

Hacker filo russi attaccano il sito del porto di Genova: nessun danno

Nessun dato sensibile è andato perduto, migliaia di attacchi sventati da Liguria Digitale

3 minuti e 48 secondi di lettura

di Matteo Cantile

venerdì 03 giugno 2022



Ci sono gli hacker filo russi di We are Killnet dietro l'attacco che questa mattina ha messo fuori uso il sito dell'Autorità portuale di Genova e Savona, lo confermano fonti della polizia postale. L'ultima aggressione informatica è avvenuta poco dopo le 7 di questa mattina e ha colpito i server di Liguria Digitale, che custodiscono i dati del sito www.portsofgenoa.com: la struttura difensiva realizzata a Erzelli ha però retto l'urto, il portale dell'Authority è andato off line solo per qualche minuto prima di riprendere regolarmente a funzionare.

Nessun dato sensibile è andato perduto nel corso di questo attacco, subito rivendicato su Telegram dagli autori: al momento la polizia postale sta lavorando per cercare di risalire all'esatta identità degli assalitori informatici.

In realtà quello di oggi non è il primo attacco contro il sito del porto di Genova: sono almeno quattro giorni che gli hacker filo russi, che avevano ampiamente annunciato questa loro attività criminosa, stanno tentando in tutti i modi, con attacchi ripetuti, di entrare nei server di Liguria Digitale ma il personale, che è attivo 24/7 è sempre riuscito a impedirlo.

I primi attacchi sono datati domenica 29 maggio: la squadra di Liguria Digitale era già in allerta poiché la cybersicurezza italiana era già nel mirino degli hacker del partito Legion da qualche giorno; nel mirino dei pirati informatici erano finiti la Banca d'Italia, il ministero del Tesoro, la corte di giustizia, il sito della Rai, quello degli aeroporti di Forlì, Firenze, Torino e Bologna. Il 29 è stata poi la volta del sito del porto di Genova che però è stato attaccato non sul suo dominio attuale (portsofgenoa) ma su quello non più in uso (porto.genova): è dal vecchio dominio che gli hacker sono poi riusciti a entrare in quello nuovo. Nelle stesse ore è stato attaccato anche il sito di Liguria Digitale che però è riuscito a respingere l'assalto senza particolari problemi.

Questa mattina sono arrivati ulteriori attacchi che hanno messo ko, invero per qualche minuto appena, il sito portsofgenoa: il Security Operation Centre di Liguria Digitale ha ricevuto richieste di accesso nella misura di 8mila al minuto e ha lavorato per circoscrivere l'aggressione, impedendo l'accesso a tutti gli IP provenienti da paesi stranieri, così da limitare all'Italia la possibilità di accesso al sito del porto di Genova; nel corso della giornata ci sono state diverse recrudescenze, sempre controllate e

circoscritte dal personale del SOC. "Voglio ringraziare tutti i nostri ragazzi che hanno lavorato giorno e notte per respingere gli attacchi", ha dichiarato a Primocanale l'amministratore unico di Liguria Digitale Enrico Castanini.

Anche il sito di Psa-Sech, uno dei due principali terminal contenitori del porto di Genova, insieme con Psa Genova Pra', è bloccato da questa mattina, vittima di un attacco hacker che ha saturato il sistema sommergendolo con un traffico anomalo. Sono rimasti bloccati il sito web e il link al Genoa Port community system. L'operatività interna e il sistema operativo invece funzionano regolarmente. La società informa con una nota che sta lavorando "per risolvere il problema il più velocemente possibile", presumibilmente già in serata.

"Il tentativo di attacco ai porti di Genova e Savona da parte del gruppo filorusso Killnet pone con urgenza il tema della difesa cybernetica di un segmento nevralgico del nostro sistema logistico ed economico". Lo scrive in una nota Raffaella Paita, presidente della Commissione Trasporti della Camera. "Come dimostrano le vicende di oggi, il rischio è altissimo. Per questo aprirò una serie di audizioni per sapere a che punto è il lavoro di rafforzamento delle difese cibernetiche di ogni polo portuale italiano - ha concluso -. Corriamo un rischio troppo alto in uno dei settori più delicati del nostro sistema infrastrutturale per non intervenire con rapidità".

"Di fronte ad un pericolo reale e ad un numero sempre più rilevante di Autorità di sistema portuale, fra cui quelle di Genova e Savona e quella di Venezia, nonché di alcuni terminal, bersaglio di offensive di hacker, il ministero delle Infrastrutture e della mobilità sostenibili continua a comportarsi come se nulla stesse accadendo e si dedica, in maniera monotematica, al tema legittimo e certo importante della sostenibilità". Lo denuncia il presidente di Federlogistica - Confrtrasporto Lugi Merlo. Negli ultimi anni il rischio di attacchi cyber è cresciuto e le strutture portuali sono nel mirino come accaduto in questi giorni: "ma i reiterati appelli rivolti al Mims non hanno trovato ascolto - aggiunge Merlo -. Mentre i principali porti europei sono stati inseriti dai rispettivi governi nella direttiva NIS (Network and Information Security) il nostro dicastero competente non si muove e le Autorità di sistema portuale, che avrebbero immediatamente bisogno di disporre di un cyber manager, sono costrette a navigare a vista".