PARADIGMA, No.4, 2025, səh.137-141
https://doi.org/10.30546/30015.2025.01.4.1072

TƏŞKİLATLARDA DDoS HÜCUMLARINDAN MÜDAFİƏNİN EFFEKTİV YOLLARI

Ş.A. Əhmədova, A.X. Xanməmmədov
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: shams.ahmadova@student.au.edu.az

Xülasə. DDoS hücumlarının mahiyyəti hədəf sistemlərin işini pozmaq, resurslarının tükənməsinə səbəb olmaqdır. Hücumların qarşısını almaq üçün şəbəkə və sistemlər izlənir, trafik təhlil olunur və qabaqlayıcı tədbirlər görülür. Bu yanaşma xidmətlərin davamlılığını və operativ müdaxiləni təmin edir.

Açar sözlər: DDoS, şəbəkə təhlükəsizliyi, trafik analizi, insident cavabı, firewall konfiqurasiyası.

Giriş

DDoS hücumları çoxsaylı mənbələrdən eyni vaxtda yönəldilən zərərli trafik vasitəsilə hədəf sistemləri əlçatmaz vəziyyətə gətirir. Paylanmış xidmətdən imtina hücumu internetdə ən geniş yayılmış kiberhücum növüdür və məqsədi hədəf sistem, server və ya xidmətin normal fəaliyyətini dayandırmaqdır. DDoS hücumu təkcə xidmətlərin dayanmasına səbəb olmur, həm də təşkilatın reputasiyasına, müştərilərin etibarına və əməliyyat davamlılığına ciddi təsir göstərə bilir [2]. Bu cür hücumların mahiyyəti ondan ibarətdir ki, xidmət göstərən resurslar qısa müddətdə həddindən artıq yüklənir. Nəticə olaraq, sistem ya yavaşlayır, ya da xidmət göstərə bilmir (əlçatan olmur). Buna görə də təşkilatlar yalnız hücum baş verdikdə ona qarşı müdafiə olunmaqla kifayətlənməməlidirlər. Əsas məsələ mümkün riskləri əvvəlcədən görmək, kritik infrastrukturun zəif tərəflərini müəyyənləşdirmək və hücum baş vermədən qarşısını ala biləcək tədbirləri planlaşdırmaqdır. DDoS təhlükəsinə qurumun hazır olması onun informasiya sisteminin texniki cəhətdən dayanıqlığını artırır, gözlənilməz vəziyyətlərdə operativ qərar vermə imkanı yaradır. Bu baxımdan təşkilatların hücumdan əvvəl atmalı olduğu addımlar böyük əhəmiyyətə malikdir.

Preventiv tədbirlərin əsas istiqamətləri

İnformasiya sistemləri olan müəssisələr DDoS hücumlarının dəqiq vaxtını əvvəlcədən təxmin edə bilməz, bu cür hücumlar gözlənilmədən baş verir. Buna baxmayaraq, zərərli şəxslər, kibercinayətkarlar şəbəkə və sistemlərin zəif tərəflərini aktiv şəkildə axtarır və tapdıqları boşluqlardan hücum məqsədilə istifadə etməyə çalışırlar. Bu səbəbdən təşkilatların təhlükəsizlik komandaları yalnız hücumun təsirlərini azaltmaqla kifayətlənməməli, həm də mümkün hücumları əvvəldən nəzərə alaraq qabaqlayıcı tədbirlər görməlidirlər [4]. Bu tədbirlər şəbəkənin dayanıqlığını artırmaq, kritik xidmətlərin işini qorumaq və potensial itkiləri minimuma endirmək məqsədi

daşıyır. Beləliklə, preventiv strategiyalar tətbiq etməklə təşkilatlar hücum baş verməzdən əvvəl riskləri qiymətləndirər, zəiflikləri aradan qaldırar və hücum zamanı operativ müdaxilə edə bilər.

1. Risklərin təhlili və qiymətləndirilməsi

Təşkilatların paylanmış xidmətdən imtina hücumuna qarşı həssalığını qiymətləndirmək üçün hərtərəfli risk analizi aparmaq vacibdir. Bu proses şəbəkə infrastrukturunda, sistem və tətbiqlərdə mövcud olan potensial zəiflikləri müəyyən etməyə imkan verir. Risklərin dəyərləndirilməsi eyni zamanda DDoS hücumlarının təşkilata təsirini anlamağa kömək edir və təhlükəsizlik tədbirlərinin prioritetləşdirilərək sistematik şəkildə həyata keçirilməsinə şərait yaradır. Risklərin təhlili ilə şəbəkədə, sistemdə olan zəifliklər müəyyən olunur, onlara qarşı müdafiə strategiyaları hazırlanır.

2. Şəbəkə monitorinqi

DDoS hücumlarına qarşı şəbəkə monitorinqi şəbəkənin və sistemin təhlükəsizliyini təmin edir, sistemin işinin fasiləsizliyi üçün əhəmiyyətə malikdir. Baş verə biləcək əvvəlcədən məlum təhlükələrə qarşı şəbəkə monitorinqi vacib addımlardan biri hesab olunur. Monitorinq zamanı anomaliyalar aşkar edilir:

- Trafik həcminin qəfildən artması (saniyədə 100 sorğu gəlirdisə, birdən 10000 olur);
- Şübhəli və bilinməyən İP-lərdən oxşar sorğuların gəlməsi (HTTP flood);
- Minlərlə yarımçıq olan SYN paketlərinin görünməsi;
- Resurların tükənməsinə qədər gətirən RAM, CPU istifadəsi;
- Bant genişliyi (band with) istifadəsinin birdən 100% olması. Normal şəbəkə trafikində bu istifadə 20-30% arası olur;
- Eyni porta anidən yüzminlərlə sorğunun gəlməsi;
- Loglarda qeydlərin təkrarlanması – "request timeout", "too many connection", "max client reached";
- Anomal paket ölçüləri: Çox böyük UDP paketləri, boş TCP paketləri, çox kiçik paket axınları (ping flood);

Monitorinq nəticəsində normal və şübhəli trafik müqayisə olunur, hücum növünü müəyyənləşdirib operativ cavab vermək, resursların həddindən artıq yüklənməsinin qarşısını almaq mümkündür.

3. Captcha inteqrasiyası

Vebsaytlar və onlayn xidmətlərdə Captcha mexanizminin tətbiqi kompüter istifadəçilərin real insan yoxsa avtomatlaşdırılmış botlar olduğunu fərqləndirməyə imkan verir. Əsas məqsədi botları

(avtomatik proqramları) bloklamaq, veb səhifələrə spam hücumlarının qarşısını almaqdır. Bu profilaktik müdafiə üsulu, DDoS hücumlarının təsirini azaltmaq və sistemlərin dayanıqlığını artırmaq üçün effektiv vasitədir. Beləki, botlar veb səhifələrə avtomatlaşdırılmış sorğular göndərdikdə captcha onların qarşısını alır, serverin resurslarını qorumaq üçün istifadə edilə bilər. Lakin böyük volumetrik hücumlarda isə (bandwidth overload) Captcha kifayət qədər səmərəli deyil [1].

4. Bant Genişliyi Tutumunun Planlaşdırılması

DDoS hücumları zamanı trafikin anidən artması şəbəkənin fəaliyyətinə ciddi təsir göstərə bilər. Buna görə də təşkilatlar cari bant genişliyi tutumunu qiymətləndirməli və lazım gələrsə, onu artırmaq üçün tədbirlər görməlidirlər. Bant genişliyinin optimal səviyyədə saxlanması, həm qanuni istifadəçilərin xidmətlərə çıxışını təmin edir, həm də hücumun yaratdığı təsiri azaltmağa kömək edir. Bu yanaşma, kritik şəbəkə və server resurslarının həddindən artıq yüklənməsinin qarşısını almaq üçün qabaqlayıcı tədbir kimi qəbul edilir.

5. Trafik analizi

Şəbəkə trafiki mütəmadi olaraq təhlil edilməli və şəbəkənin normal fəaliyyət göstərməsi müəyyənləşdirilməlidir. Bu təhlil şəbəkə təhlükəsizliyini qorumaq üçün əsas addımlardan biri hesab olunur və paylanmış xidmətdən imtina (DDoS) hücumu zamanı anomaliyaların, əhəmiyyətli fərqliliklərin aşkarlanmasını asanlaşdırır.

6. Hadisələrə cavab planı (Incident response plan)

DDoS hücumları üçün hərtərəfli insident cavab planı hazırlanmalıdır. Plan hücum baş verdikdə atılacaq addımları, məsuliyyət bölgüsünü, kommunikasiya kanallarını (communication channels) və təsirin minimuma endirilməsi üçün əvvəlcədən müəyyən edilmiş strategiyaları əhatə etməlidir. Belə bir plan təşkilatın hücum zamanı operativ və koordinasiyalı şəkildə reaksiya verməsinə imkan yaradır.

7. DDoS azaldılması xidməti (DDoS mitigation service)

DdoS hücumlarının qarşısının alınması üçün xüsusi xidmətlər təşkilatlara DDoS hücumlarının təsirini minimuma endirməyə imkan verir. Bu xidmətlər provayderlər tərəfindən təqdim olunur və genişmiqyaslı hücumları idarə etmək üçün xüsusi infrastruktur və dərin təcrübəyə malikdirlər. Belə xidmətlər zərərli trafikin şəbəkəyə daxil olmadan əvvəl süzülməsini təmin edir, kritik sistemlərin və xidmətlərin normal fəaliyyətini qoruyur. Nəticədə, həm əməliyyat itkisi azalır, həm də təşkilatın müştərilərə və istifadəçilərə təqdim etdiyi xidmətin dayanıqlılığı təmin edilir. Bu

xidmətlər həmçinin hücum zamanı resursların həddindən artıq yüklənməsinin qarşısını almağa, şəbəkə performansını qorumağa və təşkilatın təhlükəsizlik strategiyalarını gücləndirməyə kömək edir.

8. Yük Balanslaşdırma (Load balancing)

Şəbəkə trafiki və tətbiq sorğularını serverlər və ya məlumat mərkəzləri arasında paylamaq üçün yük balanslaşdırma həllərindən istifadə mütləqdir. Yük balanslaşdırma sistemi dedikdə, trafiki optimal şəkildə paylayaraq, hər hansı bir serverin və ya xidmət nöqtəsinin donmasının qarşısını alır. Bu vasitə sistemin normal işləməsi zamanı performansını artırır, həm də DDoS hücumları zamanı sistemin davamlılığını, istifadəçi sorğularında vaxtında cavab verməsini təmin edir. Beləliklə, kritik xidmətlər hücum olsa belə əlçatan qalır və infrastruktura, şəbəkə təhlükəsizliyinə yönəlmiş risklər azaldılır.

9. Firewall Konfiqurasiyası

Müəssisələr firewall-larını elə konfiqurasiya etməlidirlər ki, bilinən zərərli IP-lərdən (şəbəkələrə hücum etmək, virus yaymaq, spam göndərmək və ya DDoS hücumları həyata keçirmək üçün əvvəllər istifadə edilmiş IP-lər) şübhəli trafik axınlarını filtr edə bilsinlər. Firewall-da qayda təyin etmək yazılı xarakter daşıyır, lakin yeni hücum vektorları və IP-lər sürətlə dəyişdiyi üçün bunu mütəmadi olaraq yeniləmək lazımdır. Şəbəkə və resursları yükləyən trafiki idarə etməkdə sürət məhdudlaşdırılması (rate limiting) vacib vasitədir [3]. Belə tədbirlər sistemi daha dayanıqlı etməklə yanaşı, istifadəçi əməliyyatlarını da qorumağa kömək edir.

10. İşçilərin maarifləndirilməsi və təlimi

Kritik informasiya sistemlərinə sahib təşkilatlarda işləyən işçilərin DDoS hücumu barədə maarifləndirilməsi əhəmiyyətli proses hesab olunur. İşçilərə DDoS hücumunun təsviri verilməli, hücum barədə onlarda ilkin anlayış yaradılmalıdır. Paylanmış xidmətdən imtina hücumunun xarakterik əlamətləri göstərilməli (saytın və ya sistemin yavaş işləməsi, internet sürətinin anidən azalması), hücum zamanı ediləcək tədbirlərlə tanış olmalıdırlar. Şübhəli fəaliyyətləri tanıyan işçilər onlara qarşı yönəlmiş sosial mühəndislik üsullarından və bu üsulların nəticəsində sistemə edilə biləcək DDoS hücumlarından qorunmuş olacaqdır. Maarifləndirmə formaları olaraq simulasiya testlərindən, video və slayd təqdimat formalarından, qısa (aylıq) təlimlərdən, elektron xəbərdarlıq mesajlarından istifadə etmək səmərəlidir.

Nəticə

DDoS hücumları təşkilatların xidmətlərinin əlçatanlığına, nüfuzuna və əməliyyat davamlılığına ciddi təsir edən əsas kibertəhlükələr arasındadır. Bu hücumların əsasını qısa müddət ərzində xidmət resurslarının həddindən artıq yüklənməsi təşkil etdiyinə görə, yalnız hücum anında müdafiə tədbirləri görmək kifayət deyil. Təşkilatlar riskləri vaxtında aşkar etməli, şəbəkə monitorinqi, bant genişliyi planlaması, trafik analizi, DDoS azaldılması xidmətləri, yük balanslaşdırılması daxil olmaqla profilaktik tədbirlərdən istifadə etməli və həmçinin mütəmadi olaraq əməkdaşlarını maarifləndirməlidirlər. Bu tədbirlər vasitəsilə təşkilatın texniki dayanıqlılığı artırılır, hücumların təsiri minimuma endirilir və kritik xidmətlər müntəzəm olaraq təmin edilir.

Ədəbiyyat

1. OWASP, (2021), Automated Threats to Web Applications, The Open Web Application Security Project: : [Elektron resurs] / - 02 dekabr, 2025. URL: https://owasp.org/www-project-automated-threats-to-web-applications/
2. Mirkovic J., & Reiher P., (2004), A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review, 34(2), p. 39-53.
3. Stallings W., (2018), Network Security Essentials: Applications and Standards (6th Edition), Pearson Education.
4. 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), p. 2046-2069.

EFFECTIVE WAYS TO DEFEND ORGANIZATIONS AGAINST DDoS ATTACKS

Sh.A. Ahmadova, A.Kh. Khanmammadov
Azerbaijan University, Jeyhun Hajibeyli 71, Baku, Azerbaijan

Abstract: The essence of DDoS attacks is to disrupt the operation of target systems and deplete their resources. To prevent these attacks, networks and systems are monitored, traffic is analyzed, and proactive measures are implemented. This approach ensures service continuity and enables prompt response.

Keywords: DDoS, network security, traffic analysis, incident response, firewall configuration.