Chi c’è dietro alla scomparsa del collettivo di hacker russi REvil

it.insideover.com/criminalita/chi-ce-dietro-alla-scomparsa-del-collettivo-di-hacker-russi-revil.html

July 16, 2021

Qualcuno ha staccato la spina a **REvil**, il più potente e temuto collettivo di hacker russi, accusati di aver lanciato un pesante attacco informatico ai danni della più grande azienda di carne statunitense, la Jbs; oltre ad aver bloccato i server di migliaia di aziende statunitensi il giorno della Festa d’indipendenza.

La scomparsa dagli schermi di REvil coincide con l’incontro al vertice tra il presidente americano **Joe Biden** e il presidente **Vladimir Putin**. Già durante il meeting avvenuto lo scorso 17 giungo a Ginevra, l’inquilino della Casa Bianca aveva discusso di tematiche inerenti la “sicurezza” e i “cybercrimini” con l’omologo russo. Poi questa settimana, strana coincidenza, gli aggressivi e temuti pirati informatici di Mosca sono scomparsi dalla rete.

Ciò che resta da chiedersi, è se siano state le divisione cibernetiche del Cremlino a “inibire” gli hacker di REvil – conoscendone probabilmente posizione e identità -, o se siano stati gli specialisti delle agenzie governative americane a lanciare la loro vendetta cyberspazio. “**Aspettiamo che agiscano**”, aveva dichiarato Joe Biden in una sorta di ultimatum lanciato la scorsa settimana. Lasciando intendere che se non fosse stato il Cremlino ad agire, sarebbero stati hacker del **Pentagono** a individuare e tagliare fuori i server incriminati dalla rete. Server dai quali, secondo gli analisti dell’intelligence americana, sarebbero stati lanciati il 42% degli **attacchi ransomware** più recenti. Tutti

ricollegabili alla Russia; sia perché i pirati cibernetici che li adoperano “dialogano in russo”, sia perché il codice malevolo sembrerebbe non colpire mai computer impostati russo.

“Sebbene sia abbastanza plausibile che i massimi funzionari russi non abbiano diretto né fossero a conoscenza dell’ultimo attacco di REvil, è certamente concepibile che i funzionari di basso e medio livello siano a conoscenza degli hacker e delle loro attività”, aveva scritto sul *Washington Post* Dmitri Alperovitch, esperto del settore, tra i fondatori di un’importante società di sicurezza informatica. Asserendo che i servizi di sicurezza di Mosca – in particolar modo l’Fsb – “potrebbero catturare gli aggressori”, ma ricordando anche che tale decisione potrebbe non essere considerata tra gli interessi di Putin. Questo a meno che non sia stata prevista una qualche contropartita.

Dato che né americani né russi non hanno rilasciato nessuna dichiarazione riguardo un’operazione mossa nel campo di battaglia del cyberspazio per colpire REvil, rimane plausibile anche l’ipotesi che i pirati cibernetici si siano limitati a sparire dagli schermi in un momento delicato, rimanendo nascosti nel dark web fino alla prossima sortita.

Secondo alcuni esperti, gli hacker in questione avrebbero esibito un livello di sofisticazione che lascia immaginare un “supporto” o almeno un “lascia passare” da una potenza statale che agisce sul territorio russo. Questo potrebbe anche tradursi, quindi, in una soffiata. Che non implicherebbe dunque un attacco da parte dei servizi segreti russi esperti in cyberwarfare, ma soltanto in un puntuale avvertimento. Un messaggio che abbia esortato REvil a prendersi una lunga vacanza dalle loro scorribande cibernetiche. Del resto Mosca ha ancora molti grossi **contratti con l’Occidente**, e con altre potenze estere sensibili al problema della **cyber sicurezza**, da portare a dama. Il complimento concesso loro dal *commander in chief* delle forze armate degli Stati Uniti, che li ha definiti “il pericolo più importante per la sicurezza nazionale”, insieme a tutti i dati sottratti, potrebbero essere sufficienti a soddisfare le loro bramosie. Almeno per il tempo necessario a far quietare le acque.