ISSN 3060-4567

DoS/DDoS HUJUMLARI VA ULARNI BARTARAF ETISH USULLARI

Yariqulov Sherzod Shokirovich, *University of management and future technologies universiteti M021-23KIDTo‘ guruh magistri*

Annotatsiya: DDoS (Distributed Denial of Service) hujumi – bu bir nechta *manbalardan server yoki tarmoq xizmatlarini haddan tashqari yuklash orqali ularning ish faoliyatini izdan chiqarishga qaratilgan kiberhujumdir. Ushbu hujumlar ko‘pincha botnetlar yordamida amalga oshiriladi.DDoS hujumlarini bartaraf etish usullari quyidagilardan iborat. Maqolada DDoS hujumlarining zamonaviy metodlari, real vaqtli tahlil vositalari hamda samarali himoya choralariga oid yondashuvlar yoritilgan.*

Kalit so‘zlar: *DoS, DDoS hujumi , kiberxavfsizlik, tarmoq himoyasi,xakerlik hujum, botnet, trafik filtrlash,IP bloklash, zararli trafik,tarmoq monitoringi, Cloud-based himoya Firewall, Load balancing, , UDP floo, HTTP flood CDN (Content Delivery Network, Rate limiting*

Abstract: DDoS (Distributed Denial of Service) attack *is a cyber attack aimed at disrupting the functionality of a server or network services by overwhelming them with excessive traffic from multiple sources. These attacks are often carried out using botnets. The methods for mitigating DDoS attacks include the following. This article discusses modern methods of DDoS attacks, real-time analysis tools, and approaches to effective protection measures.*

Keywords: *DoS attack, DDoS attack, cybersecurity, network protection, hacker attack, botnet, traffic filtering, IP blocking, malicious traffic, network monitoring, cloud-based protection, firewall, load balancing, UDP flood, HTTP flood, Content Delivery Network (CDN), rate limiting.*

Аннотация: DDoS (Distributed Denial of Service) атака *— это кибератака, направленная на выведение из строя работы серверов или сетевых сервисов путем их чрезмерной загрузки с нескольких источников. Такие атаки*

часто осуществляются с помощью ботнетов. Методы защиты от DDoS-атак включают в себя следующие меры. В статье рассматриваются современные методы проведения DDoS-атак, инструменты анализа в реальном времени, а также эффективные подходы к защите от них.

Ключевые слова: *DoS-атака, DDoS-атака, кибербезопасность, защита сети, хакерская атака, ботнет, фильтрация трафика, блокировка IP-адреса, вредоносный трафик, мониторинг сети, облачная защита, межсетевой экран (фаервол), балансировка нагрузки, UDP flood, HTTP flood, сеть доставки контента (CDN), ограничение частоты запросов (rate limiting)*

Kirish. Axborot texnologiyalari rivojlanishi bilan birga kiberxavfsizlik tahdidlari ham ortib bormoqda. Shulardan biri – DDoS (Distributed Denial of Service) hujumi, ya’ni tarqatilgan xizmat ko‘rsatishdan voz kechish hujumidir. Ushbu hujumlar tizim yoki serverga haddan tashqari ko‘p so‘rov yuborish orqali uning normal ishlashini izdan chiqarishga qaratilgan. Natijada veb-saytlar, internet xizmatlari yoki korporativ tarmoqlar ishdan chiqishi mumkin. DDoS hujumlari odatda botnetlar orqali amalga oshiriladi, bunda bir nechta zararli qurilmalar boshqarilib, maqsadli serverga bir vaqtda hujum uyushtiriladi. Bu esa hujumni aniqlash va oldini olishni qiyinlashtiradi. Mazkur mavzuda DDoS hujumlarining turlari, ularning ishlash mexanizmi hamda bunday tahdidlardan himoyalanish usullari haqida so‘z yuritamiz. Zamonaviy xavfsizlik choralarini qo‘llash orqali bunday hujumlarning oldini olish va ularning zararini kamaytirish mumkin. DDoS hujumlarining asosiy turlari:Volume-based (hajmga asoslangan) hujumlar – server yoki tarmoqni haddan tashqari katta trafik bilan bosib, uning ishlashini izdan chiqaradi. UDP flood – ko‘p sonli UDP paketlar yuborish orqali tarmoqni yuklash. ICMP flood (Ping flood) – ortiqcha ping so‘rovlar bilan serverni ishdan chiqarish.DNS amplification – so‘rovlarni ko‘paytirish orqali tarmoq bandligini to‘ldirish.Protocol-based (protokolga asoslangan) hujumlar – tarmoqning ishlash mexanizmlaridan foydalanib hujum uyushtirish.

1. DDoS hujumlarining zamonaviy shakllari va xususiyatlari

DDoS hujumlari ilk marotaba 1990-yillarda paydo bo‘lgan bo‘lsa-da, hozirgi kunda ularning shakl va mexanizmlari sezilarli darajada rivojlangan. Hujumchilarning maqsadi tizimga haddan ortiq trafik yuborib, u resurslarni ishlamay qolish holatiga olib kelishdir. Bugungi kunda DDoS hujumlarining quyidagi shakllari keng tarqalgan:

- Volumetrik hujumlar - ko‘pincha sun’iy ravishda katta hajmdagi trafik yuborilishi orqali amalga oshiriladi. Masalan, UDP flood, ICMP flood kabi texnikalar orqali serverlar zo‘riqishga duchor qilinadi.
- Protokol darajasidagi hujumlar - SYN flood yoki Ping of Death kabi hujumlar tarmoq protokollari orqali tizimning zaifliklaridan foydalanib amalga oshiriladi. Bu usullar tarmoq infratuzilmasini ishdan chiqarishga qaratilgan.
- Ilova darajasidagi hujumlar- ko‘proq veb-ilovalarga yo‘naltirilgan bo‘lib, HTTP GET/POST so‘rovlar orqali ishlaydi. Ular ancha murakkab va aniqlash qiyin bo‘lishi mumkin.

DDoS hujumlari bugungi kunda katta xavf tug‘diradi, chunki ular tezda tashkilotlar uchun jiddiy biznes xavfini keltirib chiqaradi. Hujumlar turli shakllarda bo‘lishi mumkin, va har bir hujumning oldini olish uchun turli xil himoya choralarini qo‘llash zarur. DDoS hujumlarini oldini olishda eng samarali yondashuvlardan biri har tomonlama himoya tizimlarini yaratishdir. DDoS hujumlarining bartaraf etilishida har bir kompaniya uchun mos keladigan usullarni tanlash zarur. Bu usullar trafikni filtrlash, load balancing, rate limiting, WAF va scrubbing markazlarini o‘z ichiga oladi. Bularning barchasi tizimlarni himoya qilishda samarali bo‘lishi mumkin, ammo ularni birgalikda qo‘llash, hujumlarni to‘liq bartaraf etishga yordam beradi. Bulutli xavfsizlik xizmatlari (masalan, Cloudflare yoki AWS Shield) DDoS hujumlarini bartaraf etishda juda samarali hisoblanadi. Bu xizmatlar katta miqdordagi trafikni tozalashga yordam beradi, shu bilan birga resurslarni himoya qiladi va hujumlarni aniqlashni osonlashtiradi.Tizim va tarmoq monitoringi ham DDoS hujumlarini tezda aniqlashda muhim rol o‘ynaydi. Muntazam ravishda tarmoq faoliyatini monitoring qilish va xavfsizlik tizimlarini yaxshilash kompaniyaning himoya imkoniyatlarini oshiradi.DDoS hujumlarining oldini olish uchun ko‘p bosqichli xavfsizlik choralarini ishlab chiqish zarur. Bu faqat bitta usulga tayanib qolmasdan, barcha imkoniyatlarni

birlashtirishni talab qiladi. Masalan, tarmoqda yukni taqsimlash va zararlangan trafikni so‘rovlardan ajratish samarali bo‘lishi mumkin.

2. DDoS hujumlarini tahlil qilish usullari

DDoS hujumlarini samarali aniqlash va ularga qarshi kurashish uchun ularni chuqur tahlil qilish talab etiladi. Tahlil jarayoni hujumlarni erta bosqichda aniqlash va ularning oqibatlarini kamaytirishga qaratilgan. DDoS hujumlari tashkilotlar va foydalanuvchilar uchun turli xil salbiy oqibatlarga olib kelishi mumkin. Ularning asosiy natijalari quyidagilardir: DDoS hujumlari eng birinchi navbatda xizmatni to‘xtatadi yoki uning ishlashini sekinlashtiradi. Masalan, katta miqdordagi so‘rovlar tufayli serverlar yuki oshadi va foydalanuvchilar saytlarga kira olmaydi. Bu kompaniyalar uchun jiddiy muammolarni keltirib chiqarishi mumkin.DDoS hujumlari davom etgan paytda xizmatlar ishlamasligi sababli kompaniyalar savdo yoki foydalanuvchilardan daromad olish imkoniyatidan mahrum bo‘ladi. Ularning ` 140 ishdan chiqish vaqti ko‘p hollarda biznes uchun katta moliyaviy zararga olib keladi, ayniqsa bu oylik yoki har yilgi daromadlar bilan bog‘liq bo‘lsa.Doimiy ravishda DDoS hujumlariga duchor bo‘lgan kompaniyalar o‘z mijozlarining ishonchini yo‘qotishi mumkin. Bu esa kompaniyaning obro‘siga zarar yetkazadi va uzoq muddatli biznes munosabatlariga salbiy ta'sir qiladi. Bu holatda, mijozlar xizmatlarining barqarorligi va xavfsizligi haqida salbiy fikrda bo‘lishadi. DDoS hujumlari tizimning resurslarini befoyda ishlatishga olib keladi. Tizim administratorlari zararli trafikni ajratib olish va tarmoqni himoya qilish uchun qo‘shimcha vaqt va resurslarni sarflaydilar. Bu holatda kompaniyaning texnik xodimlarining ishtiroki va tizim resurslarining samarali ishlatilishi cheklanadi.

3. Hujumni bartaraf etish choralari va ularning turlari.

DDoS hujumlari bugungi kunda katta xavf tug‘diradi, chunki ular tezda tashkilotlar uchun jiddiy biznes xavfini keltirib chiqaradi. Hujumlar turli shakllarda bo‘lishi mumkin, va har bir hujumning oldini olish uchun turli xil himoya choralarini qo‘llash zarur. DDoS hujumlarini oldini olishda eng samarali yondashuvlardan biri har tomonlama himoya tizimlarini yaratishdir. DDoS hujumlarining bartaraf etilishida har bir kompaniya uchun mos keladigan usullarni tanlash zarur. Bu usullar trafikni

filtrlash, load balancing, rate limiting, WAF va scrubbing markazlarini o‘z ichiga oladi.

Bularning barchasi tizimlarni himoya qilishda samarali bo‘lishi mumkin, ammo ularni birgalikda qo‘llash, hujumlarni to‘liq bartaraf etishga yordam beradi. Bulutli xavfsizlik xizmatlari (masalan, Cloudflare yoki AWS Shield) DDoS hujumlarini bartaraf etishda juda samarali hisoblanadi. Bu xizmatlar katta miqdordagi trafikni tozalashga yordam beradi, shu bilan birga resurslarni himoya qiladi va hujumlarni aniqlashni osonlashtiradi.Tizim va tarmoq monitoringi ham DDoS hujumlarini tezda aniqlashda muhim rol o‘ynaydi. Muntazam ravishda tarmoq faoliyatini monitoring qilish va xavfsizlik tizimlarini yaxshilash kompaniyaning himoya imkoniyatlarini oshiradi.

DDoS hujumlarining oldini olish uchun ko‘p bosqichli xavfsizlik choralarini ishlab chiqish zarur. Bu faqat bitta usulga tayanib qolmasdan, barcha imkoniyatlarni birlashtirishni talab qiladi. Masalan, tarmoqda yukni taqsimlash va zararlangan trafikni so‘rovlardan ajratish samarali bo‘lishi mumkin.

Xulosa va takliflar

DDoS (Distributed Denial of Service) hujumlari internet xavfsizligi uchun jiddiy tahdid tug‘diradi va nafaqat texnik, balki biznes va moliyaviy nuqtai nazardan ham katta zararlar keltirishi mumkin. Bu hujumlar serverlar va tarmoqlarni ortiqcha trafik bilan to‘ldirib, xizmatlarning ishlashini to‘xtatadi yoki sekinlashtiradi. Natijada, tashkilotlar mijozlar ishonchini yo‘qotishi, moliyaviy yo‘qotishlarga uchrashi va obro‘larini zarar ko‘rishi mumkin.

DDoS hujumlarini samarali tarzda bartaraf etish uchun turli xil usullar, jumladan, trafikni filtrlash, load balancing, rate limiting, WAF tizimlari va bulutli xavfsizlik xizmatlari kabi himoya choralarini qo‘llash zarur. Biroq, DDoS hujumlarining to‘liq oldini olish mumkin emas, chunki hujumchilar har doim yangi usullarni ishlab chiqishadi. Shuning uchun tashkilotlar ko‘p bosqichli himoya strategiyasini amalga oshirib, tizimlarni muntazam ravishda monitoring qilishlari va xavfsizlikni doimiy ravishda yaxshilashlari kerak.DDoS hujumlarini to‘liq oldini olish mumkin bo‘lmasa ham, ko‘p bosqichli himoya tizimini joriy etish muhimdir.

Bu tizimga trafikni filtrlash, so‘rovlarni cheklash, WAF tizimlaridan foydalanish, va bulutli xavfsizlik xizmatlaridan foydalanishni o‘z ichiga olishi kerak. Tizim va tarmoqni doimiy ravishda monitoring qilish DDoS hujumlarini tezda aniqlash va ularni bartaraf etishda yordam beradi. Hujumlarni dastlabki bosqichlarda aniqlash va to‘xtatish uchun zamonaviy monitoring vositalaridan foydalanish zarur. Tarmoq va serverlar resurslarining ortiqcha yuklanishini oldini olish uchun load balancing (yukni taqsimlash) texnologiyalarini joriy qilish tavsiya etiladi. Bu, tarmoqdagi talablarni bir nechta serverga taqsimlash orqali tizimning barqarorligini saqlashga yordam beradi. Ular hujumlarni tezda aniqlash, bartaraf etish va zararni kamaytirish bo‘yicha aniq protokollarga ega bo‘lishlari zarur. Bulutli xavfsizlik xizmatlari va scrubbing markazlaridan foydalanish DDoS hujumlarini samarali bartaraf etish uchun yaxshi yechimdir. Bu xizmatlar tarmoqda zararli trafikni aniqlab, tozalab, faqat haqiqiy foydalanuvchi so‘rovlarini serverga yuborish imkonini beradi.Hujumlardan keyin tahlil qilish va ularni o‘rganish, kelajakdagi hujumlarga qarshi yangi himoya choralarini ishlab chiqish uchun muhimdir. Har bir DDoS hujumi va uning samarasini o‘rganish, tashkilotlarga yangi xavfsizlik strategiyalarini yaratishda yordam beradi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. (2020). *Network Security Essentials*. Pearson.
2. Mirkovic, J., & Reiher, P. (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms". *ACM SIGCOMM*.
3. Roesch, M. (1999). "Snort - Lightweight Intrusion Detection for Networks". *LISA*.
4. CICIDS2017 Dataset. Canadian Institute for Cybersecurity.
5. Tavallaee, M. et al. (2009). "A Detailed Analysis of the KDD CUP 99 Dataset". *IEEE Symposium on CISDA*.
6. Sommers, J., & Barford, P. (2004). "Self-configuring network traffic generation". *ACM IMC*.
7. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun va K. Long, “Past chastotali Shrew DDoS hujumi uchun matematik model haqida,” IEEE Axborot forensikasi va xavfsizlik bo‘yicha tranzaksiyalar jurnali, jild 9, 2014-yil iyul.

ISSN 3060-4567

8. Y. Xiang va Z. Li, “DDoS hujumlari va ularga qarshi himoya uchun analitik model,” Global axborot texnologiyalari sohasida hisoblash konferensiyasida, 66-bet, 2006-yil avgust.

9. S. Ramanauskaite, N. Goranin, A. Cenys va J. Juknius, “Botnet xususiyatlarining DDoS hujumlar samaradorligiga ta’sirini modellashtirish,” Xavfsizlik va aloqa tarmoqlari jurnali, jild 8, №12, 2090–2101-betlar, 2015-yil.

10. M. Eian va S. F. Mjølsnes, “Simsiz tarmoqlarga qarshi xizmatdan voz kechirish (DoS) hujumlarini modellashtirish va taqqoslash,” ACM Operatsion tizimlar prinsiplari (SOSP) bo‘yicha simpozium workshopida, 7-bet, ACM, 2011-yil.