

Shipping Italy

Il quotidiano online del trasporto marittimo

Porti italiani sotto attacco informatico

Nicola Capuzzo · Friday, June 3rd, 2022

I siti web delle principali Autorità di sistema portuale italiane nelle ultime ore sono state sotto attacco informatico.

Il sito della port authority del Mar Ligure occidentale (Genova e Savona) è tra quelli finiti questa mattina sotto attacco hacker. E' stata la stessa Autorità portuale a darne notizia con una breve nota stampa in cui si legge: "Traffico anomalo al sito Adsp – E' stato registrato un traffico anomalo al sito istituzionale le cui cause sono in fase di analisi per valutare i possibili scenari e le azioni da intraprendere".

Qualche ora più tardi il seguente aggiornamento: "Il sito dei Ports of Genoa, come i siti di altri enti, è stato oggetto di un attacco cyber preannunciato da Killnet. Dalla mattina di ieri i sistemi di difesa di AdSP e di Liguria Digitale hanno rilevato picchi anomali di traffico; tecnicamente si tratta di attacchi di tipo DDoS, che generano un numero spropositato di accessi contemporanei ai siti web con lo scopo di provocare una congestione e conseguente interruzione di servizio. Al momento i servizi sono attivi e non si segnalano compromissioni di dati: la squadra dei tecnici è costantemente impegnata, in stretta collaborazione con la Polizia Postale, per integrare le attività di monitoraggio automatico con interventi ad hoc, al fine di contrastare gli attacchi ed evitare disservizi".

Secondo quanto riferisce l'Ansa l'attacco è stato respinto grazie al pronto intervento della polizia postale di Genova, in collaborazione con i tecnici della stessa autorità portuale e gli esperti di Liguria digitale, che gestisce il sito della port authority. Secondo quanto appreso, l'attacco pare sia stato sferrato dal gruppo di attivisti filorussi Killnet che da ieri, Feste della Repubblica italiana, ha messo nel mirino i principali porti italiani.

L'offensiva – di tipo DDoS – ha 'saturato' più di un indirizzo ma la difesa si è rivelata efficace. La Polizia postale è ancora al lavoro.

La 'firma' dell'attacco è ancora una volta quella del collettivo filo russo Killnet, che proprio oggi sul suo canale italiano chiama 'alle armi' i 'fratelli italiani'. Nei giorni scorsi erano stati preannunciati attacchi a una cncantina di indirizzi web rilevanti tra cui un buon numero di aeroporti (tra cui Malpensa Milano e Bologna) ma anche Banca d'Italia, Credite Agricole e Csirt.

Anche il terminal contaienr Sech di Genova risulta fra le società vittima di attacco hacker e in quel

caso le attività sono state temporaneamente fermate.

Un paio di settimane fa il presidente di Federlogistica, Luigi Merlo, aveva preannunciato il rischio di attacchi chiedendo il coordinamento del Ministero delle Infrastrutture e della Mobilità Sostenibili per evitare azioni di pirateria informatica contro i terminal portuali e un piano di formazione per disporre delle figure professionali oggi praticamente inesistenti.

“La minaccia è esplicita fra i siti nel mirino del collettivo russo di haker Killnet, figurano in primo piano le aziende di trasporto e logistica, le dogane, il trasporto ferroviario, gli aeroporti e i terminal portuali. E per gli aeroporti la minaccia è già diventata realtà” aveva detto l’associazione. “Il Ministero delle infrastrutture e della mobilità sostenibile deve farsi immediatamente carico delle funzioni di regia e supporto sia alle strutture pubbliche sia a quelle imprese del settore trasporti/logistica/shipping che svolgono un ruolo strategico, come i terminal portuali, coordinandosi con l’Agenzia nazionale per la cybersicurezza”.

SHIPPING ITALY nei giorni scorsi ha pubblicato un [inserto speciale intitolato “Rischi e assicurazioni nei trasporti”](#) dove ampio spazio è dedicato alle minaccia rappresentata da attacchi di pirateria informatica.

ISCRIVITI ALLA NEWSLETTER QUOTIDIANA GRATUITA DI SHIPPING ITALY

This entry was posted on Friday, June 3rd, 2022 at 4:28 pm and is filed under [Porti](#)
You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. Both comments and pings are currently closed.