ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4824 di Mercoledì 25 novembre 2020

Siamo certi di sapere tutto sugli attacchi DDoS?

Questa tipologia di attacchi, chiamata Distributed Denial of Service (DDoS), ha caratteri di estrema criticità per i gestori di siti, a rischio specifico.

Questa tipologia di attacco è caratterizzata dal fatto che vengono coinvolti numerosi sistemi informativi, che vengono coordinati dall'attaccante, per cercare di collegarsi a un sito Web o altra risorsa di rete, creando un sovraccarico dei collegamenti e rendendo inaccessibile il sistema preso a bersaglio.

Questa tipologia di attacco è stata già perpetrata da gruppi di criminalità organizzata, oltre che semplici hacker. In certe circostanze, si afferma che anche i servizi di intelligence di paesi stranieri abbiano attaccato i sistemi informatici di un altro paese, ad esempio per rendere difficoltosa la votazione elettronica.

La sequenza di questa tipologia di attacchi è la seguente:

il criminale informatico individua una vulnerabilità in un computer e lo trasforma in coordinatore degli attacchi successivi. Questo coordinatore identifica altri sistemi vulnerabili e ne acquista il controllo, sia superando i sistemi di autentica, sia iniettando del malware.

I computer così presi sotto controllo vengono normalmente chiamati zombie, oppure bot. La catena di comando dei bot viene chiamata botnet. Catene di comando della dimensione di migliaia di computer possono essere affatto normali.

Una volta preso il controllo della rete, vediamo come si comporta l'attaccante. La tecnica più diffusa è quella di avviare contemporaneamente numerosi tentativi di collegamento al computer bersaglio, mettendolo in difficoltà, fino al punto da creare un crash. Negli ultimi tempi la tecnologia di attacco si è evoluta, sfruttando innumerevoli dispositivi, dotati di applicazioni Internet of Things IoT. Purtroppo, questi dispositivi sono dotati di misure di sicurezza facilmente superabili e quindi possono essere inseriti senza difficoltà nel botnet. È purtroppo ben noto il fatto che ancora oggi vengono immessi in commercio dispositivi, che possono facilmente collegarsi ad Internet, che non sono dotati di sufficienti e aggiornabili misure di sicurezza. In certi casi, addirittura le credenziali di autentica di questi dispositivi non possono essere modificate, come minime sono le possibilità di aggiornamento degli applicativi ivi presenti.

Se l'attacco DDoS viene portato in periodi particolarmente critici per il sistema informativo attaccato, ad esempio durante un periodo di votazioni elettroniche, o di accettazione di richieste di erogazioni di fondi di emergenza, l'immagine dei responsabili del sistema attaccato può essere irrimediabilmente compromessa.

Ecco perché il responsabile della sicurezza informatica deve attivare un piano preventivo di difesa da questi attacchi, adottando delle tecniche ormai ben note, come test di attacchi per phishing, sistemi avanzati di monitoraggio dei collegamenti e mantenendo un costante aggiornamento di tutti gli applicativi di difesa informatica, installati nel sistema informativo.

Ancora una volta, si conferma la validità dell'ormai ben noto detto anglosassone: un'oncia di prevenzione vale più di 1 tonnellata di misure reattive.

Adalberto Biasiotti

---

www.puntosicuro.it