PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5040 di Mercoledì 03 novembre 2021

Come contrastare gli attacchi DDoS, che diventano sempre più pericolosi

Negli ultimi tempi è stata registrato un significativo incremento degli attacchi DDoS (distributed denial of service). Vediamo come funzionano e come è possibile attivare misure di prevenzione e mitigazione.

Questa tipologia di attacchi, che è apparsa per la prima volta parecchi anni fa, negli ultimi tempi è cresciuta in volume, dimensioni ed intensità. Gli studiosi parlano di un aumento del 200% nell'ultimo anno, rispetto a periodi precedenti.

Molti professionisti della sicurezza informatica ritengono che questa tipologia di attacco sia una delle più temibili per l'organizzazione, affidata alle loro cure.

Questo attacco mira a impedire la funzionalità di un sito Web, oppure di una applicazione on-line, sovraccaricando la rete e le risorse del server, in modo tale da impedire ad un utente legittimo di accedere ai servizi colpiti.

Oggi diverse aziende si sono proposte sul mercato per mettere a punto tecniche di difesa, che possono almeno limitare i danni conseguenti.

Gli ultimi dati statistici parlano di un danno, legato a questa tipologia di attacco, che varia da 50.000 $ a 2, 5 milioni di dollari, in funzione del sito attaccato e della profondità o durata dell'attacco.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Purtroppo, come accade per il ransomware, le aziende attaccate spesso non hanno una sufficiente sensibilità per studiare un piano di prevenzione di questo attacco ed ecco la ragione per la quale le aziende maggiori sono oggi ad un rischio proporzionalmente inferiore, mentre le aziende più piccole possono essere facilmente attaccate ed il loro sito messo fuori servizio, impedendo ad esempio l'attività di vendita on-line od altre attività, basate su una piena funzionalità del sito Web.

Tra le categorie di aziende attaccate si mettono in particolare evidenza l'imprese finanziarie, perché ormai una gran parte di banche metta a disposizione dei clienti attività on-line, riducendo le visite agli sportelli.

Oggi purtroppo sono già disponibili migliaia di apparati compromessi, che possono essere utilizzati per lanciare degli attacchi devastanti contro istituzioni finanziarie, collegandosi simultaneamente al server bancario, per avviare procedure di banking on-line.

Come spesso accade, le pur incisive indagini delle forze dell'ordine possono trovarsi in difficoltà per le tecniche elusive messe in atto dai malviventi.

Un altro problema che si è recentemente messo in evidenza riguarda il rispetto dei dettati del regolamento generale europeo per la protezione dei dati. Questo regolamento fa obbligo al titolare del trattamento di rispondere tempestivamente a richieste di accesso, che provengono da interessati. La impossibilità di accedere al sito Web può ritardare in misura significativa il recepimento e l'evasione della richiesta di accesso, con conseguenze, anche economiche, sulla credibilità e sulla immagine del titolare.

Vediamo ora quale potrebbero essere le tecniche di difesa.

Uno dei metodi più diffusi è evidentemente quello di mettere a disposizione delle strutture di rete, che possono assorbire dei picchi di traffico, in modo da rendere meno pericoloso questo tipo di attacco.

Un'altra tecnica efficiente ed efficace consiste nel tenere sotto controllo il traffico di rete, per individuare tempestivamente un'impennata del traffico, che potrebbe essere legato appunto ad un attacco di questo tipo.

Altre tecniche efficienti ed efficaci riguardano la individuazione tempestiva di utenti, con un profilo potenzialmente criminoso, analizzando l'origine di attacchi similari, perpetrati in precedenza.

Per quanto riguarda la protezione di siti Web, la misura maggiormente efficace, alla luce dell'esperienza, riguarda la installazione di un firewall in grado di bloccare questa tipologia di attacco.

Non è evidentemente possibile approfondire ulteriormente questo argomento, per il quale un utente, che si ritiene a rischio, farà bene a prendere contatto con esperti del settore.

Ancora una volta, secondo l'ormai tradizionale detto anglosassone, "un'oncia di prevenzione vale 1 tonnellata di repressione"!

Adalberto Biasiotti

.

Licenza Creative Commons

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

www.puntosicuro.it