KOMPYUTER TIZIMLARINI DDOS-HUJUMLARIDAN HIMOYALASH

Artikov Nodirbek Axmedjan o‘g‘li
O‘zbektelekom AK Xorazm filiali JvaYuShMBI guruhi 1-toifali mutaxassis
Nasrullayev Nurbek Baxtiyorovich
Abdullayeva Haitjon Atabekovna
Ibodullayev Abdulla Zokir o'g'li

Annotatsiya: *Mazkur maqolada asosan veb-saytlar va DDOS hujumlarini tahlil qilish usullari haqida ma’lumot berilgan. Veb-saytlarni tahdidlardan va xavfsizlikdan himoya qilishda algoritmlar tushunchasini shakllantirish. HTTP-flood ga qarshi qarshi algoritm haqida islohotlar yoritilgan.*

Kalit so‘zlari: *Proksi-server, algoritm, veb-sayt, DDOS, HTTP-flood, hujum, xafsizlik.*

Taqsimlangan xizmat ko‘rsatishni rad etish (DDoS) hujumlari bugungi kunda tashkilotlar va shaxslar oldida turgan eng jiddiy kiberxavfsizlik muammolaridan biriga aylandi. Ko'pincha xizmatlarni buzish yoki pul undirishga intilayotgan yovuz niyatli shaxslar tomonidan amalga oshiriladigan DDoS hujumlari maqsadli kompyuter tizimini tirbandlik bilan to'ldirishni o'z ichiga oladi, bu esa uning ishdan chiqishiga yoki unga kirish imkonsiz bo'lishiga olib keladi. Bunday hujumlarning oqibatlari og'ir bo'lishi mumkin, natijada moliyaviy yo'qotishlar, obro'ga putur etkazadi va hatto jamoat xavfsizligiga xavf tug'diradi.

DDoS hujumlaridan himoya qilish uchun tadqiqotchilar va kiberxavfsizlik bo'yicha mutaxassislar turli strategiyalarni, jumladan, matematik modellardan foydalanishni ishlab chiqdilar. Ushbu modellar tarmoq trafigini tahlil qilish, potentsial tahdidlarni aniqlash va ularning ta'sirini yumshatish uchun profilaktika choralarini ko'rish uchun ilg'or algoritmlardan foydalanadi.

Ushbu maqolada biz kompyuter tizimlarini DDoS hujumlaridan himoya qilish uchun matematik modellar bo'yicha tadqiqotlarning hozirgi holati haqida umumiy ma'lumot beramiz. Biz mavjud modellarning cheklovlarini ko'rib chiqamiz va qo'shimcha tadqiqotlar zarur bo'lgan sohalarni aniqlaymiz. Shuningdek, biz zamonaviy tarmoqlarning dinamik va doimiy o‘zgaruvchan tabiati sharoitida samarali modellarni ishlab chiqish bilan bog‘liq muammolarni muhokama qilamiz.

Maqola kiberxavfsizlik sohasida ishlovchi mutaxassislar, tadqiqotchilar va kompyuter tizimlarini DDoS hujumlaridan himoya qilishning zamonaviy holati haqida ko'proq ma'lumot olishga qiziqqan har bir kishi uchun mo'ljallangan. Ushbu sohada olib borilayotgan tadqiqotlarning so'nggi sharhini taqdim etish orqali biz DDoS hujumlarining ta'sirini yumshatish va tarmoq xavfsizligini oshirish bo'yicha samarali strategiyalarni ishlab chiqishga hissa qo'shishga umid qilamiz.

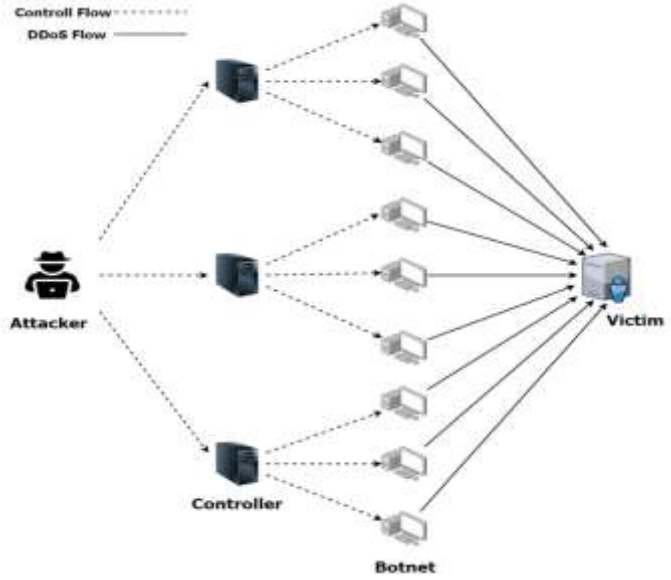
DDoS hujumlarini amalga oshirishning ko‘plab usullari orasida eng samaralisi botnet tarmog‘idan yuborilgan ko‘p sonli noto‘g‘ri so‘rovlarni qayta ishlash orqali

serverda joylashgan resurslarning katta ish yukini ta’minlashga qaratilgan hujumdir. Ushbu hujum ko‘pincha tarmoqqa kirish imkoniga ega bo‘lgan haqiqiy foydalanuvchilarning virusli qurilmalaridan uyushtiriladi, ular hatto o‘z qurilmasidan har qanday hujum amalga oshirilayotganiga shubha qilmaydi. Shunday qilib, tizimga viruslar, qurtlar va "Troyan otlari" viruslarini kiritish orqali tarmoqqa ulangan himoyalanmagan qurilmalarga zararli dasturlar o‘rnatiladi. Ko‘p sonli tarmoq xostlarining infektsiyasi shunday sodir bo‘ladi, shundan so‘ng ushbu kompyuterlar ustidan nazorat tajovuzkorga o‘tadi. Keyin hujum qiluvchi obyekt bir vaqtning o‘zida infektsiyalangan tarmoqning barcha tugunlariga qandaydir buyruqni yuborishga asoslangan hujumni amalga oshiradi. Natijada, foydalanuvchi qurilmasiga o‘rnatilgan dasturiy ta’minot faollashadi. Xost ma’lumotlari tajovuzkor nazorati ostida uzatiladi, shuning uchun "Xizmatni rad etish" tarqatilgan hujumning manbai bo‘ladi.[1]

“Ta’minotni rad etish” yoki qisqartirilgan DDOS hujumlarining hujumlari, umumiy voqea va dunyo bo‘ylab Internet resurslari egalari uchun jiddiy bosh og’rig’i bo‘ldi. Shuning uchun Saytda DDOS hujumlaridan himoya qilish bugungi kunda qo‘shimcha variant emas, balki kam vaqtdan qochishni istaganlar uchun zaruriy shart, katta zarar va buzilgan obro‘ga ega bo‘lganlar uchun zarur shartdir. Xizmatni rad etish yoki "texnik xizmat ko‘rsatishni rad etish" - Axborot tizimiga hujum - bu foydalanuvchi so‘rovlarini qayta ishlash qobiliyatiga ega emas. Oddiy so‘zlar, DDOS veb-resurs yoki transport serverini juda ko‘p manbalardan bostirishda, uni kamdan-kam hollarda qabul qilmaydi. Ko‘pincha bunday hujum tarmoq resurslari ishida yirik firma yoki davlat tashkilotida uzilishlarni qo‘zg’atish uchun amalga oshiriladiDDOS hujumi boshqa umumiy veb-tahdidga o‘xshaydi - Xizmatni rad etish, DOS. Faqatgina farq shundaki, odatiy taqsimlangan hujum bir nuqtadan kelib chiqadi va DDOS hujumi yanada katta va turli manbalardan kelib chiqadi.[2]

DDOS hujumining asosiy maqsadi o‘z ishini blokirovka qilish orqali tashrif buyuruvchilarga kirish mumkin emas. Ammo bunday hujumlar diqqatni boshqa zararli ta’sirlardan chalg’itishi uchun ishlab chiqarilgan holatlar mavjud. DDOS hujumi, masalan, xavfsizlik tizimini tashkilotning ma’lumotlar bazasiga ega bo‘lish uchun xavfsizlik tizimini buzishda amalga oshirilishi mumkin. 1999 yilda ko‘plab yirik kompaniyalar (Yahoo, eBay, Amazon, CNN) bir qator hujumlar uyushtirgan. O‘shandan beri, kiber jinoyatchining ushbu turi global miqyosda tahdidni rivojlantirdi. Mutaxassislarning fikriga ko‘ra, so‘nggi yillarda ularning chastotasi 2,5 baravar ko‘paydi va bu juda yuqori darajada 1 tbit / s dan oshdi. DDOS qurboni kamida oltinchi Rossiya kompaniyasining kamida bir marta sodir bo‘ldi. 2020 yilga kelib, ularning umumiy javobi 17 millionga etadi. DDSS oddiy bloglardan, eng yirik korporatsiyalar, banklar va boshqa moliyaviy institutlar bilan tugaydigan har qanday shkala saytlarini buzishi mumkin. "Kasperskiy laboratoriyasi" tadqiqotlariga ko‘ra, hujum kompaniyaning 1,6 million dollargacha bo‘lishi mumkin. Bu jiddiy zarar, chunki hujum qilingan veb-resurs bir muncha vaqt bo‘lolmaydi, shuning uchun sodda bo‘lishi kerak.

Korsero tarmog'iga ko'ra, dunyodagi barcha kompaniyalarga qaraganda "rad etish huquqi" hujumlariga duchor bo'lishadi. Bundan tashqari, ularning soni 50 ga etadi.



1-rasm DDOS hujumi

DDOS-hujumlardan serverni himoya qilishni ta'minlamagan saytlar egalari nafaqat katta yo'qotishlarga, balki mijozning ishonchining pasayishi, shuningdek, bozorda raqobatbardoshlikni pasaytirishi mumkin. DDOS-hujumdan himoya qilishning eng samarali usuli bu Provayder tomonidan yuqori darajada o'tkazish qobiliyati bilan Internet kanallariga etkazib beriladigan filtrlar hisoblanadi. Ular butun trafikni izchil tahlil qilishadi va shubhali tarmoq faoliyatini yoki xatolarini aniqlaydilar. Filtrlar yo'l-yo'riqlar darajasida va maxsus apparat qurilmalaridan foydalangan holda o'rnatilishi mumkin. Hatto dasturiy ta'minotni yozish bosqichida ham saytning xavfsizligi haqida o'ylashingiz kerak, DDoS hujumlarini aniqlash uchun maxsus choralar kerak emas, DDoS hujumi faktini eslamaslik mumkin emas. Boy vipadkada bu haqiqat. Namoyishchilar ko'pincha masofadagi DoS hujumlaridan qo'rqishardi, chunki ular 2-3 dobidan kamroq qurbonlar tomonidan belgilangan edi.[3]

Ilgari hujumning (toshqin hujumi) salbiy oqibatlari arizachi hisobidan ortiqcha internet-trafikni to'lash hisobiga tugaydi, bu faqat hisob Internet-provayderdan olib tashlanganida sodir bo'ldi. Bundan tashqari, hujumlarni aniqlashning ko'plab usullari hujum ob'ekti yaqinida samarasiz, lekin asosiy kanallarda samarali. Bunday paytda siz tizimlarni tekshirishlarni emas, balki o'zingiz joylashtirishingiz kerak, koristuvach esa hujumlarni tanib, o'zini eslab, yordam so'rab g'azablanadi. Bundan oldin, DDoS-hujumlarning samarali oldini olish uchun DoS-hujumlarning turini, xarakterini va boshqa xususiyatlarini bilish kerak va namoyon bo'lish tizimining o'zi buni tezda aniqlashga imkon beradi. Hujum sifatida bir vaqtning o'zida ko'p sonli kompyuterlar g'alaba qozonadi DDoS hujumlari(Vid ingliz. Taqsimlangan Xizmatni rad etish, rozpodylena hujum turi "xizmatdagi vydmova"). Ba'zi hollarda, haqiqiy DDoS hujumidan oldin, baxtsiz hodisaga sabab bo'ladi, masalan, saytga yuborilgan mashhur Internet-resursga joylashtirish, samarasiz serverga joylashtirish (slash nuqta effekti). Íx xizmat qismida, keyin, server í uchun joiz behuda o'tkazish qadar ishlab chiqarish

uchun coristuvachív katta oqimi.Hujum sifatida bir vaqtning o'zida ko'p sonli kompyuterlar g'alaba qozonadi DDoS hujumlari(Vid ingliz. Taqsimlangan Xizmatni rad etish, rozpodylena hujum turi "xizmatdagi vydmova"). Ba'zi hollarda, haqiqiy DDoS hujumidan oldin, baxtsiz hodisaga sabab bo'ladi, masalan, saytga yuborilgan mashhur Internet-resursga joylashtirish, samarasiz serverga joylashtirish.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI:

1. Karimov.K. Veb-saytlarni DDOS kabi hujumlardan himoya qilish usullari va algoritmlarni ishlab chiqish. Toshkent.2022.
2. https://sukachoff.ru/uz/ustrojjstva/v-svyazi-s-ddos-atakoi-ddos-ataki-napadenie-i-zashchita-zashchita-ot/
3. https://androidas.ru/uz/chto-soboi-predstavlyaet-ddos-ataka-dos-i-ddos-ataki-znachenie-i/