



AdSP del Mar Tirreno Settentrionale - Sventato attacco hacker al sistema portuale

Nei giorni scorsi i sistemi informatici dell'Autorità di Sistema Portuale hanno subito un pesante attacco hacker da parte di alcuni criminali non ancora identificati

Si è trattato di un attacco di tipo Ddos, acronimo di distributed denial of service, il cui obiettivo è ingolfare il portale inondandolo di false richieste di accesso

L'attacco, rilevato internamente con sistemi di monitoraggio, è stato segnalato alla ADSP anche dalla Polizia Postale, con la quale era stato firmato un protocollo di collaborazione al riguardo.

A partire da venerdì scorso, con continuità per alcuni giorni, gli attacchi provenienti da centinaia di server mondiali hanno avuto un traffico sostenuto di più di 10 milioni di richieste all'ora, con picchi di 13 milioni all'ora.

Gli esperti informatici della Port Authority hanno contrastato l'attacco grazie a sistemi di protezione installati in precedenza, e adottando prontamente configurazioni ulteriori di sicurezza nella fase di attacco più consistente.

“È stato necessario monitorare con continuità l'intensità e l'evolversi dell'attacco” ha dichiarato **Paolo Scarpellini**, Responsabile dell'Area Transizione Digitale, Tecnologie Informatiche e Porto Digitale dell'Ente.

“Per mitigare l'attacco *distributed-denial-of-service* abbiamo dovuto adottare, ed adattare, nuove contromisure che garantissero l'accesso al sito del traffico normale, bloccando o limitando al tempo stesso quello potenzialmente dannoso” hanno aggiunto **Maurizio Tonelli** e **Andrea Biondi**, dei sistemi informativi dell'Ente.

Soddisfatto il segretario generale dell'AdSP, **Matteo Paroli**: “Gli attacchi sul sito istituzionale sono durati molti giorni, ma sono stati bloccati dai sistemi di protezione adeguatamente configurati, la potenza dell'attacco è dimostrata dal fatto che quasi tutti i siti delle altre ADSP hanno avuto blocchi prolungati” ha detto.

“Mi compiaccio per la risposta difensiva che i tecnici informatici dell'Ente hanno saputo mettere in piedi da venerdì scorso. Anche secondo la cellula di crisi del MIT siamo stati efficaci e tempestivi” ha aggiunto, sottolineando come il 2022 abbia fatto registrare una crescita nel numero e nella gravità degli attacchi DDOS: “Gli

investimenti nella digitalizzazione sono ormai un elemento cardine del Codice degli Appalti e richiedono una sempre più elevata attenzione alle strategie di mitigazione delle minacce informatiche. Questo episodio ci insegna che non dobbiamo mai abbassare la guardia, dato che gli attacchi sono sempre più frequenti e in evoluzione” ha concluso.