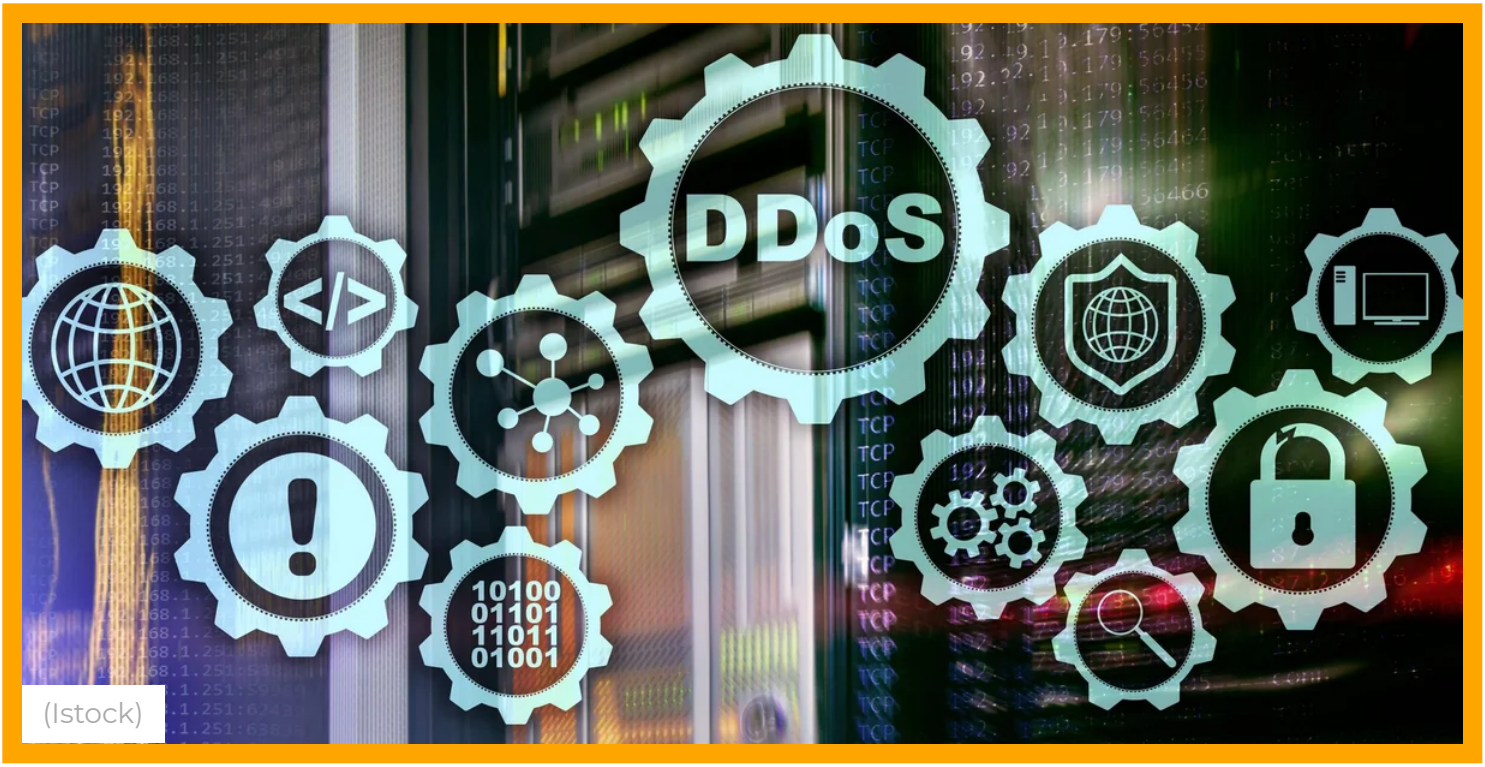
PANORAMA



(Istock)

TECNOLOGIA 13 Gennaio 2021

Dentro l'attacco Ddos al Politecnico di Torino

La Rubrica Cybersecurity Week

Alessandro Curioni

Questa settimana ho deciso di fare qualche riflessione su un caso molto specifico che ha interessato una nota università italiana, che sforna notevoli talenti in ambito informatico, alcuni dei quali conosco e stimo. Tuttavia penso che sia ora di iniziare a essere un

po' pignoli, soprattutto per permettere a chi non è del "mestiere" di capire un po' di più dal punto di vista tecnico.

Il Politecnico di Torino ha dichiarato di essere stato soggetto a un attacco cyber di tipo DDos. Riprendo un articolo apparso su "La Stampa" di Torino e mi permetto di fare alcune considerazioni, rispetto all'articolo e poi rispetto ai dati di traffico che hanno interessato l'università. Vediamo cosa ci racconta l'articolo pubblicato online l'11 gennaio. Esordisce parlando di un'aggressione iniziata "*giovedì 7 gennaio fra le 21:50 e le 22:05 «con un attacco mirato contro il server di autenticazione unica di ateneo che ha provocato l'interruzione di tali servizi». Attacco che poi è ripreso il giorno successivo, venerdì, dalle 10 alle 10:30, «in concomitanza ad un attacco di tipo "SynFlood" contro il sistema della app di ateneo»*".

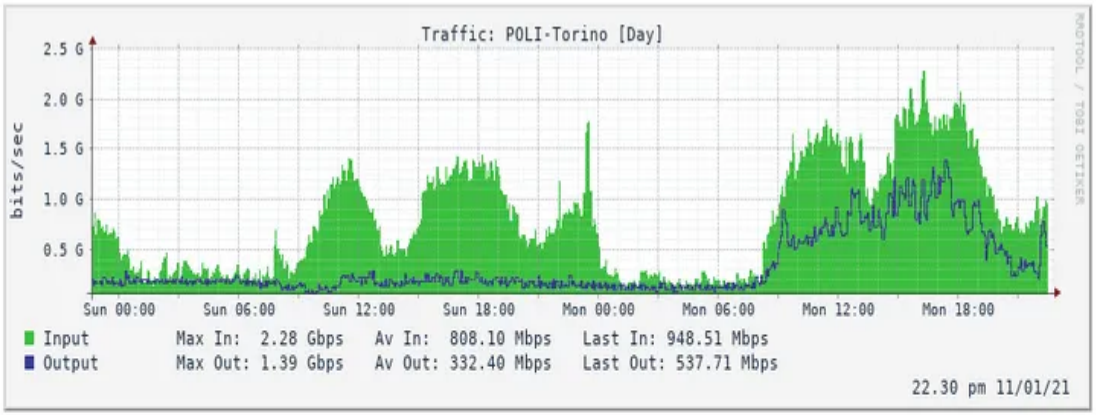
I lettori meritano una spiegazione almeno sommaria di cosa sia un attacco SynFlood.

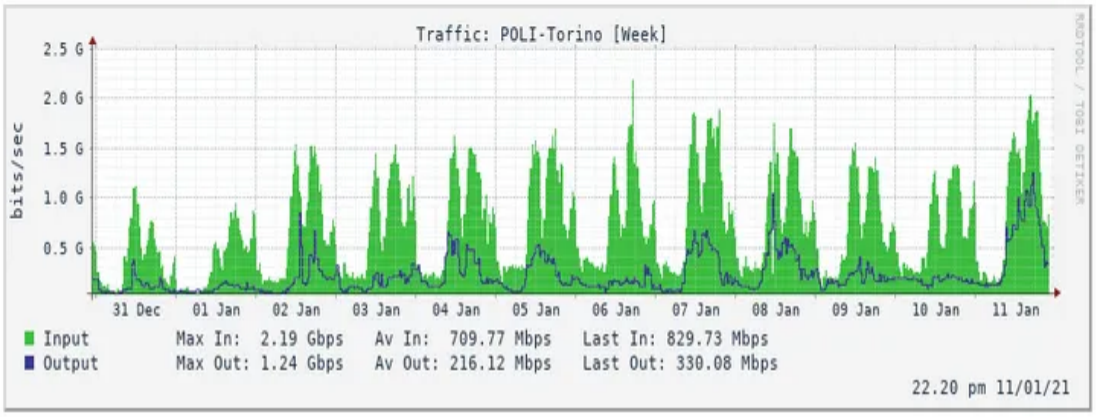
Quando due computer si parlano, si riconoscono attraverso quello che viene definito handshake a tre vie. Si tratta di una stretta di mano virtuale. Nel momento in cui a un sistema vengono "date" molte mani e nessuno la ritira, il sistema finisce per non averne abbastanza per i nuovi arrivati, quindi diventa indisponibile (sono finite le sue mani). Ergo siamo in presenza di un attacco che porta alla negazione del servizio (tecnicamente DoS).

L'articolo prosegue riferendosi di nuovo all'8 gennaio. *"Sempre venerdì, esaurito il primo tentativo di danneggiare il Poli, ne è poi seguito un altro ma di diversa tipologia, questa volta «Ddos» (Distributed Denial of Services), focalizzato su tutte le porte di rete del sistema della app di ateneo."* A questo punto nasce l'equivoco perché si fa confusione tra il tipo di attacco e la tecnica utilizzata. SynFlood indica la tecnica, mentre DDoS specifica il tipo. In altre parole un DDoS può essere perpetrato (spesso è così) attraverso un SynFlood, La massima distinzione possibile riguarda un aspetto quantitativo: proviene da un solo sistema (DoS) oppure da un numero maggiore (DDos). Il risultato, in caso di successo, è sempre e comunque l'irraggiungibilità del sistema obiettivo. Questo significa che i sistemi del Politecnico hanno ricevuto un traffico dati da uno o più sistemi in quantità tale da mettere in crisi la capacità di rispondere.

A questo punto sono andato a dare un'occhiata ai dati relativi al traffico sul sito del GARR (la rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca) che mostra i dati di traffico anche delle università italiane, tra cui il Politecnico di Torino, e ho notato che il giorno 8 gennaio si è effettivamente verificato un picco di traffico. Tuttavia se, per esempio, lo si paragona all'11 non è propriamente "sconvolgente".

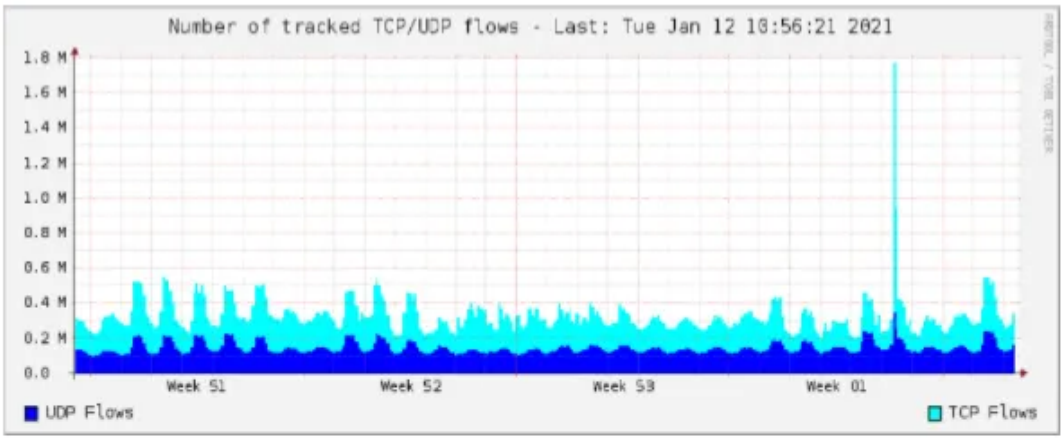
Link name	Equipment	IP	url
POLI-Torino -- PoP Torino-Giuria	rx1.to1.garr.net	193.206.132.33	->
POLI-Torino -- PoP Torino-Giuria backup	rx1.to1.garr.net	193.206.132.145	->



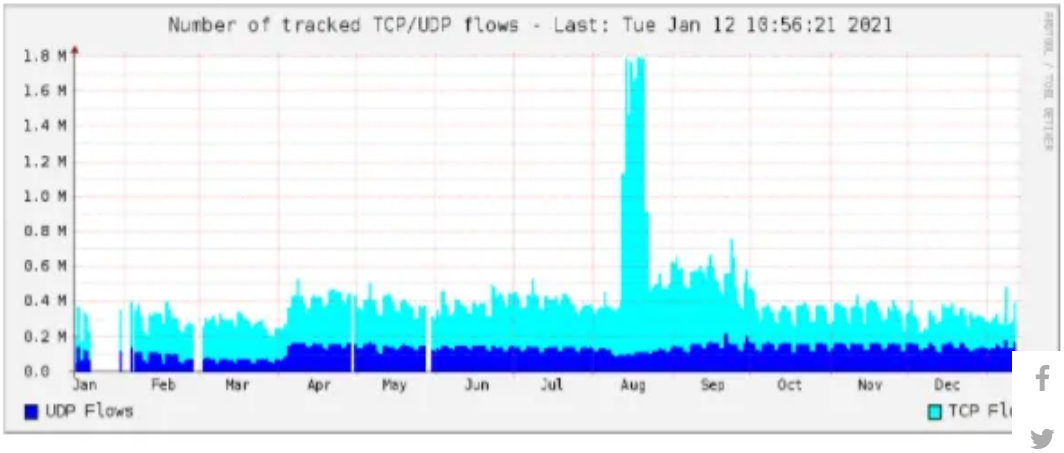


Giustamente si potrebbe obiettare che un attacco DDoS produce un picco istantaneo di connessioni, quindi non gestibile come dimostra l'altra immagine in cui si vede che anche ad agosto si è verificato molto probabilmente un attacco, e molto più massiccio e più lungo.

Monthly Graph



Yearly Graph



Possiamo di conseguenza immaginare che quei sistemi siano strutturati e anche configurati per reggere carichi di molto superiori rispetto a quelli raggiunti nei giorni 7 e 8 gennaio. Quello che mi lascia un po' perplesso è la durata dell'attacco, piuttosto breve per lasciare intendere un'aggressione su larga scala, ma abbastanza puntuale e precisa in termini di orario, soprattutto quella di venerdì 8 gennaio che forse, ma dico forse, era una mattina di esami. Tanti anni fa in licei e università italiane non mancavano i "burloni" che con una telefonata anonima denunciavano la presenza di una bomba nell'istituto e facevano "saltare" compiti in classe e sessioni di esame. I "burloni" non credo siano scomparsi, ma di certo per operare di questi tempi dovrebbero avere cambiato i loro metodi. Un'ultima, ma non insignificante nota.

Gli attacchi DDoS sono un problema, ma tra tutti quelli che possono essere perpetrati contro un'organizzazione sono quelli meno "pericolosi", perché si limitano a rendere sistemi e informazioni indisponibili per un certo periodo di tempo, normalmente piuttosto limitato, ma non causano danni permanenti. Talvolta sono dei semplici diversivi per nascondere aggressioni ben più gravi che puntano al furto dei dati, alla loro distruzione oppure a entrambi i risultati. Insomma fanno molto rumore, ma di solito ben pochi danni.

LEGGI ANCHE

Gli attacchi hacker, urge una nuova visione per le leggi sulla ... ›

Hacker senza freni, colpiti i maestri della cybersecurity - Panorama ›

Gli hacker nel 2021 avranno nuovi obiettivi - Panorama ›