Cosa è Pegasus, la cyber-spia che minaccia la libertà del mondo

infopal.it/cosa-e-pegasus-la-cyber-spia-che-minaccia-la-liberta-del-mondo/

infopal July 28, 2021

Ildigitale.it. Di Cecilia Capanna. *Sono oltre 50.000 le persone nel mirino di Pegasus, il sistema israeliano che spia giornalisti, attivisti e semplici cittadini violando i diritti e minacciando la libertà del mondo.*

Giornalisti, politici, attivisti e difensori dei diritti umani in 45 paesi di tutto il mondo sono stati spiati attraverso il software **Pegasus**. Un sistema prodotto dalla società israeliana **NSO Group**, nato per tenere sotto controllo la criminalità e gli illeciti e invece utilizzato per violare la privacy di liberi cittadini attraverso l'accesso a tutte le informazioni contenute nei loro palmari e telefoni: un attacco ai diritti, alla libertà e alla democrazia.

Il sistema si introduce nei device senza che la vittima se ne accorga, ma già nel 2015 alcuni hackers specializzati nel scovare le verità nascoste ne avevano scoperto l'esistenza. Successivamente, l'inchiesta del **Washington Post**, con altre 16 testate internazionali coordinate dal consorzio francese **ForbiddenStories**, ha portato alla luce tutti i dettagli di questa vicenda di vero e proprio cyber-spionaggio, incluse le liste degli spiati presunti e verificati. A coadiuvare le indagini, **Amnesty International Security Lab** è riuscita a fare l'analisi forense e a inchiodare definitivamente Pegasus, dimostrando come funziona il bug fantasma e come attacca le sue vittime.

Laddove i malware più comuni sono stati chiamati **Trojan** (horse), a ricordare il celeberrimo cavallo ideato da Ulisse per ingannare i nemici troiani, Pegasus sembra voler fare il verso a quella tecnologia oramai superata, facendo un upgrade di quel cavallo che ora è alato, mitologico e di fatto assai più performante e assai più pericoloso.

Un mondo di spiati.

Che veniamo spiati è una cosa che ci diciamo tutti, **a prescindere dal nostro lavoro e dal nostro ruolo sociale o politico**. Il nostro mondo globalizzato e digitale ci rende tutti cittadini virtuali di un iper mondo ancora senza regole in cui è facilissimo tracciare il nostro identikit: sapere dove ci troviamo, cosa diciamo e a chi, quanto spendiamo ecc., solitamente per fini commerciali.

Non dimentichiamo però che la rete **Internet**, al secolo **ARPANET**, era nata negli anni '60 come sistema operativo di comunicazione militare, quindi anche per lo scambio di informazioni sensibili, per lo spionaggio in definitiva. E il caso di **ECHELON**, il sistema di sorveglianza di massa e spionaggio industriale nato negli anni '70 e investigato dal Parlamento europeo appena nel 2001, dimostra che **lo spionaggio non è solo cosa militare e gli spiati sono liberi cittadini**.

Come Pegasus esistono altri sistemi informatici che riescono ad hackerare telefoni e computer (**FinFisher**, **HackingTeam**) ma mai così capaci di non lasciare traccia. Se da una parte la società produttrice continua ad affermare che l'obiettivo era quello di sventare la criminalità e l'illegalità, purtroppo "i clienti sono clienti" ed evidentemente si è chiuso un occhio nel controllarne le intenzioni quando è stato venduto il software. Pegasus infatti è stato utilizzato non per scoperchiare vasi di Pandora in nome di verità e giustizia ma, al contrario, per violare e neutralizzare chi se ne fa garante.

Come funziona Pegasus e chi ha spiato.

Già nel 2015 sul celeberrimo sito di Wikileaks il leak **SPyFiles** parlava di Pegasus e subito dopo l'azienda **Lookout** aveva proseguito l'indagine scoprendo che questo bug invisibile era in grado di introdursi nei device mobili delle vittime per copiare e trasferire in modalità totalmente anonima tutte le loro informazioni al "customer". Oltre a rubare contatti, chiamate, password, foto e video, Pegasus è anche capace di:

- intercettare chiamate in tempo reale
- bypassare la crittografia SSL
- tracciare in tempo reale la posizione gps
- autodistruggersi in caso di rischio che venga scoperto
- utilizzare android, ios, blackberry e persino symbian

Sono oltre **50.000** i numeri di telefono della lista di Pegasus, di cui una grossa parte sono stati controllati e spiati per più di 3 anni. Oltre ai politici come **Emmanuel Macron** e **Romano Prodi** e il fondatore di Telegram **Pavel Durov**, sono stati intercettati più di 200 giornalisti e alcuni loro contatti, come i familiari di **Jamal Khashoggi**, infettati da Pegasus pochi giorni prima del suo omicidio, o **Javier Valdez**, il giornalista messicano ucciso nel 2017.

La condanna di Ue e ONU e l'allarme per la cybersicurezza.

Se già assistiamo quotidianamente ad una vera e propria persecuzione – nei casi peggiori di mattanza – di giornalisti e attivisti nel mondo, Pegasus ne rappresenta l'arma più micidiale. Le sue violazioni dei diritti sono gravissime e si riapre in modo dirompente la questione della cybersicurezza.

La Procura di Parigi ha aperto un'inchiesta e nei giorni scorsi il commissario alla giustizia dell'Unione Europea **Diddier Reynder** ha annunciato indagini informali, dato che il governo ungherese è pesantemente coinvolto nella vicenda. Inoltre, l'Alto Commissario delle Nazioni Unite per i diritti umani **Michelle Bachelet** ha definito "estremamente allarmante" l'utilizzo di Pegasus che conferma "alcune delle peggiori paure" che circondano il potenziale uso improprio di questo tipo di tecnologie.

Ma l'allarme arriva soprattutto dal mondo dei giornalisti. **Beppe Giulietti**, Presidente di **FNSI** e portavoce di **Articolo21** ha dichiarato:

> *Spiare cronisti e oppositori significa tutelare mafiosi, corrotti, regimi. Occorre una risposta immediata e rigorosa. Ad oggi sono in galera i giornalisti che hanno illuminato le oscurità e restano in libertà i mandanti dello spionaggio illegale.*

Sta di fatto che mentre le guerre commerciali tra grandi blocchi mondiali si fanno a strali di diritti umani violati, che diventano le armi per sanzionare i paesi concorrenti come per esempio gli USA contro Russia, Bielorussia e Cina in difesa dei rispettivi dissidenti, gli stessi sedicenti garanti della libertà di espressione e di parola condannano chi ha detto la verità sui loro governi, come nel caso del fondatore di Wikileaks **Julian Assange**.

Pegasus distrugge i diritti a più livelli.

Si parla sempre più spesso di reato di ostacolo all'attività giornalistica. La **Costituzione italiana**, come tutte le costituzioni di paesi democratici, nell'**Articolo 21** sancisce che:

> Tutti hanno **diritto di** manifestare liberamente il proprio **pensiero** con la **parola**, lo scritto e ogni altro mezzo **di** diffusione. La stampa non puo' essere soggetta ad autorizzazioni o censure.

Un diritto che dovrebbe essere garantito in tutto il mondo, come sancisce l'**Articolo 18** della **Dichiarazione Universale dei Diritti Umani**:

> Tutti hanno **diritto di** manifestare liberamente il proprio **pensiero** con la **parola**, lo scritto e ogni altro mezzo **di** diffusione. La stampa non può essere soggetta ad autorizzazioni o censure.

Pegasus, insieme alla violazione illegale della privacy, viola questo diritto e di conseguenza i diritti sociali e umani che giornalisti e attivisti garantiscono e intendono far rispettare con il loro lavoro: diritti umani, diritti per l'ambiente, diritti sociali, libertà e democrazia in paesi con regimi autoritari. **Pegasus viola i diritti a diversi livelli e in modo esponenziale**. Il sospetto è che quanto venuto a galla sia solo la punta di un iceberg.

PEGASUS. La Nso accusa il Bds. Ma Israele ora teme l'effetto boomerang

nena-news.it/pegasus-la-nso-accusa-il-bds-ma-israele-ora-teme-leffetto-boomerang/

July 26, 2021

La Francia apre un'inchiesta sul cyberspionaggio. Londra: «Ci eravamo già lamentati con il governo israeliano». La società si difende parlando di hackeraggio. Gli esperti: «La cyber diplomacy di Tel Aviv sta causando più danni che benefici»

La sede della Nso

di Chiara Cruciati – Il Manifesto

Roma, 26 luglio 2021, Nena News – Tutta colpa del Bds. È questa la reazione del co-fondatore e amministratore delegato della società israeliana Nso, Shalev Hulio, alla bufera che si è abbattuta sulla compagnia, e di riflesso su Tel Aviv, dopo le rivelazioni di Forbidden Stories, Amnesty International e un gruppo di quotidiani internazionali: lo spyware Pegasus, fiore all'occhiello della Nso, ha hackerato 50mila telefoni in tutto il mondo. Attivisti e giornalisti (si sapeva già, ma all'epoca importava poco) e leader mondiali, da Macron a Khan.

Se il *chief minister* dello Stato indiano di Assam ha pensato bene di proporre la messa al bando di Amnesty per aver rivelato i dettagli del cyberspionaggio mondiale, Hulio se la prende con la campagna di Boicottaggio Disinvestimento e Sanzioni, nata nel 2005 in Palestina e divenuta presto una rete globale. «Uscirà fuori che è stato il Qatar, o il Bds. O entrambi», ha detto alla stampa israeliana accusando parti terze di aver hackerato Pegasus e averlo usato per creare lo scandalo. Fosse vero, la Nso non ne uscirebbe comunque benissimo.

In ogni caso **la società insiste: loro forniscono lo strumento, poi cosa ne facciano i paesi acquirenti non c'è modo di saperlo. La questione politica però resta e travolge il governo israeliano**. Se nel paese sembra che lo scandalo interessi poco – si parla e ci si indigna molto di più del gelato Ben&Jerry's fuggito dalle colonie nei Territori Occupati – le reazioni degli alleati occidentali preoccupano il neonato esecutivo Bennet-Lapid.

La Francia – colpita al cuore, con l'Eliseo spiato d'eccellenza – ha avviato un'inchiesta interna per valutare l'ampiezza dell'attacco subito, mentre emerge che la Gran Bretagna si era da tempo lamentata con Tel Aviv per le attività della Nso e il loro impatto su democrazia e libertà d'espressione. A dirlo è Nicholas True, ministro dell'ufficio del gabinetto britannico: «Abbiamo manifestato diverse volte al governo israeliano le nostre preoccupazioni sulle operazioni della Nso».

Israele risponde indirettamente con la creazione di un team interministeriale che indaghi su eventuali violazioni della licenza da parte della società. **Il deputato Ram Ben-Barak, capo della commissione parlamentare affari esteri e difesa (nonché ex capo del Mossad), ha annunciato l'intenzione di rivedere tutte le licenze di esportazione e di introdurre maggiori controlli sull'export di prodotti opachi come Pegasus**, la cui autorizzazione ricade sulla Deca, l'agenzia di controllo del ministero della Difesa.

Per quanto Tel Aviv provi a gettare acqua sul fuoco, **i legami politici rimangono. A partire dagli investimenti delle autorità israeliane nel settore cyber (non a caso i due co-fondatori della Nso erano membri dell'unità di ricerca e sviluppo del ministero della Difesa) e dal loro capillare utilizzo sulla popolazione palestinese, per proseguire con l'uso di tali prodotti per costruire relazioni internazionali.** Una cyber diplomacy fotocopia di quella – di successo – della vendita di armi e tecnologie militari, che ha permesso a Israele di rafforzare legami con alleati meno solidi di altri o di creare ponti con Stati apparentemente rivali.

Il caso delle monarchie del Golfo o dei paesi africani è uno di questi: la vendita di sistemi di sorveglianza e controllo sociale ha spalancato porte già semi aperte da interessi politici comuni (il contrasto all'Iran).

Una politica che oggi però potrebbe rivelarsi un boomerang, secondo alcuni esperti sentiti dal portale *al-Monitor*: «Le esportazioni di armi israeliane hanno aiutato il paese a forgiare ogni tipo di legame – dice Yoel Guzansky dell'Istituto di Studi sulla sicurezza nazionale di Tel Aviv – Ma **a volte i danni sono più grandi dei benefici: Israele può essere visto come colui che aiuta regimi autocratici a reprimere le società civili».**

«Israele è un incubatore di tecnologia oppressiva», gli fa eco l'avvocato esperto in cyber law, Jonathan Klinger. Dopotutto la Nso opera da Israele. E lo fa con l'approvazione del governo.