PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5140 di Venerdì 08 aprile 2022

Come proteggersi dagli attacchi informatici DDos

Gli attacchi Distributed denial-of-service (DDoS) appartengono alla categoria degli attacchi informatici più frequenti e più temibili: qualche suggerimento protettivo.

DDoS (*Distributed denial-of-service*) è una sigla che incute timore in tutti i responsabili della sicurezza informatica. Anche se questi attacchi assumono forme diverse, l'obiettivo è sempre quello di impedire il regolare funzionamento delle utenze colpite, grazie a flussi immensi di traffico. Ecco qualche suggerimento che può aiutare nel proteggersi da questa temibile tipologia di attacchi.

Un attacco di questo tipo si manifesta creando un notevole disturbo al regolare traffico di un obiettivo, sia esso un server, un servizio od una rete. Questi attacchi vengono perpetrati coinvolgendo un grande numero di computer, precedentemente infettati, che si collegano contemporaneamente al bersaglio. Le macchine infettate da malware vengono utilizzate come arma, grazie a una botnet, che viene attivata con un controllo remoto.

Quando il computer infettato riceve un indirizzo IP o le coordinate di un bersaglio, lancia richieste di varia natura che, giungendo contemporaneamente ed in gran numero, possono portare al blocco completo della funzionalità del bersaglio. È infatti estremamente difficile per il bersaglio capire quali richieste di collegamento siano legittime e quali siano di origine criminosa.

Anche se esistono varie tipologie di attacco, la più diffusa è certamente quella chiamata "volumetrica", durante la quale il computer preso a bersaglio viene sovraccaricato da richieste di collegamento.

Altre tipologie di attacco operano a livello di rete, vale a dire a livello 3, oppure addirittura a livello applicativo, cioè al livello 7.

I danni conseguenti all'attacco possono essere gravi, soprattutto perché impediscono al computer preso a bersaglio di interagire con i suoi clienti, in condizioni di normalità.

Da ciò possono discendere incomprensioni, ritardi, pagamenti scaduti, ordini non ricevuti, perdita di immagine e di clienti e via dicendo.

Le principali tecniche di difesa

Le principali tecniche di difesa devono mirare ad individuare le differenze fra picchi di traffico, del tutto legittimi, e picchi di traffico di origine criminosa; deve essere possibile bloccare il traffico in arrivo da botnet, senza interrompere il traffico legittimo e smistare il traffico in arrivo su diversi canali, per impedire che si arrivi al blocco del sistema (denial of service).

A questo fine, un responsabile della sicurezza informatica deve valutare quale possa essere la massima capacità di assorbimento del traffico della rete, affidata alle sue cure, in modo da allestire per tempo possibili misure di contenimento del traffico.

Tra queste misure è possibile individuare delle soluzioni di messa sotto controllo, basate sul cloud, che possono offrire una capacità pressoché illimitata di difesa da sovraccarico di traffico.

A questo proposito, un approccio efficiente ed efficace nasce dal costante monitoraggio del traffico: quando il traffico supera dei livelli che sono ritenuti normali ed accettabili, si attiva la soluzione di messa sotto controllo, basata sul cloud.

È ben vero che purtroppo spesso i responsabili della sicurezza informatica sono obbligati a trovare un compromesso tra la necessità di soddisfare le esigenze di collegamento dei clienti e la garanzia di sicurezza del collegamento.

Come regola generale, la sicurezza del collegamento dovrebbe essere sempre prioritaria, rispetto a possibili ritardi, che i clienti potrebbero subire, durante una fase di attacco DDoS.

Ancora una volta, il vero problema da superare, per fronteggiare questa tipologia di attacchi informatici, è rendersi conto che essi possono effettivamente verificarsi ed allestire per tempo un appropriato piano di difesa.

Intervenire ad attacco iniziato, ahimè, è certamente poco efficace e produttivo.

Adalberto Biasiotti

www.puntosicuro.it