Ce sunt atacurile Denial-of-Service si Distribute-Denial-of-Service?

Atacurile Denial-of-Service (DoS) și Distributed-Denial-of-Service (DDOS) sunt cunoscute în principal pentru capacitatea lor de a refuza accesul la mai multe resurse a calculatoarelor sau de a reduce performanța unui anumit serviciu sau conectivitate prin supraîncărcarea resurselor de rețea sau de sistem cum ar fi lățimea de bandă a rețelei, capacitatea de procesare a routerului etc.

Atacurile DoS pot apărea în două moduri:

1. Atacatorul determină ca serverele să se prăbușească sau să-și degradeze performanța prin exploatarea defectelor existente ale software-ului.

2. Atacatorul trimite un număr mare de solicitări frauduloase până când procesorul, memoria sau resursele de rețea ale victimei sunt coplesite.

Atacurile Distributed-Denial-of-Service (DDoS) sunt o versiune mai actualizată a atacurilor Denial-of-Service. Utilizează “slave machines” carora le distribuie responsabilitățile și, în consecință, sporește amenințarea. Impactul atacatorilor multipli nu este doar mai mare, ci și mult mai dificil de detectat.

In functie de numarul atacatorile si al volumui de pachete trimise, atacurile DoS pot fi clasificate astfel:

1. Software exploits: poate dezactiva cu ușurință țintă cu un singur pachet sau cu câteva pachete folosind anumite bug-uri. Singurul mod în care acest tip de atac DoS poate fi împiedicat este actualizarea versiunii software-ului in momentu in care apare un nou update.
2. Flooding attacks: în funcție de numărul de atacatori, acestea pot fi împărțite în continuare în atacuri cu o singură sursă și cu mai multe surse. Acest tip de atac funcționează prin trimiterea de fluxuri de pachete nesfârșite până când toate resursele sunt copleșite.

Există două categorii principale în care putem împărți atacurile DDoS:

1. Diminuarea lățimii de bandă: rețeaua victimelor este inundată cu solicitări, astfel încât cele legitime ajung sa fie impiedicate de a ajunge la sistem.
2. Scăderea resurselor: vizează un proces sau un server pe sistem, ceea ce face imposibilitatea procesării cererilor prin legarea resurselor. Ea utilizează porțiuni vulnerabile ale unui protocol sau trimite pachete IP incorect formate cu scopul de a prăbuși sistemul.

Cum detectam un asemenea atac?

Este aproape imposibil să detectezi astfel de atacuri. Cu toate acestea, cele generate de aplicatiile disponibile au caracteristici de identificare care fac posibilă detectarea în unele cazuri.

Au fost propuse mecanisme de detectare, cum ar fi detectarea bazată pe entropie, detectarea statistică și a UNN.

Masuri de precautie

Actualizarea software-ului defect sau filtrarea anumitor secvențe de pachete sunt cele mai eficiente metode atunci când vine vorba de prevenirea acestor atacuri.

Adesea, adresele IP sursă falsificate sunt folosite pentru ca atacatorul să nu fie urmărit înapoi, prin urmare, o altă măsură de prevenire ar putea fii impiedicarea IP-spoofingu-ului.