Spyware Pegasus, quando lo spionaggio si scontra con i media

Autore: Bruno Cantamessa

Fonte: Città Nuova

La polemica contro il famoso trojan Pegasus non è una novità. Di nuovo ci sono gli obiettivi emersi da un'indagine che ha individuato tra le utenze telefoniche "infettate" anche quelle di 600 politici (compresi capi di Stato e primi ministri), 189 giornalisti, 85 attivisti per i diritti umani e 65 dirigenti aziendali. Non solo criminali e terroristi come sostiene Nso Group, produttore di Pegasus.

Si chiama Pegasus e non è soltanto uno spyware. Secondo molte legislazioni Pegasus è un'arma, **uno strumento di attacco cyber.** In pratica è **un software che costringe uno smartphone a fare cose per le quali non è programmato, contro il suo proprietario.** Infetta senza troppa difficoltà lo smartphone della persona designata, ne estrae informazioni e le invia allo "spione". Può sbirciare dentro email, chat, foto, video (anche del passato) e perfino attivare fotocamera e microfono della vittima, a sua insaputa. **Pegasus è stato progettato e commercializzato dal 2016 da Nso group, che ha sede a Herzliya, vicino a Tel Aviv, in Israele.** La società è stata fondata nel 2010: oggi con 750 dipendenti e un fatturato di 240 milioni di dollari è probabilmente una delle prime agenzie al mondo di intelligence tecnica. Da sempre guardata con diffidenza da molte persone (e con simpatia da alcuni governi), la Nso è balzata nuovamente all'attenzione (dopo lo **scandalo ai danni di Whatsapp di 4 anni fa**) nelle scorse settimane per i risultati di un'indagine coordinata da **Forbidden Stories**, un organismo senza scopo di lucro con sede a Parigi e costituito da 80 giornalisti di 17 organi di stampa di 10 paesi, con l'assistenza tecnica di **Amnesty International. Pegasus Project** (questo il nome dell'indagine) ha riguardato circa 50 mila utenze telefoniche oggetto di potenziale sorveglianza perché appartenenti a capi di stato, politici, giornalisti, attivisti e difensori dei diritti umani. **Agnés Callamard, segretaria generale di Amnesty International, ha dichiarato la scorsa settimana che 'Il Pegasus Project rivela come lo spyware della Nso Group sia un'arma a disposizione di governi repressivi che vogliono ridurre al silenzio i giornalisti, attaccare gli attivisti e stroncare il dissenso, mettendo a rischio innumerevoli vite umane'.** Per altri dettagli si può leggere il documento pubblicato il 19 luglio anche sul sito di [Amnesty Italia](#). Comunque in questi giorni le testate giornalistiche che hanno aderito al Pegasus Project stanno pubblicando una serie di articoli su leader mondiali, esponenti politici, attivisti per i diritti umani e giornalisti individuati come potenziali vittime dello spyware a "beneficio" di alcuni governi e istituzioni che avrebbero acquistato il software dalla Nso Group. Tra i media coinvolti ci sono: **Financial Times, Wall Street Journal, Cnn, the New York Times, Al Jazeera, Ha'aretz, France 24, Radio Free Europe, El Pais, Associated Press, Le Monde, Bloomberg, France-Presse, Economist, Reuters, the Guardian e Washington Post.** In pratica una nutrita schiera delle maggiori testate del mondo. Secondo Pegasus Project **gli acquirenti dello spyware israeliano sarebbero di circa 40 paesi e fra essi figurano** certamente diversi paesi mediorientali come **Arabia Saudita, Marocco, Emirati Arabi e Bahrein.** Ma anche **India, Messico, Azerbaïjan, Kazakistan, Togo, Ruanda e, in Europa, l'Ungheria.** Indignate le proteste di Nso Group, che sostiene di fornire soltanto a stati e istituzioni pubbliche uno strumento utile a contrastare criminali e terroristi. Con l'autorizzazione del Governo israeliano. Pur scegliendo di non fare polemiche e neppure nomi, i termini "criminale" e "terrorista" hanno ormai, purtroppo, estensioni inaccettabili in mano a regimi che **giustificano in questo modo le peggiori persecuzioni ai danni di chi ha l'unica colpa di pensarla in un altro modo** e di non essere al potere. Come tutti i venditori di armi, anche per chi produce e vende cyberwar l'argomento principe è sempre quello che il prodotto in sè non ha un rapporto etico con l'uso che ne fa chi lo acquista. Ma al di là di questa retorica piuttosto scontata, **Agnés Callamard di Amnesty International** pone una questione importante, alla luce

degli indizi emersi dal Pegasus Project, all'opinione pubblica mondiale: "Queste rivelazioni devono generare un cambiamento. **All'industria della sorveglianza non può più essere concesso un approccio indulgente proprio da parte di quei governi che hanno interesse a usare le nuove tecnologie per violare i diritti umani**".