DOI: https://doi.org/10.36719/2789-6919/57/243-248

Nihad Məhəmmədli
Odlar Yurdu Universiteti
magistrant
https://orcid.org/0009-0008-1465-3420
nihadmehemmedli2004@gmail.com

Şəbəkə hücumlarının (DoS, DDoS) aşkarlanması və qarşısının alınması

Xülasə

Müasir rəqəmsal infrastrukturun genişlənməsi və internet vasitəsilə xidmətlərin göstərilməsi şəbəkənin risksizliyini mühüm strateji məsələyə çevirib. Bu kontekstdə Xidmətdən İmtina Hücumları (DoS) və Paylaşılan Xidmətdən İmtina Hücumları (DdoS) informasiya sistemlərinin sabotajına ən çox yayılmış kibertəhdidlərdən biridir. DoS hücumları əsasən bir mənbədən həyata keçirilir və 243ntell resurslarını – server proseslərini, serverləri, şəbəkə bağlantısını və tətbiqi səviyyəli xidmətləri tükəndirir. Bu, onun həddindən artıq yüklənməsinə səbəb olur. DdoS hücumları bir çox mürəkkəb cihazlardan (botnetlərdən) istifadə etməklə daha geniş diapazonda və əlaqələndirilmiş şəkildə həyata keçirilə bilər ki, bu da xidmətlərin tam və ya qismən pozulmasına səbəb olur. Tədqiqat sahəsində DoS və DdoS hücumlarının növləri (həcmli hücumlar, 243ntellec səviyyəli hücumlar və təcrübə səviyyəli hücumlar) onların biznes mexanizminə və şəbəkə infrastrukturuna yaratdığı hücum növləridir. Risklər təhlil edilib. Hücumları aşkar etmək üçün ənənəvi imza əsaslı metodların, anomaliya aşkarlama modellərinin, trafik təhlilinin, davranış əsaslı monitorinqin və süni 243ntellect əsaslı metodların effektivliyi araşdırılıb.

Açar sözlər: *DoS hücumu, DdoS hücumu, şəbəkə təhlükəsizliyi, xidmətin əlçatanlığı, IDS/IPS sistemləri*

Nihad Mahammadli
Odlar Yurdu University
Master's student
https://orcid.org/0009-0008-1465-3420
nihadmehemmedli2004@gmail.com

Detection and Prevention of Network Attacks (DoS, DDoS)

Abstract

The expansion of modern digital infrastructure and the provision of services via the Internet have made network security an important strategic issue. In this context, Denial of Service Attacks (DoS) and Distributed Denial of Service Attacks (DDoS) are one of the most common cyber threats to sabotage information systems. DoS attacks are mainly carried out from a single source and exhaust system resources – server processes, servers, network connectivity and application-level services. This leads to its overload. DDoS attacks can be carried out on a wider range and in a coordinated manner using many complex devices (botnets), which leads to complete or partial disruption of services. The types of DoS and DDoS attacks in the research area (volume attacks, protocol-level attacks and experience-level attacks) are the types of attacks they cause to the business mechanism and network infrastructure. The risks are analyzed. The effectiveness of traditional signature-based methods, anomaly detection models, traffic analysis, behavior-based monitoring, and artificial intelligence-based methods for detecting attacks was examined. The application of firewall systems, IDS/IPS technologies, traffic filtering methods, load balancing, rate limiting mechanisms, network segmentation, and cloud-based DDoS protection services, as countermeasures, was evaluated.

At the same time, it was emphasized that organizational and disciplinary measures – conducting risk analysis, developing risk-free policies, and creating permanent monitoring systems – complement technical defense measures. As a result, effective defense against DoS and DDoS attacks is possible not only through the application of technical means, but also by creating a complex and multi-level vulnerability architecture. Proactive monitoring, real-time analysis mechanisms, and adaptive security models play a key role in ensuring network resilience and information security.

Keywords: *DoS attack, DDoS attack, network security, service availability, IDS/IPS systems*

Giriş

İnformasiya və kommunikasiya texnologiyalarının sürətli inkişafı dövlət idarəçiliyi, maliyyə sistemi, təhsil, mühəndislik, sənaye və hərbi infrastruktur da daxil olmaqla bütün strateji sahələrin sürətli inkişafına səbəb olacaq. Bu, səbəb olub. Rəqəmsal transformasiya prosesləri xidmətlərin işləkliyini, səmərəliliyini artırsa da, yeni təhlükəsizlik risklərini də rəsmiləşdirib. Bu risklər arasında şəbəkə infrastrukturlarını aldatmağa yönəlmiş Xidmətdən imtina (DoS) və Paylaşılan Xidmətdən imtina (DDoS) hücumları xüsusi yer tutur. DoS və DDoS hücumlarının əsas məqsədi server və şəbəkə resurslarını həddindən artıq yükləməklə və xidmətləri istifadəçilər üçün əlçatan etməklə informasiya sistemlərinin normal fəaliyyətini pozmaqdır. Bu, hələ də davam etdirilməlidir. Müasir dövrdə bu hücumlar yalnız texniki problemlər kimi deyil, həm də iqtisadi və milli təhlükə məsələsi kimi qiymətləndirilir. Xüsusilə, bank sektoruna, dövlət informasiya sistemlərinə, enerji və nəqliyyat infrastrukturlarına qarşı kütləvi DDoS hücumları ciddi maliyyə gərginliklərinə, nüfuz risklərinə və sosial iğtişaşlara səbəb olur. DDoS hücumlarının təhlükəsi onların ortaq xarakteri ilə bağlıdır. Minlərlə və ya milyonlarla cihaz (botnet şəbəkələri) istifadə edilərək həyata keçirilən hücumlar klassik müdafiə mexanizmlərini çətin vəziyyətə salır. Hücum trafikini qanuni istifadəçi trafikindən fərqləndirmək, onu real vaxt rejimində təhlil etmək və süzgəcdən keçirmək mürəkkəb texniki yanaşmalar tələb edir (Ouhssini və b., 2024).

Müasir təhlükəsiz konsepsiyada şəbəkə hücumlarının aşkarlanması və qarşısının alınması çoxsəviyyəli müdafiə modelinə əsaslanır. Buraya perimetr təhlükəsizliyi, tətbiq səviyyəli qorunma, şifrələnmiş rabitə mexanizmləri, davranış təhlili və süni intellekt əsaslı monitorinq sistemləri daxildir. Anomaliya aşkarlama metodları, maşın öyrənmə alqoritmləri və böyük məlumatların təhlili texnologiyaları DDoS hücumlarının erkən mərhələdə aşkarlanmasına və zərərin minimuma endirilməsinə imkan verir. Bu, onun yüklənməsinə imkan verir. Məqalənin aktuallığı ondan ibarətdir ki, ədədi iqtisadiyyatın inkişaf etdirildiyi bir vəziyyətdə xidmətlərin səmərəliliyi strateji əhəmiyyət kəsb edir. Elektron hökumət platformaları, rəqəmsal bank sistemləri və bulud əsaslı xidmətlər yüksək səviyyədə təvazökarlıq tələb edir. Bu səbəbdən şəbəkə hücumlarının mexanikasını dərindən öyrənmək, aşkarlama metodlarını təkmilləşdirmək və effektiv müdafiə strategiyaları hazırlamaq müasir azadlıq siyasətinin əsasını təşkil edir. Onun istiqamətlərindən biridir (Pakmehr və b., 2024).

Tədqiqat

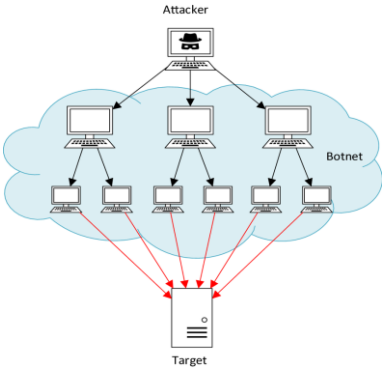
Müasir informasiya cəmiyyətində dövlət qurumları, bank sektoru, elektron ticarət platformaları, təhsil və səhiyyə sistemləri fasiləsiz şəbəkə əlçatanlığına əsaslanır. Rəqəmsal xidmətlərin 24/7 rejimində fəaliyyət göstərməsi artıq texniki üstünlük deyil, strateji zərurət hesab olunur. Bu kontekstdə şəbəkə infrastrukturuna qarşı yönəlmiş Xidmətin İnkarı (DoS) və Paylanmış Xidmətin İnkarı (DDoS) hücumları əlçatanlıq prinsipini (availability) hədəf alan ən təhlükəli kiber təhdidlər sırasındadır. Şəbəkə təhlükəsizliyində üç əsas prinsip – məxfilik (confidentiality), bütövlük (integrity) və əlçatanlıq (availability) – mövcuddur. DoS və DDoS hücumları məhz əlçatanlıq komponentinə qarşı yönəlir. Məqsəd məlumatı oğurlamaq deyil, sistemi istifadəçilər üçün əlçatmaz etməkdir. Bu isə iqtisadi itkilərə, xidmət dayanmasına, reputasiya risklərinə və bəzi hallarda milli təhlükəsizlik problemlərinə səbəb ola bilər (Cichonski və b., 2012).

Cədvəl 1.
DoS və DDoS Modellərinin Müqayisəli Analizi

Meyar	DoS	DdoS
Mənbə sayı	Tək və ya məhdud	Minlərlə və milyonlarla
Aşkarlanma	Nisbətən asan	Çətin və kompleks
Filtrasiya	IP bloklama mümkündür	IP filtrasiya effektiv deyil
Hücum gücü	Məhdud	Böyük miqyaslı
Risk səviyyəsi	Orta	Yüksək

Aparılan müqayisəli təhlil göstərir ki, DoS hücumları struktur baxımından daha sadə, mənbə baxımından məhdud və texniki vasitələrlə nisbətən daha asan idarəolunan xarakter daşiyir. Buna qarşılıq olaraq, DDoS hücumları paylanmış arxitekturaya əsaslandığı üçün genişmiqyaslı, koordinasiyalı və daha yüksək risk səviyyəsinə malikdir.

Şəkil 2. DoS hücumunun sadə modeli

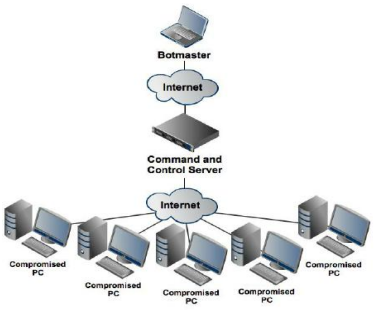


DSoS hücumlarinin təhlükəliliyi onların çoxsaylı mənbələrdən həyata keçirilməsi və hücum trafikinin legitim istifadəçi trafikindən seçilməsinin çətinləşməsi ilə bağlıdır. Bu xüsusiyyət klassik firewall və ip-filtrasiya mexanizmlərinin effektivliyini azaldır və daha kompleks, çoxsəviyyəli müdafiə yanaşmalarını zəruri edir. Məhz buna görə də müasir kibertəhlükəsizlik strategiyası yalniz perimetr müdafiəsi ilə kifayətlənməməli, real vaxt trafik monitorinqi, anomaliya aşkarlama sistemləri, davranış analizi və bulud əsaslı DDoS qoruma xidmətləri kimi inteqrasiya olunmuş mexanizmlər üzərində qurulmalıdır. Beləliklə, DoS və DDoS hücum modellərinin müqayisəli analizi göstərir ki, təhlükəsizlik risklərinin miqyası hücumun struktur mürəkkəbliyi ilə birbaşa əlaqəlidir. Xüsusilə DDoS hücumları müasir şəbəkə sistemləri üçün yüksək səviyyəli təhlükə formalaşdırdığından, adaptiv və proaktiv müdafiə arxitekturasının qurulması kibertəhlükəsizliyin əsas prioritet istiqaməti kimi çıxış edir (Handley və Rescorla, 2006).

DoS (denial of service) hücumu bir və ya məhdud sayda mənbədən hədəf serverə intensiv trafik göndərilməsi yolu ilə həyata keçirilən və sistem resurslarının süni şəkildə tükəndirilməsinə əsaslanan kiber hücum modelidir (Kessler, 2012). Bu hücumun əsas məqsədi serverin cpu, ram və şəbəkə bant genişliyi kimi resurslarini yükləyərək real istifadəçilərin sorğularını emal etməsini əngəlləmək və nəticədə, xidmətin əlçatanlığını pozmaqdır. DoS hücumları, adətən, tək ip ünvanından və ya sabit mənbədən həyata keçirildiyi üçün onların identifikasiyası və bloklanması nisbətən daha asandır. Firewall, access control list (acl) və ip-filtrasiya mexanizmləri vasitəsilə hücum mənbəyi məhdudlaşdırıla və ya tamamilə bloklana bilər. Bununla belə, DoS modeli struktur baxımından sadə olsa da, daha mürəkkəb və genişmiqyaslı DDoS hücumlarının ilkin forması kimi çıxış edə bilər. Bu

səbəbdən DoS hücumlarının vaxtında aşkarlanması və effektiv qarşısının alınması şəbəkə təhlükəsizliyinin təmin olunmasinda mühüm əhəmiyyət kəsb edir.

Şəkil 3. DDoS hücumunun paylanmış modeli



DDoS (distributed denial of service) hücumu DoS modelinin daha mürəkkəb, koordinasiyalı və yüksək riskli formasıdır. Bu hücum növündə məqsəd eyni qalır – xidmətin əlçatanlığını pozmaq – lakin tətbiq mexanizmi daha genişmiqyaslı və sistemlidir. DDoS hücumları minlərlə, hətta milyonlarla yoluxdurulmuş cihazdan ibarət botnet şəbəkələri vasitəsilə həyata keçirilir. Bu cihazlar – kompüterlər, İOT qurğuları, serverlər və digər şəbəkə elementləri – uzaqdan idarə olunan vahid hücum mexanizmi kimi fəaliyyət göstərir (Mirkovic və Reiher, 2004). DDoS hücumlarının əsas təhlükəliliyi onların paylanmış xarakterindən irəli gəlir. Çoxsaylı mənbələrdən eyni anda göndərilən intensiv trafik legitim istifadəçi trafikinə bənzəyə bildiyindən, onun filtrasiya edilməsi və bloklanması çətinləşir. Klassik ip-filtrasiya və perimetr müdafiə mexanizmləri belə hallarda effektivliyini itirir. Hücum nəticəsində yalnız server resursları deyil, həm də şəbəkə infrastrukturu – routerlər, switch-lər və firewall sistemləri – yüklənə və iflic vəziyyətinə düşə bilər (Singh və b., 2024). Müasir dövrdə DDoS hücumlarının miqyası terabit/saniyə səviyyəsinə çata bilir ki, bu da ənənəvi müdafiə arxitekturalarını aşaraq genişmiqyaslı xidmət dayanmasına səbəb olur. Bu səbəbdən DDoS hücumları kibertəhlükəsizlik sahəsində ən ciddi və kompleks təhdidlərdən biri kimi qiymətləndirilir və onların qarşısının alınması üçün çoxsəviyyəli, adaptiv və real vaxt əsaslı müdafiə strategiyaları tələb olunur.

Qarşısının alınması baxımından ilk vacib istiqamət preventiv şəbəkə konfiqurasiyasıdır. Buraya Access Control List (ACL), ingress və egress filtrasiya, source address validation, unicast Reverse Path Forwarding (uRPF) kimi mexanizmlər daxildir. NIST tövsiyələrinə görə, IP spoofing-in qarşısının alınması DDoS riskinin azalmasında əsas tədbirlərdən biridir. Əgər saxta mənbə ünvanları şəbəkə sərhədində bloklanarsa, əks etdirmə əsaslı hücumların effektivliyi əhəmiyyətli dərəcədə azalır. Bundan əlavə, RTBH (Remotely Triggered Black Hole), Flowspec və Response Rate Limiting kimi texnologiyalar operator səviyyəsində hücum trafikinə daha çevik reaksiya verməyə imkan yaradır. Bu vasitələr xüsusilə böyük həcmli hücumlarda mühüm rol oynayır. Müdafiənin ikinci istiqaməti infrastrukturun dayanıqlılığının artırılmasıdır. Yük balanslaşdırma, CDN istifadəsi, coğrafi paylanmış server infrastrukturu, autoscaling, ehtiyat kanal və rezerv resurslar hücum təsirini azalda bilər. CISA-nın həcm əsaslı DDoS hücumlarına dair texniki rəhbərliyində CDN və bulud əsaslı qoruma xidmətlərinin hücum trafikinə qarşı absorbsiya və yayma qabiliyyətinə görə mühüm əhəmiyyət daşıdığı göstərilir. Xüsusən veb xidmətlər üçün WAF, rate limiting, CAPTCHA, sessiya nəzarəti və tətbiq səviyyəli sorğu filtrasiya mexanizmləri HTTP flood kimi tətbiq qatında baş verən DDoS hücumlarının qarşısını almaqda effektivdir. Burada məqsəd təkcə zərərli trafiki azaltmaq deyil, həm də qanuni istifadəçinin xidmətə çıxışını maksimum dərəcədə qorumaqdır (Nelson və b., 2025).

Müasir yanaşmalarda avtomatlaşdırılmış cavab sistemləri də xüsusi əhəmiyyət kəsb edir. Təhlükəsizlik orkestrasiya platformaları, SIEM inteqrasiyası və telemetriya əsaslı DDoS siqnallaşma mexanizmləri hücumun erkən mərhələdə müəyyən edilməsinə və cavabın avtomatik şəkildə işə salınmasına imkan verir. IETF-in DOTS yanaşması da DDoS hadisələri zamanı hücum siqnallarının və telemetriyanın standartlaşdırılmış şəkildə paylaşılmasını nəzərdə tutur (Somani və b., 2017). Bu,

xüsusilə provayder, müştəri və müdafiə xidməti arasında koordinasiyanı yaxşılaşdırır. Belə sistemlər vasitəsilə trafik diversion, scrubbing center aktivləşdirilməsi, qayda yenilənməsi və hücum mənbələrinin dinamik bloklanması daha operativ icra olunur. Nəticə etibarilə, DoS və DDoS hücumlarının aşkarlanması və qarşısının alınması yalnız bir təhlükəsizlik vasitəsi ilə təmin oluna bilməz. Effektiv müdafiə üçün trafik monitorinqi, anomaliya aşkarlanması, çoxsəviyyəli filtrasiya, tətbiq təhlükəsizliyi, provayder əməkdaşlığı və insidentə cavab planları bir-birini tamamlamalıdır (Sriram və b., 2019). Ən səmərəli model proaktiv yanaşmaya əsaslanır: normal trafik profilinin qurulması, riskli nöqtələrin əvvəlcədən müəyyənləşdirilməsi, ehtiyat resursların planlaşdırılması və avtomatlaşdırılmış cavab mexanizmlərinin hazırlanması. Belə kompleks yanaşma həm hücumların vaxtında aşkarlanmasına, həm də onların xidmət davamlılığına təsirinin minimuma endirilməsinə imkan verir.

Nəticə

Təhlillər göstərir ki, DoS və DDoS hücumları müasir şəbəkə infrastrukturlarının gizli fəaliyyətinə qarşı əsas təhdidlərdən biridir. DoS hücumları struktur baxımından daha sadə və məhdud olsa da, DDoS hücumları ortaq arxitekturasına görə daha geniş əsaslı və təhlükəlidir (Zargar və b., 2013). Xüsusilə, botnet şəbəkələri vasitəsilə həyata keçirilən əlaqələndirilmiş hücumlar eyni vaxtda server resurslarını, şəbəkə bant genişliyini və infrastruktur elementlərini hədəf alır və xidmətlərin tam mövcudluğunu təmin edir. Bu, səbəb ola bilər. Müasir şəraitdə klassik firewall və ip-filtrləmə mexanizmləri təkcə kifayət deyil. Effektiv müdafiə üçün çoxsəviyyəli zərərsizlik arxitekturası yaratmaq lazımdır. Bu model real vaxt rejimində trafik monitorinqi, anomaliya aşkarlama sistemləri, davranış təhlili, ids/ips texnologiyaları və bulud əsaslı DDoS qoruma xidmətlərini əhatə etməlidir. Proaktiv risk təhlili və davamlı monitorinq mexanizmləri hücumların erkən mərhələdə aşkarlanmasına və zərərin minimuma endirilməsinə imkan verir. Nəticədə, DoS və xüsusilə DDoS hücumlarına qarşı mübarizə yalnız texniki məsələ deyil, həm də strateji risksiz prioritetdir. Rəqəmsal xidmətlərin səmərəliliyini təmin etmək üçün adaptiv, inteqrasiya olunmuş və daim yenilənən təkəbbür strategiyası tətbiq etmək lazımdır (Zhou və b., 2022).

Ədəbiyyat

1. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2).* National Institute of Standards and Technology.
2. Handley, M., & Rescorla, E. (2006). *Internet Denial-of-Service Considerations (RFC 4732).* RFC Editor. https://doi.org/10.17487/RFC4732
3. Kessler, G. C. (2012). *Denial-of-Service Attacks. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), Computer security handbook (6th ed.).* Wiley.
4. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53. https://doi.org/10.1145/997150.997156
5. Nelson, A., Quinn, S., Johnson, V., Scarfone, K., & Smith, M. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
6. Ouhssini, M., El Haddad, S., Mansouri, K., & Qbadou, M. (2024). Advancements in detecting, preventing, and mitigating distributed denial-of-service attacks in cloud environments: A systematic review. *Ain Shams Engineering Journal*. *Advance online publication*.
7. Pakmehr, A., Ghaffari, A., & Hosseinzadeh, M. (2024). *DDoS attack detection techniques in IoT networks: A survey. Cluster Computing*. Advance online publication.
8. Singh, C., De, D., & Buyya, R. (2024). A comprehensive survey on DDoS attacks detection and defense in SDN-based IoT networks. *Array, 24*, Article 100361.

9. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications, 107*, 30–48. https://doi.org/10.1016/j.comcom.2017.03.010
10. Sriram, K., Montgomery, D., Borchert, O., Kim, O., & Seo, S. (2019). Problem definition and technical requirements for a more resilient Internet routing infrastructure (NIST SP 800-189). *National Institute of Standards and Technology*.
11. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.
12. Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2022). Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer Networks, 174*, Article 107247.

Daxil oldu: 02.01.2026
Qəbul edildi: 08.04.2026