Distributed Denial-of-Service: Descriere, prevenție și răspuns la incident

Ce reprezintă un DoS vs DDoS

Un atac de tip **Denial-of-Service (DoS)** se referă la o încercare răuvoitoare a infractorilor cibernetici de a face indisponibile serviciile sau resursele unui calculator pentru utilizatorii vizați. Un atac DoS reușit epuizează toate resursele de rețea sau sistem disponibile temporar sau pe termen nelimitat prin suprasolicitarea țintei sau a infrastructurii din jurul acesteia cu trafic de internet fraudulos, ceea ce duce la încetinire sau căderea serverului.

Când mai multe sisteme de calculatoare (sau botnet-uri - formate din rețele de dispozitive compromise) coordonează un atac DoS, acesta este denumit atac **Denial-of-Service de tip Distribuit (DDoS)**.

Atacurile **DDoS** sunt deosebit de distructive deoarece un atac bine sincronizat în timpul orelor de vârf sau un atac asupra serviciilor sensibile la timp ar putea avea un impact substanțial asupra operațiunilor de afaceri.

Scopul acestui ghid este facilitarea Echipelor de răspuns la incidente cibernetice cu instrumente și informațiile necesare pentru a răspunde eficient la incidentele **DDoS** și a se asigura că sunt luate măsuri pentru protejarea sistemelor și datelor critice ale organizației.

Indicatori de atac DDoS:

- Aflux brusc de solicitări către un anumit punct final sau pagină web.
- Creștere rapidă a traficului, care apare la intervale regulate sau în perioade neobișnuite de timp, provenind de la o singură adresă IP sau de la multiple adrese IP.
- Performanță neobișnuit de lentă a rețelei sau a conexiunii Wi-Fi.
- Performanță lentă a aplicațiilor.
- Incapacitate prelungită de a accesa site-uri web sau fișiere de sistem.
- Utilizare ridicată a procesorului și a memoriei.
- Deconectări frecvente de la conexiunile la internet wireless sau prin cablu.
- Volum crescut de emailuri spam.

Descrierea modului de atac

Deși scopul unui atac DDoS este de a copleși un sistem țintă, instrumentele, tacticile și procedurile (TTP) utilizate pot varia. Există trei categorii largi de atacuri DDoS, enumerate mai jos. *(detalii ANEXĂ)*

I. ATACURI VOLUMETRICE

Această categorie de atacuri încearcă să copleșească sistemul țintă și să creeze congestionare prin generarea unui volum mare de trafic și consumarea întregii lățimi de bandă disponibile a țintei. Atacurile volumetrice pot fi realizate prin tehnici simple de inundare, cum ar fi inundațiile User Datagram Protocol (UDP) sau Internet Control Message Protocol (ICMP), unde atacatorul trimite un număr mare de solicitări de rețea către sistemul țintă.

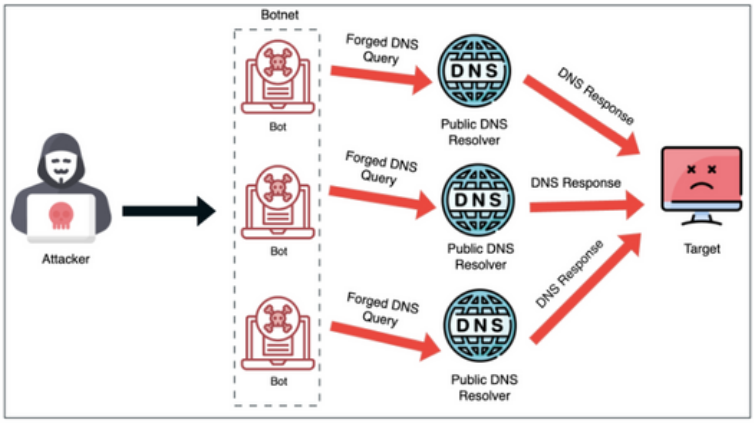

Figura 1

Cel mai comun exemplu de atac volumetric este atacul de amplificare a sistemului de nume de domeniu (DNS). Așa cum se arată în Figura 1, un atacator amplifică substanțial răspunsul DNS către țintă trimițând cereri DNS special create către un server DNS public folosind o adresă IP falsificată. Când este realizat la scară mare cu ajutorul botnet, afluxul de răspunsuri DNS poate afecta semnificativ performanța sau poate opri complet serverul țintă.

II. ATACURI BAZATE PE PROTOCOL

Această categorie de atacuri încearcă să facă o țintă inaccesibilă prin exploatarea unor vulnerabilități specifice în stiva de protocoale de rețea de Layer 3 (Network Layer) sau Layer 4 (Transport Layer) a sistemului țintă. Aceste atacuri au ca scop perturbarea funcționării normale a sistemului țintă prin exploatarea vulnerabilităților în modul în care sistemul gestionează solicitările primite.

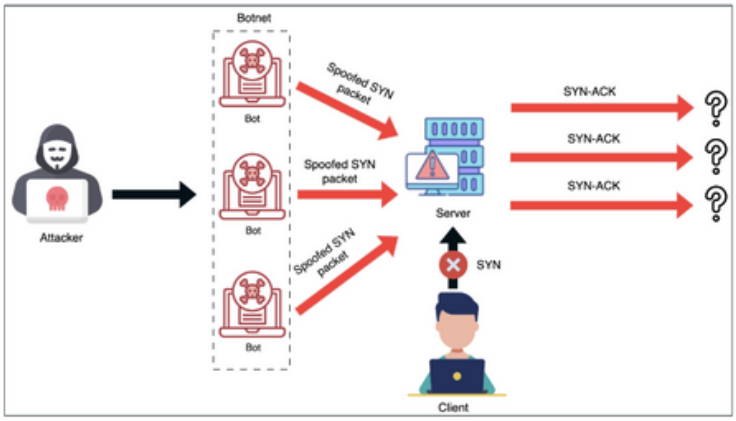

Figura 2

Cel mai comun exemplu de atac bazat pe protocol este atacul de tip SYN Flood. Așa cum se arată în Figura 2, un atacator exploatează procesul de handshake al Protocolului de Control al Transmisiunii (TCP), care constă într-o secvență de comunicări între două calculatoare pentru a iniția o conexiune de rețea.

Trimițând un număr mare de pachete SYN de "Cerere de Conexiune Inițială" cu o adresă IP falsificată, atacatorul determină sistemul țintă să aloce resurse, cum ar fi socket-uri sau conexiuni, pentru a procesa fiecare solicitare primită. Cererile TCP frauduloase din partea atacatorului vor consuma aceste resurse și, în cele din urmă, vor duce la epuizarea completă a resurselor și la o condiție de negare a serviciului pentru utilizatorii legitimi.

III. ATACURI LAYER 7

Această categorie de atac vizează vulnerabilități specifice în stiva de protocoale de rețea de Layer 7 (Application Layer) a sistemului țintă, cum ar fi un server web sau o bază de date. Acest tip de atac are ca scop perturbarea funcționării normale a sistemului țintă prin trimiterea unui volum mare de solicitări către funcțiile sau caracteristicile specifice ale aplicației.

Atacurile de la nivelul aplicației sunt sofisticate și dificil de identificat și de atenuat, deoarece deseori par a fi solicitări legitime, iar măsurile de securitate precum firewall-urile s-ar putea să nu poată să le distingă de traficul autentic.

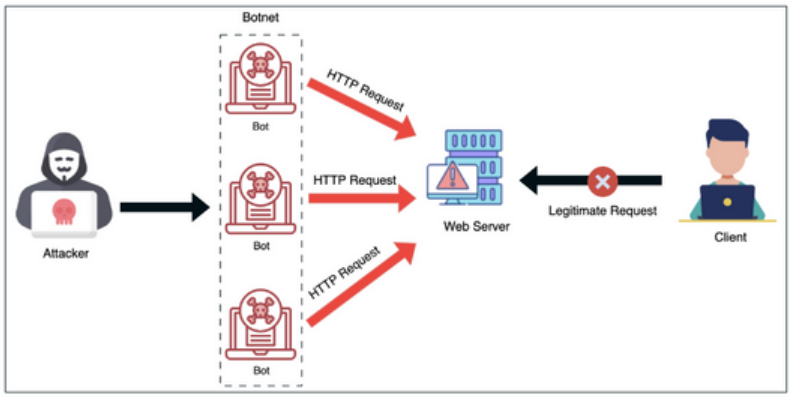

Figura 3

Cel mai comun tip de atac la nivelul aplicației este atacul de tip HTTP Flood. Așa cum este prezentat în Figura 3, un atacator trimite un număr mare de solicitări HTTP GET, solicitând repetat același resursă folosind diferite mașini pentru a inunda un server web țintă, rezultând în inaccesibilitatea acestuia și incapacitatea de a răspunde.
Atacul face dificilă distingerea traficului malefic de cel legitim, deoarece acestea adesea par a fi solicitări legitime.

Protecția împotriva atacurilor DDoS

Organizațiile ar trebui să-și revizuiască procesele și să implementeze măsuri defensive adecvate pentru a crea un mediu mai rezilient cibernetic și pentru a reduce riscul de atacuri DDoS asupra rețelei lor.

Utilizarea de parole puternice și activarea autentificării cu doi factori (2FA)

Prin impunerea unei politici de parole robuste și implementarea autentificării cu doi factori, organizațiile pot minimiza riscul de acces neautorizat și pot preveni compromiterea sistemelor lor, reducând astfel probabilitatea de atacuri DDoS. Organizațiilor **se recomandă** să:

- Schimbe toate parolele implicite ale dispozitivelor și routerelor lor cu parole puternice (ex: de cel puțin 12 caractere, incluzând litere majuscule și minuscule, cifre și caractere speciale).
- Activeze autentificarea cu doi factori (2FA) ca un strat adițional de securitate pentru a preveni accesul neautorizat și preluarea posibilă a dispozitivelor și routerelor din rețea în cazul compromiterii datelor de autentificare.

Monitorizarea și examinarea traficul de rețea pentru activități neobișnuite sau suspecte

Prin monitorizarea și examinarea traficului de rețea, organizațiile pot detecta și răspunde mai rapid la atacurile DDoS, reducând impactul acestora. Organizațiilor **se recomandă** să:

- Înțeleagă modelele de trafic de bază prin măsurarea regulată a tipului de dispozitive de rețea utilizate și a volumului de trafic de protocol (adică UDP, TCP sau ICMP)
- Monitorizeze continuu traficul de rețea prin configurarea firewall-urilor și a sistemelor de detectare/prevenire a intruziunilor pentru a detecta tipuri de trafic anormal, suprasolicitări ale capacității sistemului și dispozitive **rogue** (*se referă la dispozitive care sunt conectate la rețea fără autorizare sau cunoștința administratorilor de rețea. Acestea pot fi dispozitive care nu respectă politica de securitate a rețelei sau care sunt compromise și folosite în mod neautorizat.*) conectate la rețea.
- Raportați activitățile suspecte departamentului sau furnizorului de servicii IT relevant pentru o analiză suplimentară.

Protecția perimetrului de rețea

Implementați protecții la perimetrul rețelei ca primă linie de apărare pentru a proteja rețelele private ale organizației împotriva atacurilor DDoS. Astfel de protecții pot lua forma firewall-urilor din zona demilitarizată (DMZ) plasate între rețelele interne și punctele de conectivitate externe (adică rețelele orientate spre internet). Organizațiilor **se recomandă** să:

- Configureze firewall-urile și routerele pentru a accepta doar traficul descris în politica de securitate a organizației, necesar pentru activitățile operaționale, și să respingă pachetele de rețea care îndeplinesc anumite criterii (adică pachete deformate și falsificate).
- Definirea strictă a "TCP keepalive" și a "maximum connection" pe toate dispozitivele de perimetru, cum ar fi firewall-urile și serverele proxy, pentru a preveni atacurile de tip SYN flood.
- Limitarea ratei de acceptare a numărului de cereri pe care un server le va accepta într-o anumită fereastră de timp pentru a preveni atacurile volumetrice DDoS.
- Luarea în considerare a filtrării porturilor și dimensiunii pachetelor.
- Stabilirea limitelor acceptabile pentru traficul SYN, ICMP și UDP.

Protecția împotriva atacurilor DDoS

Majorarea Lățimii de Bandă a Rețelei

Prin mărirea cantității de bandă disponibilă, poate fi absorbit traficul generat de un atac DDoS și poate fi prevenită suprasolicitarea sistemelor țintă. Organizațiilor **se recomandă** să:

- Utilizeze rețelele de livrare a conținutului (CDN). CDN sunt rețele mari și distribuite de servere care ajută la distribuirea conținutului pentru organizații și oferă un anumit grad de protecție împotriva atacurilor DDoS.
- Implementeze servicii de protecție împotriva atacurilor DDoS oferite de furnizorii de servicii internet și de cloud. Aceste servicii oferă lățime de bandă suplimentară și capacități de filtrare pentru a apăra împotriva atacurilor DDoS. Aceste servicii funcționează prin redirecționarea traficului către un centru de curățare bazat în cloud, unde traficul de intrare este filtrat, iar doar traficul legitim este transmis către sistemele țintă.
- Asigure redundanța serverelor prin utilizarea unui load-balancer și având mai multe servere care pot prelua și continua să gestioneze sarcina de lucru. Acest lucru ajută la asigurarea disponibilității sistemelor țintă, chiar și dacă un server nu poate gestiona traficul generat de un atac DDoS.
- Implementeze routere bastion fie în afara firewall-ului, fie într-o zonă demilitarizată (DMZ). Aceste routere sunt orientate către public și sunt concepute pentru a rezista la atacuri de mare lățime de bandă prin internet.

Creșterea conștientizării în rândul angajaților

Organizațiile ar trebui să desfășoare regulat sesiuni de formare în ceea ce privește conștientizarea securității pentru angajați, inclusiv cum să identifice activitatea suspectă și să răspundă la atacurile DDoS.

În plus, angajații ar trebui să fie instruiți cu privire la planul de răspuns al organizației și cum să-l implementeze în cazul unui atac. Acest lucru ar putea include:

- Instruire în procedurile specifice de raportare a unui atac DDoS și a altor incidente de securitate cibernetică la departamentul sau echipa responsabilă.
- Educație despre rolurile și responsabilitățile individuale în cadrul planului de răspuns, inclusiv cine trebuie contactat și ce acțiuni trebuie întreprinse în diverse scenarii.
- Exerciții practice și simulări de incidente pentru a familiariza angajații cu procesele și protocoalele de răspuns și pentru a le pregăti să acționeze eficient în timpul unui atac real.
- Actualizarea regulată a cunoștințelor și a planului de răspuns pentru a ține pasul cu schimbările în peisajul amenințărilor cibernetice și pentru a asigura o pregătire continuă a personalului.

Pașii de răspuns la incident DoS/DDoS

Dacă organizația dvs. este victima unui atac DoS sau DDoS, următorii pași vă pot ajuta în limitarea, remedierea și recuperarea sistemului:

Pasul 1: Identificarea Atacului

- Verificați că traficul suspect este într-adevăr un atac DDoS verificând jurnalele de sistem și datele de trafic de rețea
- Asigurați-vă că pierderea serviciului nu se datorează altor factori precum o defecțiune a serverului intern sau o indisponibilitate a furnizorului de servicii de internet/cloud
- Verificați dacă organizația se așteaptă la un volum mare de trafic (lansare de servicii sau produse noi, promoții cu timp limitat etc.)
- Identificați activele critice precum serverele și bazele de date care sunt vizate de atac (obțineți adresele IP ale sistemelor vizate; diagrama rețelei pentru sistemele vizate, identificați serviciile pe care sistemul le furnizează (server web, DNS, server de poștă etc.))
- Identificați tipul de atac DDoS (volumetric, amplificare, inundare Syn, protocol etc.) obțineți mai multe detalii despre pachetele malițioase (nivel OSI, număr de port destinație, protocol de comunicare etc.).

Pasul 2: Limitarea Atacului

- Identificați dacă atacul DDoS exploatează un serviciu specific (de exemplu, ICMP) sau atacă un anumit port. Dezactivați acel serviciu sau închideți portul dacă acestea nu sunt esențiale pentru funcționarea sistemului vizat.
- Obțineți adresele IP ale pachetelor DDoS de intrare și implementați controlul accesului pentru a bloca acele adrese IP.
- Implementați limitarea ratei pentru a restricționa numărul de pachete care pot fi trimise de la o singură adresă IP:
- Verificați dacă furnizorii de servicii de internet sau cloud sunt capabili să furnizeze organizației orice formă de apărare împotriva atacurilor DDoS
  - Curățarea traficului ("Scrubbing/Clean Pipe")
  - Sinkholing (blocarea adreselor IP cunoscute ca fiind malițioase)
  - Rutare nulă (implementată ca ultimă soluție)
  - Redirecționați traficul și operațiunile către servere alternative, dacă există.

Pasul 3: Obținerea de Probe pentru Analiză

Colectarea de probe va oferi informații utile despre natura atacului, incluzând tipul de atac DDoS, sursa traficului de atac, impactul atacului și tipurile de sisteme vizate. Analizați datele pentru a determina cauza rădăcinii a atacului și identificați orice vulnerabilități care ar fi putut fi exploatate. **Tipurile de probe** includ:

- Jurnale de trafic de rețea: de la firewall-uri, routere, switch-uri și alte dispozitive de rețea pentru a identifica sursa și tipul traficului implicat în atac.
- Jurnale de sistem de la servere și alte sisteme pentru a identifica orice activitate neobișnuită sau probleme de performanță.
- Date de flux de rețea pentru a analiza volumul și direcția traficului și pentru a identifica orice modele sau anomalii.
- Capturi de pachete pentru a analiza conținutul traficului de rețea și pentru a identifica orice încărcături sau exploatare malițioase.

Pașii de răspuns la incident DoS/DDoS

Pasul 4: Întăriți Sistemele

Întărirea sistemelor poate ajuta la protejarea site-urilor web și a rețelelor împotriva atacurilor DDoS și este crucială pentru a asigura că site-ul rămâne disponibil și accesibil pentru utilizatorii legitimi.
Iată câțiva pași pentru a întări resursele web:

- Utilizați firewall-uri de aplicație web (WAF) pentru a filtra traficul provenit de la adrese IP sau intervale cunoscute ca fiind malițioase.
- Implementați limitarea ratei pentru a restricționa cantitatea de trafic care poate fi trimisă către site de la o singură sursă sau adresă IP.
- Implementați load-balancer pentru a distribui traficul de intrare către mai multe servere, împiedicând supraîncărcarea unui singur server de către un atac DDoS.
- Mențineți dispozitivele de rețea actualizate cu cele mai recente firmware-uri și patch-uri de securitate pentru a remedia vulnerabilitățile cunoscute.
- Revizuiți și actualizați configurațiile firewall-ului și ale securității rețelei pentru a limita accesul la sisteme și a proteja împotriva traficului neautorizat.
- Realizați segmentarea rețelei pentru a separa activele critice de serverele orientate către public.
- Abonați-vă la un serviciu de protecție împotriva atacurilor DDoS de la furnizorii de servicii de internet sau cloud.

Pasul 5: Notificați Părțile Interesate și Raportați Incidentul

- Dacă sunteți o organizație, notificați beneficiarii, furnizorii și angajații despre posibilele perioade de nefuncționare a sistemului sau dispozitive de rețea compromise.
- Dacă suspectați că organizația dvs. este victimă a atacurilor DDoS, vă recomandăm raportați cazul în cadrul platformei ***cyberevent.gov.md*** prin intermediul formularului nostru de raportare a incidentelor, deoarece informațiile ar putea ajuta la alertarea și asistarea altor persoane și organizații.
- Dacă este implicată o pierdere financiară sau activitate criminală, puteți depune o plângere la orice post de poliție sau apelați 112.

ANEXA : Tipuri comune DDoS

Nume	Tip	Descriere
ICMP (Ping) Flood	Volumetric	Un atac de tip ICMP flood implică supraîncărcarea unui dispozitiv vizat cu pachete ICMP Echo Request (ping) de către un atacator, făcându-l inaccesibil traficului normal.
Ping of Death	Protocol-based	Un atac **ping of death** implică un atacator care trimite mai multe pachete modificate sau de dimensiuni mari folosind o simplă comandă ping către un calculator țintă. Lungimea maximă a unui pachet IP (inclusiv antetul) este de 65,535 de octeți. Cu toate acestea, atunci când un pachet malițios de dimensiuni mari este transmis de atacator către țintă, pachetul este fragmentat în segmente, fiecare dintre ele fiind sub limita maximă de dimensiune. Când computerul țintă încearcă să adune bucățile împreună, totalul depășește limita de dimensiune și poate apărea o supraîncărcare a buffer-ului, determinând blocarea, blocarea sau repornirea acestuia.
Slowloris	Application Layer	Un atac **Slowloris** implică un atacator care încearcă să stabilească multiple conexiuni TCP către un server web țintă și să le mențină deschise cât mai mult posibil trimițând cereri parțiale către server, cu scopul de a supraîncărca capacitatea acestuia de a procesa și răspunde, făcându-l inaccesibil pentru orice cereri legitime.
UDP Flood	Volumetric	Un atac de tip UDP flood implică inundarea unui server vizat cu un număr mare de pachete UDP, cu scopul de a supraîncărca capacitatea sa de procesare și răspuns, făcându-l inaccesibil pentru orice cereri legitime.
Network Time Protocol (NTP) Amplification	Volumetric	Un atac de Amplificare NTP implică exploatarea funcționalității unui server NTP cu scopul de a suprasolicita o rețea sau un server vizat cu o cantitate amplificată de trafic UDP, făcând ca ținta și infrastructura sa înconjurătoare să devină inaccesibile traficului obișnuit.