

Attacco hacker a siti di aziende e istituzioni italiane

Data: Invalid Date | Autore: Redazione



L'Italia è di nuovo sotto attacco da parte degli hacker filorussi, a neanche 48 ore di distanza dalla visita della premier Giorgia Meloni a Kiev: i siti di diverse aziende e istituzioni sono stati presi di mira dal collettivo NoName057 con un attacco Ddos che ha l'obiettivo di smascherare, dicono loro stessi, "l'Italia russofoba".

Un'azione su più fronti che però, sottolineano gli investigatori italiani, al momento non è riuscita del tutto nel suo intento in quanto i sistemi di difesa cyber sono riusciti a limitarne gli effetti.

In realtà, stando a quando il Collettivo ha rivendicato sui propri canali Telegram, l'attacco è partito proprio mentre la presidente del Consiglio era ancora sul suolo ucraino, per rendere omaggio alle vittime di Bucha e incontrare il presidente Zelensky: "Dopo la colazione con i croissants francesi, siamo andati a mangiare una pizza in Italia" hanno scritto gli hacker sostenendo di aver bloccato gli accessi al sito del ministero della Difesa. Il movente? Le armi che l'Italia sta dando all'Ucraina per difendersi dall'aggressione russa.

"L'Italia fornirà all'Ucraina il sesto pacchetto di assistenza militare, che includerà tre tipi di sistemi di difesa aerea. Come ha detto il primo ministro italiano Giorgia Meloni durante una conferenza stampa a Kiev, si parla dei sistemi anticarro Sampt-t, Skyguard e Spike".

Dunque, aggiungono, "continueremo il nostro affascinante viaggio attraverso l'Italia russofoba". Sono

così finiti nel mirino anche il sito del ministero degli Esteri, quello del Viminale e quello delle Politiche Agricole, il portale per il rilascio della carta d'identità elettronica e quello dei Carabinieri ma anche il sito della banca Bper e quello della società di utility A2a nonché quello del gruppo Tim. L'attacco è di tipo Ddos (Distributed denial of service): in sostanza, i server che gestiscono i siti vengono presi di mira da migliaia di false richieste di accesso che ne rallentano il funzionamento e li rendono irraggiungibili. "Stiamo analizzando l'attacco, che riguarda una decina di soggetti pubblici e privati, e seguendo gli eventi" confermano fonti dell'Agenzia nazionale per la cybersicurezza sottolineando che quello in corso un "attacco diretto alle applicazioni, quindi più complesso".

Stavolta però, affermano fonti investigative, le contromisure hanno funzionato e non si sono verificati i problemi del maggio scorso, quando decine di siti, compreso quello del Senato e dello stesso ministero della Difesa andarono in down a causa di un attacco da parte degli hacker di Killnet, altro collettivo filorusso che dall'inizio della guerra ha preso di mira tutti i paesi che sostengono l'Ucraina. Sono infatti scattate immediatamente le procedure di sicurezza e sono stati bloccati tutti gli accessi provenienti da indirizzi Ip all'estero.

Con gli esperti della Polizia Postale, in stretto contatto con i responsabili della sicurezza informatica di aziende e istituzioni, che stanno monitorando costantemente le dimensioni e l'estensione dell'attacco e cercando di individuarne la provenienza. Il risultato è che l'accesso ai siti non è stato, per il momento, bloccato, ma solo rallentato.

"Molti servizi sono stati prontamente ripristinati - ribadiscono dall'Agenzia Cyber - è stata data un'allerta" ed il sistema di sicurezza "nell'insieme ha reagito molto bene". Il collettivo NoName57, secondo le ricostruzioni degli esperti, è apparso a marzo del 2022, a ridosso dell'invasione russa, e ha iniziato a prendere di mira i paesi dell'Est Europa, dalla Polonia alla Lettonia. "Queste formazioni utilizzano i gruppi Telegram per vere e proprie chiamate alle armi - spiega l'esperto di cybersicurezza Pierluigi Paganini - si tratta di gruppi criminali ed attivisti che a vario titolo operano in supporto di Mosca". Gruppi che, in alcuni casi, avevano e hanno legami diretti con l'intelligence militare russa. (Ansa)