Universitatea Politehnica Timișoara  
Facultatea de Automatică și Calculatoare

**Protecția împotriva atacurilor DDoS – Tehnici și strategii**

Securitatea sistemelor de calcul

An universitar 2024-2025

**Valcea Ilie-Cosmin**

***Anul 3, secția Tehnologia Informatiei***  
E-mail: [ilie.valcea@student.upt.ro](mailto:ilie.valcea@student.upt.ro)

Cuprins

[**Protecția împotriva atacurilor DDoS – Tehnici și strategii** 4](#_Toc193294848)

[Ce este un atac DDoS? 4](#_Toc193294849)

[Istoricul important al DDoS 4](#_Toc193294850)

[Motive pentru aparitia unui atac DDoS 4](#_Toc193294851)

[Principalele tipuri de atacuri DDoS 5](#_Toc193294852)

[ Atacuri volumetrice: 5](#_Toc193294853)

[ Atacuri la nivelul protocoalelor 5](#_Toc193294854)

[ Atacuri la nivelul aplicatiilor 6](#_Toc193294855)

[Cum ne dam seama ca un atac de tip DDoS are loc? 6](#_Toc193294856)

[Metode de atenuare a riscului de atac DDoS 6](#_Toc193294857)

[Metode de evitare a compromiterii dispozitivelor utilizatorilor 7](#_Toc193294858)

[Masuri de luat in timpul unui atac 7](#_Toc193294859)

[Perspectiva Legala 7](#_Toc193294860)

[Experiente personale 8](#_Toc193294861)

[Resurse in realizarea proiectului 8](#_Toc193294862)

[Link-uri 8](#_Toc193294863)

## **Protecția împotriva atacurilor DDoS – Tehnici și strategii**

## Ce este un atac DDoS?

Atacurile DDoS reprezinta una dintre cele mai serioase amenintari la adresa disponibilitatii serviciilor in retelele moderne. Prin coplesirea resurselor sistemelor tinta cu un volum mare de trafic aparent legitim, aceste atacuri pot perturba semnificativ sau chiar bloca complet accesul utilizatorilor la servicii critice.

## Istoricul important al DDoS

Panix, al treilea cel mai vechi ISP din lume, a fost tinta a ceea ce se considera a fi primul atac DoS. Pe 6 septembrie 1996, Panix a fost supus unui atac de tip SYN flood, care a dus la intreruperea serviciilor sale timp de cateva zile, in timp ce furnizorii de hardware, in special Cisco, cautau o aparare corespunzatoare. O alta demonstratie timpurie a atacului DoS a fost realizata de Khan C. Smith in 1997, in cadrul unui eveniment DEF CON, perturband accesul la internet pe Las Vegas Strip pentru mai bine de o ora. Lansarea codului de exemplu in cadrul evenimentului a condus la atacuri online asupra Sprint, EarthLink, E-Trade si a altor corporatii mari in anul urmator. Cel mai mare atac DDoS de pana acum a avut loc in septembrie 2017, cand Google Cloud a fost atacat cu un volum de varf de 2.54 Tb/s, dezvaluit de Google pe 17 octombrie 2020. Detinatorul recordului a fost considerat a fi un atac executat de un client nenumit al furnizorului de servicii Arbor Networks din Statele Unite, atingand un varf de aproximativ 1.7 Tb/s.

## Motive pentru aparitia unui atac DDoS

* Dorinta de a se distra, de a-si face loc, de a reglementa conturile sau pur si simplu de huliganism. De obicei, aceste motive sunt urmarite de tineri talentati care incearca sa isi puna la incercare abilitatile de hacking, doresc sa demonstreze ceva lor insisi sau prietenilor lor sau sa le faca rau intr-un mod mic, de exemplu, facand inaccesibil site-ul scolii lor sau un serviciu de jocuri cu care nu au stabilit o relatie. In astfel de cazuri, atacurile DDoS sunt de obicei efectuate folosind mijloace simple, ieftine, dar destul de eficiente. Este relativ usor sa te aperi impotriva unor astfel de atacuri — daca resursele tale sunt protejate profesional.
* Apararea sau impunerea unor idei — politice, sociale, de mediu, culturale etc. Cei care ataca „pentru o idee” incearca de obicei sa dauneze celor care nu sunt de acord cu ei sau sa obtina un raspuns public larg. Aceste atacuri nu trebuie subestimate deloc.
* Daunarea concurentilor — pana de curand, aceasta motivatie a atacatorilor era poate cea mai comuna in practica noastra: in efortul de a obtine macar un mic avantaj competitiv, unii jucatori de pe piata lipsiti de scrupule lansau atacuri asupra concurentilor lor pentru a le dauna si a forta clientii sa migreze pe alte site-uri. Astfel de atacuri sunt deosebit de puternice si dureroase in perioadele cand traficul creste sezonier, cum ar fi perioada dinaintea Craciunului. Atacurile DDoS de acest tip se dovedesc a fi adesea foarte puternice, iar apararea lor necesita nu doar implicarea serviciilor profesionale anti-DDoS, ci si elaborarea atenta a unui intreg set de masuri pentru a asigura stabilitatea resurselor de Internet impotriva atacurilor DDoS, deoarece daca comanda de atac este bine platita, hackerul va face tot posibilul pentru a o executa.
* Am intalnit, de asemenea, frecvent cazuri de santaj si extorcare in ultimii ani. Atacatorii motivati de aceasta dorinta nu doar ca ataca, dar isi formuleaza si cerintele catre victima — de obicei, numesc suma de compensatie in criptomonede, dupa primirea careia promit sa opreasca atacul. Si, desi atacatorii de ransomware de obicei nu duc atacuri extrem de puternice, ei arata adesea o perseverenta demna de invidiat in atingerea obiectivelor lor: chiar daca proprietarii resurselor atacate conecteaza protectie, extorcionarii incearca sa gaseasca vulnerabilitati in acestea pentru a lansa noi atacuri DDoS. In plus, acestia pot desfasura atacuri complexe pe mai multe vectori, in care atacul DDoS este folosit ca tactica de diversiune, de exemplu, pentru a obtine acces la datele confidentiale ale victimei si apoi pentru a le extorca, promitand sa „incorporeze” datele in retea sau sa le distruga in cazul refuzului de a plati o rascumparare.
* Ciberterorismul este una dintre cele mai rare si cele mai greu de detectat situatii, iar o varietate de motive pot sta in spatele acestuia: atacuri de razbunare la scara larga, spionaj industrial, atacuri cibernetice in cadrul razboiului cibernetic etc. De obicei, astfel de atacatori nu se limiteaza doar la atacuri DDoS, ci le folosesc pentru a disimula hacking-ul. Obiectivele lor pot acoperi un spectru larg – de la publicarea de stiri false si furarea de date confidentiale, pana la falsificarea de date, preluarea controlului asupra sistemelor victimei, schimbarea logicii de afaceri, injectarea de cod malitios etc., pana la distrugerea completa a datelor si sistemelor — imediat sau cu o intarziere in timp.

## Principalele tipuri de atacuri DDoS

### Atacuri volumetrice:

Acestea au ca scop saturarea latimii de banda a retelei victimei

cu un flux masiv de pachete, impiedicand traficul legitim sa ajunga la destinatie.

Exemple populare includ atacurile de amplificare folosind protocoale precum DNS

sau NTP, cat si atacurile de flood TCP SYN sau UDP. Tehnicile de aparare includ overprovisioningul latimii de banda, utilizarea serviciilor de atenuare DDoS si filtrarea

traficului la nivel de ISP.

### Atacuri la nivelul protocoalelor

Aceste atacuri exploateaza vulnerabilitati specifice

ale stivei TCP/IP sau ale protocoalelor de aplicatie pentru a consuma resursele

sistemelor tinta. Exemple includ atacurile Ping of Death, SYN flood sau Slowloris.

Masuri de protectie precum aplicarea patchurilor asupra sistemelor, configurarea

adecvata a stivei TCP/IP si utilizarea de proxy-uri specializate pot atenua impactul

acestora.

### Atacuri la nivelul aplicatiilor

Acestea vizeaza epuizarea resurselor aplicatiilor web

prin exploatarea vulnerabilitatilor specifice sau prin trimiterea de cereri aparent

legitime, dar costisitoare din punct de vedere computational. Exemple includ

atacurile de tip HTTP flood sau cele bazate pe vulnerabilitati precum SQL Injection

sau XXE. Tehnicile de aparare includ implementarea de WAF-uri (Web Application

Firewalls), limitarea ratei de cereri si securizarea corespunzatoare a aplicatiilor.

## Cum ne dam seama ca un atac de tip DDoS are loc?

Simptomele unui atac DoS pot semana cu probleme de disponibilitate non-malicioase, cum ar fi probleme tehnice ale unei anumite retele sau un administrator de sistem care efectueaza intretinere. Cu toate acestea, urmatoarele simptome ar putea indica un atac DoS sau DDoS:

* Performanță de rețea neobișnuit de lentă (deschiderea fișierelor sau accesarea site-urilor web);
* Indisponibilitatea unui anumit site web;
* Imposibilitatea de a accesa orice site web;

Cea mai buna metoda de a detecta si identifica un atac DoS ar fi prin monitorizarea si analiza traficului de retea. Traficul de retea poate fi monitorizat printr-un firewall sau un sistem de detectie a intruziunilor. Un administrator poate chiar sa configureze reguli care sa creeze un alert la detectarea unei incarcaturi de trafic anormale si sa identifice sursa traficului sau sa elimine pachetele de retea care indeplinesc anumite criterii.

## Metode de atenuare a riscului de atac DDoS

Desi nu exista solutii pentru a evita complet un atac DDoS, exista cateva solutii proactive, pe care administratorii de retele le pot implementa pentru a reduce efectele unui astfel de atac:

* Monitorizarea continua a traficului si definirea unor baseline-uri pentru detectia

prompta a anomaliilor;

* Segmentarea infrastructurii si izolarea serviciilor critice pentru a limita raza de

impact a unui eventual atac;

* Implementarea unor mecanisme de auto-scalare si load-balancing pentru

absorbtia traficului suplimentar;

* Dezvoltarea si testarea periodica a unui plan de raspuns la incidente, inclusiv

comunicarea cu ISP si furnizorii de servicii pentru atenuarea atacurilor;

* Utilizarea unor servicii specializate de protectie anti-DDoS, care pot filtra traficul

malitios in afara retelei organizatiei;

* Realizarea unui plan in caz de dezastru pentru a asigura eficienta comunicarii, ameliorarii si recuperarii in contextul unui atac DDoS;

## Metode de evitare a compromiterii dispozitivelor utilizatorilor

Exista diferite metode prin care un utilizator poate preveni compromiterea dispozitivului si includerea acestuia intr-un botnet care lanseaza atacuri DDoS, precum:

* Utilizarea unei solutii antivirus
* Instalarea unui firewall si configurarea acestuia astfel incat sa restrictioneze traficul care vine spre sau pleaca dinspre dispozitiv
* Implementarea unor bune practici securitate in sensul minimalizarii accesului altor persoane la informatiile de pe dispozitiv si gestionarii traficului nedorit

## Masuri de luat in timpul unui atac

Daca credeti ca dumneavoastra sau afacerea dumneavoastra sunteti victime ale unui atac DoS sau DDoS, este important sa contactati profesionistii tehnici adecvati pentru asistenta.

* Contactati administratorul de retea pentru a confirma daca intreruperea serviciului este cauzata de intretinere sau de o problema interna a retelei. Administratorii de retea pot, de asemenea, sa monitorizeze traficul de retea pentru a confirma prezenta unui atac, sa identifice sursa acestuia si sa atenueze situatia prin aplicarea unor reguli de firewall si, posibil, prin redirectionarea traficului printr-un serviciu de protectie impotriva DoS.
* Contactati furnizorul de servicii Internet (ISP) pentru a intreba daca exista o intrerupere la nivelul lor sau daca reteaua lor este tinta atacului si sunteti o victima indirecta. Acestia ar putea sa va ofere sfaturi despre un curs de actiune adecvat.

In cazul unui atac, nu pierdeti din vedere celelalte gazde, active, sau servicii aflate pe reteaua dumneavoastra. Multi atacatori desfasoara atacuri DDoS pentru a distrage atentia de la tinta lor principala si folosesc oportunitatea pentru a lansa atacuri secundare asupra altor servicii din reteaua dumneavoastra.

## Perspectiva Legala

Multe dintre jurisdictiile internationale au legi prin care atacurile de tip denial-of-service (DoS) sunt ilegale. UNCTAD subliniaza ca 156 de tari, adica 80% la nivel global, au adoptat legi impotriva criminalitatii cibernetice pentru a combate impactul sau raspandit. Rata de adoptare variaza in functie de regiune, Europa avand o rata de 91%, iar Africa de 72%.

In Statele Unite, atacurile de tip denial-of-service pot fi considerate o crima federala in cadrul Computer Fraud and Abuse Act, cu pedepse care includ ani de inchisoare. Sectiunea de Criminalitate Informatica si Proprietate Intelectuala din Departamentul de Justitie al SUA se ocupa cu cazurile de DoS si DDoS. De exemplu, in iulie 2019, Austin Thompson, cunoscut si sub numele de DerpTrolling, a fost condamnat la 27 de luni de inchisoare si la restituirea a 95.000 de dolari de catre o instanta federala pentru efectuarea mai multor atacuri DDoS asupra unor companii mari de jocuri video, perturbandu-le sistemele intre cateva ore si cateva zile.

In tarile europene, comiterea unor atacuri criminale de tip denial-of-service poate duce, cel putin, la arestare. Regatul Unit este o exceptie, intrucat a interzis in mod specific atacurile de tip denial-of-service si a stabilit o pedeapsa maxima de 10 ani de inchisoare prin Legea Politiei si Justitiei din 2006, care a modificat Sectiunea 3 din Legea privind Abuzul Computerelor din 1990.

## Experiente personale

Experientele pe care le-am intampaniat in legatura cu atacurile de tip DDoS au avut loc in mediul jocurilor video multiplayer, unde un jucator a lansat un astfel de atac asupra server-ului pe care ma aflam, provocand tuturor participantilor cresterea in latenta(ping), oferindu-i astfel un avantaj enorm impotriva adversarilor.

## Resurse in realizarea proiectului

Pentru a realiza proiectul respectiv, am folosit diferite tool-uri pentru traducerea textelor din alte limbi, dar si pentru a scapa de diacritice, pentru a oferi un aspect corespunzator documentului si un „flow” constant al informatiei. Pe langa materialul oferit de cursul „Securitatea Sistemelor de Calcul”, am folosit si informatii gasite pe site-uri ale caror link-uri sunt atasate in continuare.

### Link-uri

* <https://www.dnsc.ro/citeste/recomandari-gestionarea-atacurilor-ddos>
* <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>
* <https://stormwall.network/resources/blog/why-do-ddos-attacks-happen>
* <https://en.wikipedia.org/wiki/Denial-of-service_attack>