PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3885 di lunedì 31 ottobre 2016

DoS e DDoS: le tipologie di attacchi cibernetici contro i server

L'attacco cibernetico che ha bloccato per qualche tempo l'accesso ai siti Web di prestigiose istituzioni: illustro brevemente ai lettori questa tipologia di attacco, della quale può rimanere vittima qualunque sito Web. Di Adalberto Biasiotti.

La elevata tensione che si sta creando fra gli Stati Uniti e la Russia, a causa di attacchi informatici portati da hacker russi verso siti americani, ha posto le premesse perché gli Stati Uniti minacciassero una rappresaglia. Anticipando questa rappresaglia, gli hackers russi hanno attaccato con un attacco devastante le strutture informatiche, presso le quali sono alloggiati i server che gestiscono i siti Web di prestigiose istituzioni.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

La tecnologia di attacco è ben nota e viene classificata a due livelli:

- DoS, che significa Denial of Service, cioè blocco del servizio,
- DDoS, che significa Distributed Denial of Service, cioè blocco del servizio, causato da una moltitudine di attaccanti.

Vediamo qual è la differenza fondamentale tra queste tipologie di attacco.

Credo che un esempio telefonico possa rispecchiare bene la situazione.

Supponiamo che un attaccante voglia impedire ad una utenza telefonica di funzionare regolarmente. L'attaccante non farà altro che chiamare in continuazione questo numero telefonico, agganciando il microtelefono, non appena l'utente chiamato risponde. Con questa tecnica di attacco nessuno riesce a chiamare l'utenza in questione, perché essa risulta permanentemente occupata dalle chiamate dell'attaccante.

Se poi l'utenza in questione è dotata di un centralino a molte linee, con ricerca automatica della linea libera, occorre chiamare in causa numerosi attaccanti, che da diversi apparati telefonici sviluppano allo stesso attacco. Anche in questo caso, tutte le linee telefoniche risultano occupate e l'utenza in questione è irraggiungibile per i propri clienti.

Operando nel mondo informatico, è possibile che l'attaccante si colleghi ad un sito Internet, il quale evidentemente avrà un numero limitato di utenze contemporanee che possono essere servite. Se l'attaccante è in grado di chiamare contemporaneamente da più utenze, il sito andrà in blocco e si avrà quindi una negazione del servizio nei confronti di altri utenti legittimi.

Il secondo tipo di attacco è sostanzialmente simile al precedente ma, soprattutto quando si devono attaccare contemporaneamente molti siti, che sono ubicati su server di grande potenza e quindi in grado di gestire numerose chiamate contemporaneo, occorre attuare una strategia diversa.

In questo caso l'attaccante, grazie ad un applicativo che viene inserito su un gran numero di computer, obbliga questi computer a chiamare tutti insieme i siti sotto attacco. Non si ha quindi soltanto un attaccante all'opera, ma centinaia di migliaia di attaccanti, perché ogni computer infetto cerca di collegarsi al sito sotto bersaglio.

A questo punto appare evidente che, per quanto grande sia la capacità di gestione delle chiamate, da parte del server del sito attaccato, vi sono comunque sempre dei limiti che possono essere superati, bloccando il sito, grazie all'aumento esponenziale del numero dei computer che contemporaneamente cercano di collegarsi al sito.

È una tecnica oltremodo pericolosa, perché la efficacia dell'attacco dipende molto dalle caratteristiche tecniche del server, ove il sito Web è alloggiato.

Da notare inoltre che questo tipo di negazione del servizio non si verifica solamente quando l'attaccante ha intenti dolosi, ma si verifica anche quando numerosi utenti cercano di collegarsi tutti insieme, in perfetta buona fede, presso una sito istituzionale.

Sono certo che anche i lettori hanno avuto occasione di leggere sui quotidiani del fatto che, quando venivano aperte le iscrizioni a particolari attività, svolte da un'istituzione pubblica, il sito Web dell'istituzione pubblica poteva andare in tilt perché numerosissimi utenti, da diverse parti d'Italia, cercavano contemporaneamente di accedere al sito, ad esempio per ottenere una priorità nella assegnazione di contributi o altre attività connesse appunto all'accesso al sito Web.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it