettata con il nobile scopo di aiutare i governi a combattere il terrorismo e la criminalità.

Ma la startup è diventata l'obiettivo dell'indignazione internazionale quest'anno dopo le accuse secondo cui il suo software, chiamato Pegasus, è stato utilizzato da una galleria di paesi canaglia, tra cui Arabia Saudita, Emirati Arabi Uniti e Messico, per attaccare giornalisti, dissidenti e politici bersagli.

Una causa contro NSO Group intentata nel 2018 dal dissidente saudita Omar Abdulaziz sostiene che l'Arabia Saudita abbia utilizzato Pegasus per tracciare le sue comunicazioni con l'editorialista del Washington Post Jamal Khashoggi nei mesi precedenti al brutale assassinio di Khashoggi da parte di agenti sauditi.

Cause simili in Israele e Cypress affermano che Pegasus è stato utilizzato dagli Emirati Arabi Uniti e dal Messico per prendere di mira lavoratori e giornalisti per i diritti umani. Il New York Times ha riferito nel 2017 che le autorità messicane hanno utilizzato Pegasus per spiare i membri di una commissione internazionale che cercava di risolvere i famigerati omicidi di 43 studenti universitari scomparsi nel 2014.

Forse l'accusa più strabiliante è stata il rapporto dello scorso maggio secondo cui Pegasus aveva la capacità di compromettere i dispositivi semplicemente effettuando una telefonata al bersaglio utilizzando WhatsApp, anche se la chiamata non ha mai ricevuto risposta. Secondo il Financial Times, che ha diffuso la notizia, l'exploit è stato tentato contro uno degli avvocati che hanno citato in giudizio NSO Group. Il capo della sicurezza di Jeff Bezos ha persino suggerito che Pegasus fosse dietro l'hack che ha quasi portato alla pubblicazione di foto di nudo del fondatore di Amazon (un'accusa che la società nega).

Ma come startup, NSO Group è un successo in fuga. È stato valutato 1 miliardo di dollari, una fortuna nell'ambiente tecnologico israeliano, dove le aziende di maggior successo vengono acquisite per meno di 500 milioni di dollari. Ed è estremamente redditizio, può riferire Business Insider: l'anno scorso ha realizzato un profitto di $ 125 milioni.

Tutto quel denaro ha generato una nuova rete di startup altamente specializzate finanziate dai fondatori e dagli investitori di NSO Group, conosciute nei circoli tecnologici come "la NSO Mafia", che vendono strumenti di nicchia per penetrare router WiFi, altoparlanti domestici e altri dispositivi.

Queste aziende spesso descrivono le loro merci come "intercettazioni legali" o strumenti di "intelligence", anche se questo non racconta l'intera storia. Vendono tutti strumenti che prendono dispositivi e li rivoltano contro i loro utenti per spiare segretamente senza lasciare traccia.

Qualunque cosa tu chiami questa tecnologia, gli affari vanno a gonfie vele. I governi e le forze dell'ordine di tutto il mondo stanno pagando milioni di dollari. E le startup sia all'interno che all'esterno di Israele sono pronte a vendere.

NSO Group è stato avviato in Israele nel 2010 dagli amici Niv Carmi, Omri Lavie e Shalev Hulio. Carmi ha lasciato l'azienda subito dopo la sua fondazione e, a quanto pare, da allora ne ha mantenuto le distanze.

Lavie e Hulio, invece, restano in azienda. Hanno raggiunto un livello di notorietà raro nell'affiatata scena tecnologica di Herzliya, in Israele, dove le aziende rimangono in "modalità invisibile" per anni e persino noti imprenditori locali possono essere sospettosamente difficili da trovare tramite Google. Nelle fotografie, i due sembrano fratelli, con teste rasate, stoppie e corporature abbinate che tradiscono le loro carriere informatiche, con entrambi ora rimossi dal loro tempo trascorso in servizio obbligatorio per le forze di difesa israeliane.

Il modo preciso in cui funziona la tecnologia di NSO Group è un mistero. Ma nelle conversazioni con Business Insider, due persone che hanno familiarità con l'azienda hanno affermato che i clienti hanno pagato per utilizzare gli strumenti di Pegasus in base al numero di persone che vogliono prendere di mira. La maggior parte dei clienti acquista tra i 15 ei 30 obiettivi, ha affermato una persona. La società non rivela quanto costano questi exploit. Il quotidiano israeliano Haaretz ha riferito a

novembre che l'Arabia Saudita ha pagato 55 milioni di dollari per l'accesso a Pegasus nel 2017.

NSO Group non monitora l'utilizzo di Pegasus né svolge un ruolo attivo nella distribuzione del suo software per conto dei suoi clienti. Ma una delle persone che hanno familiarità con l'azienda ha affermato che i suoi contratti le davano il diritto di richiedere un controllo dei numeri di telefono presi di mira dai clienti. L'audit richiede la collaborazione del cliente, ha affermato la persona, e se il cliente si rifiuta di collaborare, NSO Group può utilizzare un kill switch per disabilitare la tecnologia da remoto.

Ha premuto il kill switch sui clienti per un totale di tre volte, ha detto la persona.

Il 10 settembre, la società dovrebbe rispondere alle preoccupazioni sul modo in cui Pegasus è stato utilizzato annunciando un nuovo "codice dei diritti umani", secondo persone che hanno familiarità con i tempi. Il codice dovrebbe guidare NSO Group nel determinare in quali paesi venderà i suoi prodotti in futuro.

Hulio insiste sul fatto che la sua tecnologia rende il mondo più sicuro.

"Stiamo vendendo Pegasus per prevenire il crimine e il terrore", ha detto a Lesley Stahl in "60 Minutes" a marzo, affermando che decine di migliaia di vite sono state salvate dalla sua tecnologia. Alla domanda sull'uso del suo spyware per rintracciare e uccidere Khashoggi, Hulio ha insistito sul fatto che le mani di NSO Group sono pulite. La compagnia non aveva nulla a che fare con il suo "orribile omicidio", ha detto.

Quando Stahl ha chiesto a Hulio di confermare di essersi recato lui stesso in Arabia Saudita per assicurarsi una vendita, il CEO ha sorriso ed ha evitato la domanda. "Non credere ai giornali", ha detto.

L'anno scorso NSO Group ha realizzato profitti per 125 milioni di dollari

A chiunque stia vendendo Hulio, sta funzionando.
Al gruppo NSO, le entrate sono raddoppiate in tre anni da $ 100 milioni nel 2014 a $ 200 milioni nel 2017, secondo una persona che ha visto un'offerta di debito che è stata diffusa dalla società all'inizio di quest'anno. Ha avuto oltre $ 250 milioni di entrate nel 2018, ha detto questa persona, ed è estremamente redditizio, rivendicando un margine di profitto prima di interessi, tasse, deprezzamento e ammortamento di oltre il 50%. Ciò significa che la società ha guadagnato circa $ 125 milioni

di profitti nel 2018.

Secondo l'offerta di debito, NSO Group aveva 60 clienti attivi in tutto il mondo. Di questi, l'80% era governativo; Il 20% erano dipartimenti di polizia, autorità correttive o militari.
Più del 60% dei suoi clienti erano in Medio Oriente e in Asia. Meno del 30% era in Europa. Solo il 3% si trovava nei Caraibi e in America Latina e l' 1% in Nord America.

La mafia NSO
Con la crescita del gruppo NSO, attorno ad esso si è sviluppato un groviglio di startup simili, in molti casi fondate, finanziate o gestite da ex dipendenti del gruppo NSO. Secondo una stima di una persona, ci sono più di 20 startup fondate da ex studenti del gruppo NSO.

L'azienda sta sviluppando un acceleratore interno per i fondatori sia all'interno che all'esterno dello spazio della sicurezza informatica, con l'obiettivo di mettere in contatto le startup con tecnologie come il riconoscimento facciale e l'intelligenza artificiale con i grandi acquirenti del governo, secondo una persona che ha familiarità con il progetto.

Per saperne di più: *McDonald's, Nvidia e Salesforce vogliono tutti un morso del raccolto tecnologico di Tel Aviv. Ecco cosa devi sapere sulla vivace scena di fusioni e acquisizioni in Israele.*
Una delle aziende più visibili è Interionet, che sviluppa malware per router Internet. Nel suo profilo sul database del Centro di ricerca IVC, la società si descrive come una piattaforma di spionaggio informatico "che consente alle agenzie di intelligence di tutto il mondo di ottenere grandi quantità di intelligence sensibile e di alta qualità". È stata fondata da Yair Ceache, l'ex CEO di NSO Group, e Sharon Oknin, l'ex vicepresidente delle consegne del gruppo NSO. Anche Joshua Lesher, ex membro del consiglio di NSO Group, fa parte del consiglio di Interionet.

Esiste anche una startup informatica offensiva chiamata Wayout, fondata da Gil Dolev, fratello del presidente del gruppo NSO Shiri Dolev. La startup ha raccolto fondi dai fondatori di NSO Group per costruire strumenti di intercettazione per dispositivi "Internet delle cose", secondo le persone nello spazio. Dolev non ha risposto a una richiesta di commento.

Un'altra società segreta è Grindavik Solutions, nota anche come Candiru, una startup fondata dall'ex dirigente di Gett Eitan Achlow e dal dirigente del gruppo NSO Isaac Zack, e sostenuta finanziariamente da Zack. A gennaio, la pubblicazione israeliana TheMarker ha riferito che Candiru

vende strumenti per hackerare computer e server e ha citato fonti che affermano che la società potrebbe anche hackerare dispositivi mobili. TheMarker ha ipotizzato che Candiru - che prende il nome da un pesce amazzonico che, secondo la leggenda, si infiltra nell'uretra di chiunque urini nell'acqua - abbia generato circa $ 30 milioni di vendite all'anno. Né Achlow né Zack hanno risposto alle richieste di interviste.
Poi c'è Intellexa, un consorzio internazionale di società che vendono tecnologie di intercettazione ed estrazione, inclusi strumenti di intercettazione 2G, 3G e 4G della Nexa con sede a Parigi, strumenti di intercettazione WiFi a lungo raggio della WiSpear con sede a Cipro e un dispositivo di estrazione dati di Cytrox, acquisita da WiSpear nel 2018. Oggi il consorzio è composto da società separate, ma il piano è quello di fondersi in un'unica società, secondo una persona che ha familiarità con la materia.

Il legame più profondo di Intellexa con NSO Group è attraverso Tal Dilian, il fondatore israeliano di WiSpear. La società Circles di Dilian, che vendeva tecnologia di localizzazione e intercettazione, è stata acquisita per 130 milioni di dollari dalla società di private equity Francisco Partners prima di essere fusa con NSO Group nel 2014.
In primavera, Dilian ha mostrato al reporter di Forbes Thomas Brewster la straordinaria nuova offerta di prodotti di Intellexa: un furgone di sorveglianza truccato che viene venduto da $ 3,5 milioni a $ 9 milioni e può presumibilmente tracciare volti, ascoltare chiamate, localizzare telefoni e accedere da remoto ai messaggi WhatsApp.

Tuttavia, lo spazio non è limitato solo agli ex studenti della NSO. Esistono diverse società israeliane che sviluppano malware per router WiFi o attacchi alle reti WiFi, che consentono ai propri utenti di intercettare le informazioni inviate su Internet. Questi includono Merlinx, un tempo noto come Equus Technologies; Wintego; Laboratori informatici di Jenovice; e PICSIX. C'è anche Quadream, che sviluppa attacchi al sistema operativo mobile di Apple. Una società chiamata Rayzone Group e un'altra chiamata Magen 100 vendono entrambe strumenti per l'intercettazione dei dati degli smartphone. Poi ci sono Toka e Incert Intelligence, che creano entrambi strumenti per accedere da remoto ai dispositivi Internet delle cose. Non è chiaro se qualcuna di queste società sia collegata a NSO Group o sia finanziata dai suoi alunni.

La Silicon Valley flirta con il diavolo

Uno dei motivi per cui così tante di queste società promuovono gli investimenti angelici di Lavie, Hulio e altri ex alunni del gruppo NSO è che gli investitori più tradizionali stanno alla larga.

I venture capitalist sia nella Silicon Valley che a Tel Aviv hanno affermato di ricevere occasionali presentazioni da startup nello spazio: un investitore ha affermato di aver sentito da 10 a 20 diverse società a Tel Aviv, in Israele, con tecnologia offensiva. Ma per molti, non vale la pena essere coinvolti.

Alcuni venture capitalist hanno messo in dubbio la logica aziendale di sostenere un'azienda come NSO Group, che non ha molti acquirenti validi e le cui tecniche controverse possono essere disapprovate dai mercati pubblici. Mentre molte delle più grandi aziende di Sand Hill Road non hanno regole esplicite contro l'investimento dei propri soldi in armi informatiche, gli investitori lo hanno paragonato all'investimento in cannabis o armi, campi rischiosi che è meglio tenere a distanza.

Udi Doenyas, cofondatore ed ex chief technology officer di NSO Group che ha lasciato l'azienda nel 2014, ha affermato che un maggiore controllo sulla legalità della tecnologia informatica offensiva ha aumentato i costi per fare affari e ha spaventato le fonti di finanziamento.

"Siamo stati davvero fortunati", ha detto del primo successo di NSO Group sotto il radar. "Eravamo lì al momento giusto."
Yoav Leitersdorf, il fondatore della società di capitale di rischio israelo-americana YL Ventures, ha affermato che la sua azienda non ha mai investito e non avrebbe mai investito in una società di cyber offensiva.

"La ragione principale di ciò è etica, poiché spesso i clienti di questi fornitori finiscono per utilizzare la tecnologia in un modo che viola i diritti umani, con o senza la conoscenza dei fornitori", ha affermato Leitersdorf in una e-mail. "Il motivo secondario è che è molto più difficile uscire da tali investimenti rispetto ai più tradizionali investimenti nella sicurezza informatica perché ci sono molti meno potenziali acquirenti per i fornitori di sicurezza informatica offensiva: in pratica stai guardando società di private equity e appaltatori della difesa e questo è praticamente tutto".

C'è una recente eccezione, tuttavia: il concorrente del gruppo NSO Toka ha raccolto un seed round di $ 12,5 milioni da Andreessen Horowitz, Dell Technologies Capital, LaunchCapital, Entrée Capital e l'investitore Ray Rothrock l'anno scorso.

Toka crea strumenti informatici su richiesta con particolare attenzione allo spyware per l'Internet delle cose. Il suo obiettivo è offrire ai propri clienti l'accesso remoto a dispositivi come Amazon Echoes,

elettrodomestici intelligenti e termostati.

Il suo team fondatore è un who's who del mondo della sicurezza informatica israeliana. L'amministratore delegato di Toka è Yaron Rosen, l'ex capo informatico delle forze di difesa israeliane. Il suo chief operating officer è Kfir Waldman, un imprenditore seriale ed ex dirigente di Cisco. C'è anche Alon Kanton, un ex dirigente di Check Point Security. E il suo ultimo cofondatore e direttore è l'ex primo ministro israeliano Ehud Barak.

Tre investitori e due tecnologi con conoscenza di Toka hanno detto a Business Insider che la società ha capacità offensive, anche se la società contesta tale caratterizzazione.

"Toka non costruisce cyber offensivi, strumenti di attacco o armi", ha detto a Business Insider Kenneth Baer, portavoce dell'azienda. "Toka costruirà solo strumenti di intelligence, non armi offensive. Un'area su cui ci stiamo concentrando, che riteniamo poco servita, è il settore IoT. Presenta enormi opportunità - e sfide - per le forze dell'ordine e le agenzie di sicurezza".

Toka, come NSO Group, è regolamentata dal Ministero della Difesa israeliano, che alla fine approva tutte le esportazioni di tecnologie di sicurezza informatica che potrebbero essere classificate come strumenti per la guerra informatica. Inoltre, come NSO Group, Toka formerà un consiglio consultivo per "supervisionare tutte le attività e le operazioni di vendita", ha affermato Baer.

Nessuna responsabilità significativa

In gran parte del mondo, la vendita di software offensivo è ampiamente regolamentata come le armi. L'accordo di Wassenaar di 42 paesi, i cui firmatari includono tutto il Nord America e la maggior parte dell'Europa, ha linee guida per le esportazioni globali di armi, che hanno incluso le armi informatiche dal 2013.

Sebbene Israele non faccia parte dell'accordo, il paese afferma di seguire le linee guida e tutte le esportazioni di software devono essere approvate dal Ministero della Difesa. Gli addetti ai lavori del settore hanno descritto le leggi come opache e hanno affermato che le aziende spesso non hanno molte informazioni sui criteri per l'approvazione. Ci sono poche informazioni pubbliche su quali esportazioni superano l'adunata. (Reuters ha riferito il mese scorso che il Ministero della Difesa israeliano ha allentato alcune delle sue regole per accelerare la vendita di tecnologia informatica offensiva.)

I critici del settore sostengono che i controlli nazionali non sono sufficienti e stanno cercando di stabilire precedenti legali globali per ritenere responsabili le società tecnologiche se e quando i loro prodotti vengono utilizzati in modo improprio da governi stranieri.

"Non ci sono prove in questo momento che ci sia una responsabilità significativa sugli abusi che sono già avvenuti", ha affermato John Scott-Railton, ricercatore senior presso il Citizen Lab dell'Università di Toronto, che tiene traccia dell'uso di Pegasus. "Nessuno può ragionevolmente affermare che l'industria si stia controllando da sola o sia ritenuta responsabile per ciò che sta facendo".

Per saperne di più: *Esperto delle Nazioni Unite chiede di fermare le vendite di spyware che potrebbero aver aiutato l'Arabia Saudita a rintracciare e uccidere Jamal Khashoggi*
A parte le tre cause civili in corso che NSO Group sta affrontando in Israele e Cipro, alcuni gruppi hanno cercato di affrontare la questione a livello governativo. A maggio, un gruppo per i diritti umani in Israele ha presentato una petizione contro il ministero della Difesa, chiedendo ai tribunali di revocare la licenza di esportazione di NSO Group alla luce delle rivelazioni sulla sua tecnologia.

"Alcuni governi sono tutt'altro che entusiasti della prospettiva di questo tipo di causa transfrontaliera per abusi", ha affermato Scott-Railton. "È più probabile che quelle azioni legali provengano dalle aziende che dalle vittime in futuro".
Le tensioni legali globali hanno fatto ben poco per scoraggiare la condanna di alcuni dipendenti vicini a NSO Group, che si sono affrettati a sottolineare il bene che è possibile dalla tecnologia, in particolare il suo precedente utilizzo per fermare il traffico di droga e sesso, nonché atti di terrorismo.

"In Israele, NSO è stato un pioniere in questo campo e ha svolto un lavoro straordinario dal punto di vista tecnologico raggiungendo le capacità. Questa tecnologia ha davvero salvato molte vite", ha affermato Amir Bar-El, ex direttore delle vendite di NSO Group. "C'è un motivo per cui questa tecnologia è molto redditizia. Ci sono pochissime persone in grado di sviluppare questo tipo di tecnologia. È unica."
Doenyas, l'ex chief technology officer del gruppo NSO, pensa che sia "bello" che gli alunni della NSO stiano avviando le proprie società, purché, ha detto, agiscano moralmente. Ma era riluttante a parlare di aziende specifiche. Preferiscono la segretezza, ha detto, perché rende i loro prodotti più efficaci.

"Quando vuoi mantenere la pace, è meglio non spaventare l'intera popolazione", ha detto Doenyas. "Vuoi mantenere le informazioni e le capacità per te stesso e usarle solo quando devi."