DDOS HUJUMLARINI ANIQLASH VA OLDINI OLISHGA YO'NALTIRILGAN TARMOQ MONITORING TIZIMI

Babakulov Bekzod Mamatkulovich o‘g‘li
Assistant. Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
babakulov.bekzod23@gmail.ru
Rahmonjonov Ibrohimjon Raim o’g’li
Talaba. Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
i40990077@gmail.com

Kalit so’zlar: DDoS, tarmoq elektron resurslari, botnet, mashinali o‘qitish, axborot xavfsizligi

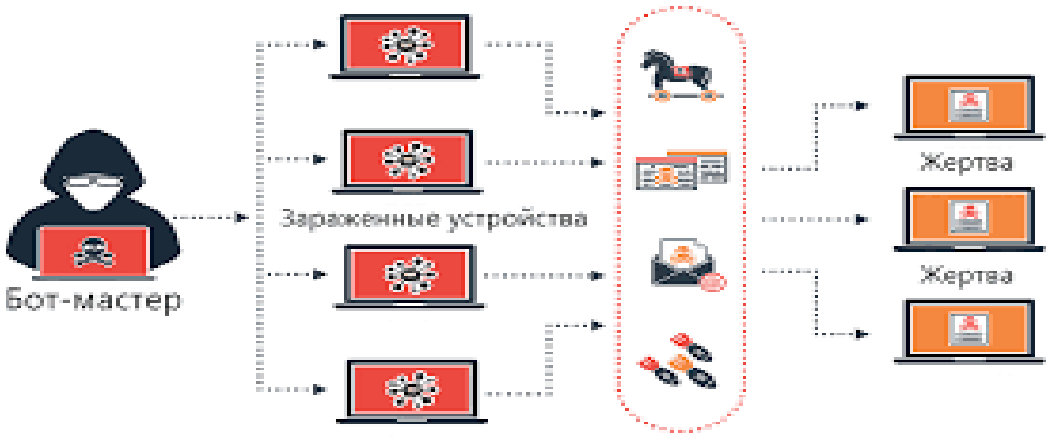
Maqsadi : Ushbu maqola tarmoqqa ulangan elektron resurslarga DDoS hujumlari va ularni aniqlash va oldini olishda mashinali o‘qitishdanfoydalanishning afzalliklari haqida umumiy ma’lumot beradi. Hujumlarning turlari, an’anaviy xavfsizlik usullari bilan bog‘liq muammolar va mashinali o‘qitishning roli ko‘rib chiqiladi. Algoritm tanlash, o‘qitish ma’lumotlari va noto‘g‘ri ijobiy boshqaruv muhokama qilinadi. Tadqiqot natijalari va xulosalari taqdim etiladi. Maqola axborot xavfsizligi sohasidagi mutaxassislar uchun foydalidir.

Kirish

Onlayn xizmatlar, pochta, ijtimoiytarmoqlar, elektron tijorat va onlayn banking kabi tarmoq elektron resurslari. zamonaviy axborot asrimizda tobora muhim rol o‘ynamoqda. Biroq, ularning ahamiyati oshgani sayin, axborot xavfsizligiga tahdid ham ortadi. Ayniqsa, jiddiy tahdid DDoS (Distributed Denial of Service) hujumlari bo‘lib, bu tarmoq elektron resurslarining mavjudligi va ishlashida jiddiy buzilishlarga olib kelishi mumkin. Veb-saytlar va onlayn xizmatlar hujumlar uchun mashhur nishon hisoblanadi, chunki ularga kirish imkonsizligi jiddiy biznes oqibatlariga olib kelishi yoki foydalanuvchilarga noqulaylik tug‘dirishi mumkin.

DDoS hujumlari - bu kompyuter tizimlariga(tarmoq resurslari yoki aloqa kanallari) ularni qonuniy foydalanuvchilar uchun imkonsiz qilishga qaratilgan hujumlar. DDoS hujumlari bir vaqtningo‘zida ma’lum bir manbaga Internetda joylashganbir yoki bir nechta kompyuterlardan ko‘p sonli so‘rovlarni yuborishni o‘z ichiga oladi. Agar minglab, o‘n minglab yoki millionlab kompyuterlar bir vaqtning o‘zida ma’lum bir serverga (yoki tarmoq xizmatiga) so‘rov yuborishni boshlasa, u holda server uni boshqara olmaydi yoki ushbu serverga aloqa kanali uchun tarmoqli kengligi etarli bo‘lmaydi. Ikkala holatda ham Internet foydalanuvchilari hujum qilingan serverga, hatto bloklangan aloqa kanali orqali ulangan barcha serverlar va boshqa resurslargakira olmaydi.

1-rasmda DDos hujumlarining sxemasi ko‘rsatilgan.



1-rasm. DDos hujumi sxemasi

Boshqacha qilib aytganda, veb-saytlar va onlayn xizmatlarga DDoS hujumlari protsessor, xotira yoki tarmoq o‘tkazish qobiliyati kabi server resurslarini ortiqcha yuklashga qaratilgan bo‘lishi mumkin. Misol uchun, tajovuzkorlar bir vaqtning o‘zida veb-sayt yoki xizmatga minglab yoki hatto millionlab so‘rovlarni yuborish uchun botnetdan (o‘g‘irlangan kompyuterlar tarmog‘i) foydalanishi mumkin. DDoS hujumlari natijasida veb-saytlar va ilovalar sekinlashadi yoki umuman ishlamay qoladi .

Dunyo miqyosida har kuni ikki mingga yaqin DDoS hujumlari qayd etiladi. O‘rtacha DDoS hujumi yirik kompaniyaga soatiga 250 dollar turadi.

Botnetlar kiberxavfsizlikka jiddiy tahdid soladi va katta zarar keltirishi mumkin

Botnet - bu tajovuzkor nazorati ostida DDoS hujumlarini amalga oshirishi mumkin bo‘lgan “zombi” deb nomlangan zararlangan kompyuterlar tarmog‘i. Zombi kompyuterlari troyan otlari yoki viruslar kabi zararli dasturlar bilan zararlangan bo‘lishi mumkin, bu esa tajovuzkorlarga o‘z faoliyatini masofadan turib kuzatish imkonini beradi.

Botnetlar hujumchilarga quyidagilarga imkon beradi:

- ko‘p sonli zombi kompyuterlardan foydalangan holda miqyosli hujumlar, bu ularni yanada samarali va halokatli qiladi;
- ularning haqiqiy shaxsini va joylashuvini yashirish, ularni aniqlash va ta’qib qilishni qiyinlashtiradi;
- mudofaa hujumlariga yoki blokirovkaga chidamli.

Botlar Internetda turli yo‘llar bilan tarqaladi, odatda zaif himoya xizmatlariga ega bo‘lgan kompyuterlarga hujum qilish va ularga zararli dasturlarni o‘rnatish yoki foydalanuvchilarni aldash va boshqa xizmatlar yoki dasturlarni taqdim etish niqobi ostida botlar o‘rnatiladi. Botlarni tarqatishning ko‘plab usullari mavjud va muntazam ravishda yangi usullar ixtiro qilinadi.

Agar botnet etarlicha katta bo‘lsa - o‘nlab yoki yuz minglab kompyuterlar - bu kompyuterlarning barchasidan bir vaqtning o‘zida ma’lum bir tarmoq xizmatiga (masalan, ma’lum bir saytdagi veb-xizmatga) to‘liq qonuniy so‘rovlar yuborilishiga olib keladi. xizmatning o‘zi yoki server resurslarining tugashi yoki aloqa kanali imkoniyatlarining tugashi. Qanday bo‘lmasin, xizmat foydalanuvchilar uchun mavjud bo‘lmaydi va xizmat egasi bevosita, bilvosita va obro‘siga putur etkazadi. Va agar har bir kompyuter sekundiga bitta so‘rovni emas, balki o‘nlab, yuzlab yoki minglab so‘rovlarni yuborsa, hujumning ta’siri ko‘p marta ortadi, bu esa hatto eng samarali resurslarni yoki aloqa kanallarini o‘chirishga imkon beradi .

Tarmoq elektron resurslariga DDoshujumlari

Onlayn elektron resurslarga DDoS hujumlari ko‘plab tashkilotlar va veb-xizmatlar duch keladigan jiddiy muammodir. Tarmoq elektron resurslariga DDoS hujumlari turli maqsadlar va oqibatlarga olib kelishi mumkin. Hujumning maqsadi quyidagilar bo‘lishi mumkin:

- veb-sayt, onlayn platforma yoki xizmat kabi tarmoq resursining to‘liq o‘chirilishi yoki ishlash samaradorligining pasayishi;
- diqqatni parallel ravishda amalga oshirilishi mumkin bo‘lgan boshqa kiberhujumlardan chalg‘itish;
- moliyaviy zarar, bu ayniqsa onlayn savdo maydonchalari uchun to‘g‘ri keladi, bu erda tegishli xizmatlarning ishlamasligini har bir daqiqasi daromadning sezilarli darajada yo‘qolishiga olib keladi.

DDoS hujumini aniqlash

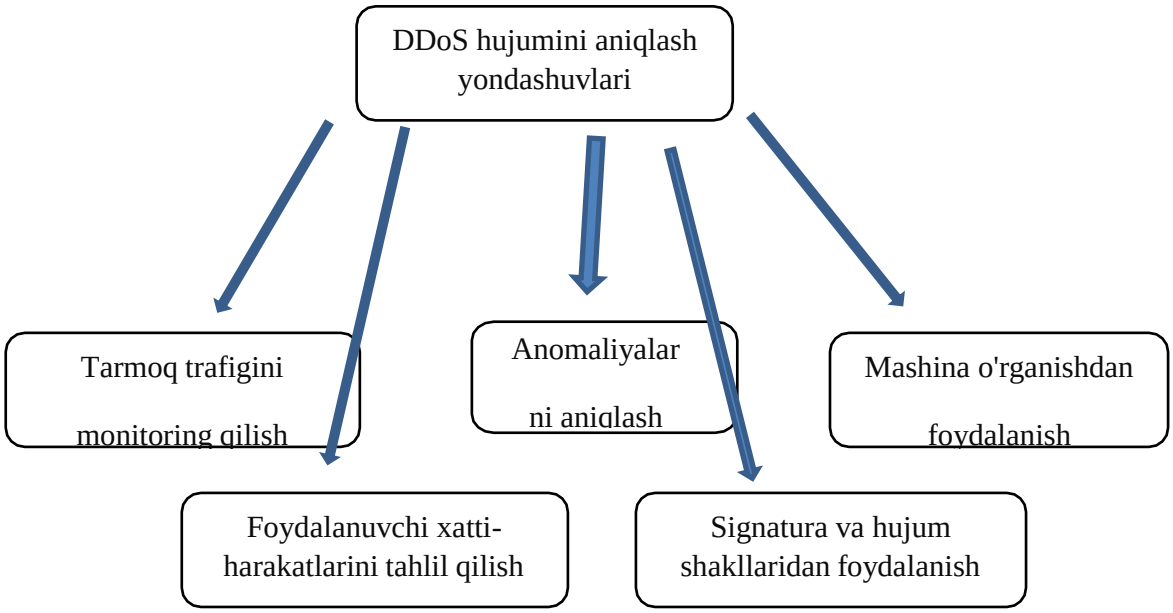
Onlayn elektron resurslarga DDoS hujumlarini aniqlash qiyin bo‘lishi mumkin, ammo bu jarayonda yordam beradigan ba’zi strategiyalar va usullar mavjud. 2-rasmda DDoS hujumlarini aniqlashning asosiy yondashuvlari ko‘rsatilgan.

DDoS hujumlarini aniqlashning asosiy usullaridan biri bu tarmoq trafigini kuzatishdir. Anomaliyalar va hujumlarni aniqlash uchun tarmoq trafigini tahlil qiladigan va qayd etadigan vositalar mavjud. Monitoring trafik hajmidagi o‘zgarishlarni, paketlar turlarini, manbalar va yo‘nalishlarni, odatdagi xatti-harakatlardan chetga chiqishni kuzatish imkonini beradi.

Yana bir yondashuv foydalanuvchi xatti- harakatlarini tahlil qilishdir. Bunga resursdagi foydalanuvchi faolligini kuzatish, noodatiy xatti- harakatlar namunalari va anomal faollikni aniqlash kiradi. Misol uchun, agar bitta IP-manzildan yoki ma’lum IP-manzillar to‘plamidan ko‘p sonli so‘rovlar kelib tushsa, bu DDoS hujumini ko‘rsatishi mumkin.

Anomaliyalarni aniqlash usuli resursning normal xatti-harakatining profilini yaratishga va ushbu profildan chetlanishlarni aniqlashga asoslangan. Bu so‘rovlar soni, serverning javob vaqti, o‘tkazish qobiliyati va boshqa omillar kabi turli parametrlarni tahlil qilishni o‘z ichiga olishi mumkin. Agar ushbu parametrlarda g‘ayritabiiy o‘zgarishlar kuzatilsa, bu DDoS hujumini ko‘rsatishi mumkin.

Signatura va hujum shakllaridan foydalanishDDoS hujumlari joriy trafikni ma’lum hujumlar bilan solishtirish imkonini beradi. Agar moslik topilsa, bu DDoS hujumini ko‘rsatishi mumkin.



2-rasm. DDoS hujumlarini aniqlashning asosiy yondashuvlari.

Mashinali o‘qitish (MO‘) tarixiy trafik ma’lumotlariga asoslangan o‘qitish modellari orqali DDoS hujumlarini aniqlash uchun qo‘llanilishi mumkin. Modellar DDoS hujumlariga xos bo‘lgan anomaliyalar va noodatiy naqshlarni aniqlashi mumkin. Anomaliyalar aniqlanganda, model hujum haqida ogohlantirishi yoki uning ta’sirini kamaytirish uchun avtomatik ravishda choralar ko‘rishi mumkin.

Botnetlar tahdidini butunlay yo‘q qilishning iloji bo‘lmasa-da, profilaktika choralarini ko‘rish orqali ushbu hujumlarning ta’siri va ko‘lamini cheklash usullari mavjud.

Tarmoqning elektron resurslarini himoya qilish uchun mashinali o‘qitishdan foydalanish

Tarmoqning elektron resurslarini DDoS hujumlaridan himoya qilish uchun MO‘dan foydalanish anomaliyalarni aniqlashni, modellarni avtomatik o‘qitishni, noto‘g‘ri pozitivlarni kamaytirishni ta’minlaydi, yuqori ishlov berish tezligini, hujumlarni bashorat qilishni va oldiniolishni ta’minlaydi. MO‘ modellari:

- noodatiy yoki shubhali trafik namunalari asosida hujumlarni aniqlash imkonini beruvchi anomaliyalarni aniqlash uchun tarmoq trafigining normal harakati bo‘yicha o‘qitilishi va joriy trafikni tahlil qilish;
- hujumlarni aniqlashda noto‘g‘ri pozitivlarni minimallashtirish uchun sozlanishi, bu aniqlikni oshirish va hujumni oddiy trafikdan ajratish uchun kontekstual omillar vaqo‘shimcha funktsiyalarni hisobga olishi mumkin;
- ma’lumotlardagi ko‘plab belgilar va korrelyatsiyalarni tahlil qilish, bu boshqa himoya usullariga ko‘rinmas bo‘lishi mumkin bo‘lgan murakkab hujumlarni aniqlashgayordam beradi;

- kelajakdagi hujumlarni bashorat qilish va profilaktika choralarini ko‘rish uchun tarixiy ma’lumotlar tahlilidan foydalaning, bu esa hujumlarning oldini olish va o‘z vaqtida profilaktika choralarini ko‘rish imkonini beradi.

MO‘ algoritmlari real vaqtda katta hajmdagi ma’lumotlarni qayta ishlash va tezkor qarorlar qabul qilish imkonini beradi. Bu hujumlarga tezda javob berish va ularning tarmoq resurslariga ta’sirini kamaytirish imkonini beradi.

MO‘ tizimlari:

yangi ma’lumotlardan o‘qitish va o‘zgaruvchan hujum usullariga moslashishi, bunda ular doimiy ravishda qo‘lda sozlashni talab qilmasdan aniqlash modellarini avtomatik ravishda yangilashlari mumkin;

- katta hajmdagi trafikni boshqarish va alohida serverlarni va butun tarmoqlarni himoya qilish uchun kengaytiriladigan bo‘lishi, bu esa turli darajadagi hujumlarni aniqlash muammosini hal qilishi mumkin.

DDoS hujumlaridan himoya qilish uchun mashinali o‘qitishdan foydalanish hujumni aniqlashda yuqori samaradorlik va aniqlikka erishish, shuningdek, noto‘g‘ri pozitivlar sonini kamaytirish imkonini beradi. Bu DDoS hujumlarining ortib borayotgan tahdidiga qarshi kurashish va tarmoqqa ulangan elektron resurslar xavfsizligini ta’minlashda muhim vositahisoblanadi.

Ammo onlayn elektron resurslarni DDoS hujumlaridan himoya qilish uchun MO‘dan foydalanganda quyidagi muhim jihatlarni hisobga olish kerak:

1. Mashinali o‘qitish modellarini samarali o‘qitish uchun yuqori sifatli va xilma-xil o‘qitish ma’lumotlariga ega bo‘lish kerak. Modellar hujumlar va oddiy trafikni farqlashni o‘rganishi uchun oddiy trafik, shuningdek, turli xil DDoS hujumlari haqida etarli ma’lumot to‘plash muhim hisoblanadi.
2. DDoS hujumlarini aniqlash uchun mos keladigan ko‘plab mashinali o‘qitish algoritmlari mavjud. Tegishli algoritmni tanlash ma’lumotlarning xususiyatlariga va tizim talablariga bog‘liq. Ba’zi mashhur algoritmlar klassifikatsiya, klasterizatsiya usullari va neyron tarmoqlarini o‘z ichiga oladi.
3. Hujum usullari doimo rivojlanib bormoqda va vaqt o‘tishi bilan yangi turdagi DDoS hujumlari paydo bo‘lishi mumkin. Shuning uchun, yangi turdagi hujumlarni samarali aniqlash uchun mashinali o‘qitish modellarini muntazam yangilash va ularni yangi ma’lumotlarga o‘rgatish muhimdir.
4. DDoS hujumlarini aniqlash jarayonida mashinali o‘qitish modellari noto‘g‘ri pozitivlarga ruxsat berishi, ya’ni oddiy trafikni hujum sifatida noto‘g‘ri tasniflash mumkin. Tizimning keraksiz yuklanishi va noto‘g‘ri signallarning oldini olish uchun hujumlarni aniqlash va noto‘g‘ri pozitivlar sonini kamaytirish o‘rtasidagi muvozanatni topish muhimdir.
5. DDoS hujumlaridan himoya qilish uchun mashinali o‘qitishdan foydalanadigan tizimlar real vaqt rejimida ishlashi va tarmoq trafigini doimiy ravishda kuzatib borishi kerak. Bu hujumlarni aniqlash va darhol himoya choralarini ko‘rish imkonini beradi.
6. Mashinali o‘qitishni DDoS hujumlaridan himoya qilishning kompleks

tizimidagi vositalardan biri sifatida ko‘rib chiqish kerak. Kuchliroq himoyani ta’minlash uchun MO‘ bilan birgalikda paket filtrlari, xavfsizlik devorlari va tarmoq yukni muvozanatlash kabiqo‘shimcha mexanizmlarni ishlatish mumkin.

7. Mashinali o‘qitish tizimining samaradorligini davriy sinovdan o‘tkazish va baholash uning kuchli va zaif tomonlarini aniqlashga yordam beradi. Bu modellar va algoritmlarni yaxshilaydi, shuningdek, DDoS hujumlaridan himoyalanishning umumiy samaradorliginioshiradi.

Ushbu muhim fikrlarni hisobga olgan holda, mashinali o‘qitishdan foydalanish tarmoqqa ulangan elektron resurslarni DDoS hujumlaridan himoya qilishda samarali vosita bo‘lishi mumkin.

Xulosalar

Maqolada tarmoqdagi elektron resurslarga jiddiy tahdid soladigan DDoS hujumlari haqida umumiy ma’lumot berilgan. Ular tamoq elektron resurslarning ishmasligi va unumdorlikning pasayishi tashkilotlar uchun katta moliyaviy yo‘qotishlarga olib kelishi mumkin.

DDoS hujumlaridan himoyalanishning an’anaviy usullari har doim ham samarali bo‘lavermaydi, chunki tajovuzkorlar doimiy ravishda moslashib, yangi usullardan foydalanishadi. Shu nuqtai nazardan, mashinalio‘qitishdan foydalanish DDoS hujumlariga qarshikurashish uchun kuchli vositadir.

Mashinali o‘qitish tarmoq trafigidagi anomaliyalarni aniqlashi, bir nechta atributlarnitahlil qilishi va kelajakdagi hujumlarni bashorat qilishi mumkin, bu esa yanada samarali va aniq himoya qilishga olib keladi. Mashinali o‘qitish hujumlarni aniqlash modellarini avtomatikravishda yangilash mumkin, bu doimiy ravishda o‘zgarib turadigan hujum usullarini hisobga olganholda ayniqsa muhimdir.

Maqolada, shuningdek, DDoS hujumlaridan himoya qilish uchun mashinali o‘qitishdan foydalanishning muhim jihatlari, jumladan, yuqorisifatli o‘quv ma’lumotlariga bo‘lgan ehtiyoj vahimoyaga kompleks yondashuv zarurligi muhokama qilindi.

Xulosa qilib aytganda, maqolada DDoS hujumiga qarshi mashinali o‘qitishdan foydalanish katta imkoniyatlar bersada, shuni esda tutish kerakki, DDoS hujumlaridan himoya qilish doimiy jarayon bo‘lib, mashinali o‘qitish modellarini doimiy yangilash va sinovdan o‘tkazishni talabqiladi.

Maqola doirasida oligan natijalar va xulosalari ushbu sohada mashinali o‘qitish imkoniyatlarini kengligini tasdiqlaydi va xavfsizlik tizimlarini takomillashtirish hamda DDoS hujumlari bilan bog‘liq zamonaviy muammolarni bartaraf etish uchun keyingi tadqiqotlar va ishlanmalar zarurligini ko‘rsatadi.

Kelajakdagi tadqiqotlar mashinalio‘qitishning yangi algoritmlarini ishlab chiqishga, hujumlarni aniqlashning aniqligini oshirishga va keng qamrovli DDoS himoya tizimlarini, jumladan, turli usullar va texnologiyalar kombinatsiyasini ishlab chiqishga qaratilishi mumkin.

ADABIYOTLAR RO‘YXATI:

1.Botta, A., De Donato, W., Persico, V., & Pescape, A. (2017). On the use of machine learning techniques for the detection of distributed denial-of-service attacks. Journal of Network and Computer Applications, 80,31-44.

2.Siddiqui, M. S., & Gani, A. (2018). DDoS attacks in software-defined networking: A comprehensive survey. Journal of Network and Computer Applications, 102, 1-14.

3.DDoS hujumlarini tushunish va ularga chorako‘rish: [Электронный ресурс]. URL: https://csec.uz/uz/news/maqolalar/ddos- hujumlarini-tushunish-va-ularga-chora-ko-rish/. (Дата обращения: 29.04.2024).