BERTO MARTINA

ATTACCHI DDoS

DISTRIBUTED DENIAL-OF-SERVICE

ATTACCO DDoS

Un attacco DDoS è una variante di un attacco **DoS** (Denial-of-Service), ovvero un attacco mirato ad arrestare un computer o una rete, per impedirne l'accesso da parte degli utenti effettivamente autorizzati;essi inondano l'obiettivo con traffico o inviano informazioni che generano un blocco.

L'attacco **DdoS**,invece,impiega un vastissimo numero di computer infetti per sovraccaricare il bersaglio con traffico fasullo.
Per raggiungere le dimensioni necessarie, essi vengono spesso eseguiti da botnet in grado di cooptare milioni di computer infetti affinché partecipino involontariamente all'attacco.
L'autore degli attacchi sfrutta l'ingente numero di computer infetti per inondare l'obiettivo remoto con traffico e causare un attacco DoS.

ATTACCO DDoS

L'attacco DDoS viene utilizzato più frequentemente dell'attacco DoS per via delle sue **caratteristiche**:

- L'autore degli attacchi può eseguire un attacco più dirompente perché la rete di computer infetti, ai suoi comandi risulta di maggiori dimensioni.
- La distribuzione di sistemi infetti rende difficoltoso individuare la posizione in cui si trova l'autore effettivo degli attacchi.
- È difficile per il server di destinazione riconoscere il traffico come non autorizzato e quindi rifiutarlo a causa della distribuzione apparentemente casuale dei sistemi infetti.
- Essi sono più difficili da bloccare rispetto ad altri attacchi DoS a causa del numero di computer che è necessario arrestare a differenza di uno soltanto.

SCOPO DELL'ATTACCO DDoS

Gli attacchi DDoS sono spesso mirati a organizzazioni specifiche per motivi personali o politici o per estorcere denaro in cambio della cessazione dell'attacco DDoS.

In genere, i danni di un attacco DDoS si calcolano in perdite di tempo e costi causate dall'inattività dei sistemi e dalla perdita di produttività.

ESEMPI DI ATTACCHI DDoS

Nel gennaio del 2012, il gruppo informatico hacktivist Anonymous lanciò un attacco ai principali sostenitori della legge antipirateria SOPA (Stop Online Piracy Act). In dissenso rispetto a questa legge, Anonymous eseguì una serie di attacchi DDoS che riuscirono a disabilitare i siti web del Dipartimento di Giustizia degli Stati Uniti d'America, dell'FBI, della Casa Bianca, della MPAA, della RIAA, della Universal Music Group e della BMI.

Per facilitare l'attacco, Anonymous creò la sua botnet utilizzando un modello non convenzionale che consentiva agli utenti che sostenevano l'organizzazione di offrire i propri computer come bot per gli attacchi.

Gli utenti che desideravano partecipare come volontari potevano unirsi alla botnet di Anonymous facendo clic su una serie di link che l'organizzazione aveva pubblicato su vari siti online, ad esempio Twitter.

ESEMPI DI ATTACCHI DDoS

Gli attacchi DDoS possono inoltre essere sfruttati come armi di guerra informatica.

Nel 2008 durante la guerra in Ossezia del Sud, i siti web del governo georgiano furono bloccati da un attacco che sembrava provenire da bande criminali russe con l'appoggio dei servizi di sicurezza russi. L'attacco informatico fu lanciato poco prima che la Russia cominciasse ad attaccare effettivamente il suolo della Georgia.

PREVENZIONI DI UN ATTACCO DDoS

È stata messa a punto una serie di tecniche di mitigazione degli attacchi DDoS che le organizzazioni possono implementare per ridurre al minimo i rischi di un attacco.

L'infrastruttura di sicurezza della rete dovrebbe includere strumenti di rilevamento degli attacchi DDoS in grado di identificare e bloccare gli exploit e gli strumenti utilizzati dagli autori degli attacchi.

Gli amministratori di rete, inoltre, possono creare profili che consentano di osservare e controllare flussi di traffico specifici.

Grazie alla possibilità di visualizzare tutto il traffico in modo aggregato, è possibile impostare soglie per il monitoraggio e il blocco di comportamenti che indicano un potenziale attacco DDoS.