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

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

La Cina paga criminali

Ora sappiamo molte cose in più sulle operazioni tra hacker e servizi russi, cinesi e israeliani

Roma. La mappa degli attacchi informatici sponsorizzati in segreto dai governi e compiuti da quel settore anonimo in bilico fra i servizi di intelligence e i gruppi privati che aggrediscono per denaro non era mai stata così chiara come negli ultimi dieci giorni, grazie a informazioni uscite tra il 9 e il 19 luglio. Ieri l'Amministrazione Biden ha accusato per la prima volta la Cina di pagare organizzazioni criminali per compiere attacchi contro aziende e istituzioni nei paesi occidentali. Il governo cinese è accusato in particolare di essere responsabile della violazione del sistema di posta elettronica di Microsoft, usato da molte delle aziende più importanti del mondo, da governi e da forze armate. Secondo il dipartimento di Giustizia americano, il governo cinese si serve di un'azienda fittizia, la Hainan Xiandun Technology Development, come paravento per arruolare e creare squadre di hacker e di traduttori che da almeno dieci anni in collaborazione con i servizi segreti attaccano bersagli in occidente. Lo scopo è duplice: i servizi rubano informazioni in campi strategici – come segreti industriali e progetti ancora in fase di studio – e per il resto lasciano che gli hacker si arricchiscano con i ricatti contro le aziende colpite (ransomware: se non paghi non rientri in possesso della memoria dei tuoi computer) e anche questo fa parte delle intimidazioni e delle operazioni di disturbo contro l'occidente.

C'è un punto interessante: l'Amministrazione Biden accusa la Cina ma non minaccia sanzioni, perché ha coinvolto altri e il prezzo da pagare per un comunicato collettivo è rinunciare alle sanzioni.

Grandi accuse contro i servizi cinesi, ma per ora niente sanzioni: c'è paura

Assieme agli Stati Uniti ci sono Australia, Regno Unito, Canada, l'Unione europea, la Nato, il Giappone e la Nuova Zelanda. Alcuni tra questi, come la Germania, si sentono troppo deboli ed esposti nei confronti della Cina per arrischiarsi a parlare di sanzioni: temono rappresaglie. Invece il 9 luglio contro la Russia il presidente Biden aveva minacciato sanzioni o per meglio dire altre sanzioni, visto che arrivano a ondate: l'ultima venerdì contro sei aziende russe accusate di aiutare i servizi segreti russi nelle loro campagne di attacchi. In breve: contro la Cina niente sanzioni, contro la Russia sì. Martedì 13 luglio, pochi giorni dopo le minacce di Biden, uno dei gruppi russi più forti e specializzati in ransomware, REvil, è sparito dal dark web, come se qualcuno l'avesse spento: il blog dove aggiornava le conquiste è scomparso e così anche le chat room dove negoziava i riscatti con le vittime. Non si capisce se siano stati gli americani o i russi messi sotto pressione.

Domenica 18 luglio uno scoop internazionale frutto della collaborazione di molte testate ha accusato un'azienda israeliana, la NSO, di avere una lista di cinquantamila bersagli per il suo software Pegasus, che viola con discrezione gli Iphone e i sistemi Android. Ci sono giornalisti, dissidenti e attivisti politici. NSO ha come clienti decine di governi, inclusi Messico e Arabia Saudita, che hanno usato il software per operazioni sporche (vedi il caso Jamal Khashoggi, trucidato a Istanbul). Di fatto però i ricercatori che hanno la lista sono riusciti a esaminare soltanto 67 telefonini e hanno trovato tracce sicure di Pegasus su 24. La NSO risponde che la lista è falsa. C'è un punto interessante: l'azienda, che non agiva senza la licenza del governo, collabora da tempo con Emirati Arabi Uniti e Arabia Saudita: in pratica è più avanti dei rapporti ufficiali e diplomatici. E non prendeva di mira bersagli negli Stati Uniti, alleato strategico di Israele. Come si diceva all'inizio, la mappa di alleati e nemici nelle aggressioni informatiche è più allo scoperto del normale.

Daniele Raineri