Дәріс №4: Желілік қызметтерге шабуыл

DDoS-шабуыл (ағылш. Distributed Denial of Service – «қызмет көрсетуден бас тарту») – кең таралған және қауіпті желілік шабуылдардың бірі болып табылатын қызмет көрсетуден бас тарту түріндегі үлестірілген шабуыл. Шабуыл нәтижесінде заңды пайдаланушыларға, желілерге, жүйелер мен өзге де ресурстарға қызмет көрсету бұзылады немесе толық істен шығарылады. DDoS-шабыл нәтижесінде сайтқа қызмет көрсететін серверлерге үлкен көлемдегі жалған сұратуларды өңдеуге тура келеді және сайт қарапайым пайдаланушы үшін қолжетімсіз болып қалады.

DDoS-шабуылдан кім зардап шегуі мүмкін?

Мұндай шабуылдардан коммерциялық және ақпараттық сайттар зардап шегеді. Соңғы кезде хакерлер шабуылдардың мұндай түрін шабуылды тоқтату үшін ақша беруді талап ету мақсатындағы алаяқтық ретінде қолданады.

DDoS-шабуыл қалай жүргізіледі?

DDoS-шабуыл сызбалық түрде келесі көрініске ие: зардап шегуші ретінде таңдап алынған серверге әлемнің түрлі нүктелерінде орналасқан компьютерлерден көптеген жалған сұратулар келіп түседі. Нәтижесінде сервер өзінің бүкіл ресурстарын осы сұратуларды өңдеуге жұмсайды да, қарапайым пайдаланушылар үшін толық дерлік қолжетімсіз болып қалады. Жалған сұратулар жіберілген компьютерлердің пайдаланушылары өздерінің машиналарының хакерлер тарапынан қолданылғанын білмеуі де мүмкін. Осы компьютерлерде зиянкестер тарапынан орнатылған бағдарламалар «зомби» деп аталады. Компьютерлерді «зомбилендірудің» қорғалмаған желілерге рұқсатсыз кіруден троян-бағдарламаларды қолдануға дейін баратын көптеген жолдары белгілі. Бұл дайындық кезеңі зиянкес үшін ең күрделі кезең болып табылады деуге болады.

DDoS-шабуылдың ішкі көрінісі

DDoS түріндегі желілік шабуыл басқару орталығынан (зиянкестен) берілетін команда бойынша шабуылдауға ұшырайтын компьютерге оған заңды пайдаланушылардың қолжетімділігін тоқтатуға алып келетін ерекше сұратуларды жібере бастайтын ботнет (зомби-желі) – арнайы зиянкес бағдарламамен зарарланған үлкен көлемдегі компьютерлер көмегімен жүзеге асырылады. Бұл сызбаға қатысушылар саны өте көп болады: ботнетті әзірлеуге арналған бағдарламалық қамтамасыз етуді жазатындар, оны әзірлеуге тапсырыс беретіндер, зомби-желіге әкімгер болып, оны жалға беретіндер, шабуылға тапсырыс берушілер. Өкінішке орай, бүгінгі күні ботнеттермен күрес компьютерлерден зиянкес бағдарламалық қамтамасыз етуді жоюмен шектеліп отыр. Ботнет иелері мен оның «қызметтеріне» тапсырыс берушілер «кадр артында» қалады.

Ақпараттық қауіпсіздік мамандары DDoS-шабуылдардың келесі түрлерін бөліп қарастырады:

UDP flood – нысана-жүйе мекенжайына үлкен көлемдегі UDP (User Datagram Protocol) пакеттерді жолдайды. Бұл әдіс ең алғашқы шабуылдарда қолданылған болатын және қазіргі таңда ең зиянсыз шабуыл ретінде қарастырылады. Бас контроллер мен агенттер арасындағы алмасу барысында шифрленбеген TCP және UDP хаттамалары қолданылатындықтан, шабуылдың бұл түрін пайдаланатын бағдарламалар тез анықталады;

TCP flood – желілік ресурстарды «байлауға» алып келетін үлкен көлемдегі TCP-пакеттерді нысана мекенжайына жолдау;

TCP SYN flood – нәтижесінде жекелеген ашық қосылымдарды қадағалау үшін өзінің барлық ресурстарын жұмсауға тура келетін нысана-тораппен арадағы TCP-қосылымдарды анықтау үшін үлкен көлемдегі сұратуларды жолдау;

Smurf-шабуыл –пакеттерде осы сұратуды пайдаланатын бағытталған кең тарататын жіберілім мекенжайы бойынша ICMP (Internet Control Message Protocol) пинг-сұратулары, нәтижесінде дереккөздің жалған мекенжайы шабуыл нысанасына айналады;

ICMP flood – Smurf тектес, бірақ жіберілімдерсіз жүзеге асырылатын шабуыл.

Сипатталған шабуылдардың бірнеше түрін бірден қолданатын бағдарламалар ең қауіпті болып табылады. Олар TFN және TFN2K атауларына ие болды және хакерден жоғары деңгейдегі дайындықты талап етеді.

DDoS-шабуылдарды ұйымдастыруға арналған соңғы бағдарламалардың бірі болып табылатын Stacheldracht (тікенді сым) шабуылдардың түрлі типтері мен кең тарататын және контроллер мен агенттер арасында деректермен алмасуды шифрлейтін пинг-сұратулар тасқынын ұйымдастыру мүмкіндігін береді.

Алайда бағдарламалар спектрі әлдеқайда кең және әрдайым толықтырылып тұрады. Осы себептен DDoS-шабуылдардан универсалды сенімді қорғау әдістерін сипаттау жеткіліксіз болып қалады. Универсалды әдістер жоқ, алайда шабуылдардан келетін зардап пен қауіпті азайтуға арналған жалпы ұсыныстарға маршрутизаторлар мен желіаралық экрандардағы анти-DoS пен анти-спуфинг функцияларының сауатты конфигурациясы сияқты шараларды жатқызуға болады.

Сервер деңгейінде серверді алыстан қайта жүктеу мүмкіндігі үшін сервер консолінің SSH-хаттамасы бойынша басқа IP-мекенжайға шығарылуына ие болуы жақсы болып табылады. DDoS-шабуылдарға тойтарыс берудің ұтымды әдістерінің бірі IP-мекенжайды бүркемелеу болып табылады.

DDoS-шабуылға қалай тойтарыс беруге болады?

Сұратулар түрлі тараптардан келіп түсетіндіктен, шабуылдардың мұндай түріне тойтарыс беру біршама қиын болып табылады. Әдетте, қорғауға фильтрлеу мен блэкхолинг, сервер осалдықтарын жою, ресурстарды күшейту, бытыратып орналастыру (пайдаланушыларға қызмет көрсетуді жалғастыратын үлестірілген және көшірмесі бар жүйелерді қалыптастыру), бас тарту (шабуылдың нақты мақсатын басқа байланысы бар ресурстардан алу, IP-мекенжайды бүркемелеу) сияқты іс-шаралар жатады.

DDoS-шабуылды уақтылы анықтау

Егер Сіздің жеке серверлеріңіз бар болса, онда Сізге жасалатын шабуылды анықтауға арналған құралдарға ие болуыңыз қажет. DDoS-шабуыл нәтижесінде Сіздің сайтыңызға қолжетімділікпен байланысты туындаған мәселелерді неғұрлым ерте анықтасаңыз, оған тойтарыс беруге қажет шараларды соғұрлым ерте қолдана аласыз.

DDoS-ты кіріс трафигі профильдерінің механизмін жүзеге асыру көмегімен анықтауға болады. Егер серверіңіздегі трафиктің орташа есеппен санағандағы көлемі мен өзгеру динамикасын білсеңіз, оған тән емес өзгерістерді тез анықтау мүмкіндігі туады. DDoS-шабуылдардың басым бөлігі кіріс трафигі көлемінің шұғыл артуымен сипатталады және профильдер механизмі бұл секірудің шабуыл болып-болмағанын анықтауға көмектеседі.

Өткізу мүмкіндіктерінің есептері қосымша арналарды қосу керексіз екенін көрсетсе де, оларды қосу тиімді тәсіл болып табылады. Бұл жағдайда Сіз, мысалы, жарнамалық кампания, арнайы ұсыныстар немесе компанияңыздың БАҚ-та жарықтандырылуы нәтижесінде орын алуы мүмкін трафиктің күтпеген секірулерін еш зардапсыз билей аласыз.

DDoS-тан қорғауды қамтамасыз ету күрделілігі:

· **Желінің табиғи осалдықтары.** Зиянкестер тарапынан қолданылатын желі осалдықтарының болмауы. Барлық компьютерлік платформалар табиғатында белгілі бір жеткізу деңгейі болғандықтан, кез келген шабуыл сәтті жүзеге асырылуы мүмкін. Компьютерлер, кластерлер немесе бұлтты жүйелер – бұлардың барлығы белгіленген уақыт аралығында өңдей алатын сұратулар саны бойынша белгілі бір физикалық шектеулерге ие болып табылады. Сәтті өткен DDoS-шабуыл осы шектеуден өту үшін трафиктің жеткілікті деңгейін генерациялауы қажет. Басқа шабуылдардың басым бөлігі арнайы патчтарды қолданумен, қауіпсіздік жүйесінің конфигурациясы мен саясаттарды өзгертумен тойтарыс бере алады. Алайда бұл амалдардың бір де бірі DDoS-қа қарсы тұра алмайды. Қызметтер әрдайым қолжетімді болуы керек, демек олар шабуылдар алдында әрдайым осал болып табылады.

· **Топты оқшаулау мүмкінсіздігі.** Шабуылдың өте көп дереккөздері болғандықтан, DDoS-ты оқшаулау өте қиын болып табылады. Шабуылдаушы IP-мекенжайлардың ұзын тізімін тиімді оқшаулауды қамтамасыз ету өте қиын. Шабуылды тоқтату үшін мыңдаған мекенжай уақытша болса да, қара тізімге енгізілуі тиіс. Егер шабуылдаушы шабуылды заңды хосттар (spoofing) арқылы жүргізсе, онда қара тізімге шабуылға еш қатысы жоқ хосттар да енуі мүмкін.

· **Жауаптыларды іздеу.** Осы жерде үшінші мәселемен бетпе-бет келеміз: пайдаланушылардың қай бөлігі толықтай заңды сұратулар жасап жатқанын, қайсыларының DDoS-қа қатысқандарын анықтау өте қиын. Қызметтерге қол жеткізген компьютерлердің барлығы серверге салмақ түсіретіндіктен, олардың барлығы өздері білмей-ақ, шабуылға қатысады. Клиенттік хосттардың қайсылары «жақсы», қайсылары «жаман» екенін анықтау үшін өте мұқият тексеру қажет. Қандай да болмасын шешімдер қабылданбай тұрып, аз уақыт аралығында бірқатар есептеулер жүргізілуі тиіс.

DDoS-шабуыл неге бағытталған

DDoS-шабуылдардан тиімді қорғану үшін ықтимал қауіптерді бөліп қарастыру қажет. Шабуыл нысанына қарай:

· Ресурстарды қажет ететін жалған мекенжайлары бар пакеттер байланыс арналарын «толтырып тастап», сайтқа заңды пайдаланушылардың қолжетімділігін қиындатады немесе оқшаулайды. Байланыс арналарының кең өткізу мүмкіндіктері осы типтегі шабуылдардан қорғануға мүмкіндік береді.

· Егер шабуыл жүйе ресурстарына бағытталса, онда оның өнімділігі төмендейді, нәтижесінде жүйе ақырын жұмыс істей бастайды. Шабуылдаушылар жүктеу үшін зардап шегуші компьютерге қандай деректер пакеттерін жолдау қажет екенін жақсы біледі.

· Қиратушы шабуыл бағдарламалық қамтамасыз етудің осалдықтарын пайдаланып, жүйенің конфигурациясы мен параметрлерін өзгертуі мүмкін. Кез келген рұқсатсыз іс-қимылдар бақылауға алынып, жойылуы тиіс. Жеке алып қарастырылатын әр жағдайда DDoS-тан қорғауға арналған өзіндік скрипт қолданылады.

Сервер, желіаралық экран және интернет арнасы осал элементтер болып табылады

Зиянкестер өз шабуылдарын шабуыл жасалған кезде серверге тиесілі ресурстардан әлдеқайда көп ресурстарды пайдалануға алып келетін түрде ұйымдастырады.

· Өткізу мүмкіндігінің азаюына бағытталған және «көлемді флуд» атауына ие шабуылдар үшін Интернет-арна осал болып табылады. Мұндай шабуылдарға арнаның өткізу мүмкіндігінің басым бөлігін қажет ететін UDP-флуд немесе TCP-флуд жатады.

· Желіаралық экран қауіпсіздікті қамтамасыз ету құралы болып табылатынына және SYN-флуд, UDP-флуд тектес шабуылдарды өткізу барысында және қосылудың толығуы барысында DoS/DDoS-шабуылдарға арналған осал жері болмауына қарамастан, зиянкестер желіаралық экранның өзі инфрақұрылымның осал жеріне айналмайынша, желіаралық экран ресурстарын азайтатын бірқатар ахуалдарды қалыптастырады.

DDoS-шабуылға тап болған жағдайда қолданылуы тиіс шаралар тізімі

· Шабуылдың орын алғанына көз жеткізіңіз. DNS-тің дұрыс емес конфигурациясын, маршрутизациямен байланысты мәселелерді және адами факторды қоса есептегенде, жұмыстағы іркілістің жалпы себептерін жойыңыз.

· Техникалық мамандарға жүгініңіз. Техникалық мамандардың көмегімен шабуылға ұшыраған ресурстарды анықтаңыз.

· Қосымшалардың маңыздылық басымдықтарын қалыптастырыңыз. Басымдыққа ие қосымшаларды сақтау үшін маңыздылық басымдықтарын қалыптастырыңыз. Интенсивті DDoS-шабуыл мен шектеулі ресурстар жағдайында негізгі пайда көздерін қамтамасыз ететін қосымшаларға баса назар аударыңыз.

· Қашықтықтан қосылған пайдаланушыларды қорғаңыз. Ісіңіздің жұмысын қамтамасыз етіңіз: қолжетімділікке ие болуы тиіс қашықтықтағы сенімді пайдаланушылардың IP-мекенжайларын ақ тізімге енгізіп, бұл тізімді негізгі етіңіз. Бұл тізімді желіде таратып, оны қолжетімділік қызметін берушілерге жолдаңыз.

· Шабуыл санатын анықтаңыз. Шабуылдың қандай түрімен бетпе-бет келдіңіз: Көлемді ме? Аз мөлшердегі әрі баяу ма? Сізге қызмет көрсетуші шабуылдың неғұрлым көлемді екенін хабарлайды.

· Шабуыл дереккөздерінің мекенжайларымен күрес нұсқаларын анықтаңыз. Күрделі шабуылдар жағдайында Сізге қызмет көрсетуші дереккөздер санын анықтауда қиындыққа тап болады. Сіздің желіаралық экраныңыздағы шабуылдаушы IP-мекенжайлардың шағын тізімдерін оқшаулаңыз. Көлемді шабуылдарды геоорналасуы туралы деректер негізінде оқшаулауға болады.

· Шабуылдарды қосымша деңгейінде оқшаулаңыз. Зиянкес трафикті анықтап, оның қандай құрал арқылы әзірленгенін анықтаңыз. Қосымша деңгейіндегі шабуылдардың белгілі бір бөлігін әрбір нақты жағдайда Сізде бар шешімдермен ұсынылатын контршаралардың көмегімен оқшаулауға болады.

· Өзіңіздің қорғаныс периметріңізді күшейтіңіз. Мүмкін бұл 7-ші деңгейлі асимметриялық DDoS-шабуыл шығар. Қосымшалар деңгейіндегі қорғауға баса назар аударыңыз: логиндер жүйелерін, адамдарды айыру жүйесін қолданыңыз.

· Желілік ресурстарды шектеңіз. Егер осыған дейінгі шаралар көмектеспесе, ресурстарды шектеу қажет – осылайша «жақсы» және «жаман» трафик шектеледі.

· Қоғаммен қарым-қатынасты басқарыңыз. Егер шабуыл жария болса, ресми хабарлама дайындап, қызметкерлеріңізді хабардар етіңіз. Егер салалық саясаттар мұны ескерсе, шабуылдың орын алу фактісін растаңыз. Егер ескермесе, техникалық қиындықтар бар екенін айтып, қызметкерлеріңізге сұрақ қойылған жағдайда, барлық сұрақтармен қоғаммен қарым-қатынас бөлімінің басшылығына жүгіну керек екенін айтыңыз.