Размисли върху компютърните атаките от тип „отказ на услуга”

„Дайте ми опорна точка и достатъчно дълъг лост, и ще повдигна Земята!“

Архимед

ВЪВЕДЕНИЕ

Статията цели да представи и опише същността и принципите на компютърните атаки от тип „отказ на услуга” („отказ от обслужване”) с цел по-доброто им разбиране, предотвратяване и адекватно реагиране при регистриране на такава атака в компютърните системи. Фокусът е върху принципните положения, а не върху техническото реализиране на този вид атаки, защото броят на видовете атаки е много голям и включва аспекти започващи от стила на писане на компютърни програми, минава през тяхното конфигуриране, физическото изграждане на компютърните мрежи и сървърното оборудване и стига до компетентността, както на атакуващата, така и на атакуваната страна.

Нерегламентираното вмешателство в компютърните системи с цел нарушаване на тяхната нормална работа може да се извърши по множество начини. Атаките от тип DoS (denial-of-services) целят да натоварят дадена система с повече работа отколкото тя може да изпълни за единица време, което влошава качеството или напълно спира предоставянето на дадена услуга. Това свръх натоварване може да се разпредели както по различните компоненти и подсистеми в сървъра (диск, памет, процесор), върху външната инфраструктура (маршрутизатори, комутатори, защитни стени и др.), така и по различните комуникационни канали на атакуваната система. Тъй като няколко компютърни системи могат да ползват общ комуникационен канал или мрежова инфраструктура, освен атакуваната система и други могат да бъдат засегнати, въпреки че не са прекият обект на атаката. Аналогично, при атака на една услуга, всички останали услуги работещи на същото устройство могат да бъдат засегнати.

Щетите от такива атаки, могат да бъдат от временно забавяне на отварянето на WEB сайтове, напълно неработещи програми разчитащи на комуникация с други компютри до задействане на други атаки, прикриване на други незаконни действия или следите от тях и др. При този вид компютърни атаки не се изтриват, променят или крадат файлове от системата, нито се придобива достъп до нея, но въпреки това тези атаки могат са причина за големи финансови загуби от пропуснати ползи за компании зависещи в голяма степен от присъствието си в Интернет.

ВИДОВЕ

DoS атаките могат да се разделят в следните групи според това, към кой комуникационен компонент са насочени:

- Препълване на комуникационните канали

Запълването на цялата пропускателна способност на комуникационните канали с Интернет трафик влияе по два начина върху предоставяната услуга. Заявките на реалните потребители към системата не могат да бъдат обработени, поради изчерпване на пропускателната способност на канала от големия обем фалшиви заявки. Цел на атакуващите могат да бъдат както входния, така и изходния комуникационен канал на системата.

- Претоварване на мрежовата инфраструктура

Поради особеностите на Интернет, въпреки че отпадането на един възел или връзка от мрежата може да не е фатално, то това би породило пренасочването на трафика по друг

маршрут, ако такъв съществува, и той би се натоварил допълнително, което може да доведе до изпускане на част от легитимните заявки. В случай, че такъв няма, то въпреки че атаката не е насочена към дадена компютърна система, тя може да бъде откъсната от мрежата като се извадят от строя околните мрежови устройства свързани с нея.

- Претоварване на сървърите и крайните потребители

Големия брой заявки за обработване от системата могат да изискват по-големи изчислителни ресурси от колкото има налични, което отново ще бъде причина за невъзможност за обработване на всички постъпили заявки поради неправилно оразмеряване на изчислителните ресурси. Претоварването на конкретни сървъри може да стане на няколко нива, без да е необходим голям трафик. Това е възможно поради различни грешки и пропуски в операционната система и приложния софтуер на сървъра или тяхното конфигуриране, водещи до лавинообразно нарастване на използваните ресурси. За да се ограничат негативните ефекти трябва да се внедрят механизми за ограничаване на натоварването и изолиране на приложенията, както и механизми за автоматично рестартиране на забили такива, както на ниво операционна система, така и на ниво приложен софтуер.

Според вида на използвания трафик, DoS атаките биват:

- С генериран трафик

За генерирането на достатъчно голям Интернет трафик обикновено се използват голям брой Интернет потребители, които биват заразявани с програми за отдалечен скрит контрол и задействани от атакуващия т.н. „зомбирани компютри”. С развитието на електрониката все повече „умни” устройва от различни области на живота, биват снабдени с достъп до Интернет. Поддържането на висока сигурност в най-различни Интернет приложения е трудно и възможностите за компрометирането им не трябва да се пренебрегват. Това улеснява създаването на т.н. „ботнет мрежи”, т.е. мрежи от зомбирани устройства.

Това обаче не е единственият начин за създаване на трафик. Историята познава случаи на използване на peer-to-peer мрежи за обмен на файлове, съобщения и видео разговори в реално време, за генериране на фалшив трафик. Този тип мрежи се състоят от равноправни възли поддържащи списък с други такива възли. Това позволява бързото откриване на голям брой еднотипни компютри, които могат да бъдат заразени. Характерът на трафика между различните възли не може да се предвиди и евентуалното му рязко увеличение не би било толкова подозрително.

- С пренасочен трафик

Придобиването на контрол над чужд компютър или заразяването му с вируси изисква време и познания. Трафика в Интернет обаче така и така тече навсякъде и постоянно нараства. По-лесно би било той да се пренасочи и концентрира към един адрес или мрежа. Изпълнението на този сценарии може да се реализира по няколко начина, изискващи намесата само в една точка от мрежата, което обаче би имало голям ефект. Компрометирането на мрежови маршрутизатори и комутатори в опорни мрежи на Интернет доставчици или точки за взаимен обмен на трафик е логичното място за проникване и промяна на маршрутните таблици така, че целият трафик да бъде насочен към целта на атаката.

Според мащаба на атаката и това от колко места идва фалшивия трафик, DoS атаките се делят на:

- Такива с един източник или източници в една подмрежа

Атаките с един източник са по-малко опасните, тъй като източника може лесно да се идентифицира и да се блокира, като вероятността да бъдат блокирани реални клиенти е много малка. Тук и големината на фалшивия трафик е ограничена от възможностите на един атакуващ и е възможно да не води до претоварване.

- Атаки с множество източници разпръснати по целия свят

Атаките идващи от множество адреси се блокират по-трудно, защото тяхната ефективност може да е наистина голяма и наличното оборудване да не смогва да идентифицира целия фалшив трафик и да го блокира. За ускоряване на блокирането може да се блокират цели подмрежи, от които идва атаката, но така може да бъдат блокирани и редовните потребители освен зомбираните.

РЕАЛИЗАЦИЯ

Характерът на атаката е такъв, че няма принципно никакъв проблем да се реализира, тъй като тя може да представлява съвсем легитимни действия на потребители на дадена система или услуга с тази разлика, че в даден отрязък от време те се увеличават значително над възможностите на системата да им отговори. Едно условия за реализиране на ефективна атака с генериран трафик е наличието на по-големи компютърни ресурси при атакуващата страна отколкото при атакуваната. Това може да стане по два начина: използване на компютърни центрове с различно предназначение и големи изчислителни ресурси или използване на голям брой устройства със стандартни възможности но широко разпространени, като домашни персонални компютри, мобилни телефони, автомобилни системи за забавление, „умни" телевизори, VoIP телефони и др.

Използването на компютърни центрове за генерирането на голям трафик към даден компютър или мрежа улеснява реализирането на DoS атака. Работата им обаче се следи непрекъснато и персоналът им би спрял атаката бързо след засичането ѝ което в някои случаи може да стане и автоматично от програмите за мониторинг. От друга страна, големия брой устройства с възможност за свързване с Интернет и тяхното използване от хора, които не са специалисти в областта на компютрите, както и тяхното стандартно конфигуриране, създават възможност за заразяване им с вирусоподобни програми използвани за различни цели включително и за DoS атаки. В този случай се налага едновременното задействане на множество заразени устройства за да се осигури достатъчно голям трафик към избраната цел.

Възможен начин за прикриване на източника на атаката е използването на междинна система за генериране на трафик към действителната цел на атаката. Чрез подменянето на IP адреса на атакуващия с този на обекта на атаката и изпращането на заявки към дадена система, тя ще изпрати отговор не на атакуващия, а на подменения адреса в заявките, т.е. на целта на атаката. В този случай ще изглежда че двете системи се атакуват взаимно и действителния атакуващ остава почти невидим. Този вид DoS атака се нарича огледална. Той може да се прикрие допълнително с използването на proxy сървъри. Междинната система трябва да е достатъчно мощна за да устои на големия брой заявки, както и да генерира съответния отговор към целта на атаката, иначе самата тя ще стане жертва на атаката, а не крайната.

Метод за увеличаване на трафика е използването на принципите на работа на Интернет вместо да се разчита на много участници. Така, с по-малки ресурси може да се генерира голям трафик. Едно приложение на този метод е адресирането на echo или ping заявки до броудкаст адреса на дадена мрежа. Заявката бива препратена до всички крайни устройства в мрежата, като техния отговор се връща на подменения адрес т.е. на атакуваната

система. По този начин се постига усилване на атакуващия трафик. Тази атака е особено ефективна ако съществуват два или повече пътя между две комутиращи устройства, тъй като те ще си препращат трафика помежду си, ако не са взети мерки за предотвратяване на това и всички клиенти свързани към тези устройства ще изпитват затруднения при комуникация.

Друг начин за реализиране на наистина голяма DoS атака е като се променят DNS записите на един или няколко масово посещавани сайтове с тези на атакуваната система. Така всички потребители опитващи се да посетят тези сайтове ще се опитват да се свържат с атакуваната система. Атаката ще продължава докато не се забележи промяната на DNS записите и те не бъдат коригирани.

Следващ пример за създаване на DoS атака, неизискващ задълбочени познания, е посещаването на статична WEB страница съдържаща голям брой изображения или други файлове нужни за зареждането на страницата, с адрес на атакуваната система. Така, един човек може да генерира много бързо голям брой заявки, като с увеличаване на посещенията се увеличава и генерирания трафик към атакуваната система. Интересно е да се провери възможността за задействане на такава атака при посещение на подобна страница от Интернет търсачките. Този метод може да се приложи и като се вгради зловреден код, който няма визуална част, в често посещавани сайтове. Достатъчно е в кода да има обръщение към ресурси разположени на атакуваната система, като те могат да са съществуващи или не.

Изкуствено генерираните заявки към системата цел на атаката, могат да съдържат невалидни или липсващи параметри, което може да предизвика срив в системата дори и ако броят им е сравнително малък, в случай, че софтуера не отхвърля такива пакети. Когато софтуера е настроен да записва в log файл тези заявки, то свободното дисково пространство ще се запълни с ненужни файлове, както и производителността на дисковата система ще се използва не за полезното съдържание.

Изпращането на електронно писмо до несъществуващ потребител в даден сървър ще върне отговор на подателя с грешка. Ако адреса на подателя е адрес от атакувания mail сървър или клиентска пощенска кутия и изпращането на писмата става автоматично от зловредна програма или от много такива, то сървъра бързо ще изразходва наличните си ресурси за обработка или съхранение на писмата. В случай, че първият сървър е конфигуриран да добавя прикачените файлове в оригиналното писмо, то те ще бъдат изпратени и на атакуваната система, което ще увеличи и трафика към сървъра цел на атаката. Ако има зададен максимален брой писма или обем на пощенската кутия за даден клиент, то след запълването на квотата, редовният клиент няма да може да получава нови писма. Друга разновидност на атаката е когато към писмото е прикачен голям файл, който е компресиран до малък размер. Когато e-mail сървъра получи писмото и провери прикачените файлове за вируси, като разкомпресира файловете, ще получи много големи файлове, които изискват повече ресурси за проверка.

Следваща разновидност на e-mail DoS атаките е вграждането на изпълним от клиента скрипт (примерно JavaScript) в HTML форматираните електронни съобщения, който да изпълнява различни операции заемащи различни ресурси водещи до загуба на работоспособност на операционната система. Компютърните вируси от тип „червей”, често се разпространяват по електронната поща, генерирайки постоянен поток от вредоносни писма до всички открити е-маил адреси в адресната книга на пощенския клиент. Това тяхно поведение има лавинообразен характер поради постоянни поток между всички e-mail адреси и сървъри.

Без значение на метода за разпространение, компютърните вируси могат да имат различни функции използвани за разнообразни цели, включително участие в DoS атаки към отдалечени системи. Със същата лекота те могат да бъдат насочени и към някоя от подсистемите в системата гостоприемник. Например, заделянето на част или на цялата оперативната памет за вирусният процес ще натовари дисковата система за прехвърляне на други процеси във виртуалната памет. Отварянето на неограничен брой файлове и записването в тях на произволна информация ще има същият ефект. Положението става

наистина напечено, когато вирусният процес първо се самоизпраща до всички открити е-майл адреси и след това създава неограничен брой свои копия, които повтарят горните действия. Ако вируса е написан добре и не претоварва системата до степен тя да блокира, вируса може да остане работоспособен за сметка на човека пред монитора. Към този похват може да се добави и скриването на вируса чрез rootkit техники, така че и след рестартиране или използване на антивирусна програма, действията му ще се възстановят и системата отново ще стане неизползваема.

Заразените по подобен начин компютри могат да участват в DoS атака, насочена към техните потребители, а не към външна цел. Така може да се изразходва бързо месечната квота за трафик, ако има такова ограничение или да се натрупа голяма сметка за допълнителния трафик.

Лесен метод за DoS атака е като се изпращат пакети с подменен адрес на източника с този на атакуваната система и с малка стойност на TTL параметъра. Така скоро след изпращането на пакета, поредният маршрутизатор ще види че TTL параметъра е 0 и ще върне отговор, че пакета е блокиран на атакуваната система. Тази функция е включена стандартно и за да се избегне, трябва да се промени конфигурацията на съответното устройство.

Не е задължително DoS атаките да идват от външен източник. Веднъж компрометирани компютрите във вътрешната мрежа могат да участват в DoS атака насочена към други потребители във същата мрежа. Обикновено вътрешните мрежи са по-слабо защитени от действията на собствените си потребители. При неподходящо оборудване или конфигуриране и голяма мрежа ефекта й може да е достатъчен за да претовари мрежовата инфраструктура и локалните услуги в организацията, без да има увеличен трафик идващ от вън.

Друг метод за реализиране на DoS атака е като се изпращат заявки с подправен адрес на изпращача, който съвпада с адреса на получателя. Така трафика, който получава целта на атаката изглежда, че идва от самата нея, което обикновено не е забранено. Ресурсите й биват изразходвани освен за генерирането на отговор, така и за генерирането на втори отговор изпратен към себе си. Този вид атака лесно се блокира, като се забрани входящия трафик с източник същата система и изходящия трафик с цел същата система.

ЕФЕКТИВНОСТ НА АТАКАТА

При препълване на комуникационните канали е по-добре да се генерират заявки с голям размер за да може с по-малко участници в атаката да се напълни канала. Фрагментирането и дефрагментирането на големите мрежови пакети по пътя ще натовари допълнително оборудването. Този механизъм може да се използва и за прескачане на защитните стени. При претоварване на мрежово оборудване или сървъри се използват заявки с малък размер, за да може големият им брой да доведе до изпускане на легитимните заявки. Примерни заявки могат да бъдат такива за претърсване на голяма базаданни, списъци с адреси в маршрутизатори, списъци с правила за филтриране, опити за регистриране на валидни или невалидни потребители, едновременни VoIP разговори, трансфер на големи файлове и др.

При задействане на DoS атака, трафикът към компютърната система или мрежа нараства рязко за кратко време, което може да бъде регистрирано от автоматични наблюдаващи програми, които активират различни филтри върху трафика. За да се избегне това, фалшивите клиенти могат да симулират интензивно, но в нормални рамки потребление. Така общото натоварване ще се повиши, но няма да е много подозрително, още повече ако се осъществява постепенно. В този случай, разликата между истинските и фалшивите клиенти няма да е явна и може да се окаже, че са блокирани и много истински клиенти заедно с фалшивите.

В голяма степен преките проявления на тези атаки зависят от компютърната подсистема където се появява претоварването и качеството на софтуера. При добре написан софтуер може да се стигне до само използване на всички достъпни ресурси за дадена програма. Ако те бъдат ограничени до по-малка стойност от всички налични ресурси, то останалата част от системата няма да е засегната. Ако обаче софтуера не проверява правилното форматиране на данните или тяхната валидност е възможно да се стигне до системни грешки като препълване на В/И буфери, недостиг на памет, недостиг на дисково пространство, подаване на невалидни параметри, достъп до паметта без разрешение и др., а от там и до срив на цялата операционна система на мрежовото устройство и необходимост от рестартиране.

Друг възможен сценарии е когато се изпълни лесна за откриване атака, която цели да увеличи броя на правилата за филтриране на трафика, като кратко време след нея се изпълни още една атака, която освен препълване на каналите цели и претоварване на филтриращите устройства като защитни стени и IPS системи поради многото правила за проверка. Такава атака може да се изпълни автоматично от един потребител използващ множество подменени IP адреси.

ЗАЩИТА

С развитието на мрежовото оборудване и техниките за управление на Интернет трафика се усъвършенстваха и начините за осигуряване на отказоустойчивост, висока ефективност и разпределение на натоварването за да може нарасналия брой Интернет потребители да получава качествени Интернет услуги. Част от нововъведенията целят подобрение на защитата от различни видове компютърни атаки включително и DoS атаките.

Разрастването на доставчиците на свързаност и съдържание върху няколко континента и изграждането на собствени високоскоростни мрежи, осигурява по-къс път на трафика между две произволни точки. По този начин една компания може да контролира по-голяма част от пътя на трафика и да реагира при възникване на проблеми. Конкретен пример са мрежите за доставка на съдържание (content delivery networks, CDN) и доставчиците на свързаност от ниво 1 и 2 (Tier 1 и 2). CDN мрежите създават няколко копия на статичното съдържание, разположени в различни точки на Света, намалявайки закъснението при достъпа до него, като клиентите биват препращани към най-близкия до тях сървър. В този случай една разпределена DoS атака ще се разклони към различни сървъри и ефективността й ще е по-ниска, когато се използва домейн името на ресурса за насочване на атаката.

Виртуализацията и изолацията на сървърите в облачният компютърен модел, дават възможност за миграция на нужните ресурси от едно физическо място на друго без да е нужно клиентите да променят работата си. В този случай е трудно за атакуващия да разбере къде физически се изпълнява услугата и няма да може да уцели желаната система.

Дори и атаката да е насочена към конкретен IP адрес, това не означава, че тя ще удари точно този адрес. Това се постига чрез използване на BGP протокола в маршрутизаторите и anycast (от точка до точка от няколко възможни) IP адреси на системите. Трафика към такъв адрес се пренасочва към някой от вторичните адреси в групата. Избора на конкретен адрес може да зависи от критерии като географско разположение, натоварване на подсистемите, отдалеченост на клиента и др., така фалшивият трафик ще се разклони към различни адреси. Възможно е дори поради това че той идва от разпръснати места по света, да не доведе до препълване на комуникационните канали.

В крайна сметка обработката на заявка и връщането на отговор на клиента се извършва от една система с конкретен IP адрес. Зад този адрес обаче може да стои компютърен клъстер. Тук отново натоварването се разпределя върху няколко отделни сървъра. Избирането на конкретен сървър зависи от различни фактори, което смекчава допълнително негативните ефекти от DoS атака.

Комбинирането на няколко мрежови техники на различните нива в една голяма система увеличава допълнително устойчивостта й на DoS атаки. Като още една мярка може да се посочи осигуряването на няколко пъти повече ресурси в една система, от колкото са нужни за нормалното й функциониране за дълъг времеви период, които ще осигурят работоспособността й дори и при атака.

Защитата на даден сървър се състои от четири компонента. Първият компонент представлява подобряване на общата сигурност, надеждност и производителност на машината провеждано периодично. Това е превантивна мярка намаляваща вероятността за успешна атака и евентуалните щети. Вторият компонент е блокирането на фалшивия трафик още на входа на нашата система за да се възстанови нормалната й работа и да не се затрудняват следващите действия на персонала. Третият компонент е блокирането на фалшивия трафик, колкото се може по-далеч от периметъра ни, за да изчистим и комуникационните канали и да възстановим нормалния достъп на потребителите до нашите услуги. Тези дейности целят пълното неутрализиране на ефекта от атаката. До голяма степен това са дейности извършвани от външни компании, а не от нас. Последният компонент е провеждането на задълбочен анализ върху част от записания фалшив трафик за да разберем къде е бил проблема и да отстраним евентуално причините за успешната атака.

Превантивните дейности трябва да започнат с оценка и последващо измерване на натоварването на мрежата и сървърите при нормална работа. Това цели определянето на оптималното оборудване за поддържане на предоставяните услуги и ресурси, като същевременно се измерва и реалното максимално натоварване, което няма да причини проблеми в работата на системите. Ако се установи, че наличният резерв от производителност не е достатъчен, следва увеличаване на ресурсите. Друг подход при този етап е оптимизиране на комуникационните канали, вместо инвестиране в ново оборудване, т.н. пасивна защита. Това означава капацитета на каналите да се разпредели съобразно необходимите количества за двете посоки. Ако услугите, които предоставяме не изискват голям капацитет в едната посока и особено в посока към нас, може да го намалим за сметка на обратния канал. Така ще ограничим броя входящи заявки, които ще бъдат обработвани, дори и при много голяма атака още при доставчика, като системите ни няма да се претоварват. Разбира се това разпределение може да е и динамично.

След като хардуера и комуникациите са оптимизирани, следва да се оптимизират и софтуера и мрежовото оборудване. Настройките по подразбиране в операционната система и приложния софтуер не са съобразени с нашите условия и тяхната адаптация ще осигури още по-добри производителност, надеждност и сигурност. Тази процедура изисква добри познания в съответната област, но постигането на оптималните резултати включва и експериментиране с различни комплекти параметри.

Въпреки гаранциите, че дори и по-време на DoS атака системите ни няма да се претоварят, е добре да поставим ограничения за ресурсите, които дадена подсистема, процес или потребител могат да използват. Така на още едно ниво гарантираме, че системите няма да използват повече ресурси от колкото разполагат, което може да покрие лоши сценарии, които сме пропуснали да коригираме или такива, за които не знаем. Тези действия осигуряват висока степен на сигурност, че нашите системи няма да откажат и при максимално натоварване.

За да повишим сигурността на системите първо трябва да деинсталираме всички софтуерни продукти, които няма да се ползват, след което да забраним всички останали. Знаейки какви услуги ще предоставяме и техните изисквания разрешаваме само тези протоколи и портове, които са необходими за тяхната работа. Допълнително е добре да блокираме заявки и действия, които не са очаквани при нормална работа на системата. Това могат да бъдат заявки дошли на външен мрежов интерфейс, но с адрес на източника, който не се маршрутизира в Интернет или такъв от вътрешната мрежа, заявки с необичайно голям размер и др.

Вторият компонент се активира при регистриране на DoS атака от системите анализиращи трафика и сървърното натоварване. Тук се използват различни комбинации от чисто филтриращи до извършващи сложни времеви анализи върху трафика системи. Системите следят натоварването на отделните компоненти в сървърите и мрежовата инфраструктура и генерират аларми при установяване на нередности. Тези системи попадат основно в две категории: използващи сигнатури (за добре изучени атаки) и откриващи аномалии в трафика или натоварването (за непознати или сложни атаки). Често рязкото увеличаване на броя потребители или заявките за секунда са признак за DoS атака.

Каквито и системи да се използват, генерираните правила за филтриране на трафика е добре да съдържат минимален брой параметри. Така се намаляват проверките извършвани върху всеки постъпил в системата пакет, което позволява да се анализира по-голям трафик. След преустановяване на атаката списъците с блокирани адреси могат да се изчистят или не. Допълнителен подход е използването на списъци с известни и доказани вече източници на зловредни действия, т.н. черни списъци.

В случай, че източника на атаката е един, много рядко срещан сценарий, може да се поиска съдействие от неговия доставчик и още при него да бъде спрян целия трафик. Това обаче не е гарантирано, защото адреса на източника на заявките може да е фалшифициран, което силно затруднява установяването на истинския източник на атаката.

Доставчиците на Интернет свързаност могат да ограничат злоупотребата на своите клиенти чрез изпращане на мрежови пакети с фалшифициран адрес, като блокират всички такива пакети още преди да са напуснали техните мрежи. Допълнителна мярка в тази посока, може да бъде ограничаването на TTL параметъра на изходящите пакети до по-разумни граници, за да се намали времето на съществуване на евентуалните фалшифицирани пакети. Друг параметър, който може да бъде ограничен е броя едновременни връзки, които един клиент може да има, разбира се отново в разумни граници.

По-добра защита се постига, когато се проверяват всички възможни признаци за наличието на DoS атака. Поради големият им брой обаче, тази дейност трябва да се поеме от отделно устройство поставено на входа и изхода на мрежата, за да не се товарят със странична дейност основните системи. За да изключим възможността самите ние да станем част от DoS атака, т.е. атаката да е изходяща вместо входяща, трябва да филтрираме и изхода от мрежите ни.

Осигуряването на няколко комуникационни канала през различни доставчици, т.е. създаването на multihomed сървъри или мрежи и използването на Multipath TCP протокола, позволява при отпадане или претоварване на една от връзките, останалия трафик да се насочи през другите канали. Така евентуалните задръствания могат да се заобиколят или поне ефектите от тях да се намалят. Тук сървърите трябва да са свързани чрез отделни мрежови интерфейси, всеки със собствен маршрутизатор или комутатор, за да се избегне създаването на една точка, сриването на която да предизвика отказ на цялата ни мрежа.

КОНТРА МЕРКИ

Контра мерките, които бихме могли да предприемем зависят от местата където е регистрирана атаката, т.е. доставчиците на атакуващата или атакуваната страна или самата атакувана система. За да са ефективни контра мерките, те трябва да се предприемат максимално бързо след установяване вида на атаката и докато все още е активна. След като се установи входният мрежов интерфейс на фалшивия трафик, той трябва да се филтрира още при компания доставчик, по посочени параметри. Втората компания може да проследи трафика в своята мрежа и да го блокира още на входа си. При желание или съществуваща договорка, тя може да се свърже със следващата организация от където идва трафика със същите параметри и да поиска неговото блокиране още по-близо до източника му.

При разпределена DoS атака обаче, бързо ще се достигне до точка в мрежата, в която лошият трафик идва от няколко интерфейса, което ще забави реакцията на съответните

организации. Въпреки това, при добра координация, гореописаните действия могат да се повторят.

За да се задейства горната процедура е достатъчно да се разберат MAC или IP адресите на източниците. За жалост и двата вида адреси се подправят лесно. При разпределена DoS атака броя адреси ще е много голям и натоварването на филтриращите системи ще се увеличи, което пак може да доведе до изгубване на легитимните пакети. Ако при анализа на атаката се открият други общи параметри на по-ниско ниво в TCP/IP стека на лошите пакети е по-добре да се филтрира по тях, защото ще има значително по-малко правила в защитните стени и системите за предотвратяване на проникванията.

Преодоляването на тези атаки се усложнява значително в случаите, когато всъщност протичат няколко вида разпределени DoS атаки. Тогава се налага филтрирането на различни видове мрежови пакети насочени към различни услуги. При недостатъчна подготовка за подобни ситуации е възможно усилията на персонала за възстановяване на нормалната работа на системите, да не са достатъчно ефективни. Ето защо е много важно да има внедрени автоматични програми следящи трафика и натоварването на различните системни компоненти. Поради широкия спектър на възможностите за осъществяване на DoS атаки, винаги има пропуски в защитата на компютърните системи и мрежи, които могат да се използват.

Връщането на фалшивия трафик на източника му с цел да го принудим да се откаже, трябва задължително да се избягва, защото това е принципа на действие на огледалните DoS атаки. Така ние ще станем източник на атака и нашите адреси могат да бъдат блокирани, което ще доведе до отрязване на достъпа ни до мрежата и загуба на клиенти.

Тенденцията за осъществяване на все по-сложни атаки изисква предварително проучване на инфраструктурата в целевата мрежа или система. Това включва съставяне на списък с наличните компютри в мрежата и търсене на уязвими места в тях. Обикновено тези действия остават незабелязани, което позволява на злонамерените хакери да съберат богата информация за системите ни. За да бъдат надхитрени, може да се инсталират фалшиви сървъри наподобяващи нормални услуги, които обаче не се използват от никой т.н. honeypots. Така при сканиране на локалната мрежа от външен адрес, фалшивият сървър ще отговори по обичайният начин, но освен това ще запише различни данни за отсрещната страна. Анонсирането на услуга лесна за пробиване ще отвлече вниманието на хакера от действителните производствени системи. Така ще сме сигурни, че сме обект на проучване с цел атака. Разполагайки със събраните данни за атакуващия, можем да конфигурираме предварително системите за филтриране на трафика. Освен това ще разполагаме и с време да установим истинската самоличност на атакуващия и предприемем мерки за филтрирането му от неговия доставчик или поне от нашият.

Възможен вариант за справяне с DoS атака е промяната на IP адресите ни и уведомяване на потребителите ни за тази промяна. Трафикът към старите адреси може да се блокира или да се анализира за да се подпомогнат контра мерките. Тази стратегия обаче е приложима за системи с малко на брой предварително известни потребители. Тяхното уведомяване отнема време, но по този начин се избягват напълно негативите от атаката.

В ЗАКЛЮЧЕНИЕ

Както се вижда, съществуват голям брой възможности и начини за реализиране на атаки от тип „отказ от обслужване”. Това, заедно с достъпните софтуерни инструменти за DoS, занижената сигурност при стандартното конфигуриране на сървърите, мрежовите устройства и операционните системи и недостатъчната компетентност на обслужващия персонал, създават съвсем реална опасност и често прилагана тактика за нанасяне на щети на различни организации. Забавянето в публикуването на корекции за мрежовите продукти или игнорирането на някои пропуски също увеличава риска от понасяне на финансови и други загуби следствие от такава атака. За предотвратяването на някои от тях са взети стандартни

мерки в операционните системи и приложния софтуер, докато за други е нужно допълнително конфигуриране на системите на всяко достъпно ниво.

Ако искаме добра защита на Интернет имуществото ни, а тя става все по-важна, трябва да отстраняваме всички известни пропуски в системите ни. За да се намали изложеният на външни атаки периметър на нашите системи трябва да изтеглим защитната линия, колкото се може по-навън т.е. при доставчика на свързаност. Това може да се постигне чрез съответната договорка с него или ако разполагаме с възможност за контрол на параметрите на канала от страната на доставчика в предварително договорените диапазони.

Колкото повече дупки в сигурността и възможности за DoS атаки отстраним, толкова по-малко хора ще могат да навредят на системите ни, като това ще става и по-рядко. Важно е да се отбележи, че прилаганите методи трябва да се оптимизират спрямо конкретните системи, тип на трафика и характер и разпределение на клиентите, така че да са още по-ефективни срещу DoS атаките. Наличието на методология за действие при засичане на атака и адекватната подготовка на IT персонала допълнително ще улеснят преодоляването на този, а и други видове компютърни атаки.