Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 04/2021: 25.000
Lettori: n.d.
Quotidiano - Ed. nazionale

IL FOGLIO

Dir. Resp.: Claudio Cerasa

22-LUG-2021
da pag. 1-8 /
foglio 1
www.datastampa.it

Diplomazia Pegasus

Lo spyware era "il giocattolo che tutti volevano", adesso è un problema politico serio

Roma. Due giorni fa il governo di Israele ha creato una squadra per gestire l'impatto molto dannoso del caso Pegasus, lo spyware creato da un'azienda privata israeliana – la Nso – e venduto anche a regimi che l'hanno usato per operazioni illegali. Pegasus ora è un problema diplomatico perché la Nso lo vende ad altre nazioni grazie a una licenza gestita dal governo israeliano, che può autorizzare oppure bloccare il contratto considerata la pericolosità del software. In questi anni Pegasus era diventato "il giocattolo che tutti volevano" – definizione di un esperto anonimo sentito dal Financial Times – e quindi era nata una "diplomazia Pegasus" che ruotava attorno alla concessione dello spyware. E questa diplomazia precedeva di molto le relazioni diplomatiche ufficiali. L'Arabia Saudita non ha contatti pubblici con Israele ma ha comprato Pegasus nel 2017 e questo lascia supporre che qualche conversazione ad alto livello ci sia stata. Lo stesso vale per gli Emirati Arabi Uniti e per il Marocco, che hanno firmato un patto di "normalizzazione" con Israele soltanto l'anno scorso. La lista dei numeri forse colpiti dallo spyware non include bersagli negli Stati Uniti, come se godessero di un'immunità decisa per ragioni di opportunità politica (a parte, forse, Jeff Bezos, fondatore di Amazon).

Lo spyware micidiale creato in Israele sfrutta una falla "zero click" dei telefoni

Altri esempi: il governo indiano e quello ungherese hanno ottime relazioni con Israele e sono clienti di Nso.

Pegasus valeva l'attenzione e i negoziati sottobanco. In questi giorni si è scoperto che riesce a infettare un telefono non soltanto con il metodo del link-trappola (clicchi su un link e apri la porta allo spyware) ma anche sfruttando delle vulnerabilità "zero-click": vale a dire che non c'è più bisogno di cliccare su un link, lo spyware riesce a entrare e a installarsi nel telefono senza che il proprietario faccia nulla – o si accorga di nulla. I ricercatori del CitizenLab dell'università di Toronto, che sono all'avanguardia nell'inchiesta, hanno scoperto che la falla zero-click funziona anche con l'ultimo sistema operativo IOS dei telefoni Apple, quindi anche il 14.7, l'aggiornamento più recente.

La "diplomazia Pegasus" domenica si è rotta perché sedici testate internazionali hanno pubblicato articoli basati su una lista che contiene cinquantamila numeri di telefono che – si sostiene – sono quelli dei bersagli dello spyware. La Nso risponde che la lista è falsa. Nessuno chiarisce da dove salta fuori. Si, sa, per ora, che i ricercatori sono riusciti ad associare alcuni numeri di telefono a persone reali e importanti – come il presidente francese Emmanuel Macron – ma hanno controllato soltanto 64 telefoni e hanno trovato tracce del passaggio di Pegasus su 37. C'è una peculiarità: la lista conserva i metadati di quando un numero è stato aggiunto – vale a dire che si capisce quando qualcuno ha deciso di usare Pegasus contro una persona specifica. La fidanzata del saudita Jamal Khashoggi (un caso grave di omicidio internazionale a Istanbul) è finita sulla lista pochi giorni dopo l'uccisione di lui. E quando nel 2018 la principessa Latifa tentò di fuggire dal padre, il potentissimo primo ministro degli Emirati Sheikh Mohammed bin Rashid al Maktoum, i numeri di telefono dei suoi amici apparvero sulla lista. Lei si era sbarazzata, come ovvia misura di cautela, del telefonino, ma i soldati emiratini abbordarono con precisione la nave che la portava di nascosto verso una nuova vita e la riportarono negli Emirati.

Daniele Raineri