radware

DDoS TIROQ QO'LLANMA

Siz uchun hamma narsa uchun yakuniy qo'llanma
DDoS hujumlari haqida bilishingiz kerak

Qanday:

» Hujum turlarini aniqlang va ularning ta'sirini tushuning

» Hujum vositalarini tanib olish

» Tashkilotingizni DoS va DDoS hujumlaridan himoya qiling

DDoS SURVIVAL QO'LLANISHINI BAGASHING

Mundarija

1 Kirish

Internet turli xil o'zaro bog'langan kompyuterlar va tarmoqlar o'rtasida ma'lumot almashishni osonlashtirish uchun yaratilgan bo'lsa-da, u xavfsizlikni hisobga olgan holda ishlab chiqilmagan. Viruslar, patogenlar va boshqa tahdidlarning raqamli ekvivalentlari Internet paydo bo'lganidan beri mavjud. 1988-yilda Internetning kashshofi ARPANET 60 000 ga yaqin ulangan mashinadan iborat boÿlganida, Morris Worm deb nomlangan oÿz-oÿzini koÿpaytiruvchi kompyuter dasturi beixtiyor bu mashinalarning taxminan 10% ning hisoblash resurslarini yoÿqotib, notoÿgÿri ishlashiga sabab boÿldi. Shunga qaramay, ayrim shaxslar, korxonalar va boshqa tashkilotlar hali ham o'zlarini to'g'ri himoya qila olmaydi.

Bugungi kunda 1 milliarddan ortiq foydalanuvchiga ega bo'lgan Internet o'tkazgichga aylandi odamlar va korxonalar muntazam ravishda foydali ma'lumotlarga kirishlari, bank ishi kabi vazifalarni bajarishlari va turli xil sotuvchilardan xarid qilishlari uchun. Ijtimoiy tarmoqlarning o'sishi, shuningdek, Internetni biznes va boshqa tashkilotlar uchun muhim brending va boshqa asosiy mijozlar o'zaro munosabatlari uchun foydalanish uchun bebaho joyga aylantirdi - bu jarayonda ko'pincha katta daromad keltiradi. Bu barcha qulaylikning salbiy tomoni buzilishlarga nisbatan zaiflikdir. Yovuz niyatli foydalanuvchilar ko'pincha sanoat josusligi va qasos olishdan tortib moliyaviy foyda va siyosiy maqsadlargacha bo'lgan maqsadlarda ma'lumotlarni o'g'irlashlari yoki oddiy kompyuter ishlashini to'xtatishlari mumkin.

Veb-saytni buzishni maqsad qilgan zararli tomon tomonidan kiberhujum Internet (yoki unga ulangan har qanday qurilma) mavjudlikka asoslangan hujum deb ataladi. Turli xil hujum vektorlarining keng spektridan (TCP toshqinlari, HTTP/S toshqinlari, past tezlikli hujumlar, SSL hujumlari va boshqalar) foydalanish mavjudligiga asoslangan hujumlar veb-saytlarga ta'sir qiladigan eng jiddiy xavfsizlik tahdidlaridan biridir. Ular odatda Denial-of-service (DoS) hujumlari deb ataladi. Hujum bir nechta hujum qiluvchi mashinalar tomonidan amalga oshirilsa, u tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumi deb ataladi.

DoS va DDoS hujumlari har kuni dunyo bo'ylab yangiliklar sarlavhalariga aylanadi, Qanday qilib yovuz niyatli shaxs yoki guruh veb-sayt uchun sezilarli ishlamay qolishi yoki buzilishdan xavfsizlikni buzish uchun foydalanishi, moliyaviy va obro'ga zarar yetkazishi haqida hikoya qiluvchi hikoyalar bilan. Axborot xavfsizligi tadqiqotchilari hali standartlashtirilganni ishlab chiqmagan

Dunyo bo'ylab sodir bo'ladigan DoS va DDoS hujumlarining soni yoki tabiati to'g'risida ma'lumot to'plash strategiyasiga ko'ra, har kuni 7000 dan ortiq bunday hujumlar sodir bo'lishi taxmin qilinmoqda - so'nggi yillarda ularning soni tez o'sib bormoqda.1

Veb-saytiga ega bo'lgan har bir tashkilot, ayniqsa foydalanuvchilaridan maxfiy ma'lumotlarga muntazam kirishni talab qiladigan tashkilot - DoS va DDoS hujumlaridan himoya qilish uchun shoshilinch va tegishli choralarni ko'rishi kerak. Aks holda, katta moliyaviy yo'qotishlar, shuningdek, jamoatchilik obro'siga putur etkazishi mumkin.

DDoS Survival qo'llanmasi kiberga qarshi omon qolish kalitidir
Sizni o'zingiz bilmagan holda hozir sizni ta'qib qilishlari mumkin bo'lgan hujumchilar. Ushbu qo'llanma biznesingizni DoS va DDoS hujumlaridan himoya qilish uchun ishonchli, tasdiqlangan maslahatlarni taqdim etadi. Uning maqsadi DoS va DDoS hujumlari bilan tanishishingizni oshirish va ular tashkilotingizga qanday ta'sir qilishini tushunishga yordam berishdir. Unda DoS va DDoS hujumlari qanday ishlashi, ular sizning biznesingizga qanday ta'sir qilishi, hujumlar ortida kim turgani, ular qanday vositalardan foydalanayotgani va mudofaa vositasi sifatida sizning ixtiyoringizda qanday resurslar mavjudligi tushuntiriladi.

1 http://www.prolexic.com/pdf/Prolexic_corp_brochure_2012.pdf

2 DoS va DDoS hujumlarini tushunish

DoS hujumi nima? DDoS hujumi nima? nima farq? Ular qanday yaratilgan? Ularning kuchli va zaif tomonlari qanday? Har qanday omon qolish usullarini muhokama qilishdan oldin, siz omon qolish uchun nima qilayotganingizni tushunishingiz kerak.

DoS hujumining majoziy misolini keltirish uchun o'zingizni faqat bitta kassa oynasi ochiq bo'lgan bankka kirganingizni tasavvur qiling. Siz kassaga yaqinlashmoqchi bo'lganingizda, boshqa bir kishi bankka yugurib kirib, oldingizda kesadi. Bu odam kassir bilan kichik suhbat qurishni boshlaydi va bank bilan bog'liq hech qanday operatsiyalarni amalga oshirish niyatida emas. Bankning qonuniy foydalanuvchisi sifatida siz chekingizni depozitga qo'ya olmaysiz va "zararli" foydalanuvchi suhbatni tugatmaguncha kutishga majbur bo'lasiz. Xuddi shu zararli foydalanuvchi kabi

barglari, boshqa bir kishi bankka shoshilib, yana oldingi chiziqning old qismini kesib, sizni kutishda davom etishga majbur qiladi. Bu jarayon daqiqalar, soatlar va hatto kunlar davomida davom etishi mumkin va bu sizga yoki sizning orqangizda turgan boshqa qonuniy foydalanuvchilarga bank operatsiyalarini amalga oshirishga to‘sqinlik qilishi mumkin.

DoS hujumlari paytida hujumchilar o'z nishonlarini massiv bilan bombardimon qilishadi so'rovlar yoki ma'lumotlar miqdori - uning tarmog'i yoki hisoblash resurslarini tugatadi va qonuniy foydalanuvchilarning kirishiga to'sqinlik qiladi. Soddaroq qilib aytganda, DoS hujumi bu tajovuzkor boshqa mashinaning resurslarini ishlatish uchun uning normal ishlashiga yo'l qo'ymaslik uchun bitta mashinaning resurslaridan foydalanishi. Katta veb-serverlar bitta mashinadan asosiy DoS hujumiga bardosh bera oladigan darajada mustahkamdir (tasavvur qiling-a, yuqoridagi misoldagi bank band bo'lishini kutmaslik uchun siz foydalanish uchun ko'plab kassa oynalari ochiq bo'lsa).

Biroq, tajovuzkorlar ko'pincha DDoS hujumlarini amalga oshiradilar, bu esa samaradorlikni oshirish uchun bir nechta mashinalardan foydalanadi, aslida barcha ochiq derazalardagi barcha kassalarni bog'lashga harakat qiladi. Bunday stsenariyda tajovuzkorlarni qo'lda aniqlash va blokirovka qilish ko'pincha qiyinroq bo'lishi mumkin, shuning uchun bunday keng ko'lamli hujumlarni aniqlash va himoya qilish uchun maxsus himoya vositalari kerak bo'ladi. Bundan tashqari, tajovuzkorlar deyarli hech qachon o'zlarining hujum mashinalarini qonuniy ravishda boshqara olmaydilar; aksincha, ular foyda olish uchun dunyo bo'ylab tarqalgan minglab kompyuterlarni maxsus zararli dasturlar bilan zararlaydilar

bunday mashinalarga ruxsatsiz kirish. Bitta tajovuzkorning nazorati ostidagi armiya vazifasini bajaradigan yuzlab yoki minglab buzilgan mashinalar to'plami "botnet" deb ataladi va ko'pincha botnetning bir qismi bo'lgan mashinalarning haqiqiy egalari o'zlarining kompyuterlari buzilganligini bilishmaydi. DDoS hujumlarini boshlash uchun ishlatiladi.

Botnetni yig'ish

Tajovuzkorlar ostida kompyuterlarning katta botnetlarini yaratish uchun ularning boshqaruvi (so'zda zombi deb ataladi) ikkita variantga ega: ularning mashinalari buzilganligini bilmagan foydalanuvchilarning mashinalariga zarar etkazish uchun maxsus zararli dasturlardan foydalanishning keng tarqalgan varianti yoki ko'p sonli ko'ngillilarni to'plashning nisbatan yangi varianti. DoS dasturlarini birgalikda ishlatishga tayyor.

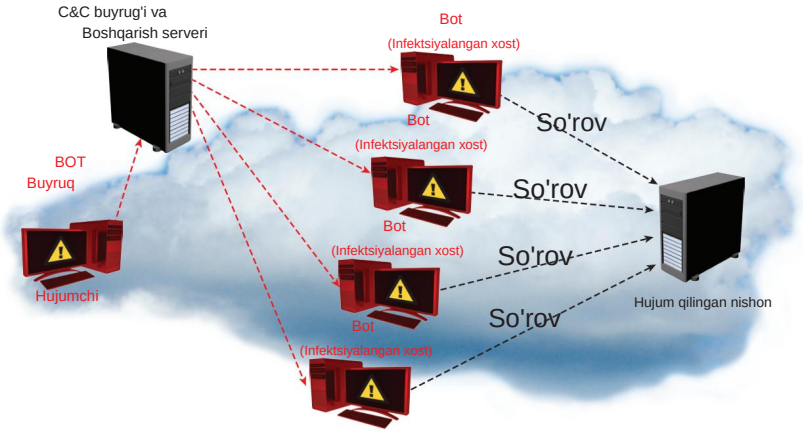
Oldingi stsenariyda (eng keng tarqalgan) tajovuzkorlar turli xil er osti kiberjinoyat forumlaridan ixtisoslashgan zararli dasturlarni ishlab chiqadilar yoki sotib oladilar, ular imkon qadar ko'proq zaif kompyuterlarga tarqaladilar. Bunday zararli dasturlarni ishga tushirish uchun aldangan har qanday foydalanuvchilar ko'pincha o'z kompyuterlarida antivirus funksiyalarini o'chirib qo'yadi va tajovuzkorlar uchun "orqa eshik" yoki kirish nuqtasini o'rnatadi. Infektsiyalangan kompyuterlar "buyruqlar va boshqaruv" (C&C) serverlaridan, odatda chat xonalari uchun mo'ljallangan aloqa protokoli bo'lgan Internet Relay Chat (IRC) orqali botnet-mashinalarga buyruqlar yuborishga qodir bo'lgan markazlashtirilgan mashinalardan aloqalarni qabul qila boshlaydi. Buzg'unchilar har qanday vaqtda DDoS hujumini amalga oshirishni xohlasalar, ular o'zlarining botnetlarining C&C serverlariga ma'lum bir nishonga hujum qilish bo'yicha ko'rsatmalar bilan xabarlar yuborishlari mumkin va aloqada bo'lgan C&C serveri bilan bog'langan har qanday virusli mashinalar muvofiqlashtirilgan hujumni boshlash orqali ularga rio

Huquq-tartibot idoralari xodimlari botnetni demontaj qilishga harakat qilganda, ko'pincha C&C serverlarini topish va o'chirish kerak bo'ladi, chunki bu ko'pchilik botnetlarning ishlashini oldini oladi. 2010-yilda demontaj qilingan “Mariposa” (ispancha “kapalak”) deb nomlangan alohida botnet butun dunyo boÿylab 15,5 millionga yaqin noyob IP-manzillarni oÿz ichiga olgani aniqlandi. Bunda koÿplab qoÿmondonlik va boshqaruv serverlari mavjud.2 Soÿnggi va ilgÿor botnet dasturlari, masalan kabi

Biroq, TDL-4 faqat C&C serverlarini o'chirib qo'yish orqali botnetlarni demontaj qilish harakatlarini chetlab o'tishga yordam berish uchun umumiy tengdoshlar orasidagi tarmoqlarda maxsus botlararo aloqa imkoniyatlarini joriy qildi.

2 Mariposa Botnetni olib tashlash (1-qism) - Chris Davis, Defence Intelligence.pdf

Agar ko'plab kompyuterlar ixtiyoriy ravishda birgalikda harakat qilsa, hujumga homiylik qiluvchi xakerlar uning tafsilotlarini ijtimoiy tarmoq yoki IRC kanali orqali, jumladan sana va vaqt, maqsadli IP yoki URL va mavjud bo'lganlardan qaysi biri haqida ko'rsatmalarni e'lon qiladilar. foydalanish uchun hujum vositalari. Ushbu modelga amal qilgan ba'zi hujum kampaniyalari ko'plab tarafdorlarni jalb qilishga muvaffaq bo'ldi. Biroq, bunday ixtiyoriy, muvofiqlashtirilgan DDoS hujumlarining asosiy kamchiligi shundaki, ishlatiladigan hujum vositalarining aksariyati foydalanuvchilarning identifikatorlarini yashirmaydi. Bunday vositalardan biri, Low Orbit Ion Cannon (LOIC) bu bilan mashhur edi - o'zlarining IP manzillarini yashirish uchun tashqi vositalardan foydalana olmagan ko'plab LOIC foydalanuvchilari FBI va butun dunyo bo'ylab boshqa huquqni muhofaza qilish tashkilotlari tomonidan kelishilgan holda ishtirok etganliklari uchun aniqlangan va hibsga olingan. ixtiyoriy hujumlar. Ushbu so'nggi hibsga olishlar haqidagi xabar ba'zi yangi foydalanuvchilarni bunday ixtiyoriy, muvofiqlashtirilgan hujumlarda ishtirok etishni tanlashdan qaytarishi mumkin.

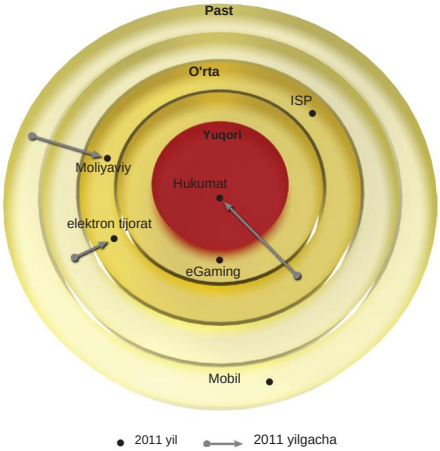


Hujumni boshlash

Botnetni to'plashdan tashqari, DDoS hujumini boshlash hatto texnik bo'lmagan shaxs uchun ham amalga oshirish qiyin ish emas. Foydalanuvchilar tartibda o'zlarining botnetlarini yaratishlari shart emas keng miqyosli hujumlarni boshlash uchun, chunki har kim foydalanishi mumkin bo'lgan turli xil maxsus to'lovli DDoS xizmatlari mavjud. Bunday xizmatdan foydalanayotgan har bir kishi o‘zi tanlagan nishonga kuchli DDoS hujumini hujumning hajmi va davomiyligiga qarab soatiga 5 dan 200 dollargacha amalga oshirishi mumkin.

Biznes ta'siri

DDoS hujumlari bo'yicha turli so'rovlar DDoS ning maqsadli kompaniyalarga ta'siri haqida qiziqarli faktlarni ta'kidladi. Neustar so‘roviga ko‘ra, so‘rovda qatnashgan kompaniyalarning 70 foizi ma’lum darajada zarar keltirgan DDoS hujumi qurboni bo‘lgan.3 O‘tmishda DDoS hujumlari ko‘proq sohaga oid maqsadlarga ega bo‘lgan bo‘lsa, bugungi kunda bunday hujumlar barcha sektorlarga – moliyaviy xizmatlarga qaratilgan. , hukumatlar, onlayn chakana sotuvchilar va onlayn o'yinlar va boshqalar. Radware kompaniyasining 2011 yilgi Global ilovalar va tarmoq xavfsizligi hisobotidan 4 olingan quyidagi diagramma bu tendentsiyani ko'rsatadi.



DDoS hujumining biznesga ta'siri katta va ta'sir qilishi mumkin hujum darajasiga qarab ma'lum vaqt davomida jabrlanuvchi.
Neustar va Radware hisobotlariga ko'ra, 2011 yilda amalga oshirilgan DDoS hujumlari bir necha soatdan bir necha kungacha davom etgan va o'rtacha 24 soat davom etgan. DDoS hujumining ta'siri maqsadli kompaniya tegishli bo'lgan sektorga va uning onlayn biznesi hajmiga qarab farq qilishi mumkin. Ko'pincha, bu ta'sirlar ham sifat, ham miqdoriy bo'lib, moliyaviy yo'qotishlar, obro'ga putur etkazishi va huquqiy oqibatlarga olib kelishi mumkin.

Moliyaviy yo'qotishlar

Tashkilotning veb-sayti ishlamay qolishi bilan bog'liq xarajatlar ushbu sohaga qarab sezilarli darajada farq qiladi

3 Neustar Insight – 2012 yil 1-chorak DDoS tadqiqoti
4 2011 yil Global ilovalar va tarmoq xavfsizligi hisoboti

tashkilotga tegishli. Neustar so'rovi shuni ko'rsatdiki, o'z biznesi uchun asosan yoki faqat Internetga bog'liq bo'lgan tashkilotlar (ayniqsa, onlayn chakana savdo yoki o'yin saytlari) o'rtacha kunlik daromad yo'qotilishini 2 000 000 AQSh dollari - soatiga qariyb 100 000 AQSh dollari - boshqa tarmoqlarda, masalan moliyaviy xizmatlar, ishlamay qolganda soatiga 10 000 AQSh dollari miqdorida kichikroq, ammo sezilarli o'rtacha yo'qotish haqida xabar beradi.

Ushbu hisob-kitobda bir nechta turli elementlar hisobga olinadi: hujumning o'zi, mijozlar va potentsial mijozlarning veb-saytga kirish imkoni yo'qligidan tushgan daromad, mijozlarni qo'llab-quvvatlash qo'ng'iroqlariga javob berishga sarflangan vaqt va mumkin bo'lgan qo'shimcha moliyaviy jarimalar.
Aksariyat jiddiy tajovuzkorlar o'z hujumlarini ehtiyotkorlik bilan rejalashtiradilar, maqsadli veb-saytlari uchun tanqidiy davrlarda, masalan, onlayn chakana sotuvchi uchun bayram xarid qilish mavsumida.

kabi yirik veb-saytlarga qaratilgan DDoS hujumlari to'lqini 2000-yilda Yahoo va Amazon jami 1,2 milliard dollardan ortiq zarar ko'rgan deb hisoblangan.5 So'nggi paytlarda Sony veb-saytlariga qilingan hujumlarning umumiy qiymati noaniqligicha qolmoqda va uni hisoblash qiyin. DDoS hujumi va ma'lumotlarning yo'qolishi bilan bog'liq muammolarni tozalash uchun Sony tomonidan 170 million dollardan ortiq mablag' sarflandi, biroq ba'zi tahlilchilar 77 million buzilgan foydalanuvchi hisoblarining har biri uchun Sony kompaniyasiga yuzlab dollarlar to'lashini taxmin qilmoqdalar - bu milliardlab dollarlarni tashkil etadi. zarar.6 Tahlilchilarning hisob-kitoblaridan qat'i nazar, bir narsa aniq: DDoS hujumlaridan yetarlicha himoyalanmagan tashkilotning xarajatlari haddan tashqari yuqori bo'lishi mumkin.

Mijozlarni yo'qotish

So'ralgan kompaniyalar tomonidan ko'rsatilgan eng muhim biznes ta'siri Bu uning mijozlari bilan bog'liq. Tashkilot veb-saytiga kirishga harakat qilgan, ammo ishlamay qolganligi sababli bunga erisha olmagan mijoz hech narsa sotib olmaydi, ma'lumotga kira olmaydi yoki umuman biron bir xizmatdan foydalana olmaydi. Agar u qoniqtirmasa, shikoyat qiladi, moliyaviy tiklash so'rovlari yoki hatto raqobatchilar uchun biznesni ko'paytirishi mumkin.

American Express 2011 Global mijozlarga xizmat ko'rsatish ma'lumotlariga ko'ra Barometr, iste'molchilar bor joyda ko'proq pul sarflashadi

5 SANS institutining "Xizmat ko'rsatishni rad etishni yumshatishning o'zgaruvchan qiyofasi"
6 Kazzuo Xirayning AQSh Kongressi Vakillar Palatasiga maktubi

ijobiy xarid tajribasi va yaxshi mijozlarga xizmat ko‘rsatish.7 Google muhandislari aniqladilarki, o‘rtacha onlayn mijoz sahifa yuklanishi uchun qo‘shimcha 400 millisekund kutishga tayyor emas – “Nyu-York Tayms”ning8 maqolasiga ko‘ra, “ko‘z ochib yumguncha”.
Onlayn mijozlar ma'lumotlarga tezkor kirishni talab qiladilar va Microsoftga ko'ra, agar veb-sayt raqobatchilarnikidan 250 millisekunddan ko'proq sekinroq bo'lsa, kamroq tashrif buyurishadi.8 Natijada, maqsadli kompaniya veb-saytiga tegishli xizmat ko'rsatishga to'sqinlik qiladigan DDoS hujumi. uning foydalanuvchilariga mijozning noroziligiga, g'azablangan qo'llab-quvvatlash qo'ng'iroqlariga va hatto mijozlarning ishdan chiqishiga olib kelishi mumkin.

Obro'ning yo'qolishi

Korxonalar yutuqlar va yutuqlarni ko'rsatish orqali sarlavhalar qilishni xohlashadi. Boshqaruv guruhlari ommaviy axborot vositalaridagi zaifliklarni tan olishga majbur bo'lishni yoqtirmaydi. Kompaniya o'z mijozlari va ularning ma'lumotlarini xavf ostiga qo'ygan kiberhujum qurboni bo'lganligi ommaga ma'lum bo'lganda, yuzaga keladigan yomon reklama ham obro'ga, ham kelajakdagi sotuvlarga halokatli ta'sir ko'rsatishi mumkin. Xakerlar qurboniga aylangan har qanday kompaniya “nima qilmaslik kerak” misoliga aylanadi va buning natijasida yuzaga keladigan oqibatlar ko'pincha buzilish yoki tanaffusga, korporativ rebrendingga va qimmat jamoatchilik bilan aloqalarga jamoatchilik ishonchini qaytarishga imkon bergan IT guruhini almashtirishni o'z ichiga oladi.

Huquqiy izlanishlar

Mumkin bo'lgan onlayn xizmatlarning mavjud emasligidan ta'sirlangan mijozlar Ular zarar ko'rganligini isbotlash, sudga da'vo arizasi berish orqali moliyaviy to'lovni amalga oshirishga urinishi mumkin, ko'pincha kompaniya bunday hujum ehtimoliga qarshi etarlicha ehtiyot choralarini ko'rmaganligini ta'kidlaydi. Bir misolda, 2011-yilda DDoS hujumiga uchragan yirik fond birjasi savdoni to‘xtatishga va savdo firmalariga normal xizmat ko‘rsata olmaganliklarini qoplash uchun jarima to‘lashga majbur bo‘ldi.

Xulosa

Tashkilotning DoS va DDoS hujumlaridan o'zini himoya qilish qobiliyati uning muvaffaqiyati uchun juda muhimdir. Tegishli himoya mexanizmlari bo'lmasa, DoS yoki DDoS hujumiga duchor bo'lgan tashkilot moliyaviy yo'qotish, obro'ga putur etkazish va yuridik xarajatlarni boshdan kechirishi mumkin - bularning barchasi uning kelajagiga doimiy ta'sir ko'rsatishi mumkin.

7 http://about.americanexpress.com/news/docs/2011x/AXP_2011_csbar_market.pdf
8 http://www.nytimes.com/2012/03/01/technology/impatient-web-users-flee-slow-loading sites.html?pagewanted=all

3 DDoS evolyutsiyasi

Dastlabki kunlar

Birinchi DoS hujumi 1974 yilda sodir bo'lgan va uni Illinoys Urbana universitetidagi Kompyuterga asoslangan ta'lim tadqiqot laboratoriyasi (CERL) qarshisida joylashgan Universitet o'rta maktabining 13 yoshli talabasi Devid Dennis amalga oshirgan. Shampan. Devid yaqinda CERL ning PLATO terminallarida ishga tushirilishi mumkin bo'lgan "tashqi" yoki "eks" deb nomlangan yangi buyruq haqida bilib oldi.

terminallarga ulangan tashqi qurilmalar bilan o'zaro ta'sir qilish. Qachon tashqi qurilmalar ulanmagan terminalda ishlaydi, ammo bu terminalning bloklanishiga olib keladi va funksionallikni tiklash uchun o'chirish va yoqishni talab qiladi. 13 yoshli yaramas bola sifatida u foydalanuvchilar bilan toÿla xona birdaniga qulflanib qolsa qanday boÿlishini koÿrishni xohladi, shuning uchun u “ext” buyrugÿini PLATO terminalidagi koÿplab terminallarga yuboradigan dastur yozdi. bir vaqtda. Bir kuni ertalab u CERLga bordi va o'z dasturini sinab ko'rdi; natijada barcha 31 foydalanuvchi birdaniga o'chirishga majbur bo'ldi. U o'z dasturini shahar va mamlakatning boshqa joylarida sinab ko'rishni davom ettirdi va oxir-oqibat PLATO terminallari yopilishi haqidagi ommaviy xabarlarni ko'rib xursand bo'ldi. Oxir-oqibat, muammoni hal qilib, masofaviy "ext" buyrug'ini qabul qilish sukut bo'yicha o'chirildi.

1990-yillarning oÿrtalari va oxirigacha Internet Relay Chat (IRC) ommalashib borayotgan vaqtda, baÿzi foydalanuvchilar roÿyxatdan oÿtmagan chat kanallarini boshqarish uchun kurash olib borishdi, bu yerda maÿmuriy foydalanuvchi tizimdan chiqsa, oÿz vakolatlarini yoÿqotadi. Bu xatti-harakat xakerlarni kanal ichidagi foydalanuvchilarni barcha tizimdan chiqishga majburlashga urinishlariga olib keldi, shuning uchun ular kanalga yakka o'zi kirib, mavjud bo'lgan yagona foydalanuvchi sifatida administrator huquqlariga ega bo'lishlari mumkin edi. Foydalanuvchilar IRC kanalini boshqarishga va uni boshqa xakerlar hujumiga qarshi ushlab turishga urinishlari mumkin bo'lgan ushbu "tepalik qiroli" janglari o'tkazish qobiliyatiga asoslangan juda oddiy DoS hujumlari va IRC chatidagi toshqinlardan foydalanish orqali amalga oshirildi. Bunday hujumlar

Haqiqiy dunyodagi "tepalik qiroli" o'yinida kuchsizroq odamlarni belgilangan tepalikdan yoki boshqa hududdan jismonan itarib yuboradigan kuchliroq odamga o'xshaydi.

DoS va DDoS hujumlari o'sha paytda dunyoda ustun bo'lganligi sababli ARM, lekin boshqa joylarda emas, jamoatchilik ularning mumkin bo'lgan ta'siriga unchalik e'tibor bermadi. Ko'pgina tashkilotlar serverlarni blokirovka qilish yoki ularni qurolsizlangan zonaga (DMZ) ko'chirish uchun IRC dan foydalanishni taqiqladi.

- tashkilotning kompyuter tarmog'i ichidagi har qanday qurilmalarni Internetga ta'sir qiladigan alohida mantiqiy kichik tarmoq. Bu amaliyot nafaqat DoS muammosini hal qilmadi, balki DoS hujumlarining bugungi kunda kiberhujumlarning kuchli shakliga aylanishi uchun mukammal muhit yaratdi.

DDoS va DDoS vositalarini demokratlashtirishning tarqalishi

Birinchi keng ko'lamli DDoS hujumlaridan biri 1999 yil avgust oyida, xaker Minnesota universiteti kompyuter tarmog'ini ikki kundan ortiq vaqt davomida o'chirib qo'yish uchun "Trinoo" deb nomlangan vositadan foydalanganda sodir bo'ldi. Trinoo asosiy va anonimlik xususiyatisiz edi; u "Masters" va "Daemons" deb nomlangan buzilgan mashinalar tarmog'idan iborat bo'lib, bu tajovuzkorga bir nechta Mastersga DoS ko'rsatmalarini yuborish imkonini beradi, so'ngra yuzlab daemonlarga UDP toshqinini boshlash uchun ko'rsatmalar yuboradi (ta'riflar uchun 7-bobga qarang). maxsus hujum turlari) maqsadli IP manziliga qarshi. Asbob Daemonlarning IP manzillarini yashirish uchun hech qanday harakat qilmadi, shuning uchun hujum qiluvchi tizimlar egalari bilan bog'lanishdi va ularning tizimlari buzilganligi va hujumda foydalanilgani haqida hech qanday tasavvurga ega emas edi. Boshqa dastlabki vositalar orasida masofadan yangilanishi va IP-spoofingni qo'llab-quvvatlashi mumkin bo'lgan Stacheldraht (nemischa "tikanli sim") va o'z qurbonlaridan hujum statistikasini yig'ish qobiliyatiga ega Shaft va Omega kabi vositalar kiradi. Keyinchalik xakerlar o'zlarining hujumlari haqida ma'lumot olish imkoniga ega bo'lganligi sababli, ular ma'lum turdagi hujumlarning ta'sirini yaxshiroq tushunishlari va hujum aniqlanganda va to'xtatilganda bildirishnoma olishlari mumkin edi.

Bir marta xakerlar tarqatilgan xizmatlardan voz kechishga e'tibor berishni boshladilar hujumlar, DoS hujumlari jamoatchilik e'tiborini jalb qila boshladi. DDoS hujumining "tarqalgan" tabiati uni sezilarli darajada kuchliroq qiladi, shuningdek uning manbasini aniqlash va blokirovka qilishni qiyinlashtiradi. O'z arsenalida shunday dahshatli qurolga ega bo'lgan xakerlar takomillashtirilgan vositalar va usullardan foydalangan holda kattaroq va ko'zga ko'ringan nishonlarni egallashni boshladilar.

DDoS hujumlari sarlavhalarga aylanadi

2000 yil fevral oyida DDoS hujumlari haqiqatan ham jamoatchilik e'tiborini tortdi. Yahoo, CNN, Amazon, Buy.com, E*Trade va ZDNet kabi o'sha paytdagi bir qancha mashhur internet saytlari nishonga olingan edi. Hatto kiberjinoyatlar bo'yicha eng yirik prokuror bo'lgan FBI veb-sayti ham DDoS hujumi tufayli uch soat davomida oflayn holatga keltirildi.

Nishon qilingan har bir sayt og'ir, o'zgaruvchan trafik hajmiga o'rganib qolgan, diqqat bilan kuzatib boriladigan va yaxshi ta'minlangan sayt edi va hozir ham shunday bo'lib qolmoqda. Shunga qaramay, har bir maqsadli veb-sayt ma'lum darajada tajribaga ega

2000 yil fevralidagi DDoS hujumlari natijasida ishlamay qolgan vaqt. Agar ushbu tashkilotlar zaif bo'lganida, o'rtacha biznes qanday fosh bo'lishini ko'rish qiyin emas.

2000-yillarning boshlarida sodir bo'lgan yana bir muhim DDoS hujumi 2002 yilda Internetning barcha 13 ta ildiz domen nomlari xizmati (DNS) serverlariga mo'ljallangan. DNS muhim Internet xizmatidir, chunki u yagona resurs lokatorlari (URL) ko'rinishidagi xost nomlarini IP manzillarga tarjima qiladi. Aslida, DNS barcha Internet manzillari va ularning tegishli URL manzillarining asosiy ro'yxatini saqlaydigan telefon kitobidir. DNS bo'lmasa, foydalanuvchilar Internetda samarali harakatlana olmaydi, chunki veb-saytga tashrif buyurish yoki ma'lum bir qurilma bilan bog'lanish uning IP-manzilini bilishni talab qiladi. DNS ierarxik tizimdir, chunki kichikroq DNS serverlar boshqa yirik DNS serverlariga tayanadi; eng yuqori darajada 13 ta ildiz nomi serverlari mavjud bo'lib, ularsiz dunyoning DNS tizimi ishlamay qoladi.

Kuchli DDoS hujumining barcha 13 ta asosiy serverga bir vaqtning o'zida ta'siri halokatli bo'ladi - Internetni ko'rish sekin yoki hatto dunyodagi hamma uchun yaroqsiz bo'ladi. 2002 yilda ildiz nomi serverlariga qilingan hujum paytida barcha 13 ta server katta yuklanishni boshdan kechirdi va ularning ba'zilariga global Internetning ayrim qismlaridan kirish imkoni bo'lmadi. Internet hali ham foydalanish mumkin bo'lsa-da, taxminan bir soat davomida foydalanuvchilar ba'zi nom so'rovlari uchun bir necha soniyagacha kechikishlarni sezishlari mumkin. Hujum to'liq muvaffaqiyatli bo'lmagan bo'lsa-da, etarli resurslar bilan bunday hujum ancha sezilarli ta'sir ko'rsatishi mumkinligini isbotladi.

Jinoiy tovlamachilik va siyosiy kun tartibini davom ettirish

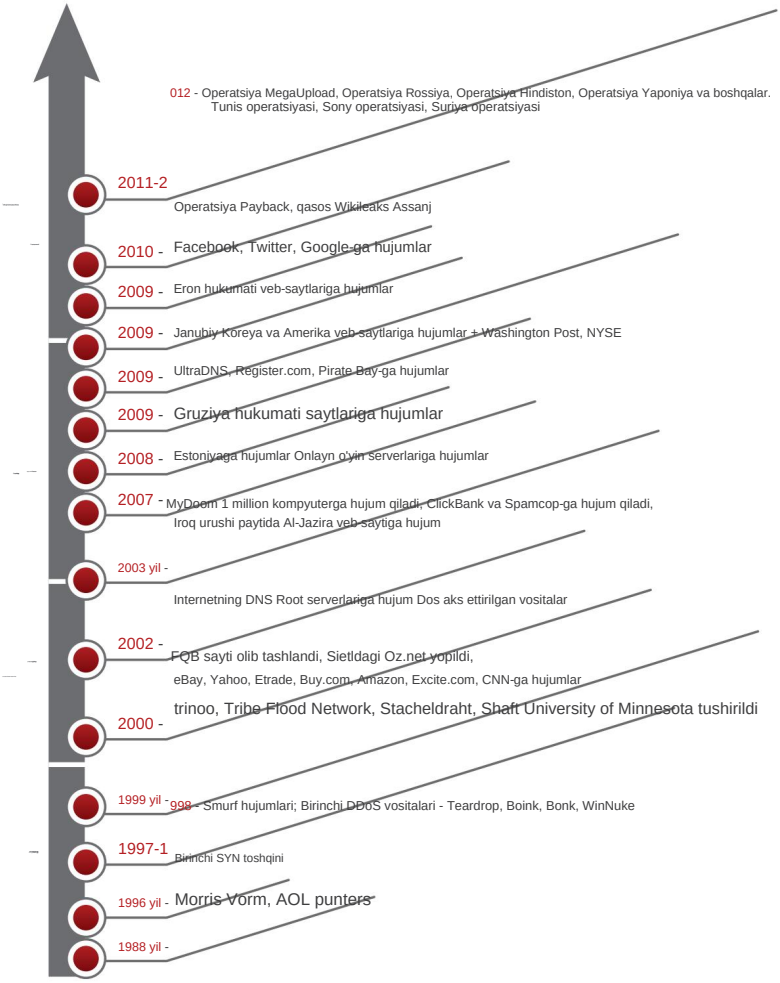
Dunyo bo'ylab DDoS hujumlari davom etar ekan, motivatsiyalar rivojlana boshladi. Xakerlar tovlamachilikka urinish vositasi sifatida maxsus hujumlarni boshladilar. Ular onlayn sotuvchi saytlari, qimor o'yinlari va pornografiya saytlariga xabarlar jo'natib, "himoya puli" evaziga asl hujumni amalga oshirgan "uchinchi tomon" tomonidan kelajakdagi hujumning oldini olishlari mumkinligini aytishdi. Shartnomaga rioya qilgan saytlar "to'lovchilar" sifatida belgilanishi va keyingi hujumlarda nishon sifatida ishlatilishi mumkin. Clickbank va Spamcop veb-saytlari 2003 yilda bunday hujumlarning nishoniga aylangan edi.

Boshqa tomondan, siyosiy sabablarga ko'ra va kiber urush bilan bog'liq DDoS hujumlari ko'paydi. Ikkinchi Fors ko'rfazi urushi paytida DDoS hujumi Qatarda joylashgan Al-Jazeera News telekanalini yo'q qildi; 2004 yilda Shimoliy Koreya xakerlari Janubiy Koreya va Yaponiyadagi kompyuterlarga hujum qilishdi; va 2007-2008 yillarda Rossiya Estoniya va keyinchalik Gruziyaga qarshi kiber urushlarining bir qismi sifatida DDoS hujumlaridan foydalanishini ta'kidladi.

Anonimning yuksalishi

Jinoiy tovlamachilik va kiber-urush bilan bog'liq DDoS hujumlari soni o'sishda davom etsa-da, siyosiy sabablarga ko'ra hujumlarning ko'p holatlari maqsadli kompaniyalar tomonidan yomon e'lon qilinmaslik uchun sir tutiladi. Xususan, 2007-yildan boshlab “Anonymous” siyosiy motivli “hacktivist” guruhining hujumlari sarlavhalarga aylana boshladi.
2008 yil (Anonim haqida ko'proq ma'lumot olish uchun 5-bobga qarang) "Loyiha Chanologiyasi" bilan boshlangan, Sayentologiya cherkovini nishonga olgan hujum. O'shandan beri Anonymous yangiliklarda tez-tez paydo bo'lib, o'z noroziliklarini muvofiqlashtirish uchun ijtimoiy tarmoq saytlarida faol ravishda video va xabarlarni joylashtirdi - ham kiber hujumlar, ham jismoniy yig'ilishlar ko'rinishida.

Vaqt jadvali



4 Hujumlar ortida kim va motivlar nima?

So'nggi yillarda kiberhujumlar chastotasi keskin oshdi, chunki o'z raqobatchilari yoki dushmanlariga bunday hujumlarni amalga oshirishni tanlagan shaxslar va tashkilotlar soni, shuningdek, potentsial zaif bo'lgan kompyuterlar va kompyuter tarmoqlaridan foydalanish ko'paydi. Ko'p sonli hujumlar moliyaviy sabablarga ko'ra bo'lsa-da, - biznes raqobatchisini mayib qilishdan tortib jinoiy tovlamachilikgacha - boshqa ko'plar siyosiy yoki hatto "lulz" ("o'yin-kulgi" uchun Internet jarangi) uchundir. Biroq, hech kim muvaffaqiyatli hujumning jiddiyligi yoki potentsial narxiga shubha qilmasligi kerak.

Moliyaviy daromad

Moliyaviy foyda olish maqsadida DDoS hujumlaridan foydalanadigan tashkilotlar ikki toifaga bo'linadi: raqobatchilardan ustunlikka erishmoqchi bo'lganlar va jinoiy tovlamachilikni amalga oshirishga uringanlar. Raqobatchilarga hujum qilish uchun uchinchi tomonning DDoS xizmatidan foydalanadigan har qanday qonuniy tashkilot ushbu raqibni sezilarli noqulay ahvolga solishi mumkin; chunki bunday hujumlar hujum qiluvchi kompaniya DDoS xizmatlari uchun to'lagan narsaga nisbatan hujum mavzusiga nomutanosib ravishda qimmatga tushadi.

Ijaraga haq to'lanadigan DDoS xizmatlarini taklif qiluvchi tashkilotlar ko'pincha jinoiy tovlamachilikka murojaat qilishadi. DDoS yordamida jinoiy tovlamachilik tovlamachi kompaniya maqsadli biznesni tanlashi va ularga nisbatan nisbatan kichik “namuna” DDoS hujumini boshlashi bilan boshlanadi. Keyin ushbu hujum qiluvchi kompaniya o'z nishoniga xabar yuboradi, ular hujumni boshlagan "uchinchi tomon" tomonidan qo'shimcha, jiddiyroq DDoS hujumining oldini olish imkoniyatiga ega ekanligini va buni ma'lum miqdorda pul evaziga amalga oshirishini taklif qiladi (odatda). minglab dollarlar oralig'ida). Agar hujumga uchragan kompaniya to'lovni bajarsa, ular DDoS-to'lov xizmati tomonidan "to'lovchi" sifatida tan olinishi va kelajakda tovlamachilik urinishlari uchun nishon sifatida ishlatilishi xavfi bor. Bunday vaziyatda, kelajakdagi hujumlarning oldini olish uchun ko'pincha DDoS yumshatish yechimining qandaydir shakllarini qo'llash zarur bo'ladi.

Anonim - so'nggi bir necha yil ichida sodir bo'lgan siyosiy sabablarga ko'ra sodir bo'lgan ko'plab yirik kiberhujumlar uchun mas'ul bo'lgan kompyuter "hacktivist" guruhi - 2003 yilda 4chan tasvirlar panelida har bir foydalanuvchining "Anonymous" nomiga hazillashgan murojaat sifatida tashkil etilgan. post. Anonim anarxistik markazlashtirilmagan organ sifatida jismoniy va kiber norozilik namoyishlari orqali Internet tsenzurasiga qarshiligini davom ettirdi. Anonymous butunlay markazlashtirilmaganligi va yetakchilik yoki reyting tizimiga ega bo‘lmaganligi sababli, har kim shunchaki buni xohlab “qo‘shilishi” mumkin. Namoyishlar va kiberhujumlar tasvirlar, forumlar, wikilar, IRC, YouTube va ijtimoiy tarmoq xizmatlari yordamida muvofiqlashtiriladi va Anonymousning har qanday aʼzosi “Anonim”ga parallel ravishda oʻz maqsadlari toʻplamiga erishish yoʻlida tadbirlar tashkil qilishi mumkin. ” kun tartibi.

Kiberkosmosda Anonymous hujumlari ko'pincha past orbitali ion to'pi (LOIC) va uning yangi qarindoshi High Orbit Ion Cannon (HOIC) kabi suv toshqini vositalarini taqsimlash orqali davom ettiriladi. Bunday hujumlarda ixtiyoriy ravishda ishtirok etish uchun ko'p sonli foydalanuvchilarni jalb qilish orqali - odatda IRC orqali, chunki bu anonim aloqa vositasidir - Anonim minglab kompyuterlardan iborat "ixtiyoriy botnet" ni samarali yaratadi. Hatto juda katta serverni nishonga olish uchun LOIC yoki HOIC bilan ishlaydigan juda ko'p sonli mashinalardan foydalanish ko'pincha xizmat ko'rsatishni rad etish holatiga olib keladi va bu Anonymous-ni kiberhujumchi sifatida dahshatli qiladi.

Siyosiy motivatsiya

Raqobatchilarni yiqitish yoki jinoiy tovlamachilikka murojaat qilish orqali moliyaviy daromad olishdan tashqari, boshqalar siyosiy yoki ko'ngilochar motivlar (ko'pincha ikkalasining kombinatsiyasi) uchun DDoS hujumlarini boshlashga undaydilar. Bu nisbatan yangiroq motivlar kiberhujumlar olamidagi evolyutsiyani belgilab beradi, bu esa siyosiy kun tartibiga erishish uchun kiberhujumlardan foydalanishni anglatuvchi “haktivizm” atamasining paydo boʻlishiga olib keladi. Anonymous va (hozirda demontaj qilingan) LulzSec kabi turli xakerlik guruhlari bunday hujumlarni amalga oshiradilar, ko'pincha ular noqulay deb hisoblagan qonun tarafdorlariga va bunday qonunchilik bilan bog'liq turli davlat idoralariga qaratilgan. Anti-qaroqchilik bilan bog'liq Operation Paybackdan tashqari, Anonymous va boshqa "hacktivist" guruhlar tomonidan boshqa hujumlar (yoki hujumlarga urinishlar) "AntiSec Operation", "Operation Blackout" va "Operation Defense" ni o'z ichiga olgan. Eng mashhur hujumlardan ba'zilari butun dunyo bo'ylab yirik davlat idoralariga, jumladan, AQSh FBI va Britaniya SOCAga qaratilgan.

Ilg'or doimiy tahdidlar va kiber urush

Bunday beg'araz, yashirin kiberhujumni amalga oshirish uchun doimiy maqsad va ilg'or vositalarga ega bo'lgan har qanday tashkilot yoki shaxs rivojlangan doimiy tahdid (APT) deb nomlanadi. APTlar kelajakda katta rol o'ynashi mumkin, chunki DDoS va boshqa hujumlar orqali razvedka ma'lumotlarini o'g'irlash yoki dushmanning kiberinfratuzilmasini buzish qobiliyati faqat jismoniy hujumlarga qaraganda bir xil yoki ehtimol undan ham halokatli bo'lishi mumkin. So'nggi yillarda kiberxavfsizlik dunyosi Duqu, Stuxnet va Flame kabi juda murakkab zararli dasturlarning topilganiga guvoh bo'ldi va bu etarli resurslarga ega bo'lgan shaxs, tashkilot yoki davlat bunday kuchli kiber urush vositasini yaratishga qodir ekanligini isbotladi. uni aniqlanmasdan tarqating.

Xususiy zararli dasturlarsiz ham, APTlar ijaraga olishlari yoki ishga olishlari mumkin qonuniy foydalanuvchilarning muhim serverlar yoki tarmoq qurilmalariga kirishiga to‘sqinlik qiluvchi tarmoq infratuzilmasiga jiddiy zarar yetkazishi mumkin bo‘lgan zaiflikka asoslangan bo‘lmagan DDoS hujumlarini ishga tushirish uchun o‘z massiv botnetlariga – zararlangan mashinalarning katta tarmoqlariga ega. Bundan tashqari, terrorchi APTlar ma'lumotlarini o'g'irlagan yoki kompyuterlari noto'g'ri ishlayotganlarga katta zarar yetkazish uchun hukumat va fuqarolik kompyuter infratuzilmasiga zarar etkazish uchun bunday ilg'or zararli dasturlardan yoki boshqa hisoblash resurslaridan foydalanishi mumkin.

Davlat idoralariga qarshi ko‘plab hujumlar siyosiy sabablarga ko‘ra hujumlar. Biroq, LulzSec xakerlar guruhi 2011 yilning yozida asosan o'yin-kulgi uchun Amerika Qo'shma Shtatlari va boshqa davlat idoralariga qarshi muvaffaqiyatli hujumlar uyushtirdi; Ularning shiori “Sizning hisobingizdan yuqori sifatli o'yin-kulgi bo'yicha dunyo yetakchilari” edi. LulzSec faoliyatining eng yuqori cho'qqisida - ular hukumatlar, kompaniyalar va boshqa shaxslarning kompyuter tarmoqlariga kirgan 50 kunlik davrda - ular juda ko'p shaxsiy ma'lumotlarni, jumladan, ko'plab foydalanuvchi nomlari, parollar va shaxsiy identifikatsiya ma'lumotlarini ommaga oshkor qildilar. Asl LulzSec endi ishlamasa-da, o'zini LulzSec Reborn deb ataydigan yangi shaxs yoki guruh mart va iyun oylarida allaqachon ikkita yuqori darajadagi hujumni amalga oshirgan.

Kompyuterlar, kompyuter qurilmalari va kompyuter tarmoqlaridan foydalanishning o'sishi bilan kiberhujumlarning tabiati va murakkabligida sezilarli evolyutsiya bo'ldi. Faqat kiberhujumlar amalga oshirilmaydi

APTlar tomonidan - katta resurslarga va aniq maqsadga ega bo'lgan shaxslar yoki tashkilotlar - shuningdek, qonuniy biznesdan uyushgan jinoyatchilikka qadar va hatto moliyaviy bo'lmagan motivlarga ega bo'lgan havaskor "xakerlar"gacha bo'lgan turli boshqa sub'ektlar tomonidan (masalan, LulzSec).

5 DDoS hujumi bilan urish qanday - Ichki ko'rinish

Tarmoq yoki tizim ma'muriga kompaniya infratuzilmasi hujum ostida ekanligi har doim ham ayon bo'lavermaydi. Hujum odatda sekin boshlanadi va faqat hujum davom etar ekan, kimdir buni sezadi. Quyida DDoS hujumi ostidagi kompaniyaning tizim administratori tomonidan soatma-soat tasvirlangan faraziy stsenariy keltirilgan.

5:30

Telefonimga kiruvchi SMS-xabar ovozidan uyg'onib ketdim. Unda "Ogohlantirish, asosiy dastur serveri 30% maksimal yuklanishda" deb o'qiladi.

Bunday xabar yangi server tomonidan yuborilgan avtomatik bildirishnomadir Biz yaqinda o'rnatgan salomatlik monitoringi vositasi, mainapp esa mijozlar so'rovlarini ko'rib chiqadigan asosiy onlayn bank ilovasi veb-serverdir. Bizning bosh direktorimiz onlayn-bankingni targ'ib qilish va mijozlarni onlayn-banking ilovasidan foydalanishga undash uchun marketing kampaniyasini boshlashga strategik qaror qilganligi sababli, bank asosiy bank ilovasi veb-serveri mustahkam, kengaytiriladigan va yuqori darajada bo'lishini ta'minlash uchun katta miqdorda mablag 'sarfladi. mavjud. Hozircha u joriy trafikni boshqarish uchun yetarli protsessor kuchi va xotiraga egadek tuyuladi, chunki o‘tgan oy statistikasi server yukini 15% dan ko‘p bo‘lmaganini ko‘rsatdi.

Server yuki 30% da ekanligi haqidagi xabarni qabul qilish tashvishli, ammo jiddiy emas. Ogohlantirish chegarasi parametrlari monitoring vositasida noto'g'ri o'rnatilgan bo'lishi mumkin, lekin men ofisga keyinroq kelganimda buni tekshirishni kutishim mumkin.

6:00

Yarim soatdan keyin yana bir SMS keladi. Bu o'qiydi "Ogohlantirish, asosiy dastur serveri 50% maksimal yuklanishda." Nimadir noto'g'ri ekanligi aniq.

Men salomatlik monitoringi vositasiga masofaviy kirishni sozlamaganim uchun uning jurnallariga qaray olmayman. Tekshirish uchun ofisga borishga shoshilayotganimda, men server yukining bunday yuqori bo'lishining mumkin bo'lgan sabablarini ko'rib chiqaman. Men o'zimni ishontirishga harakat qilaman, ehtimol bu oddiy konfiguratsiya

xato, lekin men tashvishlana boshlayman. Telefonim jiringladi - bu mening hamkasblarimdan biri, boshqa tarmoq ma'muri. U men kabi ogohlantirish xabarini oldi va vaziyatdan xabardorligimni bilmoqchi.

7:00

Mijozlarni qo'llab-quvvatlash bo'limining navbatchi menejeri hali ishlayotganimda menga qo'ng'iroq qilmoqda

Mening fikrimcha, ko'plab mijozlar onlayn-banking veb-sayti odatdagidan sezilarli darajada sekinroq ishlayotganidan shikoyat qilish uchun qo'ng'iroq qilishmoqda. Uning so‘zlariga ko‘ra, mijozlardan biri vaqt talab qiladigan pul o‘tkazmasini odatdagidek tez amalga oshira olmagani uchun g‘azablangan va bunday muammolardan qochish uchun onlayn-bankingga o‘tgan.
Bu mijoz shunchalik g'azablanganki, u sekin tranzaksiya tufayli moliyaviy yo'qotishlari uchun bankni sudga berish bilan tahdid qilgan.

Nihoyat, men ofisga keldim va server terminali ekraniga shoshildim.
Mainapp yuklanishi 70% ga yetdi — deyarli maksimal.

Salomatlik monitoringi vositalari jurnallarini tez tekshirgandan so'ng, men ogohlantirish chegaralari to'g'ri o'rnatilganligini bilib oldim. Tarmoq trafigi hali ham g'ayritabiiy darajada yuqori ko'rinadi, shuning uchun bu ogohlantirish chegarasi muammosi emas. Onlayn banking veb-saytida turli sahifalarni so'rash uchun serverga minglab ulanishlar ochildi.

Vahima qilmaslikka urinar ekanman, peshonamdan bir necha munchoq ter oqadi. Tarmoq trafigining bunday katta miqdori zararli manbadan kelib chiqishi kerak, lekin nima uchun? Buning ortida kim turibdi? To'satdan moliyaviy xizmatlarga kiberhujumlar to'lqini haqida o'tgan hafta gazeta sarlavhalarini eslayman. Men serverimiz boshdan kechirayotgani va gazetalarda o'qiganlarim o'rtasidagi o'xshashliklarni darhol eslayman, chunki serverimizga xizmat ko'rsatishni rad etish hujumi nishonga olinganidan qo'rqaman.

ertalab 8:00

Eng yomoni deb hisoblab, tabiat va manbani aniqlashga harakat qilaman zararli tarmoq trafigidan. Birinchidan, men ulanishlar qayerdan kelib chiqqanligini tekshirib ko'raman va qonuniy va zararli trafikni farqlash uchun tajovuzkorlarning IP manzillarini ajratishga harakat qilaman.
Bu orada telefonim jiringlashdan to‘xtamadi.

CIO nima bo'layotganini bilishni istab qo'ng'iroq qiladi; Men unga shunday ekanligimni aytaman muammoni hal qilishga harakat qilmoqdamiz, lekin biz server resurslarini tugatuvchi xizmat ko'rsatishni rad etish hujumi ostida bo'lishimiz mumkin. U javob bermaydi va men bir lahzalik umidsizlikni his qilaman. U faqat bosh direktor aralashishdan oldin muammoni tezda hal qilish kerakligini aytdi.

Hujumni qanday to'xtatish haqida hech qanday ma'lumotim yo'q va bu xizmatni rad etish ekanligiga ham ishonchim komil emas. Faoliyatimda hech qachon bunday narsani ko'rmaganman. Mavzu bo'yicha mening yagona bilimim o'tgan oy xavfsizlik seminarida qatnashganimdan keyin Internetda o'qiganimdan olingan.

IP iziga qaraganda, barcha zararli ulanishlar turli xil manbalardan kelganga o'xshaydi. Har bir IP qayta-qayta turli xil onlayn bank sahifalari uchun HTTP GET so'rovlarini yuboradi va bu harakat asosiy ilovaning barcha resurslarini o'zlashtirib, onlayn bank sahifalarini qonuniy foydalanuvchilar uchun sekinlashtiradi.

Nima bo'layotgani haqida bir oz tasavvurga ega bo'lib, men qisqa muddatli rejaga qaror qildim harakat qiling va favqulodda guruh yig'ilishini chaqiring.

8:30

Vaziyat yaxshilangani yo'q. Hujum sur'ati doimiy edi, ammo hozir mainapp har qanday so'rovga deyarli javob bermaydi. Mening ofisimdagi mijozlarni qo‘llab-quvvatlash bo‘limi menejeri xafa, chunki uning barcha xodimlari qo‘llab-quvvatlash qo‘ng‘iroqlari bilan to‘lib-toshgan. Mijozlar baxtsiz va g'azablangan, lekin u ularga nima deyishni buyura oladi? Men unga, menimcha, biz bir yoki bir nechta xakerlar tomonidan hujumga uchrayapmiz, biz tez orada normal xizmatga qaytamiz deb umid qilmasligimizni va yaqin kelajakda ishlamay qolganimiz haqida rasmiy bayonot berishimiz mumkinligini aytaman.

Shu bilan birga, men yordam uchun ISP bilan bog'lanib, ularga server jurnallarimizni yuboraman. Bizning tarmoqli kengligimiz hali to'liq to'yinmagan bo'lsa-da, men ular nima bo'layotganini bilishlarini va kerak bo'lganda bizga yordam berishga tayyor bo'lishlarini xohlayman.

9:00

Vaziyat endi falokatga aylandi. Gap tarqaldi, butun xodimlar vahima ichida. Men chaqirgan favqulodda majlis chaqirildi; u CIO, CTO, tarmoq ma'murlari, xavfsizlikdan iborat

menejer, dastur menejeri va tizim ma'murlari (shu jumladan men). Biz tarangmiz, lekin tushunamizki, biz mijozlarga rasmiy xabar berishimiz va hujumga qarshi harakat rejasini tanlashimiz kerak.

Men hammaga jurnallarni ko'rsataman va bir necha daqiqadan so'ng xavfsizlik menejeri Rossiyadan ba'zi zararli so'rovlar kelayotganini payqadi. Tezda, men asosiy ilova veb-serverida Rossiyadan kelgan barcha so'rovlarni rad etish qoidasini belgilayman, bu hujumni sekinlashtirishi mumkin.
Afsuski, bu yordam bermaydi. Yangi filtrimni faollashtirgandan so'ng, men zararli trafik miqdori kamayganini ko'rmayapman. Yangi ulanishlarsiz qisqa vaqtdan so'ng, qo'shimcha ulanishlar o'nlab turli mamlakatlardan, shu jumladan bizdan ham kelib chiqa boshlaydi!

9:30

Server hali ham katta yuk ostida; Shubhasiz, IP-larni blokirovka qilish geografik mintaqada yordam bermadi, shuning uchun biz boshqa yechim izlashimiz kerak. Biz bunday hujumga qarshi turishga tayyor emasligimizni tushunib, xizmatdan bosh tortish hujumini qanday oldini olish va yumshatish haqida qo'shimcha tushunchaga ega bo'lish zarur bo'ldi.

10:00

Asosiy ilovaning veb-serverini butunlay suv bosgan va onlayn bank sayti oflayn. Ushbu yangilikdan so'ng, bosh direktor ishtirok etishga qaror qiladi. U bunday hujumni e'lon qilish bank obro'si uchun qanchalik yomon ekanini ta'kidlab, daromadning yo'qolishi va mijozlarning noroziligi bankka qanchalik qimmatga tushishi bilan qiziqadi. U bu hujum tafsilotlari matbuotga chiqib ketsa, bu bank mijozlari orasida vahima keltirib chiqarishi mumkinligidan xavotirda. U yana bir bor ta'kidlaydiki, hujumni tezda, zarur bo'lgan va IT xodimlarining ishiga noaniq tahdid soladigan vositalar yordamida yumshatish kerak.

10:15

Bizga DDoS hujumlarini yumshatishda mutaxassislar yordami kerak.

DDoS hujumidan omon qolish uchun eng yaxshi ekspert darslari

Onlayn biznesingizni DDoS hujumlaridan himoya qilish haqida gap ketganda, siz beparvo va ahmoq bo'lolmaysiz. Ammo umidsizlikka tushmang: tashkilotlar oddiy choralarga rioya qilish orqali nazoratni qaytarib olishlari mumkin. Bularni bilishingiz kerak bo'lganlar ro'yxatiga qo'shing:

1 Hech bir tashkilot xavfsiz emas, faqat xavfsizroq.

2 DDoS hujumlariga tayyor bo'ling. Sizga hujum **qilishdan oldin** mudofaa strategiyasini tashkil qiling

3 Xavfsizlikka tayyorligingiz haqida halol ekanligingizga ishonch hosil qiling. Potentsial xavfsizlik teshiklarini aniqlang, kerakli vositalar va odamlarni joyiga qo'ying va "bepul" yoki "bolt-on" asboblardan ehtiyot bo'ling.

4 Ajratish uchun to'g'ri byudjetni aniqlash uchun biznes risklarini tahlil qiling.

5 Xavfsizlik guruhiga barchani jalb qiling. Xavfsizlik uchun javobgarlik endi xavfsizlik guruhining yagona viloyati emas.

6 Hujum yo'qolgan bo'lishi mumkin, ammo tahdid davom etmoqda. Hujumlar turi, hajmi va chastotasi kabi ma'lumotlarni to'plang.
Har bir hujum turi uchun to'g'ri chora-tadbirlardan foydalaning .

7 DDoS yumshatuvchi tizimlaringizni sinab ko'ring va ular bugungi tahdidlarni aniqlash va yumshata olishiga ishonch hosil qiling.

8 Tashkilotingizga DDoS hujumini simulyatsiya qiling va har bir xodim hujum paytida o'z rolini bilishiga ishonch hosil qiling.

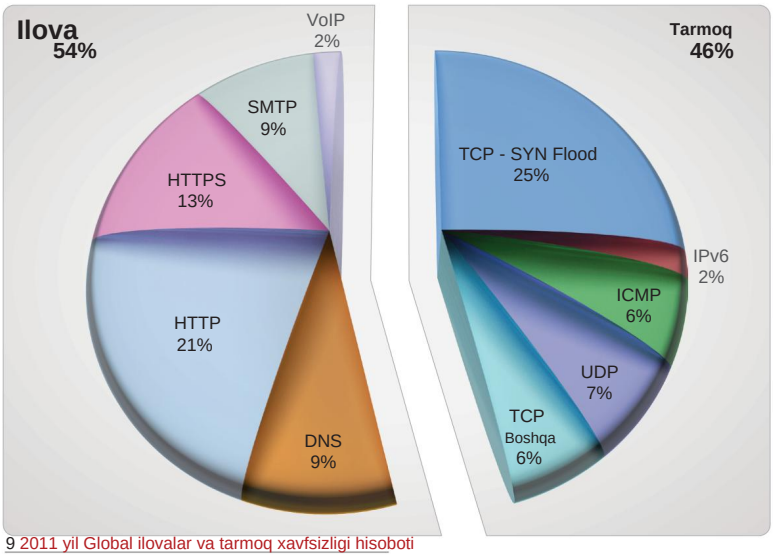
9 Siz uni o'tirib olishingiz shart emas. Hujumchini zararsizlantirishi mumkin bo'lgan hujumkor pozitsiyani egallab, o'zingizni himoya qilishingiz mumkin. Tajovuzkorning ritmi va niyatini o'rganing, shunda siz samarali qarshi texnikani qo'llashingiz mumkin.

6 Hujum turlari va ularning ta’siri

Hujumlarning evolyutsiyasi turi

Oldingi bo'limlarda aytib o'tilganidek, DDoS hujumlari yillar davomida sezilarli darajada rivojlandi. Ularning demokratlashuvi, asosan, bugungi kunda hujumni boshlashning qulayligi, shuningdek, aksariyat tashkilotlarning hatto eng oddiy DDoS hujum turlariga nisbatan yomon tayyorgarligi bilan bog'liq. Tajribasiz foydalanuvchilarga bunday hujumlarni amalga oshirish bo'yicha ko'rsatmalar Internetda keng tarqalgan va hatto hujumning kuchini oshirish uchun to'lovli DDoS xizmati orqali botnetni ijaraga olish mumkin.

Hujumchilar o'z maqsadlarini amalga oshirgandan so'ng "o'tkazib yuborish" xavfini o'z zimmalariga olmaydilar; ular amaldagi mudofaa choralarini chetlab o'tishga harakat qilish uchun tez-tez hujum vektorlarini o'zgartiradilar. Ko'pgina zamonaviy hujumlar odatda bitta hujum kampaniyasida bir nechta vektorlardan foydalanadi, ular tashkilotning tarmoq infratuzilmasi va uning ilovalarining bir nechta komponentlariga qaratilgan. 2011 yilda kiberhujumlarning 56% ilovalarga qaratilgan; 46% tarmoqda. Hujumlar endi bitta kampaniyada kamida 5 xil hujum vektorini o'z ichiga oladi.9 Va ular uzoqroq ishlamoqda - APT qisqartmasi (ilg'or doimiy tahdid) bizning leksikonimizning asosiy qismi bo'lib qolishi ta'minlanadi.



9 2011 yil Global ilovalar va tarmoq xavfsizligi hisoboti

Hujumlar nafaqat tarmoq resurslarini, balki ba'zi hollarda server (va boshqa statistik qurilma) yoki dastur resurslarini ham iste'mol qilishga harakat qiladi.

Foydalanish orqali DoS va DDoS hujumlarining har xil turlarini tasniflash faqat bitta o'lchov juda qiyin. Har bir hujum turi o'ziga xos xususiyatlarga ega, bu uning bir nechta toifalarga tegishli ekanligini ko'rsatishi mumkin. Umuman olganda, hujumlar turlari tarmoq resurslariga, server resurslariga va dastur resurslariga qaratilgan hujumlarni o'z ichiga oladi. Quyida ba'zi eng keng tarqalgan hujumlar va ularning texnik asoslari ro'yxati keltirilgan.

“Payback” operatsiyasi Amerika Qo‘shma Shtatlari hukumatining WikiLeaks’ga maxfiy hukumat hujjatlari va aloqalarini fosh qilgani uchun o‘ch olish maqsadida “Anonymous” xakerlar guruhi tomonidan uyushtirilgan bir qator kiberhujumlar edi. Payback operatsiyasi davomida Anonymous Visa, MasterCard va PayPal kabi saytlarni nishonga oldi, chunki ularning barchasi WikiLeaks uchun xayriyalarni qabul qilishni to'xtatgan edi. Ushbu hujumlarning asosiy maqsadi maqsadli kompaniyalar xizmatlarini to'xtatib, ularga moliyaviy yo'qotishlar va jamoatchilikni tahqirlash orqali qabul qilingan adolatsizlikka qarshi norozilik bildirish edi. Hujumning o‘ziga xosligi shundaki, Anonymous birinchi marta bunday keng miqyosda tajribasiz ko‘ngillilarni maxsus DDoS vositasini yuklab olish uchun jalb qildi, bu ularga botnetlardan foydalangan holda tajribali xakerlar bilan bir qatorda hujumlarda qatnashish imkonini berdi.

“Sony” **operatsiyasi Sony** PlayStation tarmog‘iga bir qator kiberhujumlar bo‘lib, Sony kompaniyasining obro‘siga putur yetkazgan va unga moliyaviy zarar yetkazgan. Bu xakerlar o'z maqsadlarini o'zlarining haqiqiy maqsadlaridan - ma'lumotlarni o'g'irlashdan chalg'itish uchun DDoS hujumidan foydalangan klassik holat edi. DDoS hujumi yaxshi rejalashtirilgan va yaxshi bajarilgan; Bu xakerlarga Sony PlayStation Network tarmog'ining 77 milliondan ortiq foydalanuvchilarining hisob ma'lumotlarini o'g'irlash imkonini berdi. Sony DDoS hujumi bilan juda band bo'lganligi sababli, uzoq vaqt davomida biron bir ma'lumot o'g'irlanganidan bexabar edi.

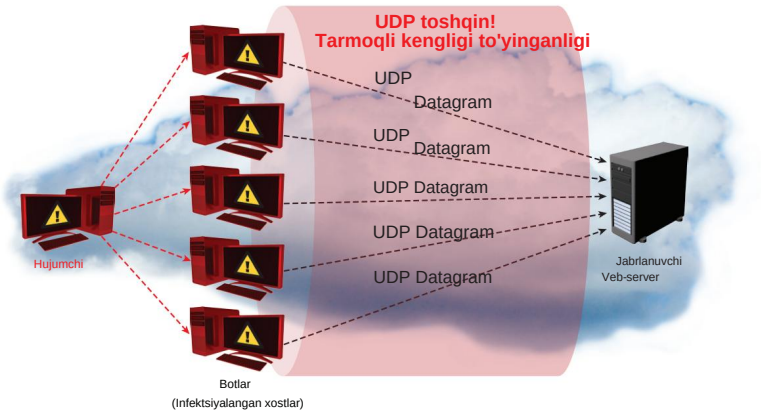
Tarmoq manbalariga qaratilgan hujumlar

Maqsadli tarmoq resurslari kompaniyaning Internet tarmog'ini to'ldirish uchun katta hajmdagi noqonuniy trafikdan foydalangan holda jabrlanuvchining barcha tarmoq o'tkazish qobiliyatini iste'mol qilishga harakat qiladi. Tarmoq toshqinlari deb ataladigan bunday hujumlar oddiy, ammo samarali. Odatiy suv toshqini hujumida jinoyat minglab ixtiyoriy yoki buzilgan kompyuterlar armiyasi o'rtasida taqsimlanadi - botnet - bu maqsadli saytga katta miqdordagi trafikni yuboradi va uning tarmog'ini bosib oladi. Bunday so'rovlar oz sonli hollarda qonuniy ko'rinishi mumkin; katta miqdorda ular sezilarli darajada zararli bo'lishi mumkin. To'fon hujumi ostida jabrlanuvchining saytiga kirishga urinayotgan qonuniy foydalanuvchi hujum qilingan saytni nihoyatda sekin yoki hatto javob bermayotganini ko'radi.

Suv toshqinlari

UDP Flood: Foydalanuvchi Datagram Protocol (UDP) ulanishsiz hisoblanadi Ikki qurilma o'rtasida seans yaratmasdan (va shuning uchun qo'l siqish jarayonini talab qilmasdan) aloqa uchun IP-paketlarga o'rnatilgan datagramlardan foydalanadigan protokol. UDP Flood hujumi ma'lum bir zaiflikdan foydalanmaydi, balki maqsadli tarmoq uchun tarmoq tiqilib qolishiga olib keladigan darajada yuqori darajada oddiy xatti-harakatlarni suiiste'mol qiladi. U potentsial soxta IP manzillardan maqsadli serverdagi tasodifiy portlarga ko'p sonli UDP datagrammalarini yuborishdan iborat; Ushbu trafikni qabul qiluvchi server har bir so'rovni qayta ishlay olmaydi va maqsadli portlarda hech qanday ilova tinglanmaganligini tasdiqlash uchun ICMP "maqsadga erishib bo'lmaydi" paketli javoblarini yuborishga urinib, uning barcha o'tkazish qobiliyatini sarflaydi.

Volumetrik hujum sifatida, UDP toshqini Mbit / s (o'tkazish qobiliyati) va PPS (sekundiga paketlar) bilan o'lchanadi.



ICMP Flood: Internet Control Message Protocol (ICMP) boshqa IP operatsiyalari, diagnostika va xatolar uchun ishlatiladigan ulanishsiz protokol. Xuddi UDP toshqinida bo'lgani kabi, ICMP toshqin (yoki Ping Flood) ham zaiflikka asoslangan hujumdir; ya'ni, xizmat ko'rsatishdan bosh tortishga erishish uchun hech qanday maxsus zaiflikka tayanmaydi. ICMP Flood har qanday turdagi ICMP xabarini o'z ichiga olishi mumkin; Maqsadli serverga yetarlicha ICMP trafik yuborilgach, u har bir so'rovni qayta ishlashga urinishdan to'lib-toshgan bo'lib, xizmat ko'rsatishni rad etish holatiga olib keladi. ICMP Flood, shuningdek, Mbit / s (o'tkazish qobiliyati) va PPS (sekundiga paketlar) bilan o'lchanadigan hajmli hujumdir.

IGMP Flood: Internet Group Management Protocol (IGMP) IP xostlar (kompyuterlar va marshrutizatorlar) tomonidan qo'shni marshrutizatorlar uchun multicast guruh a'zoliklari haqida xabar berish yoki tark etish uchun foydalaniladigan yana bir ulanishsiz protokoldir. IGMP Flood zaiflikka asoslangan emas, chunki IGMP dizayn bo'yicha multicast imkonini beradi. Bunday toshqinlar tarmoq yoki marshrutizatorga yuboriladigan ko'p sonli IGMP xabar hisobotlarini o'z ichiga oladi, bu sezilarli darajada sekinlashadi va oxir-oqibat maqsadli tarmoq bo'ylab qonuniy trafik uzatilishining oldini oladi.

Kuchaytirish hujumi - bu hujumchi hujum kuchini ko'paytirish uchun kuchaytirish omilidan foydalanishi mumkin bo'lgan har qanday hujum. Masalan, tajovuzkor marshrutizatorning IP-manzil xususiyatidan foydalanib, manba IP (qaytish manzili) maqsadli IP-ga soxtalashtirilgan bir nechta IP-manzillarga xabarlar yuborish uchun routerdan kuchaytirgich sifatida foydalanishi mumkin. Kuchaytirish hujumlarining mashhur misollariga Smurf Attacks (ICMP amplification) va Fraggle Attacks (UDP amplification) kiradi. Kuchaytirish hujumi turining yana bir misoli DNS kuchaytirilishi boÿlib, bunda tajovuzkor katta faylni keshlash uchun rekursiv DNS nom serverini oldindan buzgan boÿlsa, toÿgÿridan-toÿgÿri yoki botnet orqali ushbu rekursiv DNS serveriga soÿrov yuboradi, bu esa oÿz navbatida katta keshlangan faylni so'rab so'rov. Qaytish xabari (asl so'rovdan sezilarli darajada kengaytirilgan) keyin jabrlanuvchining (soxta) IP-manziliga yuboriladi, bu esa xizmat ko'rsatishni rad etish holatini keltirib chiqaradi.

Ulanishga yo'naltirilgan hujum - bu tajovuzkor o'zining DDoS hujumini boshlashdan oldin ulanishni o'rnatishi kerak bo'lgan hujumdir. Ushbu hujumning natijasi odatda server yoki dastur resurslariga ta'sir qiladi.
TCP yoki HTTP-ga asoslangan hujumlar ulanishga yo'naltirilgan DDoS hujumlariga misoldir.

Boshqa tomondan, **aloqasiz hujum,** tajovuzkordan jabrlanuvchi bilan to'liq aloqani ochishni talab qilmaydi va shuning uchun boshlash ancha oson. Ulanishsiz hujumning natijasi tarmoq resurslariga ta'sir qiladi, bu esa zararli paketlar serverga etib bormasdan oldin xizmat ko'rsatishni rad etishga olib keladi. UDP yoki ICMP toshqinlari ulanishsiz DDoS hujumlariga misoldir.

Hujum hujumchi o'zining hujum trafigini yuborish uchun potentsial qonuniy uchinchi shaxsdan foydalanganda, natijada o'z shaxsini yashirganida **aks** etadi.

Maqsadli server resurslariga hujumlar

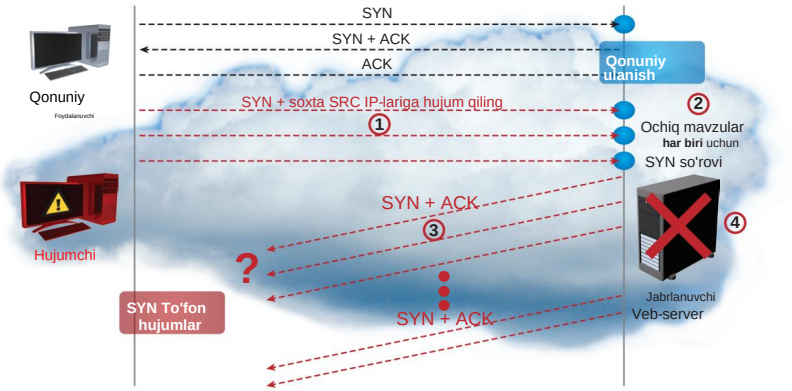
Maqsadli server resurslariga hujumlar server resurslarini tugatishga harakat qiladi qayta ishlash imkoniyatlari yoki xotira, xizmat ko'rsatishni rad etish holatiga olib kelishi mumkin. Bu g‘oya shundan iboratki, tajovuzkor maqsadli serverdagi mavjud zaiflikdan (yoki aloqa protokolidagi zaiflikdan) foydalanishi mumkin, bu maqsadli server noqonuniy so‘rovlarni ko‘rib chiqish bilan band bo‘lib qolishiga olib keladi, natijada u qonuniy so‘rovlarni boshqarish uchun resurslarga ega bo‘lmaydi. birlar. "Server" ko'pincha veb-sayt yoki veb-ilova serveriga ishora qiladi, ammo bu turdagi DDoS hujumlari xavfsizlik devori va IPS kabi statistik qurilmalarni ham nishonga olishi mumkin.

TCP/IP zaif tomonlari

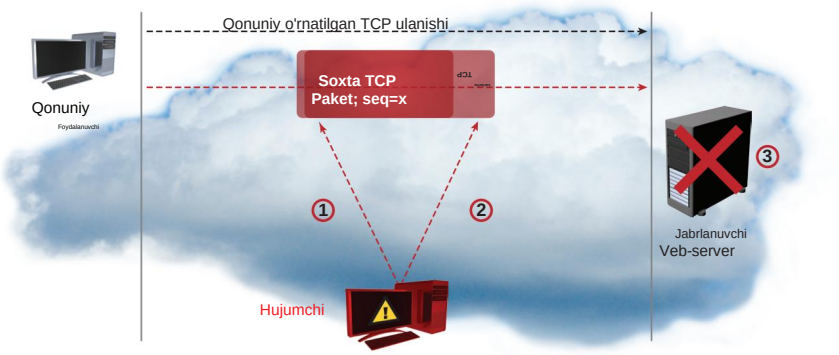
Ushbu turdagi hujumlar TCP/IP protokolini suiiste'mol qilib, uning dizayndagi ba'zi kamchiliklaridan foydalanadi. Ular odatda TCP trafigining normal mexanizmlarini buzish uchun TCP/IP protokolining SYN, ACK, RST, PSH, FIN va URG oltita boshqaruv bitidan (yoki bayroqchalaridan) noto'g'ri foydalanadilar. TCP/IP, UDP va boshqa ulanishsiz protokollardan farqli o'laroq, ulanishga asoslangan, ya'ni paket jo'natuvchisi har qanday paketlarni jo'natishdan oldin o'zining mo'ljallangan oluvchisi bilan to'liq aloqa o'rnatishi kerak. TCP/IP uch tomonlama qoʻl siqish mexanizmiga tayanadi (SYN,

SYN-ACK, ACK), bu erda har bir so'rov yarim ochiq ulanishni (SYN), javob so'rovini (SYN-ACK) va keyin javobni tasdiqlashni (ACK) yaratadi. TCP/IP protokolini suiiste'mol qilishga urinayotgan har qanday hujum ko'pincha TCP paketlarini noto'g'ri tartibda yuborishni o'z ichiga oladi va maqsadli server bunday g'ayritabiiy trafikni tushunishga harakat qilganda hisoblash resurslari tugashiga olib keladi.

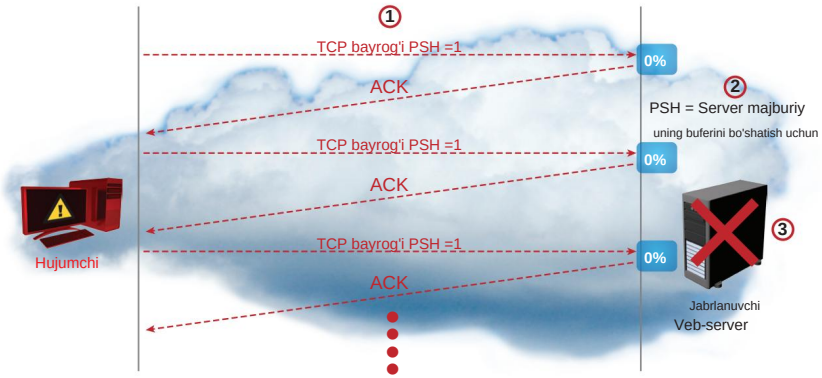
TCP SYN Flood: TCP qo'l siqish mexanizmida ulanish o'rnatilishi uchun har bir tomon o'rtasida kelishuv bo'lishi kerak. Agar TCP mijozi mavjud bo'lmasa yoki soxta IP bilan so'ramaydigan mijoz bo'lsa, bunday kelishuvni amalga oshirish mumkin emas. TCP SYN yoki oddiygina SYN toshqin hujumida, hujum qiluvchi mijozlar serverni soxta IP manzillardan kelgan TCP bayroqlari SYN ga o'rnatilgan bir qator TCP so'rovlari orqali qonuniy ulanishlarni so'rayapti, deb o'ylaydi. Ushbu SYN so'rovlarining har birini bajarish uchun maqsadli server mavzularni ochadi va ulanishga tayyorgarlik ko'rish uchun tegishli buferlarni ajratadi. Keyin u so'rovchi mijozlarga ulanish so'rovlarini tasdiqlash uchun SYN-ACK javobini yuborishga harakat qiladi, ammo mijozlarning IP manzillari soxtalashtirilganligi yoki mijozlar javob bera olmaganligi sababli, tasdiqlash (ACK paketi) hech qachon serverga qaytarilmaydi. . Server hali ham asl ulanish soÿrovlarining har biri uchun ochiq oqimlari va buferlarini saqlab qolishga majbur boÿlib, soÿrovni kutish vaqtiga murojaat qilishdan oldin oÿzining SYN-ACK soÿrovini tasdiqlash paketlarini bir necha marta qayta yuborishga harakat qiladi. Server resurslari cheklanganligi va SYN to'lqini ko'pincha ulanish so'rovlarining ko'p sonini o'z ichiga olganligi sababli, server yangi so'rovlar kelishidan oldin ochiq so'rovlarini vaqtni to'xtata olmaydi va bu xizmat ko'rsatishni rad etish holatini keltirib chiqaradi.



TCP RST hujumi: TCP RST bayrog'i serverni xabardor qilish uchun mo'ljallangan u darhol tegishli TCP ulanishini tiklashi kerak. TCP RST hujumida tajovuzkor joriy tartib raqamini taxmin qilish va mijozning IP-manbasidan foydalanish uchun TCP RST paketini aldash orqali ikki ob'ekt o'rtasidagi faol TCP ulanishiga xalaqit beradi (keyin u serverga yuboriladi). Botnet odatda minglab bunday paketlarni serverga turli xil tartib raqamlari bilan yuborish uchun ishlatiladi, bu esa to'g'risini topishni osonlashtiradi. Bu sodir bo'lgach, server tajovuzkor tomonidan yuborilgan RST paketini tan oladi va uning soxta IP manzilida joylashgan mijoz bilan aloqasini to'xtatadi.



TCP PSH+ACK Flood: TCP jo'natuvchisi o'zi bilan paket yuborganda PUSH bayrog'i 1 ga o'rnatiladi, natijada TCP ma'lumotlari darhol TCP qabul qilgichga yuboriladi yoki "itariladi". Bu amal aslida qabul qiluvchi serverni TCP stek buferini bo'shatishga va bu amal tugallangandan so'ng tasdiqlash xabarini yuborishga majbur qiladi. Odatda botnetdan foydalanadigan tajovuzkor maqsadli serverni ko'plab bunday so'rovlar bilan to'ldirishi mumkin. Bu maqsadli serverdagi TCP stek buferini to'ldiradi, bu esa so'rovlarni qayta ishlay olmaydi yoki hatto ularni tan olmaydi (natijada xizmat ko'rsatishni rad etish holatiga olib keladi).

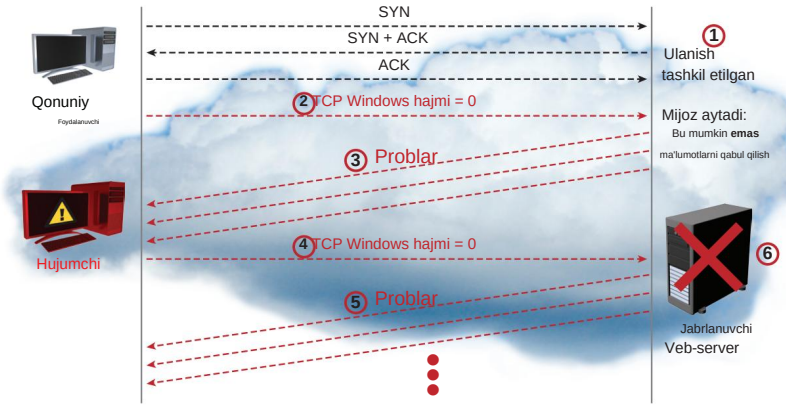


"Past va sekin" hujumlar

To'fondan farqli o'laroq, "past va sekin" hujumlar katta miqdordagi trafikni talab qilmaydi. Ular nisbatan kam miqdordagi zararli trafikka ega bo'lgan maqsadli serverdagi muayyan dizayn kamchiliklari yoki zaifliklarini nishonga oladi va oxir-oqibat uning ishdan chiqishiga olib keladi. "Past va sekin" hujumlar asosan dastur resurslarini (va ba'zan server resurslarini) maqsad qilib qo'yadi va ularni aniqlash juda qiyin, chunki ular odatdagi tezlikda sodir bo'ladigan ulanishlar va ma'lumotlarni uzatishni o'z ichiga oladi.

Sockstress: Sockstress zaifliklardan foydalanadigan hujum vositasidir TCP stekida tajovuzkorga maqsadli server uchun xizmat ko'rsatishni rad etish shartini yaratishga imkon beradi. Oddiy TCP uch tomonlama qo'l siqishida mijoz serverga SYN paketini yuboradi, server SYN-ACK paketi bilan javob beradi va mijoz SYN-ACK ga ACK bilan javob berib, ulanishni o'rnatadi. Sockstress-dan foydalanadigan tajovuzkorlar maqsadli server bilan oddiy TCP ulanishini o'rnatadilar, lekin ular oxirgi ACK ichidagi serverga "oyna o'lchami 0" paketini yuboradilar va unga TCP oynasining o'lchamini 0 baytga o'rnatishni buyuradilar. TCP oynasi qabul qilingan ma'lumotlarni dastur qatlamiga yuklashdan oldin saqlaydigan buferdir. Oyna hajmi maydoni har bir vaqt oralig'ida buferda qancha ko'proq joy borligini ko'rsatadi. Oyna o'lchami nolga o'rnatilgan bo'lsa, boshqa bo'sh joy yo'qligini va boshqa tomon keyingi ogohlantirishgacha ko'proq ma'lumot yuborishni to'xtatishi kerakligini anglatadi. Bunday holda, server yangi ma'lumotni qachon qabul qila olishini ko'rish uchun doimiy ravishda mijozga oyna o'lchamini tekshirish paketlarini yuboradi, ammo tajovuzkor oyna o'lchamini o'zgartirmaganligi sababli ulanish cheksiz ochiq qoladi.

Ushbu turdagi ko'plab ulanishlarni serverga ochib, tajovuzkor serverning TCP ulanish jadvalidagi (shuningdek, boshqa jadvallar) barcha bo'sh joyni egallab, qonuniy foydalanuvchilarning ulanishni o'rnatishiga to'sqinlik qiladi. Shu bilan bir qatorda, tajovuzkor juda kichik (taxminan 4 bayt) oyna o'lchamiga ega bo'lgan ko'plab ulanishlarni ochishi mumkin, bu esa serverni ma'lumotni katta miqdordagi 4 baytlik kichik qismlarga ajratishga majbur qiladi. Ushbu turdagi ko'plab ulanishlar serverning mavjud xotirasini iste'mol qiladi va xizmat ko'rsatishni rad etishga olib keladi.



SSL-ga asoslangan hujumlar

Turli xil tarmoq aloqa protokollari tomonidan qo'llaniladigan shifrlash usuli Secure Socket Layer (SSL) ko'tarilishi bilan tajovuzkorlar uni nishonga olishni boshladilar. SSL kontseptual jihatdan TCP/IP dan yuqori ishlaydi va aloqalarini shifrlash va muloqot qiluvchi tomonlarni autentifikatsiya qilish orqali boshqa protokollar orqali muloqot qiladigan foydalanuvchilarga xavfsizlikni ta'minlaydi. SSL-ga asoslangan DoS hujumlari ko'p shakllarni oladi: SSL qo'l siqish mexanizmini nishonga olish, axlat ma'lumotlarini SSL serveriga yuborish yoki SSL shifrlash kalitini muhokama qilish jarayoni bilan bog'liq ba'zi funktsiyalarni suiiste'mol qilish. SSL-ga asoslangan hujumlar shunchaki DoS hujumi SSL-shifrlangan trafik orqali boshlanganligini anglatishi mumkin, bu esa uni aniqlashni juda qiyinlashtiradi; bunday hujumlar ko'pincha "assimetrik" deb hisoblanadi, chunki SSL-ga asoslangan hujum bilan kurashish uchun uni ishga tushirishdan ko'ra ko'proq server resurslari kerak bo'ladi.

Shifrlangan HTTP hujumlari (HTTPS toshqinlari): Ko'pgina onlayn korxonalar o'zlarining trafigini shifrlash va ma'lumotlarning uchdan uchiga o'tishini xavfsiz qilish uchun o'z ilovalarida SSL/TLS (Transport Layer Security) dan tobora ko'proq foydalanmoqda. Shifrlangan trafikka DoS hujumlari ortib bormoqda va ularni yumshatish kutilgandek aniq emas. Aksariyat DoS yumshatish texnologiyalari SSL-trafikni tekshirmaydi, chunki u shifrlangan trafikni shifrlashni talab qiladi. HTTPS Floods - shifrlangan HTTP trafigining toshqinlari (HTTP Floods quyida tushuntiriladi) - endi tez-tez ko'p zaifliklarga qarshi hujum kampaniyalarida qatnashmoqda.
"Oddiy" HTTP Floods ta'siridan tashqari, shifrlangan HTTP hujumlari shifrlash va shifrni ochish mexanizmlari yuki kabi bir qator boshqa muammolarni ham qo'shadi.

THC-SSL-DOS: Ushbu vosita deb nomlangan xakerlik guruhi tomonidan ishlab chiqilgan Hacker's Choice (THC) sotuvchilarni SSL zaifliklarini tuzatishga undash uchun kontseptsiyaning isboti sifatida. THC-SSL-DOS, boshqa "past va sekin" hujumlarda bo'lgani kabi, hatto juda katta server uchun ham xizmat ko'rsatishni rad etish uchun oz sonli paketlarni talab qiladi. U muntazam SSL qo'l siqishini boshlash orqali ishlaydi va keyin shifrlash kalitini qayta ko'rib chiqishni darhol so'raydi va barcha server resurslari tugaguniga qadar ushbu qayta muzokara so'rovini doimiy ravishda takrorlaydi. Hujumchilar SSL-dan foydalanadigan hujumlarni boshlashni yaxshi ko'radilar, chunki har bir SSL sessiyasi mijoz tomoniga qaraganda server tomonidan o'n besh baravar ko'proq resurslarni sarflaydi. Darhaqiqat, bitta standart uy kompyuteri butun SSL-ga asoslangan veb-serverni o'chirib tashlashi mumkin va bir nechta kompyuterlar katta himoyalangan onlayn xizmatlarning to'liq fermasini o'chirib tashlashi mumkin.

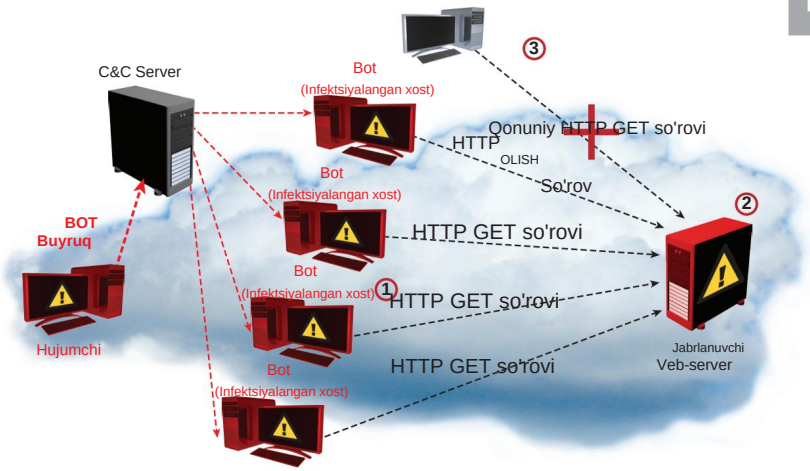
Maqsadli dastur manbalariga hujumlar

Ilova resurslarini maqsad qilib olgan DoS hujumlari hollari so'nggi paytlarda o'sib bormoqda va bugungi kunda tajovuzkorlar tomonidan keng qo'llanilmoqda. Ular nafaqat taniqli gipermatnni uzatish protokoli (HTTP), balki HTTPS, DNS, SMTP, FTP, VOIP va DoS hujumlarini amalga oshirishga imkon beruvchi zaif tomonlarga ega bo'lgan boshqa dastur protokollariga ham mo'ljallangan. Tarmoq resurslarini nishonga olgan hujumlar kabi, dastur resurslariga mo'ljallangan turli xil hujumlar ham mavjud, jumladan, suv toshqini va "past va sekin" hujumlar. Ikkinchisi ayniqsa mashhur bo'lib, asosan HTTP protokolidagi zaif tomonlarga qaratilgan. HTTP Internetdagi eng keng tarqalgan dastur protokoli sifatida tajovuzkorlar uchun jozibador maqsaddir.

HTTP toshqin

HTTP toshqin - bu eng keng tarqalgan dastur-resurs-maqsadli DDoS hujumi. U qurbonning veb-serveriga yuborilgan HTTP GET yoki POST so'rovlarining qonuniy, seansga asoslangan to'plamlaridan iborat bo'lib, ularni aniqlash qiyin. HTTP toshqin hujumlari odatda bir vaqtning o'zida bir nechta kompyuterlardan (ixtiyoriy mashinalar yoki botlar) ishga tushiriladi, ular doimiy va qayta-qayta maqsadli sayt sahifalarini yuklab olishni so'raydi (HTTP GET flood), dastur resurslarini tugatadi va xizmat ko'rsatishni rad etish holatiga olib keladi.

High Orbit Ion Cannon (HOIC) kabi zamonaviy DDoS hujum vositalari ko'p tarmoqli HTTP toshqin hujumlarini amalga oshirish uchun qulay vositalarni taklif qiladi.



DNS Flood

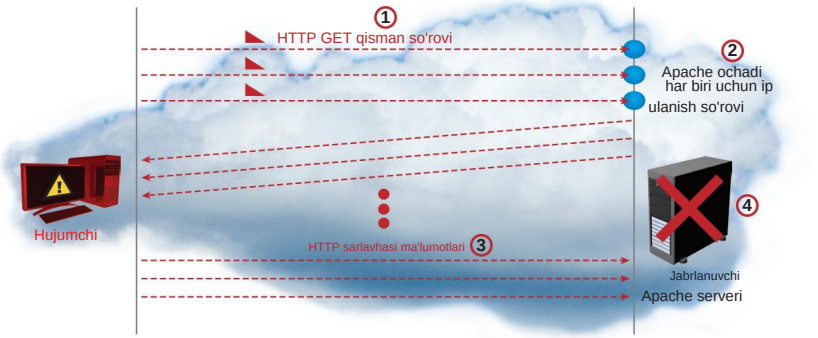
DNS to'lqinini ishga tushirish oson, ammo aniqlash qiyin. Boshqa suv toshqini hujumlari bilan bir xil g'oyaga asoslanib, DNS to'lqini katta hajmdagi DNS so'rovlarini yuborish orqali DNS ilovasi protokolini maqsad qilib qo'yadi. Domen nomlari tizimi (DNS) - domen nomlarini IP manzillarga ajratish uchun foydalaniladigan protokol; uning asosiy protokoli UDP bo'lib, tezkor so'rov va javob vaqtlaridan ulanishlarni o'rnatishga majbur bo'lmasdan (TCP talab qilganidek) foydalanadi. DNS toshqinida tajovuzkor bir nechta DNS so'rovlarini qurbonning DNS serveriga to'g'ridan-to'g'ri yoki botnet orqali yuboradi. DNS server ishlamay qolgan va uning barcha kiruvchi so'rovlarini qayta ishlay olmay, oxir-oqibat ishdan chiqadi.

"Past va sekin" hujumlar

Ushbu bo'limda "past va sekin" hujumlarning xarakteristikalari tegishli ayniqsa, dastur resurslariga (oldingi "past va sekin" hujumlar server resurslariga qaratilgan bo'lsa). Ushbu "past va sekin" hujumlar maxsus dastur zaifliklariga qaratilgan bo'lib, tajovuzkorga yashirincha xizmat ko'rsatishdan bosh tortishga olib keladi. Tabiatan volumetrik emas, bunday hujumlar ko'pincha faqat bitta mashina bilan amalga oshirilishi mumkin; qo'shimcha ravishda, bu hujumlar dastur qatlamida sodir bo'lganligi sababli, TCP qo'l siqish allaqachon o'rnatilgan bo'lib, zararli trafikni qonuniy ulanish orqali harakatlanadigan oddiy trafikka o'xshatadi.

Sekin HTTP GET so'rovi: sekin HTTP GET so'rovi ortidagi g'oya ko'plab ochiq ulanishlardan foydalanish orqali ilova resurslarining barchasida yoki ko'p qismida hukmronlik qilish, uning qonuniy ulanishlarni ochmoqchi bo'lgan foydalanuvchilarga xizmat ko'rsatishiga to'sqinlik qilishdir. Ushbu hujumda tajovuzkor to'liq bo'lmagan HTTP GET so'rovlarini yaratadi va yuboradi

server, bu ulanish so'rovlarining har biri uchun alohida mavzu ochadi va qolgan ma'lumotlar yuborilishini kutadi. Buzg'unchi HTTP sarlavhasi ma'lumotlarini ulanish ochiq qolishi va vaqt tugamasligiga ishonch hosil qilish uchun (sekin) belgilangan vaqt oralig'ida yuborishni davom ettiradi. Kerakli ma'lumotlarning qolgan qismi juda sekin kelganligi sababli, server doimiy ravishda kutib turadi va ulanish jadvalidagi cheklangan joyni tugatadi va shu bilan xizmat ko'rsatishni rad etish holatini keltirib chiqaradi.



Sekin HTTP POST so'rovi: sekin HTTP POST so'rovi hujumini amalga oshirish uchun tajovuzkor maqsadli veb-saytdagi shakllarni aniqlaydi va HTTP POST so'rovlarini ushbu shakllar orqali veb-serverga yuboradi.
POST so'rovlari odatdagidek yuborilmaydi, bayt-bayt yuboriladi. Sekin HTTP GET so'rovida bo'lgani kabi, tajovuzkor har bir yangi bayt POST ma'lumotlarini muntazam ravishda muntazam ravishda sekin yuborish orqali o'zining zararli aloqasi ochiq bo'lishini ta'minlaydi. HTTP POST so'rovining mazmuni uzunligidan xabardor bo'lgan server to'liq POST so'rovi qabul qilinishini kutishdan boshqa tanlovga ega emas (bu xatti-harakat Internetga ulanishi sekin bo'lgan qonuniy foydalanuvchilarga taqlid qiladi). Buzg'unchi bu xatti-harakatni parallel ravishda ko'p marta takrorlaydi, hech qachon ochiq ulanishni yopmaydi va bir necha yuzlab ochiq ulanishlardan so'ng maqsadli server yangi so'rovlarni bajara olmaydi, shuning uchun xizmat ko'rsatishni rad etish holatiga erishadi.

Muntazam Expression DoS hujumlari: "past va sekin" hujumlarning alohida holati RegEx DoS (yoki ReDos) hujumlaridir. Ushbu stsenariyda tajovuzkor serverda o'rnatilgan kutubxona, bu holda oddiy ifodali dasturiy ta'minot kutubxonasidagi zaiflikdan foydalanadigan maxsus tayyorlangan xabarni (ba'zan yomon RegExes deb ataladi) yuboradi. Bu foydalanuvchi tomonidan kiritilgan ma'lumotlar bo'yicha muntazam ifodani hisoblash yoki tajovuzkor tomonidan buyurilgan murakkab va resurs talab qiladigan muntazam ifodani qayta ishlashni amalga oshirishda serverning katta hajmdagi resurslarni iste'mol qilishiga olib keladi.

Xesh to'qnashuvlari DoS hujumlari: Bunday hujumlar umumiy maqsadlarga qaratilgan veb-ilovalar ramkalaridagi xavfsizlik zaifliklari. Muxtasar qilib aytganda, ko'pchilik dastur serverlari POST sessiyasi parametrlarini indekslash uchun xesh jadvallarini yaratadi va ba'zida shunga o'xshash xesh qiymatlari qaytarilganda xesh to'qnashuvlarini boshqarish talab qilinadi. To'qnashuv o'lchamlari resurslarni talab qiladi, chunki ular so'rovlarni qayta ishlash uchun qo'shimcha CPU miqdorini talab qiladi. Hash Collision DoS hujumi stsenariysida tajovuzkor ko'plab parametrlarga ega maxsus tayyorlangan POST xabarini yuboradi. Parametrlar server tomonida xesh to'qnashuviga olib keladigan tarzda qurilgan va javobni qayta ishlashni keskin sekinlashtiradi. Hash Collisions DoS hujumlari juda samarali va bitta tajovuzkor kompyuterdan ishga tushirilishi mumkin, bu esa dastur serverining resurslarini asta-sekinlik bilan tugatadi.

7 Hujum vositalari

Oldingi boblarda DDoS hujumlarining har xil turlari muhokama qilingan tarmoq va amaliy qatlamlarda sodir bo'ladi. Ushbu hujumlarning ko'pini qo'lda amalga oshirish mumkin bo'lsa-da, hujumlarni osonroq va samarali bajarish uchun maxsus hujum vositalari ishlab chiqilgan. Birinchi DDoS vositalari - misollar Trinoo va Stacheldraht - asr boshlarida keng qo'llanilgan, ammo biroz murakkab va faqat Linux va Solaris operatsion tizimlarida ishlagan.

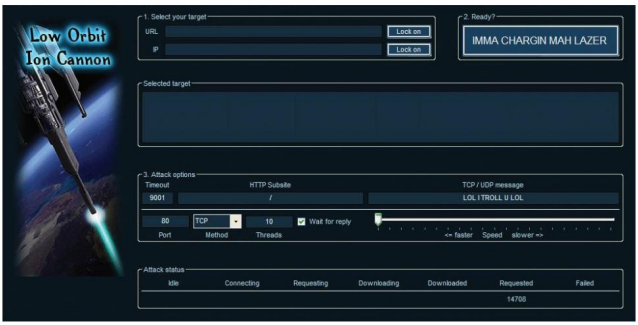
So'nggi yillarda DDoS vositalaridan foydalanish ancha sodda va o'zaro faoliyat platformaga aylandi, bu DDoS hujumlarini tajovuzkorlar uchun osonroq va nishonlar uchun xavfliroq qiladi.
Ushbu yangi DDoS vositalarining ba'zilari, masalan, Low Orbit Ion Cannon (LOIC) dastlab tarmoq stressini tekshirish vositalari sifatida ishlab chiqilgan va keyinchalik o'zgartirilgan va zararli maqsadlarda ishlatilgan, Slowloris kabi boshqalar esa "kulrang shapkali" xakerlar tomonidan ishlab chiqilgan. keng miqyosli hujumlarning oldini olish uchun zaif dasturiy ta'minotni ishlab chiqaruvchilar uni tuzatishga majbur bo'lishlari uchun bunday vositalarni ommaviy ravishda chiqarish orqali jamoatchilik e'tiborini dasturiy ta'minotning muayyan zaifligiga qaratish. Bundan tashqari, tarmoq xavfsizligi va xakerlik dunyosi doimo rivojlanib borayotgani kabi, DDoS hujumlarini amalga oshirish uchun ishlatiladigan hujum vositalari ham shunday. Yangi hujum vositalari hajmi kichikroq, xizmat ko'rsatishdan bosh tortish holatini keltirib chiqarishda samaraliroq va yashirin bo'lib bormoqda.

Past orbitali ionli to'p (LOIC)

“Hacktivist” guruhi Anonymous tanlagan asl vositasi – Low Orbit Ion Cannon (LOIC) – oddiy suv toshqini vositasi bo‘lib, serverni og‘ir tarmoq yukiga duchor qilish uchun katta hajmdagi TCP, UDP yoki HTTP trafigini yaratishga qodir. LOIC-ning asl ishlab chiquvchilari Praetox Technologies ushbu vositani sinov maqsadida o'z serverlarini shunday og'ir tarmoq trafigiga duchor qilmoqchi bo'lgan ishlab chiquvchilar tomonidan qo'llanilishini maqsad qilgan bo'lsa-da, Anonymous ochiq manbali vositani oldi va muvofiqlashtirilgan DDoSni ishga tushirish uchun foydalanishni boshladi. hujumlar.

Ko'p o'tmay, LOIC o'zgartirildi va unga "Hivemind" xususiyati berildi, bu har qanday LOIC foydalanuvchisiga o'z LOIC nusxasini IRC serveriga yo'naltirish va uni boshqarishni asosiy foydalanuvchiga o'tkazish imkonini berdi.

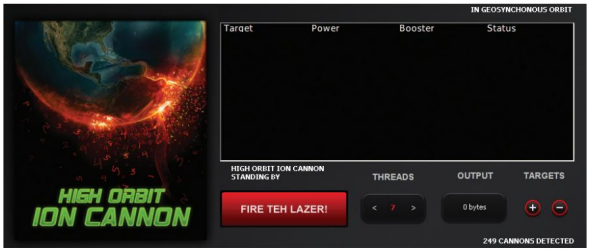
keyin har bir ulangan LOIC mijoziga bir vaqtning o'zida IRC orqali buyruqlar yuborishi mumkin. Ushbu konfiguratsiyada foydalanuvchilar bir vaqtning o'zida ishlamaydigan kamroq muvofiqlashtirilgan LOIC foydalanuvchilari guruhiga qaraganda ancha samarali DDoS hujumlarini boshlashlari mumkin. Biroq, 2011 yil oxirida Anonymous DDoS tanlagan vositasi sifatida LOIC-dan uzoqlasha boshladi, chunki LOIC o'z foydalanuvchilarining IP manzillarini yashirish uchun hech qanday harakat qilmaydi. Anonimlikning yo'qligi butun dunyo bo'ylab turli foydalanuvchilarning LOIC hujumlarida qatnashgani uchun hibsga olinishiga olib keldi va Anonymous o'zining barcha IRC kanallari bo'ylab aniq xabarni tarqatdi: "LOIC dan foydalanmang".



Yuqori orbitali ionli to'p (HOIC)

Anonim "rasmiy ravishda" LOICni tanlagan vosita sifatida tashlab qo'yganidan so'ng, LOICning "vorisi", "Yuqori orbitali ion to'pi (HOIC)" Amerika Qo'shma Shtatlari Adliya Departamentini qabul qilish qaroriga javoban nishonga olishda tezda diqqat markazida bo'ldi. Megaupload.com-ni pastga tushiring.
HOIC ayni paytda oddiy dastur bo'lsa-da - HTTP POST va GET so'rovlarini yuborish uchun o'zaro platformalar skripti - foydalanish uchun qulay grafik interfeysga o'ralgan - uning samaradorligi qo'shimcha "booster" skriptlari yoki qo'shimcha matndan kelib chiqadi. qo'shimcha asosiy kodni o'z ichiga olgan fayllar, foydalanuvchi hujumni boshlaganida asosiy dastur tomonidan izohlanadi.

HOIC to'g'ridan-to'g'ri anonimlik usullarini qo'llamasa ham, kuchaytiruvchi skriptlardan foydalanish foydalanuvchiga maqsadli URL-manzillar ro'yxatini va HOIC uchun identifikatsiya ma'lumotlarini belgilash imkonini beradi, chunki u o'z hujum trafigini hosil qiladi, bu esa HOIC hujumlarini bloklashni biroz qiyinlashtiradi. HOIC butun dunyoda Anonymous tomonidan DDoS hujumlarini boshlash uchun foydalanishda davom etmoqda, garchi Anonim hujumlar HOIC ishtirokidagi hujumlar bilan cheklanmaydi.



hping

LOIC va HOIC, Anonymous va boshqa xakerlik guruhlariga qo'shimcha ravishda va shaxslar DDoS hujumlarini boshlash uchun turli xil vositalardan foydalanganlar, ayniqsa Ion Cannons'ning anonimligi yo'qligi sababli. Bunday vositalardan biri, hping, ping yordam dasturiga o'xshash juda oddiy buyruq qatori yordam dasturidir; ammo, u pingdan an'anaviy foydalanish bo'lgan oddiy ICMP echo so'rovini yuborishdan ko'ra ko'proq funksionallikka ega. hping manba IP-manzilini aldashda nishonga katta hajmdagi TCP trafigini yuborish uchun ishlatilishi mumkin, bu esa uni tasodifiy yoki hatto ma'lum bir foydalanuvchi tomonidan belgilangan manbadan kelib chiqadigan qilib ko'rsatishi mumkin. Kuchli, yaxshi yumaloq vosita (ba'zi bir aldash imkoniyatlariga ega) sifatida hping Anonymous tanlagan vositalar ro'yxatida qoladi.

Slowloris

To'g'ridan-to'g'ri qo'pol kuch hujumlaridan tashqari, ko'plab murakkab "past va sekin" hujum turlari foydalanish uchun qulay vositalarga o'ralgan bo'lib, ularni aniqlash ancha qiyin bo'lgan xizmat ko'rsatishni rad etish hujumlarini amalga oshiradi. Slowloris, kulrang shapkali xaker tomonidan ishlab chiqilgan va "RSnake" dastagidan foydalanadigan vosita juda sekin HTTP so'rovidan foydalangan holda server uchun xizmat ko'rsatishni rad etish holatini yaratishga qodir. HTTP sarlavhalarini maqsadli saytga imkon qadar sekin kichik bo'laklarga yuborish orqali (server so'rovni kutish vaqti tugaguniga qadar keyingi kichik bo'lakni yuborishni kutish), server sarlavhalar kelishini kutishda davom etishga majbur bo'ladi. Agar shu tarzda serverga yetarlicha ulanishlar ochilsa, u tezda qonuniy so'rovlarni bajara olmaydi.

RU hali o'lganmi? (RUDY)

Slowloris-ga o'xshash yana bir sekin tezlikda xizmat ko'rsatishni rad etish vositasi - RU Dead Ha? (RUDY). "Bodom bolalari" albomining nomi "Siz hali o'lganmisiz?" RUDY, Slowloris singari HTTP sarlavhalari o'rniga HTTP POST uzun shakl maydonidan foydalanish orqali xizmatni rad etishga erishadi. POST ilovasiga bir bayt ma'lumot kiritish orqali

maydonni bir vaqtning o'zida kiritib, keyin kutib turganda, RUDY ishlov berishni amalga oshirish uchun dastur mavzularini tugamaydigan postlar tugashini kutishiga olib keladi (bu xatti-harakat veb-serverlarga sekinroq ulanishga ega foydalanuvchilarni qo'llab-quvvatlashga ruxsat berish uchun kerak). RUDY HTTP POST so'rovining qolgan qismini kutish vaqtida maqsadli veb-serverni osib qo'yishiga sabab bo'lganligi sababli, foydalanuvchi RUDY bilan serverga bir vaqtning o'zida ko'plab ulanishlarni yaratishi mumkin, natijada serverning ulanish jadvalini tugatadi va xizmat ko'rsatishni rad etish holatini keltirib chiqaradi.

#Ref

Yuqorida aytib o'tilgan barcha vositalar zaiflikka asoslangan bo'lsa-da, Anonymous arsenalidagi yana bir vosita #RefRef keng tarqalgan bo'lib foydalaniladigan SQL ma'lumotlar bazasi dasturiy ta'minotidagi zaiflikka asoslangan bo'lib, u in'ektsiya hujumiga imkon beradi. SQL in'ektsiyasidan foydalangan holda #RefRef tajovuzkorga maqsadli serverni maxsus SQL funktsiyasidan foydalanishga majburlash orqali xizmat ko'rsatishni rad etish holatini keltirib chiqarishga imkon beradi (bu har qanday boshqa SQL ifodasini takroran bajarishga imkon beradi). Bir necha qator kodlarning doimiy bajarilishi maqsadli serverlarning resurslarini sarflaydi, natijada xizmat ko'rsatish rad etiladi. LOIC yoki HOIC dan farqli o'laroq, #RefRef serverni hujum vektorining tabiati tufayli o'chirish uchun juda ko'p sonli mashinalarni talab qilmaydi. Agar serverning server qismi SQL-dan foydalansa va zaif bo'lsa, sezilarli uzilishga olib kelishi uchun faqat bir nechta mashina kerak bo'ladi. Asbobni ishlab chiqishda Anonymous uni turli saytlarda sinab ko'rdi, bu osonlik bilan bir necha daqiqada uzilishlarga olib keldi va #RefRef bilan ishlaydigan bitta mashina uchun atigi 10-20 soniyani talab qildi. Shunday hujumlardan birida (Pastebin-da) bitta mashinadan 17 soniyalik hujum saytni 42 daqiqa davomida oflayn rejimga o'tkazishga muvaffaq bo'ldi.

Botnet DDoS vositasi sifatida

Qanday bo'lishidan qat'iy nazar, ishlatiladigan hujum vositasi, ammo, ishga tushirish qobiliyati bir nechta kompyuterlardan hujum - yuzlab, minglab yoki millionlab bo'ladimi - xizmat ko'rsatishni rad etishga olib keladigan hujumning potentsialini sezilarli darajada oshiradi. Hujumchilarning ixtiyorida ko'pincha "botnetlar" mavjud - tajovuzkorga ularni boshqarishga imkon beruvchi zararli dasturlar bilan zararlangan, ko'pincha "zombi" deb ataladigan buzilgan kompyuterlarning katta to'plamlari. Botnet egalari yoki "cho'ponlar" o'zlarining botnetlaridagi mashinalarni IRC (Internet Relay Chat) kabi yashirin kanallar orqali boshqarishlari va tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumlari kabi zararli harakatlarni amalga oshirish uchun buyruqlar berishlari mumkin. , spam-xatlarni yuborish va ma'lumotlarni o'g'irlash.

2006 yil holatiga ko'ra, butun dunyo bo'ylab o'rtacha botnetning o'rtacha hajmi taxminan 20 000 ta mashinadan iborat edi (botnet egalari aniqlanmaslik uchun o'z tarmoqlarini kichraytirishga harakat qilishgan), ammo BredoLab, Conficker, TDL-4 va Zevs kabi yirikroq botnetlarda millionlab mashinalar borligi taxmin qilingan. Katta botnetlarni ko'pincha ulardan foydalanish uchun kuniga kamida 100 dollar to'lashga tayyor bo'lgan har bir kishi ijaraga olishi mumkin (aniq bir onlayn forum reklamasi kuniga 200 dollarga 80 000-120 000 virusli xostlarni o'z ichiga olgan botnetdan foydalanishni taklif qiladi), deyarli har kimga faqat botnetga ega bo'lish imkonini beradi. o'rtacha texnik bilim va halokatli hujumni boshlash uchun to'g'ri vositalar. Shuni yodda tutgan holda, barcha so'nggi hujum vositalaridan xabardor bo'lish, barcha serverlar va boshqa tarmoq qurilmalarida so'nggi dasturiy ta'minotni saqlab turish va hujumlar davom etayotganda ularni himoya qilish uchun DDoS-ni yumshatishning qandaydir ichki yechimlaridan foydalanish muhimdir. rivojlanish uchun.

8 Tashkilotingizni DDoS hujumlaridan himoya qilish

DoS va DDoS hujumlari bir necha yillardan beri mavjud bo'lsa ham, ko'plab tashkilotlar bunday tahdidlarning potentsial ta'sirini e'tiborsiz qoldirishda davom etmoqda. Anonymous kabi guruhlar tomonidan DDoS hujumlari ko'rinishidagi xaktivizmning kuchayishi korporatsiyalar nazarida DDoS hujumlariga ko'proq e'tibor qaratdi. DoS tahdidlari nodavlat notijorat tashkilotlari e'tiborini jalb qilishga muvaffaq bo'lgan bo'lsa ham, ko'plab tashkilotlar hali ham DoSga qarshi strategiyalarini aniqlamagan. Yaqinda Neustar tadqiqot firmasi tomonidan o'tkazilgan so'rovda, so'ralgan tashkilotlarning atigi 3 foizida maxsus anti-DoS yechimi borligi aniqlandi.10 Tashkilotlarning aksariyati xavfsizlik devori va IPS (hatto hattoki) kabi mavjud tarmoq xavfsizligi mahsulotlariga umid qilmoqda. kalitlari va marshrutizatorlari) DoS hujumlarini bloklaydi. Bu xavfli fikrlashdir.

Nima uchun xavfsizlik devoringiz DDoS hujumlarini bloklay olmaydi

2012-yil boshida Radware kompaniyasining ERT yillik xavfsizlik hisoboti11 2011-yil davomida jamoa tomonidan amalga oshirilgan oʻynlab DoS va DDoS hujumlari asosida oʻzining yillik xavfsizlik hisobotini eʻlon qildi. ERT ushbu DoS hujumlari paytida qaysi tarmoq qurilmalari toʻsiq boʻlganini tekshirdi va 32% hollarda buni aniqladi. maqsadli tashkilotning xavfsizlik devori va IPS qurilmalari asosiy to'siqlar edi. Bu raqam qanchalik baland bo'lsa ham, DoS va DDoS hujumlarining mohiyatini va xavfsizlik devorlari qanday yaratilganligini tushunadigan xavfsizlik mutaxassislarini ajablantirmaslik kerak.

Faervollar holatni ko'rsatadigan qurilmalar bo'lib, ular holatni kuzatib boradi ular tekshiradigan barcha tarmoq ulanishlari. Bunday barcha ulanishlar ulanish jadvalida saqlanadi va har bir paket o'rnatilgan qonuniy ulanish orqali uzatilayotganligini tekshirish uchun ushbu ulanish jadvaliga moslashtiriladi. Standart korporativ toifadagi xavfsizlik devorining ulanish jadvali o'n minglab faol ulanishlarni saqlashi mumkin va bu oddiy tarmoq faoliyati uchun etarli.

Biroq, DDoS hujumi paytida tajovuzkor maqsad tarmog'iga soniyasiga minglab paketlarni yuboradi.

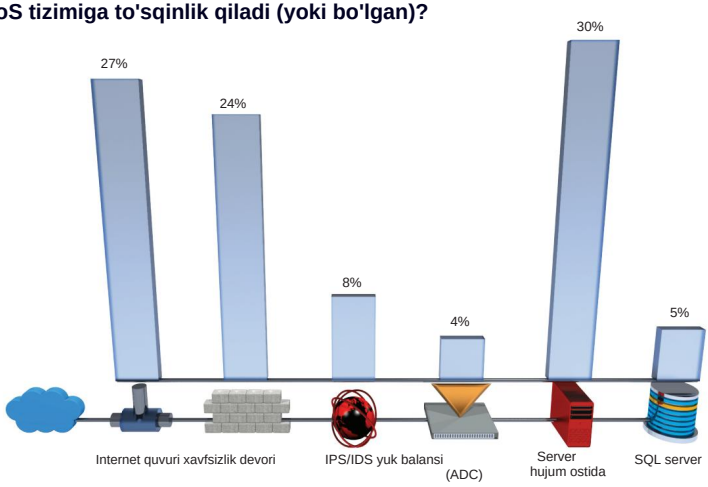
Xavfsizlik devorini bunday katta hajmdagi trafikdan himoya qilish uchun maxsus anti-DoS qurilmasi bo'lmasa, xavfsizlik devorining o'zi odatda birinchi bo'lib qoladi.

10 Neustar Insight - 2012 yil 1 chorak DDoS tadqiqoti

11 Radware 2011 Global jo'nalish va tendentsiya xavfsizligi hisoboti

DDoS hujumining kuchini boshqarish uchun tashkilot tarmog'idagi qurilma. Xavfsizlik devori yaratilganligi sababli, u har bir zararli paket uchun ulanish jadvalida yangi ulanishni ochadi, bu esa ulanish jadvalining juda qisqa vaqt ichida tugashiga olib keladi. Xavfsizlik devorining ulanish jadvali maksimal quvvatiga yetgandan so'ng, u qo'shimcha ulanishlarni ochishga ruxsat bermaydi, natijada qonuniy foydalanuvchilarning ulanishlarni o'rnatishiga to'sqinlik qiladi va keyinchalik bunday foydalanuvchilarning maqsadli tarmoq serveri yoki serverlari tomonidan joylashtirilgan onlayn xizmatlarga kirishiga to'sqinlik qiladi. Juda g'alati emas - bu stsenariyda - xavfsizlik devori mavjudligiga qaramay, shartni rad etishga erishildi.

Radware xavfsizligi so'rovi: Qaysi xizmatlar yoki tarmoq elementlari DoS tizimiga to'sqinlik qiladi (yoki bo'lgan)?



DDoS hujumlarini yumshatishdagi qiyinchiliklar

DDoS hujumlarini aniqlash va yumshatishning bir qancha sabablari bor. Hujumning ko‘p ehtimoliy stsenariylarida har bir alohida “zararli” paket o‘z-o‘zidan qonuniy tranzaksiya bo‘lib, onlayn xizmat yoki tashkilotning tarmoq infratuzilmasiga zarar yetkazadigan narsa emas. Veb-sahifani so'rash kabi qonuniy tranzaktsiyalar ularni shu qadar tez-tez bajarish orqali suiiste'mol qilinishi mumkinki, serverda har bir soniyada potentsial minglab so'rovlarning har birini qondirishga urinishda resurslar tugaydi. Bundan tashqari, DDoS hujumidagi har bir kompyuter ko'pincha o'ziga xos IP-manzilga ega bo'lgani va minglab so'rovlarning har birini boshqa soxta IP-manzil va turli sarlavha ma'lumotlari yordamida amalga oshirishga harakat qilganligi sababli, bitta hujum manbasini aniqlash va blokirovka qilish qiyin bo'lishi mumkin.

DDoS hujumlarini yumshatish uchun ishlatiladigan oddiy, ammo samarasiz usullardan biri bu **tezlikni cheklash qoidasidan foydalanishdir.** Internetdan veb-serverga kelishi mumkin bo'lgan maksimal trafik miqdoriga cheklov qo'yish (va qolgan trafikni qabul qilishdan bosh tortish) qonuniy trafikni potentsial ravishda rad etish masalasini keltirib chiqaradi. Agar foydalanuvchi tezlikni cheklash qoidasi tomonidan ruxsat etilgan maksimal trafik darajasiga yetgan serverga ulanishga harakat qilsa, uning zararli bo'lmagan niyatlariga qaramay, unga ulanish rad etiladi. Tarifni cheklash qoidalari qonuniy va noqonuniy foydalanuvchilar o'rtasida farq qilmaganligi sababli, ular odatda DDoS hujumlarini yumshatish uchun juda foydali emas, ayniqsa "Slashdot effekti" oldida - mashhur veb-sayt kichikroq saytga havola qilinganda, bu vaqtinchalik katta o'sishga olib keladi. tirbandlikda yoki kichikroq saytdagi "flesh olomon".

DDoS tajovuzkorlari o'z hujumlarini kuchaytirish uchun foydalanadigan yana bir strategiya bu shtatdan tashqari paketlarni yuborish - TCP protokoli tomonidan belgilangan oddiy ketma-ket tartibda yuborilgan **TCP paketlar .** Paketlarni tartibsiz yuborish orqali (ya'ni SYN-ACK paketidan oldin ACK paketi), tajovuzkor o'z nishonining mashinasini ushbu zararli ulanish haqidagi ma'lumotlarni ulanish jadvalida saqlashga majbur qiladi. Yuqorida aytib o'tilganidek, aksariyat qurilmalar noto'g'ri ishlamasdan, ulanish jadvallarida haddan tashqari ko'p ulanishlarni saqlashga qodir emas. Buning o'rnini qoplash uchun DDoS-ga qarshi yanada ilg'or maxsus echimlar paketning shtatdan tashqarida ekanligini aniqlash uchun murakkab usullardan foydalanadi va bunday g'ayritabiiy paket oqimlari asosida trafikni blokirovka qilish uchun yumshatish mexanizmlarini faollashtiradi.

Hujumchilar nafaqat hajmli hujumlardan, balki **"past va sekin"** ham foydalanadilar. **hujumlar,** bunday hujumlar bilan kurashish uchun maxsus yumshatish strategiyalari talab qilinadi, chunki ular qonuniy ko'rinadigan, sekin bo'lsa-da, tezlikda keladigan qonuniy ko'rinadigan trafikni o'z ichiga oladi. Slowloris va RUDY kabi vositalar qonuniy paketlarni sekin sur'atda ishlab chiqaradi va ular yordamida amalga oshirilgan hujumlar an'anaviy yumshatilish strategiyalarini aniqlanmasdan o'tkazishga imkon beradi. Bunday hujumni aniqlashning mumkin bo'lgan usullaridan biri oddiy ishlash davrida tarmoqdagi xatti-harakatlar tahlilini o'tkazish va bunday ma'lumotlarni "past va sekin" vosita tomonidan hujum paytida to'plangan ma'lumotlar bilan solishtirishdir. Misol uchun, agar ma'lum bir ilovada tranzaksiyani yakunlash uchun o'rtacha besh daqiqa va o'n HTTP seanslari kerak bo'lsa, agar foydalanuvchi besh soat vaqt sarflasa va xuddi shu tranzaksiyani bajarish uchun 1000 HTTP seanslarini talab qilsa, ular tajovuzkor bo'lishi mumkin va qo'shimcha xavfsizlik choralari talab qilinadi.

Yana bir murakkab hujum usuli HTTPS protokolida ishlatiladigan veb-shifrlashning keng tarqalgan usuli bo'lgan **Secure Socket Layer (SSL)** dagi zaiflikni suiiste'mol qiladi . Ma'lumotlarni qayta-qayta shifrlash va shifrini ochishga majburlash, ayniqsa SSL-ning "qayta muzokaralar" funksiyasidan foydalanish orqali tajovuzkor maqsadli server resurslarini to'liq egallashi mumkin, shuning uchun u qonuniy so'rovlarni qondira olmaydi.
SSL-ga asoslangan DoS hujumlarini aniqlash va kamaytirish ayniqsa qiyin, chunki serverga boradigan barcha trafik shifrlangan va shuning uchun uning qonuniy yoki zararli ekanligini aniqlashdan oldin shifrini ochish kerak - bu ko'pincha vaqt va resurslarni talab qiladigan jarayondir. keyinchalik ishlov berilgan.

DDoS mudofaa strategiyasini qanday o'rnatish kerak

Yuqorida aytib o'tilgan muammolar bu xavfsizlikning ko'pchiligidan faqat bir qismidir so'nggi va eng murakkab DoS va DDoS hujumlarini yumshatish haqida gap ketganda, provayderlar bugungi kunda duch keladigan yechimlar. Xavfsizlik devori va IPS kabi an'anaviy xavfsizlik echimlari faqat DoS va DDoS hujumlari uchun samarali yechimni ta'minlay olmasligi aniq - tashkilotlar DoS va DDoS hujumlaridan bag'ishlangan va kengroq himoyani ta'minlay oladigan hujumni yumshatish tizimini izlashga chaqiriladi.

Tashkilotlar amalga oshirishda ikkita asosiy tanlovga ega DDoS mudofaa strategiyasi: xavfsizlik provayderidan anti-DoS xizmatini sotib oling yoki mahalliy hujumni yumshatish tizimini o'rnating. Bizning fikrimizcha, tashkilotlar bu ikki muqobildan birini tanlamasliklari kerak, balki ikkalasini ham qabul qilishlari kerak, chunki ular bir-birini to'ldiradi.

Xavfsizlik provayderidan Anti-DoS xizmatini sotib olish

So'nggi paytlarda DDoS hujumlari sonining ko'payishi bilan ko'plab Internet Xizmat ko'rsatuvchi provayderlar (ISP) va boshqariladigan xavfsizlik xizmati provayderlari (MSSP) anti-DDoS xizmatlarini taklif qila boshladilar. Bunday xizmatlar tashkilotga ulanish nuqtasidan bir oz oldin ISP yoki MSSPda yumshatuvchi uskunalarni joylashtirish orqali tashkilotlarni tarmoq suv toshqini hujumlaridan himoya qiladi. Ko'pincha "toza quvur" deb ataladigan ushbu turdagi yumshatish tarmoq suv toshqini hujumlarining tashkilotga etib borishini to'sib qo'yishi kafolatlanadi, chunki hujumlar ISP yoki MSSP va tashkilot o'rtasidagi aloqaga etib borgunga qadar yumshatiladi.
Bu tashkilotning "internet quvurini" zararli trafikdan holi qiladi.

Biroq, faqat o'z joyida yumshatish uskunalarini o'rnatadigan tashkilotlar kattaroq muammolarni yumshatishga harakat qilishlari mumkin.

tarmoq suv toshqini ularning butun "internet trubkasi" ni to'ldiradi, shuning uchun anti-DDoS xizmatlari foydalidir. Boshqa tomondan, anti-DDoS xizmatlari amaliy DoS hujumlarini, shuningdek past va sekin hujumlarni bloklay olmaydi, chunki ularning yumshatish uskunalari bunday hujumlarning nozik tomonlarini aniqlash uchun etarlicha sezgir emas. Har ikkala himoya turidan birgalikda foydalanish tashkilotingizni ham hajmli, ham amaliy darajadagi DoS hujumlaridan samaraliroq himoya qilishi mumkin.

Mahalliy hujumni yumshatish tizimini o'rnatish

HTTP va HTTPS toshqinlari yoki past va sekin hujumlar kabi amaliy qatlamli DDoS hujumlarini muvaffaqiyatli aniqlash va yumshatish uchun tashkilotlar joyida yumshatish tizimlarini o'rnatishni ko'rib chiqishi kerak. Tashkilotning ma'lumotlar markazida o'rnatilgan tizimlar ma'lumotlar markazidagi butun tarmoq infratuzilmasi, xususan, ma'lumotlar markazida joylashgan serverlar orqali taqdim etiladigan har qanday onlayn xizmatlar uchun perimetr xavfsizligini ta'minlaydi. Himoya qilish uchun mo'ljallangan ilovalarga shunday yaqin joyda o'rnatilgan yumshatuvchi tizimlar dastur serverlarida va undan tashqarida tarmoq trafigidagi o'zgarishlardan ko'proq xabardor bo'lish uchun nozik sozlanishi mumkin va shuning uchun tarmoqdagi shubhali trafikni aniqlash imkoniyati ko'proq bo'ladi. dastur qatlami.

Tavsiyalar

Mahalliy hujumlarni yumshatish tizimlari har qanday dasturga xos hujumlar uchun keng qamrovli yumshatishni ta'minlashi mumkin, ammo tashkilotning Internet trubkasini to'liq to'ldiradigan katta tarmoq toshqinlaridan etarli darajada himoya qila olmaydi. Shuning uchun biz tashkilotlarga hujumni kamaytirish tizimini va bulutga asoslangan DoS-ga qarshi yechimni qo'llashni tavsiya qilamiz. Quyidagi jadval turli xil hujum turlarini va bu hujumlarni yumshatish ehtimoli ko'proq bo'lgan joylarni umumlashtiradi.

Hujum turi	Bulutli yumshatish	Saytda yumshatish
Tarmoq toshqini internet quvurini to'sib qo'ydi	●	
Ilova Flood		●
Past va sekin hujum		●
SSL asosidagi hujum		●

1-jadval: Har bir mudofaa strategiyasi taklif qiladigan yumshatish imkoniyatlarining qisqacha mazmuni

DDoS hujumini yumshatish tizimiga qo'yiladigan asosiy talablar ro'yxati

Har qanday hujumni yumshatish tizimi har xil turdagi DDoS hujumlarini muvaffaqiyatli aniqlashi va yumshatishi uchun siz bir nechta asosiy xususiyatlarni o'z ichiga olishini kutishingiz kerak:

Ma'lum va noma'lum hujum vektorlarini aniqlash va yumshatish qobiliyati

Yangi hujum vositalari va usullarini tez joriy etish bilan hujumni yumshatish tizimlari ma'lum va yangi hujum vektorlaridan foydalangan holda hujumlarni yumshata olishi kerak. Xakerlar har kuni yangi hujum vektorlaridan foydalangan holda hujum vositalarini chiqaradilar va shuning uchun yumshatish tizimini har bir yangi hujum vositasi haqida ma'lumotni o'z ichiga olgan ma'lumotlar bazasi bilan jihozlash deyarli mumkin emas. Biroq, yumshatish tizimi yangi hujum vektorining oddiy tarmoq faoliyatiga ta'sirini aniqlashi va ilgari noma'lum bo'lgan hujum vektoridan foydalangan holda hujum sodir bo'lganda real vaqt rejimida imzo yaratishi mumkin va bu sodir bo'lganda uni samarali ravishda bloklaydi. Eski statik imzoga asoslangan tizimdan, shuningdek, real vaqt rejimida imzoga asoslangan yangi ilg'or tizimdan foydalanish ma'lum va noma'lum hujum vektorlaridan foydalangan holda hujumlarni yumshatish imkonini beradi - bu eng keng qamrovli yechim.

Foydalanuvchi faoliyatini tahlil qilish va noto'g'ri xatti-harakatlarni aniqlash qobiliyati

Yuqorida aytib o'tilganidek, ko'plab DoS va DDoS vositalari qonuniy ko'rinishdagi tarmoq trafigini hosil qiladi, bu esa ommaviy ravishda qayta-qayta yuborilganda xizmat ko'rsatishni rad etish holatiga olib kelishi mumkin. Misol uchun, agar foydalanuvchi ilgari tasvirlangan SSL qayta muzokaralar zaifligini suiiste'mol qilishga urinsa, hujumni yumshatish tizimi SSL kalitining takroriy qayta ko'rib chiqilishi foydalanuvchining oddiy xatti-harakati emasligini aniqlashi kerak. Bunday shubhali faoliyatni tarmoq xatti-harakatlarini tahlil qilish paytida to'plangan bilan solishtirganda, hujumni yumshatish tizimi noto'g'ri xatti-harakatlarni bloklashi mumkin, bu SSL kalitini qayta ko'rib chiqish maqsadli server resurslarini iste'mol qilishiga yo'l qo'ymaydi va natijada xizmat ko'rsatishni rad etish holatini keltirib chiqaradi.

Soxta pozitivlarni yo'q qilish qobiliyati

Hujumni yumshatishning ilg'or tizimi qonuniy foydalanuvchilar va zararli foydalanuvchilarni ajrata olishi kerak, hech qachon qonuniy foydalanuvchini zararli (noto'g'ri ijobiy) yoki zararli foydalanuvchini qonuniy (yolg'on salbiy) deb belgilamasligi kerak. Noto'g'ri ijobiy holat qonuniy foydalanuvchilar uchun xizmat ko'rsatishdan bosh tortishga olib keladi, bu ham tashkilot, ham uning mijozlari uchun tajriba sifatini sezilarli darajada pasaytiradi, noto'g'ri salbiy holat esa zararli foydalanuvchiga aniqlanmasdan qo'shimcha kiberhujumlarni amalga oshirishga imkon berishi mumkin.

Hujumlarni yumshatishning ilg'or tizimi zararli foydalanuvchilar trafigini, jumladan, tarmoq xatti-harakatlarini tahlil qilish (oldingi bo'limda tasvirlangan) va chaqiruvga javob berish (C/R) mexanizmini aniq aniqlashi mumkin bo'lgan bir necha usullar mavjud. C/R mexanizmlari onlayn xizmatga so'rov haqiqiy veb-brauzer va shaxsiy kompyuterga ega bo'lgan haqiqiy foydalanuvchidan yoki bunday ma'lumotlarni avtomatik so'rovlar bilan soxtalashtirishga uringan zararli foydalanuvchidan kelib tushganligini tekshirish uchun mo'ljallangan. haqiqiy. C/R mexanizmidan foydalanish uchun hujumni yumshatish tizimi ko'rib chiqilayotgan so'rovning manbasiga bir qator so'rovlarni ishga tushiradi va manbadan olingan keyingi javobga ko'ra, ikkita harakat o'rtasida qaror qabul qiladi: yanada murakkab chaqiriq yuborish. , yoki manbani zararli foydalanuvchi deb belgilash. C/R mexanizmlari hujumni yumshatish tizimida ham, manba tomonlarida ham inson aralashuvini talab qilmaydigan avtomatik jarayonlar bo'lib, ularni mudofaa mexanizmi sifatida qulay va samarali qiladi. C/R mexanizmidan oqilona foydalanish va tarmoq xatti-harakatlarini tahlil qilish noto'g'ri pozitivlarni deyarli butunlay yo'q qilishi mumkin, bu qonuniy foydalanuvchilar uchun ajoyib tajriba sifatini kafolatlaydi.

Maxsus jihozlar bilan toshqinlarni yumshatish qobiliyati

Hujumni yumshatish tizimiga qo'yiladigan yakuniy muhim talab bu tegishli uskunadan foydalanishdir. Yumshatish qurilmalari katta tirbandliklarni bartaraf eta oladigan maxsus apparat tezlatgich kartalarini qo'llashi kerak, chunki katta miqdordagi zararli trafik qurilma ichidagi boshqa mexanizmlarning ishlashiga ta'sir qilmasligi muhimdir. Bu sabab bo'lishi mumkin

qurilma ichidagi turli komponentlarning noto'g'ri ishlashiga olib keladi va natijada hujumlardan etarli darajada himoya qilmaydi.

DDoS hujumining zaifligini baholash - o'zingizdan so'rash uchun 11 ta savol

Bilim korporativ tarmoqlar va ilovalarni himoya qilish uchun har qanday kompaniyaning hujumlarini kamaytirish strategiyasining asosidir. Xavfsizlik haqida gap ketganda, siz bilmagan narsalar sizga zarar etkazishi mumkin. Ushbu zaiflikni baholash tashkilotingiz xavfsizligining kuchli va zaif tomonlari haqida umumiy ma'lumot berish uchun mo'ljallangan. Bu qo'shimcha ta'lim, uzluksiz ta'lim yoki kasbiy sertifikatlashni rejalashtirish uchun hududlar uchun qimmatli ko'rsatkich bo'lishi mumkin. Agar siz ushbu savollarning birortasiga javob berishga ishonchingiz komil bo'lmasa, siz o'ylaganingizdan ko'ra zaifroq bo'lishingiz mumkin.

Bizning biznesimiz veb-ilovalarning yuqori daromad keltirishiga tayanadimi?

Mavjudlik bilan bog'liq muammolar tufayli yuzaga kelgan salbiy reklama kompaniyamizning obro'sini pasaytiradimi?

Tashkilotim uchun ishlamay qolishning soatlik/kunlik narxi qancha?

Tashkilotlarimning DDoS hujumlaridan himoya qilish strategiyasi qanday?

DDoS hujumini aniqlash va bildirish uchun qancha vaqt ketadi?

Ertaga tashkilotim DDoS hujumiga duchor bo'lsa, nima qilardim?

Bizda avtomatik DDoS hujumiga javob bormi?

O'tgan yil davomida biz necha marta hujumlarga duch keldik?

Biznesimiz mavjudligiga hujum paytida qaysi infratuzilma qurilmalarim ishlamay qolishi mumkin?

Tashkilotni 100% mavjud bo'lgan holda hujumni bartaraf etishning eng yaxshi yechimi qanday?

Tashkilotlarimiz xakerlar va boshqa kiber jinoyatchilarga qarshi chora ko'rish imkoniyati qanday?

Kutib qolish

Keyingi bir necha yil ichida Radware DDoS hujumlarining kuchayishini kutmoqda murakkablik, chastota va qat'iyatlilikda.

Birinchidan, kuchli DoS va DDoS hujumlari shifrlangan SSL trafigidan tobora ko'proq foydalanadi, moliyaviy institutlar, davlat idoralari, ijtimoiy tarmoq kompaniyalari va boshqalar kabi xavfsiz onlayn tranzaktsiyalarga bog'liq bo'lgan firmalarni nishonga oladi. Hujumni yumshatish yechimi bilan hamohang ishlaydigan to'g'ri shifrlash mexanizmisiz SSL-ga asoslangan trafikga tayanadigan har qanday tashkilot o'zini katta xavfga duchor qiladi.

Xavfsizlik kompaniyalari, shuningdek, past va sekin hujumlarning ko'payishi bilan kurashish uchun yangi usullarni ishlab chiqishga harakat qilishlari kerak. Ushbu hujumlarni boshlash qulayligi va ular olib kelishi mumkin bo'lgan halokat xakerlarni ushbu hujumlarda foydalanish uchun yanada murakkab past va sekin hujum vositalarini ishlab chiqishga undaydi.

Biz tajovuzkorlar yanada qat'iyatli va ko'proq bo'lishini kutamiz ularning qurbonlariga e'tibor qaratdi. Oxirgi 12 oy ichida biz hujum kampaniyalarining uzoq davom etishi va tajovuzkorlar tashkilotning xavfsizlik tizimlariga kirib borish va nishonlarining onlayn mavjudligini yoÿq qilish uchun kampaniya davomida hujum usullarini oÿzgartirish tendentsiyasini koÿrmoqdamiz. 2012 yildagi ba'zi hujumlar hujumchilar tomonidan o'zgartirilgan doimiy hujum usullari bilan 3 haftadan ko'proq davom etdi.

Hujumchilar endi turli maqsadlarga tasodifiy DDoS hujumlarini amalga oshirmaydilar; bugun va yana kelajakda tajovuzkorlar o'z maqsadlarini sinchkovlik bilan tanlaydilar, xavfsizlik teshiklarini topish uchun dastlabki skanerdan o'tkazadilar, hujumni boshlash uchun eng og'riqli vaqt oralig'ini tanlaydilar va uni ko'p kunlar davomida davom ettiradilar.

9 Xulosa

Tasavvur qiling-a, bir kuni barcha telekanallarda xakerlar guruhining mamlakat transport tizimlari va elektr tarmoqlarini buzish niyati haqida milliy ko‘rsatuvni eshitib uyg‘ongansiz. Ko‘pgina shaharlarning elektr tizimlari allaqachon o‘chirilgan, barcha yirik fond birjalari yopilgan, huquqni muhofaza qilish organlarining barcha kompyuterlari va kompyuter tarmoqlari ishlamay qolgan.

Bu apokalipsisga o'xshaydimi? Ehtimol, futuristik kiber urushning qandaydir shakli? Bu, albatta, faraziy stsenariydir - u 2007 yilda "Ozod yasha yoki qattiq o'l" filmida sodir bo'lgan ba'zi voqealarni tasvirlaydi, unda bir qator kiberterrorchilar Birlashgan Millatlar Tashkilotiga murakkab ko'p qismli kiberhujum uyushtirishga urinishgan. Shtatlar. Kompyuterlar va kompyuter tarmoqlarining kundalik qurilmalarga integratsiyalashuvi ortib borayotganligi sababli, bunday hujumning sodir bo'lish ehtimoli endi unchalik astronomik emas, chunki odamlarning ma'lumotlari har qachongidan ham ko'proq shakllarda va ko'proq joylarda saqlanadi.

Mashhur Maxfiylik, yaxlitlik va mavjudligida “Xavfsizlik Uchburchak”, DDoS hujumlari maqsadli mavjudligiga, qonuniy foydalanuvchilarning maqsadli tarmoq qurilmasi tomonidan taqdim etilgan xizmatlarga kirishiga to'sqinlik qiladi. Bunday hujumlar uchun ko'plab sabablar bor, ular o'yin-kulgidan tortib moliyaviy tovlamachilik, siyosiy norozilik va hatto urushgacha. Hujumlarni amalga oshirishga urinayotganlar yuqori malakali xakerlar bo'lishi shart emas, chunki hatto eng tajribali foydalanuvchilarga ham murakkab hujumlarni amalga oshirish imkonini beruvchi ko'plab vositalar ishlab chiqilgan.

Ushbu qo'llanmada biz savdolarni ishlab chiqarish, mijozlarga xizmat ko'rsatish yoki maxfiylikni saqlash uchun Internet-trafikga bog'liq bo'lgan har qanday yirik yoki kichik biznes o'z tarmoq tizimlari uchun DoS va DDoS hujumlaridan kuchaytirilgan himoyaga nomzod ekanligini ko'rsatishga harakat qildik. . Hech bir biznes yoki sanoat o'zini bunday hujumlardan butunlay xavfsiz deb hisoblamasligi kerak, chunki mudofaa choralarini qo'llamaslik jiddiy moliyaviy va obro'li oqibatlarga olib kelishi mumkin.

Xavfsizlik devorlari kabi xavfsizlik echimlarini qo'llagan kompaniyalar, IPS va antivirus dasturlari ba'zi turdagi xavfsizlik tahdidlaridan yaxshi himoyalangan bo'lishi mumkin, ammo bunday echimlar himoyani ta'minlamaydi.

DDoS hujumlariga qarshi. DDoS hujumlaridan samarali himoya qilish uchun tashkilot o'z dushmanlari kimligini, ularni nimaga undayotganini va qanday vositalardan foydalanishini bilishi kerak. Ular bir nechta qatlamlarda DDoS himoyasini o'rnatishlari kerak - provayderda tarmoqli kengligi himoyasi, shuningdek, saytdagi ilovalarni himoya qilish. Keng qamrovli bilimlar, tegishli DDoS himoya tizimlari va sog'lom paranoyya tuyg'usining kombinatsiyasi tashkilotni DDoS hujumidan eng yaxshi sug'urta bilan ta'minlaydi.

Qo'shimcha ma'lumot uchun

DDoS hujumlariga qarshi kurashda oldinda qolishni xohlaysizmi? Iltimos, tashrif buyuring: www.ddoswarriors.com qo'shimcha ekspert resurslari va ma'lumotlar uchun.

Mualliflar haqida

Radware (NASDAQ: RDWR), virtual va bulutli maʼlumotlar markazlari uchun ilovalarni yetkazib berish va ilovalar xavfsizligi yechimlari boʻyicha global yetakchi hisoblanadi. Uning mukofotga sazovor bo'lgan yechimlar portfeli biznes uchun muhim ilovalar uchun to'liq chidamlilik, maksimal AT samaradorligi va biznesning to'liq chaqqonligini ta'minlaydi. Radware yechimlari butun dunyo bo'ylab 10 000 dan ortiq korxona va operator mijozlariga bozor muammolariga tezda moslashish, biznesning uzluksizligini ta'minlash va xarajatlarni kamaytirish bilan birga maksimal mahsuldorlikka erishish imkonini beradi. Qo'shimcha ma'lumot uchun www.radware.com saytiga tashrif buyuring.

Radware' Favqulodda yordam guruhi (ERT) favqulodda yordam xizmatidir real vaqt rejimida javob bera oladigan maxsus mutaxassislar bilan faol tahdidni yumshatish uchun xavfsizlik va mahsulot ekspertlarining proaktiv, “amaliy” ishtirokini taklif qiladi. Bizning uzoq muddatli munosabatlarimiz va ishonchli maslahatchi va yechim hamkori sifatidagi obro'-e'tiborimiz ushbu qo'llanmani amalga oshirish imkonini beradi. Bizning ERT "yovvoyi tabiatdagi" hujumlarni sodir bo'lganda boshqarishda katta tajribaga ega.

Radware's ERT DoS/ ostida mijozlarga real vaqtda yordam beradi. DDoS hujumlari. Ular buni mijozning tarmoq uskunasiga bevosita kirish, fayllarni yozib olish, vaziyatni tahlil qilish va mijoz bilan vaziyatni muhokama qilish orqali amalga oshiradilar. Garchi xizmatning asosiy maqsadi hujumni to'xtatish va mijozning tiklanishiga yordam berish bo'lsa-da, jamoa hujumning o'ziga xos ko'rinishini ham oladi. Amaliy ishtiroki tufayli ular real vaqt rejimida nima haqida ma'lumot olishadi

hujum aslida o'xshaydi. Ular aslida hujumdan kelib chiqqan ta'sirni o'lchashga qodir. Boshqacha qilib aytadigan bo'lsak, ERT veb-saytga hujum qilinganda nima sodir bo'lishini chuqurroq ko'rib chiqadi.
Odatda, ERT faqat o'rta va yuqori darajadagi hujum kampaniyasi bo'lganda javob berishga chaqiriladi.

Ishtirokchilar

Ronen Kenig
Direktor, xavfsizlik mahsulotlari marketingi
Radware

Debora Manor
Xavfsizlik mahsuloti marketingi menejeri
Radware

Ziv Gadot
SOC/ERT guruhi rahbari
Radware

Daniel Trauner
Xavfsizlik bo'yicha texnik yozuvchi
Radware