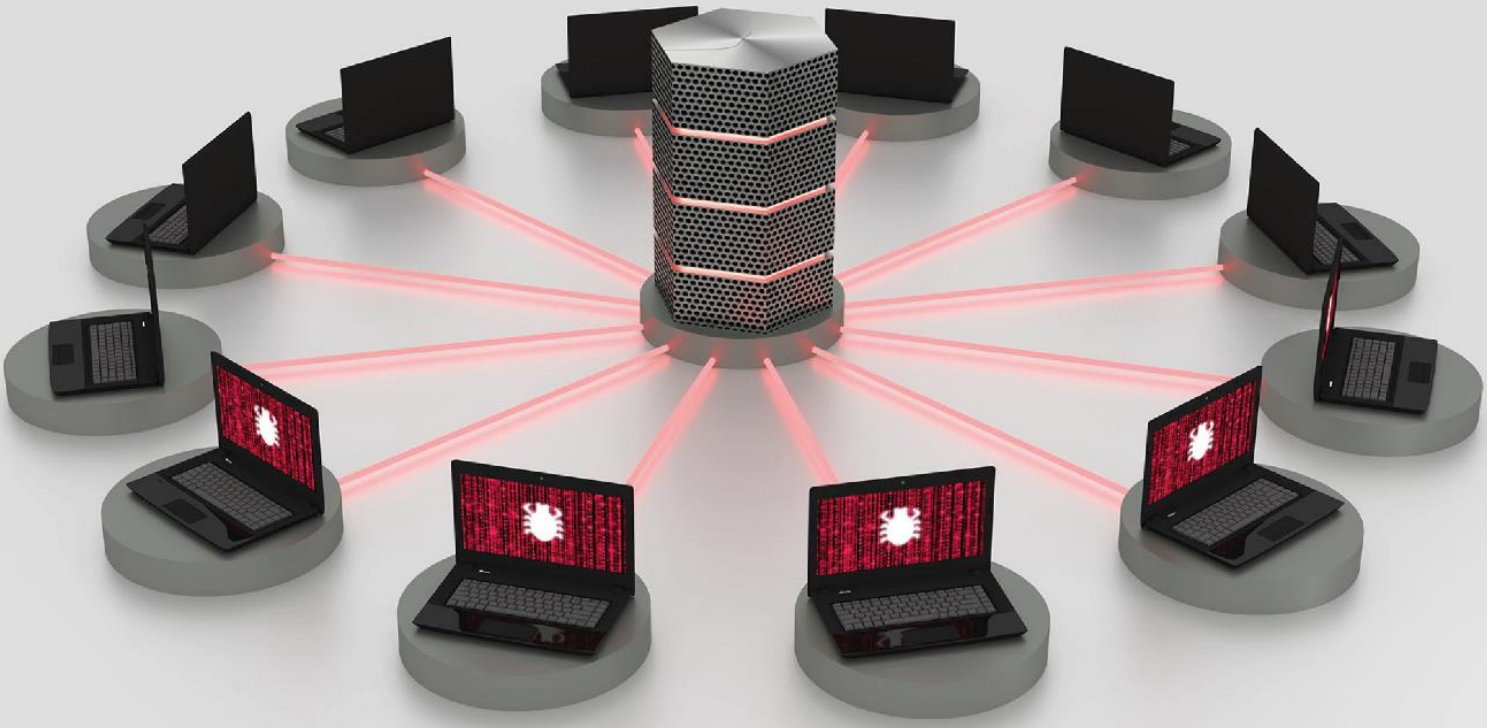
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Védekezés a szolgáltatás megtagadásra irányuló DoS támadások ellen



2022.

Tartalom

A DDoS támadások napjainkban tapasztalható felfutása kapcsán a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban: NBSZ NKI) az alábbi dokumentumban ismerteti az elosztott szolgáltatás megtagadásos (DDoS) támadásokkal kapcsolatos hasznos, a támadások megelőzéséhez, felismeréséhez, illetve az esetleges károk enyhítéséhez segítséget nyújtó információkat. A dokumentum az alábbi anyag alapján készült:

https://www.accessnow.org/cms/assets/uploads/archive/docs/Defending_Against_Denial_of_Service.pdf

Bevezetés

A technológia fejlődése és az Internet használat egyre szélesebb elterjedése révén jelentősen nőtt a társadalom kiberfenyegetettsége. Egyre gyakrabban olvashatunk szolgáltatás megtagadásra (DoS – Denial of Service) irányuló támadásokról, melynek számos szervezet/intézmény szolgáltatása esett már áldozatul és a támadások gyakorisága, valamint volumene is folyamatosan növekszik.

A DoS támadás egy szolgáltatás elérhetetlenségét igyekszik elérni. Sikeres támadás esetén a szolgáltatott tartalom egy adott időre akár teljesen elérhetetlenné válik a felhasználók számára.

A támadás általában számos, fertőzött számítógépet („zombi") alkalmaz, amelyek egy ún. botnet hálózatot alkotnak. Ilyenkor elosztott támadásról beszélünk (DDoS – Distributed Denial of Service).

A DDoS támadások ellen könnyebb védekezni, ha a támadást okozó mechanizmus ismerete rendelkezésre áll, ezért fontos a támadó szándékú forgalom elemzése.

Jelen útmutató két fő részre osztható. Az első rész körvonalazza a szükséges lépeseket egy támadás esetén a weboldalak ellenálló képességének növelése érdekében. A második rész bemutatja azt a folyamatot, amely lépésről lépésre segíti a szervezeteket a helyzet hatékony kezelésében.

Stratégiák	Előkészítő szakasz	Kezdő szakasz	Helyreállító szakasz	Hosszú távú szakasz
A hoszting helye	X		X	X
DoSP	X	X*		
Tűzfalak használata		X		
Nyílt szolgáltatói tükrök	X	X	X	
Terhelés-kiegyensúlyozott tükrök	X		X	
Nagy sávszélességű tükrök	X			
Elosztott tartalom	X	X**		
Darknet (sötét hálózat)	X	X**		
Domain feladása		X		

*Elrendelendő, ha előre elkészítették, vagy meghatározandó, ha a szolgáltatónak, vagy a szolgáltató szolgáltatójának van DoSP-je (Denial of Service Protection).

**Ha előre összeállításra került (az előkészítő szakaszban), akkor ezt a védekezési stratégiát ebben a szakaszban kell érvénybe léptetni.

Első rész: előkészítő szakasz

A támadások hatásait mérséklő stratégiák többségét célszerű jó előre érvényre juttatni. Néhány stratégiát, mint pl. a különféle oldal tükrözések (site mirroring), célszerű a normál működés részeként implementálni. Ezen stratégiák olyan architektúrákat alkalmaznak, amelyek éppúgy szolgálják a szolgáltatások elérésének hatékonyságát, mint a DDoS támadásokkal szembeni ellenálló képességet.

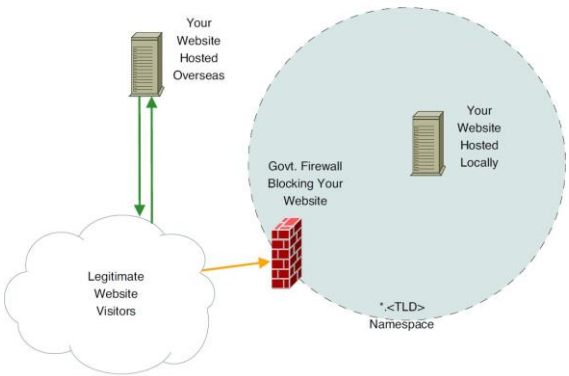
Más stratégiákat viszont csak a DDoS támadás észlelésekor léptetnek életbe. Ebbe a kategóriába tartozik a darknet, valamint az elosztott tartalom kiszolgálás védekezési stratégiaként történő alkalmazása.

A hoszting helyszíne

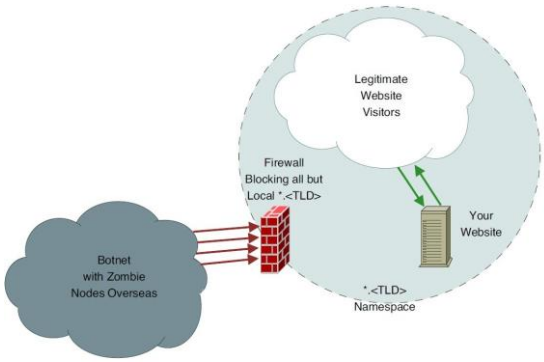
A weboldal/szolgáltatás elhelyezésének földrajzi helyszíne is fontos tényező lehet annak támadhatóságában.

Lokális elhelyezés stratégiája

Amennyiben a szolgáltatás használói túlnyomó részben országon belüliek, a támadó pedig a feketepiacon bérelhető botnet-ek szolgáltatásait veszi igénybe a weboldal/szolgáltatás támadásához, akkor igen valószínű, hogy a botnet-et felépítő „zombi” gépek túlnyomó többsége az ország ún. top level domain-jén (TLD) kívül helyezkedik el. Ezért lehetőség van arra, hogy a DDoS támadás hatásának mérséklése megoldódjon egyszerűen úgy, hogy az upstream provider tűzfalain eldobásra kerül a nem hazai forgalom az adott szolgáltatás irányába.



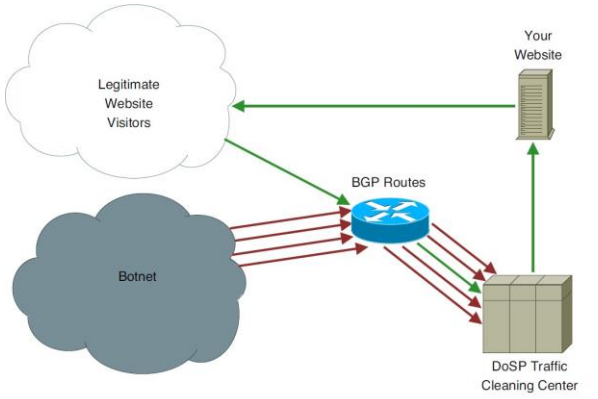
Overseas Hosting Location Strategy



Local Hosting Location Strategy

Külső fél által biztosított szolgáltatás megtagadás elleni védelem (DoSP – Denial of Service Protection)

A hoszting szolgáltató kiválasztásakor érdemes figyelembe venni a kiválasztandó szolgáltató DoSP lehetőségeit és szolgáltatásait. A hoszting szolgáltató szintjén számos formája lehet a DoSP lehetőségének. Néhány alapvető DoSP opció lehet a sávszélesség rövid távú megnövelésére vonatkozó szolgáltatási garancia, ami által a weboldal meg tud birkózni a volumetrikus DDoS támadásokkal. Azok a globális szolgáltatók, melyek a DDoS védelmi területre specializálódtak és megállapodással rendelkeznek a világ nagy telekommunikációs (Telco) cégeivel, erősebb DoSP lehetőségeket nyújthatnak, mivel ezek a megállapodások lehetővé teszik számukra, hogy „megtisztítsák" a bejövő forgalmat, vagy a forráshoz közelebb állítsák meg a támadást, megakadályozva, hogy a nem kívánt forgalom elérje a hoszting hálózatot. Az Arbor Networks (http://www.arbornetworks.com/) ilyen szolgáltatást nyújt. Léteznek DoSP közvetítő cégek is, melyek több, magasabb szintű szolgáltató csomagba szervezett szolgáltatásait egyetlen szolgáltatásként kínálják nagyszámú ügyfélnek. Ezek a közvetítők sok esetben képesek a legjobb DDoS védelmet méltányos áron biztosítani.



Third Party Denial of Service Protection Strategy

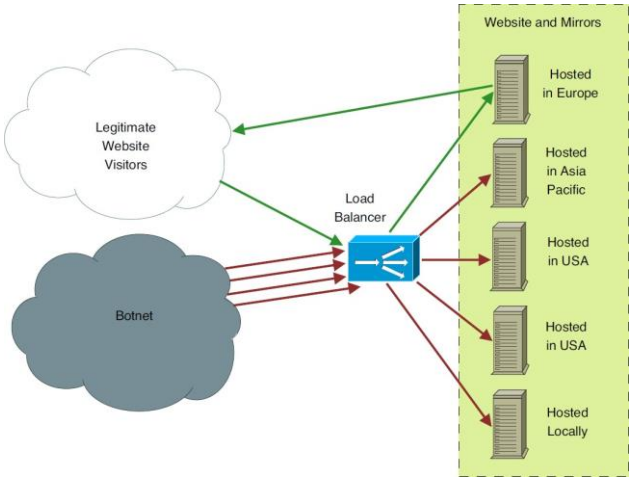
Tükrök készítése

A weboldalak tükrözésének célja, hogy a tartalom több, különböző földrajzi elhelyezkedésű szolgáltató által kerüljön megosztásra és többszörözésre. A sávszélesség elosztásával a weboldal tartalma megfelelő ellenállósággal bírhat az adatvesztést is eredményező eseményekkel szemben, legyenek azok helyi természeti katasztrófák, politikai indíttatású, vagy egyéb támadások. Természetesen figyelembe kell venni az oldal létrehozásához használt technológiák adta lehetőségeket is. A következő kérdésekre adott válaszok segítik az oldal tükrözésére való felkészülést:

1. A technológiák különbözőképpen konfigurált platformokon fognak futni?
2. Milyen szoftver-függőségek állnak fent?
3. Lehetséges ezeket a függőségeket elkülöníteni és a weboldal tartalmával csomagba szervezni?
4. Amennyiben az oldal adatvezérelt (data-driven), össze lehet ezeket az adatokat egyazon csomagba szervezni?
5. A weboldal az adatok pillanatfelvételeivel dolgozik majd, vagy az adatok annyira valós idejűek, hogy nem lehet azokat előre összecsomagolni (akár éjszakánként, vagy hasonló alapon)?

További kihívást jelent a tükrözés előkészítésekor, hogy meg legyen határozva a módja a DDoS támadás alatt tapasztalható körülmények közötti tesztelésnek. Ideális esetben az oldal rendszergazdájának több szolgáltatónál vannak felhasználói fiókjai (a hoszting tükrök céljából, ha szükséges) és ezeket a felhasználói fiókokat veszik igénybe, hogy teszteljék a műszaki csapat képességeit abban, miként tudja a teszt szerverre telepíteni és üzembe helyezni az oldal egy példányát, és ellenőrizni annak működőképességét.

Ez a mód megoldás lehet a problémára, mielőtt ezt egy valóságos támadás sokkal szélsőségesebb körülményei között kellene megtenni. A tesztnek rendszeresen ütemezett eseménynek kell lennie.



Elosztott terhelésű (load balanced) tükrök

Kiegyenlített terhelésű tükröket úgy lehet létrehozni, hogy át kell alakítani a weboldal DNS bejegyzését oly módon, hogy az olyan eszközre mutasson, amely a beérkező lekérdezéseket elosztja a weboldal tükrözött példányai között. Ideális esetben ezek a példányok különböző földrajzi helyeken lévő hoszting szolgáltatónál vannak elhelyezve. Egy weboldal terhelés megosztásos tükrözését lehetséges a DDoS támadásokra való felkészülés keretein belül elvégezni, de tekintettel a terhelésmegosztó megvalósításából fakadó további bonyolultságra és a weboldal több példányának több szolgáltatónál történő elhelyezésének költségeire, ezt gyakran elodázzák egy tényleges DDoS támadás bekövetkeztéig. Terhelésmegosztó eszközökre példa az F5 router és a „reverse proxy”.

Nyílt szolgáltatói tükrök

A nyílt szolgáltatói weboldal tükör lényegében a szolgáltatásként biztosított tartalom-közzétevő keretrendszer, mint amilyen például a Wordpress. Ezek a szolgáltatók azért jók a DDoS elleni védekezés szempontjából, mert masszív sávszélességgel bírnak. Hátrányuk, hogy ezeket a rendszereket úgy tervezték, hogy az átlagember számára csökkentsék a tartalom publikálásának korlátait, ezért csak meglehetősen általános, alapvető kereteket biztosítanak a dinamikus (változó) tartalmak megtervezéséhez és prezentálásához. A nyílt szolgáltatónál elhelyezett tükör használatának célja az eredeti tartalom legkritikusabb részeinek a saját weboldaltól eltérő helyen való hosztolása egy statikusabb formában. Egy tényleges esemény bekövetkezése előtt a weboldal tervezői végiggondolhatják a kritikus tartalom létrehozásának és fenntartásának automatikus módjait. Felhasználói fiókokat tarthatnak fenn ezeknél a nyílt

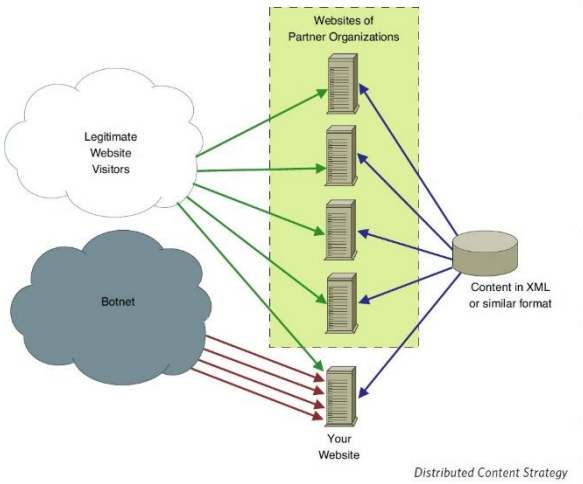
tükör szolgáltatóknál abból a célból is, hogy tartalmat publikáljanak és kétoldalú kapcsolatot tartsanak a felhasználókkal, még akkor is, ha éppen nincs folyamatban DDoS támadás.

Nagy sávszélességet nyújtó szolgáltatók

Van egy másik megoldás a nagy sávszélességet nyújtó szolgáltatók számára, ami felhasználható a DDoS támadások hatásainak enyhítésére. Ezek a nagy sávszélességet nyújtó szolgáltatók sok esetben felhő (cloud) szolgáltatók is, amilyen például az Amazon és a Rackspace. Az általuk biztosított szolgáltatások nem ingyenesek és hosszú távon nem is feltétlenül olcsóak, de igazán gigantikus számítási és hálózati erőforrások állnak rendelkezésükre, hogy biztosítsák ügyfeleik tartalmának a fogyasztóik számára való lehetséges legnagyobb hozzáférést. Tervezési és műszaki szempontból a nagy sávszélességet nyújtó szolgáltatók DDoS támadás elleni védelemre való felhasználásakor a legfőbb megfontolás, hogy a kiválasztott felhő szolgáltató(k) olyan műszaki környezetet tudjanak biztosítani, mely szükséges az adott weboldal tömörített változatának telepítéséhez és üzemeltetéséhez.

Megosztott tartalom

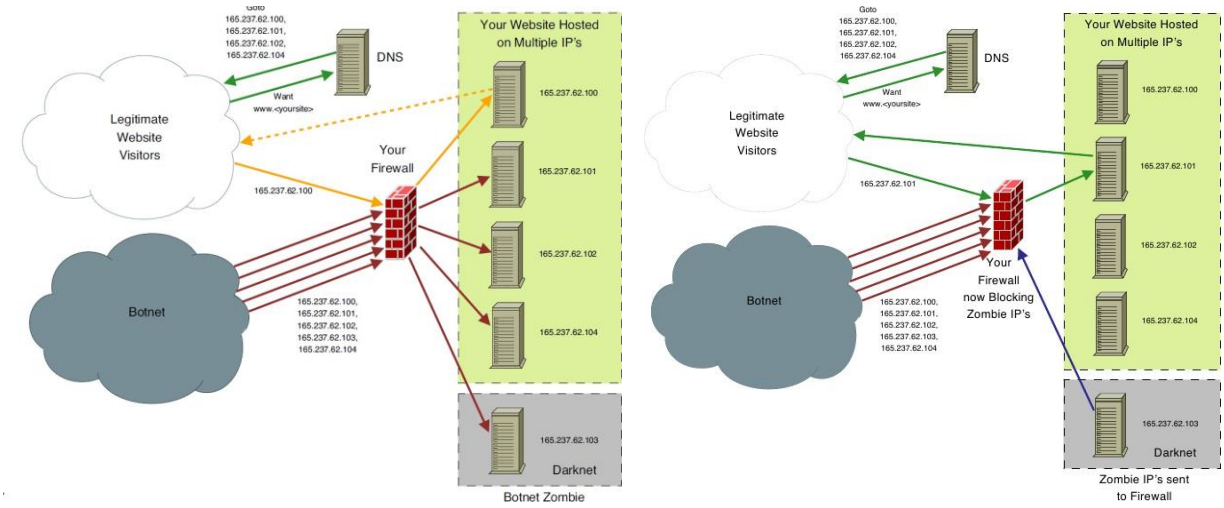
Ez a támadási hatás csökkentésére irányuló módszer arra törekszik, hogy a tartalmat olyan módon formázza meg, amely lehetővé teszi több különböző protokollon keresztül, és többféle alkalmazásokkal történő könnyű felhasználását. Fontos alkalmazni az MVC módszertant (modellezés, látvány, vezérlés - model, view, controller), mely az adatokat, az adatok feldolgozása és az adatok bemutatása szempontjából három különböző funkcióra választja. A DDoS támadás hatásainak enyhítésével összefüggésben ez lehetővé teszi, hogy az adatok terjesztés (elosztás) szempontjából mindig rendelkezésre álljanak különféle adathordozókon, ami biztosítja azok mindenkori elérhetőségét. Az ilyen védekezési stratégia kialakítása magába foglalja olyan weboldal tervezését, amely RSS-hez hasonló protokollokon keresztül valósítja meg a központi tartalom megosztását. Előre meg kell szervezni olyan csatornákat, amelyek a saját tartalmat más „szövetséges" weboldalak tartalmába ágyazzák. Ezáltal a weboldal tulajdonosa képes lesz biztosítani, hogy oldalát a felhasználók akkor is elérjék, amikor az oldal egy DDoS támadás miatt elérhetetlenné válik. Az RSS-hez hasonló protokollok szabványosítása és egyszerűsége lehetővé teszi más weboldal tulajdonosok számára, hogy gyorsan közzétegyék az ilyen csatornán keresztül érkező tartalmakat.



Distributed Content Strategy

Darknet-ek

Eltérően más stratégiáktól - amelyeket akkor lehet életbe léptetni, ha egy DoS támadás folyamatban van - a darknetek csak akkor működnek, ha egy DoS támadás elleni védelem céljából előre létrehozták azokat. Darknet létrehozásához előre meg kell vásárolni egy IP cím tartományt - például 165.237.62.100-105. A 100,101, 102, 104 és 105 címeket a weboldalt kiszolgáló szerverek példányaihoz kell rendelni és az IP címek e tömbjét kell konfigurálni a teljesítmény elosztón. Mivel a 103 nincs lefoglalva, megmarad darknetnek. A támadó a DNS lekérdezésekből látni fogja a lefoglalt IP cím tartományt és azt, hogy a weboldal e tartományra van elosztva. A támadó úgy konfigurálhatja támadását, hogy inkább az adott IP cím tartományt támadja, semmint a weboldal nevét, vagy URL-jét (pl. „sajatweb.org”). A támadó számára nem lesz ismert, hogy a tartomány darknet-et tartalmaz, ezért amikor a támadást indítja, lehetővé válik a 103-as IP című gép monitorozása. Bármilyen forgalom, ami ezen a címen látható, rosszindulatú forgalom. Így lehetővé válik, hogy azonosításra kerüljön bármilyen IP cím, amely támadja az adott szervert és beépítésre kerüljön (akár automatizált eljárással is) az upstream tűzfalba. Ez csökkenti a keresztüljutó támadó kliensek IP címeinek számát, ezáltal több erőforrást hagyva a webszervernek a legitim felhasználói kérések kiszolgálására.



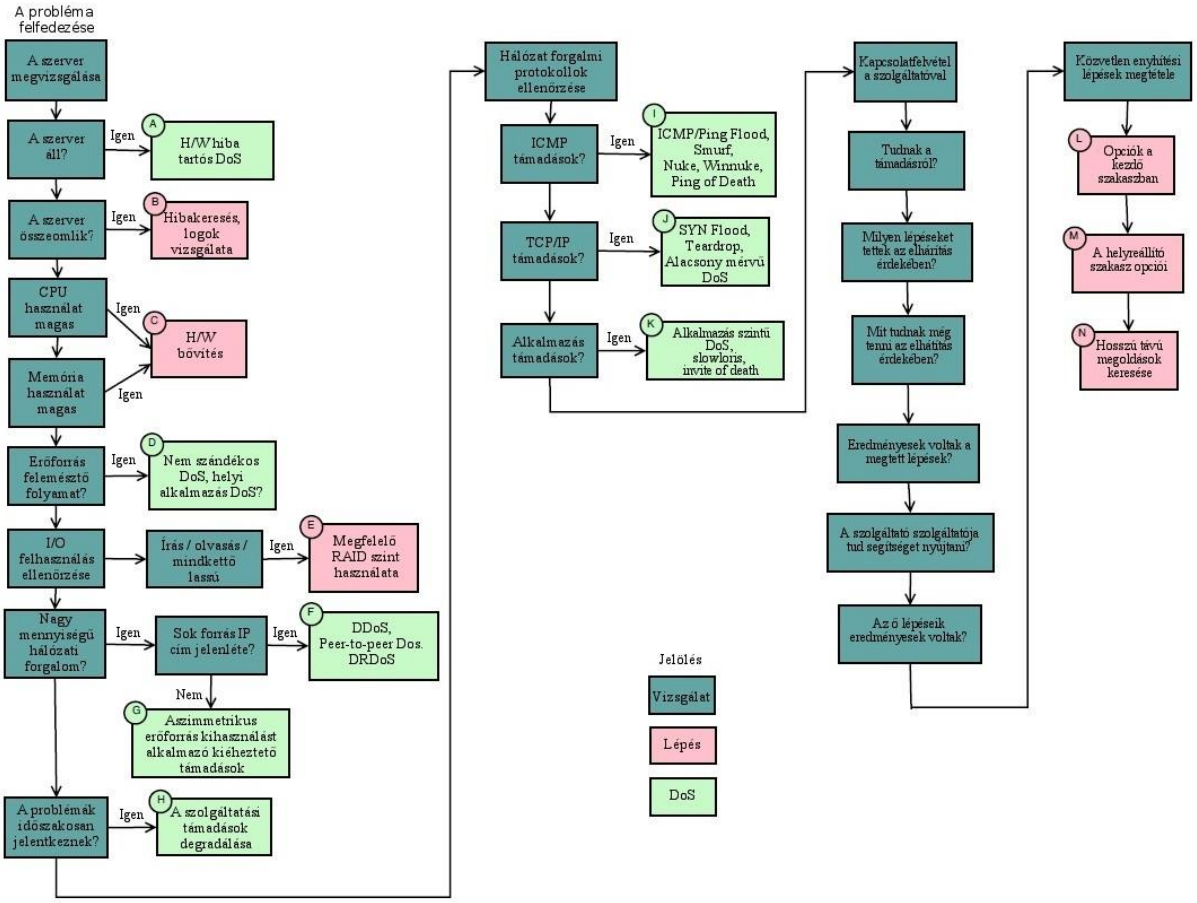
Második rész: DDoS támadásra történő reagálás

Az alábbi eljárás segíti a műszaki személyzetet a weboldal tartalmának újbóli elérhetővé tételében.

Minden kék színű lépést végig kell csinálni és minden, az azokban foglalt kérdésre kapott választ rögzíteni kell, mivel ezek a válaszok segíthetnek a támadás diagnosztizálásában.

A rózsaszínű lépések cselekvést igényelnek, legyen az a rendszer konfiguráció megváltoztatása, a hardver cseréje, vagy a jelen dokumentumban körvonalazott egy, vagy több DDoS támadás hatásait mérséklő stratégia bevezetése. A zöld lépések azokat a lehetséges DDoS támadásokat jelzik, amelyek az adott helyzetre vonatkozhatnak. Ezeket azért tartalmazza a dokumentum, hogy segítse a technikai személyzet további, az éppen tapasztalt helyzetre vonatkozó kutatás keresztmetszetének szűkítésében egyes specifikus DoS támadások esetében.

Minden számmal jelzett dobozhoz tartozik egy rövid leírás, amely a dokumentum további részében olvasható.



A reagálás folyamata

A. Hibás hardver, folytonos DoS támadás

Ellenőrizni kell a hardvert az összetevők szokásos hibáinak szempontjai szerint. A kábelek, a merevlemezek, a tápellátás, a RAM, alaplapok, CPU és hálózati kártyák kritikus összetevők, amelyek hibájából fakadóan a szerver offline üzemmódba kerülhet. Figyelembe kell venni azt, hogy létezik néhány olyan, folytonos DoS-ként ismert támadás, amelyek kihasználják a hardver, illetve a firmware sérülékenységeit hogy „befalazzák” (brick) - javíthatatlanul tönkre tegyék - a hardvert (általában úgy, hogy egy hamis (bogus) programot írnak a hardver eszköz ROM chip-jébe). Amennyiben a hibás hardver cseréje után az továbbra is hibásnak tűnik, akkor lehetséges, hogy az DDoS támadás alatt áll.

B. Hibakeresés beállítása, naplózási folyamat az összeomlás elemzéséhez

Amennyiben egy szerver gyakran összeomlik, akkor lehet, hogy néhány naplózó eljárás hibakereső szintjét alacsonyabbra kell állítani. Ez segíthet a probléma elemzésében, úgy, hogy megtekinthetővé válik mi is került a naplóba közvetlenül az összeomlás előtt.

C. A hardver bővítés (upgrade)

Amennyiben a tapasztalt szolgáltatás megtagadás úgy jelentkezik, hogy a webszerver számítási kapacitása, vagy a memóriája kevésnek bizonyul, akkor a CPU, vagy a RAM bővítése ideiglenesen azonnali segítséget jelenthet. Néhány szolgáltatás megtagadó támadás nem volumetrikus, hanem arra tesz kísérletet, hogy lokálisan emésszе fel a rendelkezésre álló erőforrásokat (CPU, RAM).

D. Nem szándékos DoS, helyi alkalmazás DoS

Minden véletlenszerű szolgáltatás megtagadás nem szándékos DoS támadásnak minősíthető. Ezt bármi okozhatja, a rosszul konfigurált helyi alkalmazástól kezdve egy gyengén megírt saját program, a patch panelből egy technikus által tévesen kihúzott kábel, vagy egészen a „Slashdot hatás”-ig[1]. Javasolt tehát olyan jelek keresése, amelyek például a weboldal nem tervezett promóciójának hatására hirtelen megnőtt legitim látogatói forgalmat jelzik. Továbbá szükséges keresni a Helyi Alkalmazás DoS jeleit, mint amilyen például a „Fork bomb” (elágazó bomba). Amennyiben ilyen alkalmazás fellelhető, akkor ezt követően kell keresni hacker tevékenységre utaló bizonyítékot. Lásd még (K) pont.

E. RAID alkalmazása a sebesség növelése céljából

A Redundant Array of Independent Disks (független merevlemezek redundáns tömbje - RAID) egy hibatűrést és a különböző típusú diszk hozzáférések hatékonyságát támogató, széles körben alkalmazott technológia. Többek közt lehetőséget adhat párhuzamos írásra, olvasásra, ami növeli az I/O (input-output) teljesítményt. A Wikipedia-ban megtalálható a különböző RAID szintek összehasonlítása és a merevlemezek I/O teljesítmények elméleti javítása (http://en.wikipedia.org/wiki/RAID).

F. DDoS, Peer-to-peer DoS, DRDoS

Néhány volumetrikus szolgáltatás megtagadásos támadás típus. SYN csomag elárasztást, vagy hasonlót alkalmazó DDoS; ADC protokollt, vagy hasonlót használó fájl megosztó hálózaton keresztüli peer-to-peer DoS, elosztott reflektív DDoS (Distributed Reflected Denial of Service), mint például az ICMP echo request/SMURF támadások, vagy a DNS amplifikációs támadások. A támadások természetétől függően a védekezés az általuk használt portok egyszerű letiltásától a bonyolultabb intézkedésig terjedhet (például, ha a támadó forgalom nem különböztethető meg a legitimtől).

G. Aszimmetrikus erőforrás kihasználást alkalmazó „kiéheztető” (starvation) támadások

Az ilyen támadást általában nagy teljesítményű géppel hajtják végre A kiéheztetés irányulhat a hálózati sávszélesség, a számítási teljesítmény, az egyidejű kapcsolatok maximális száma, vagy egyéb erőforrás ellen.

[1] A slashdot.org webhelyről kapta nevét, ahol geek-ek számára érdekes cikkeket tettek közzé, aminek közvetlen hatására a weboldal olvasói azonnal le tudták állítani bármelyik hivatkozott website-ot!

H. Szolgáltatások degradálására irányuló támadások

Ezen támadások jellemzője, hogy valamely DoS támadást közbeékelődő szünetekkel valósítanak meg annak érdekében, hogy a weboldal hibájának felderítését szolgáló kezdeti erőfeszítéseket meghiúsítsák. A felhasználók nehézségeket tapasztalnak a weboldal elérésben, de mire képesek lesznek a problémát jelezni a weboldal műszaki személyzete felé, addigra a támadás megszűnik, így amikor a műszaki személyzet megnézi a szervert, minden normálisnak tűnik. Ez a „minta" mindaddig fennmarad, amíg a szakemberek el nem kezdik a weboldal folyamatos figyelését.

I. ICMP/Ping Flood, Smurf, Nuke, Winnuke, Ping of Death

Sokféle ICMP támadás létezik, ezekből néhány a legrégebbi és leginkább használt DoS támadási módszerekből áll. Amennyiben az ICMP nem fontos az adott környezetben, akkor az ICMP forgalmat el kell dobni a tűzfalon.

J. SYN Flood, Teardrop, lassító DoS

Ezek mind a TCP/IP protokoll elleni támadások. A legtöbb operációs rendszerben már van megoldás a SYN elárasztás és a teardrop támadások ellen, így tehát gondoskodni kell arról, hogy ezek a mechanizmusok a kernel részét képezzék. A lassú (low rate) DoS támadás a TCP/IP protokollt használja ki arra, hogy elérje a szerver áteresztőképességének csökkenését. Továbbá esetenként napvilágra kerülnek olyan új támadások, amelyek a TCP/IP networking stack gyenge megvalósítására támaszkodnak. A stack-fejlesztők általában gyorsan adnak ki javító csomagokat (patches), de addig is szükséges lehet a támadások hatásainak mérséklésére különböző intézkedések végrehajtásával.

K. Alkalmazás szintű DoS, slowloris, invite of death stb.

Az alkalmazás szintű DoS támadások szimptómái gyakran tartalmazzák a rendszer összeomlást és zárolást (lockup), a CPU, vagy a RAM 100%-os kihasználtságát, vagy az alkalmazás protokollal való visszaélést, de nem korlátozódnak csak ezekre. Az alkalmazás ellen irányuló támadásokat nehezen lehet megkülönböztetni a jogszerű forgalomtól. Ezek lehetnek például az adatbázis backend-jére küldött komplex SQL lekérdezések, amelyek magas CPU terhelést, vagy az adatbázisban nagy számú tranzakciós blokkokat generálnak, ami megakadályozza más adatbázis bejegyzések, vagy folyamatok elvégzését és ezáltal az adatbázis meghibásodását okozó összeomlást váltanak ki. A versenyhelyzet (race condition) és a „szál-éheztetés" (thread starvation) kihasználása gyakori eszköze ezeknek a támadásoknak. Az alkalmazás szintű támadások másik sajátos példái a HTTP POST DoS, az invite of death és a slowloris.

A TCP protokoll feletti alkalmazásszintű támadások a kapcsolat felépítés miatt (TCP handshake), nem működnek hamisított (spoofing) IP címek használatával. Emiatt érdemes a támadásban résztvevő IP címeket ideiglenes tiltólistára felvenni.

L. Opciók a kezdő szakaszban

Léptesse életbe a kezdő szakasz opcióit az útmutatóban leírtak szerint.

M.A helyreállító szakasz opciói

Léptesse életbe a helyreállító szakasz opcióit az útmutatóban leírtak szerint.

N. Hosszú távú megoldások keresése

Léptesse életbe a helyreállító szakasz opcióit az útmutatóban leírtak szerint.

A szolgáltatás megtagadási támadás enyhítésének szakaszai

Egy DDoS támadás alatt álló weboldal esetében érdemes a védekezést három szakaszra tagolni, hogy a weboldal mielőbb online állapotba kerüljön. Ezek a szakaszok név szerint a kezdeti szakasz, a helyreállító szakasz és a hosszú távú szakasz. Kulcsfontosságú szem előtt tartani a következőt: az upstream szolgáltatóknak feltétlenül érdeke a védekezésben való közreműködés a weboldal üzemeltetőjével. Amennyiben az adott hely volumetrikus támadás alatt áll, akkor az kihat a szolgáltató sávszélességére is és nem csak az adott weboldalt fogja érinteni, hanem más felhasználók weboldalait/ hosztolt szolgáltatásait is. Ezért mindenkinek alapvető érdeke, hogy egymással hatékony kommunikációt folytassanak. Az upstream provider számára egyértelmű kell legyen, hogy a szolgáltatás előfizetőjének szándékában áll a szolgáltatóval együttműködni az ilyen támadások mielőbbi elhárítása érdekében.

Kezdeti szakasz

A helyreállítás kezdeti szakaszának célja, hogy a tartalom jelentős része visszakerüljön és elérhetővé váljon, miközben folytatódik a támadás teljes elemzése. A tevékenység jelentheti a weboldalon fellelhető témakörök teljességének romlását. Jelentheti azt, hogy a tartalom az alacsony látenciának és a nagy sávszélességnek nem (az eredetivel) azonos szintjein érhető el, de bizonyosan jelenti azt, hogy a tartalom lekérdezhető, megtekinthető. Jelentheti, hogy a tartalom nem a szokásos formátumában, vagy a szokásos dinamikus formátumában érhető el. Az adatok lehetnek statikusak, egyszerűsítettek, vagy esztétikailag egyszerűbb formátumúak, de az adatoknak elérhetőeknek kell lenniük addig is, míg a szokásosra jobban emlékeztető weboldal helyre nem állítható. A kezdeti szakasz részét kell képeznie a DDoS támadás elemzésének is. Ez az elemzés folyhat a weboldal tartalmának helyreállításával együtt, és jelentős segítséget nyújthat ahhoz, hogy meghatározásra kerüljön a helyreállítási szakaszban választandó megközelítés. Az elemzés elvégzéséhez a webszerver hálózati interfészének snifferelése és a csomagok elemzése is hozzájárulhat. Ezt olyan eszközökkel lehet megtenni, mint például a Wireshark (http://www.wireshark.org/). A DDoS támadás hatásainak csökkentése segíthet a hatékony kárenyhítő válasz kialakításában.

A kezdeti szakasz stratégiái a DoS támadások enyhítésére

A szolgáltatás megtagadás elleni védelem külső fél segítségével (DoSP)

Amennyiben korábban nem került a szolgáltatás megtagadás elleni védelmi eljárás kialakításra és a támadás éppen folyamatban van, akkor a szolgáltatót célszerű megkérdezni, tud-e ajánlani bármilyen DoSP megoldást. Amennyiben a válasz nemleges, akkor az upstream szolgáltatóhoz kell fordulni a kéréssel. Minél „nagyobb" a szolgáltató, annál valószínűbb, hogy van kész megoldása DoSP szolgáltatás biztosításához. Mielőbb kezdeményezni kell a szolgáltatás igénybevételére irányuló megbeszéléseket annak érdekében, hogy a weboldalra irányuló forgalom még a szolgáltató hálózatába kerülése előtt megtisztításra kerüljön.

Tűzfalak használata

A DoS támadások hatásainak enyhítésekor nem szabad lebecsülni még a legegyszerűbb tűzfal hasznosságát sem. Bizonyos megfontolások szerint már késő, ha egy volumetrikus DoS támadás forgalma eljut az intézményi hálózatig. Amennyiben a tűzfal konfigurálható úgy, hogy a lehető legtöbb rosszindulatú forgalmat eldobja, akkor legalább maga a webszerver visszakaphatja kiszolgáló és feldolgozó teljesítményének egy részét, így a továbbjutó legitim lekérdezések ténylegesen kiszolgálhatók lehetnek.

A tűzfal ilyen irányú alkalmasságát a rosszindulatú forgalom többitől való megkülönböztetésének képessége adja. Lehetnek bizonyos körülmények a támadás szerkezetében, amelyek segítenek, vagy kihasználhatóak olyan taktikák bevetésére, mint a darknet (lásd fentebb), amik aktív szerepet játszhatnak a rosszindulatú és szabályszerű forgalom szétválasztásában. Amennyiben a forgalom elemzése azt mutatja, hogy a támadás túlnyomó részben egyetlen, vagy kis számú TLD-ről (Top Level Domain) érkezik, akkor az azokról érkező minden forgalmat blokkolni lehet a tűzfal segítségével. Ez meglehetősen durva intézkedés és valószínűleg némi járulékos kárt is fog okozni, de az enyhítés korai szakaszában ez elfogadható.

Drasztikus esetben szükség lehet a teljes „külföldről érkező" forgalom levágására, amelyet jellemzően a szolgáltatói hálózat BGP router-ei segítségével lehet megvalósítani. Ha a támadás volumene igényli, ez a megoldás hatékony, rövidtávú intézkedés lehet egy DDoS támadás ellen, mert a botnet-et alkotó „zombi" gépek valószínűleg nem a helyi TLD-ben találhatók meg, hanem a világ különböző pontjain elszórva. A helyi TLD kivételével minden más TLD blokkolása elérhetetlenné teszi a szolgáltatást a látogatók egy vélhetően szűk köre számára, azonban egy ilyen beavatkozást igénylő, nagy volumenű támadás esetén ez elfogadható lehet.

Amikor a DoS támadás hatásai enyhítésének taktikájaként tűzfalas megoldás kerül alkalmazásra, érdemes szem előtt tartani, hogy az upstream ágban minél távolabb tudjuk a tűzfalat elhelyezni, valószínűleg annál hatékonyabban fog segíteni a helyzet megoldásában. Ez a szolgáltatóval és annak upstream szolgáltatójával való megbeszélést igényel.

Nyílt szolgáltatói tükrök

Amennyiben az előkészítő szakaszban végzett munka nyomán ez még nem áll rendelkezésre, akkor a lehető leggyorsabban célszerű létrehozni tükör másolatot egy nyílt szolgáltatónál.

Ez egy népszerű megoldás a DDoS támadás alá kerülő weboldalak számára, mert igen hatékonyan lehet egy weboldal tartalmát visszaállítani és azt elérhetővé tenni - ami a kezdeti szakasz célja. Az ilyen típusú tükrözésre vonatkozó további információkért, lásd jelen dokumentum „Felkészülési szakasz” részét.

Megosztott tartalom

Amennyiben a felkészülési szakaszban létrejött a mechanizmus, akkor azt most életbe kell léptetni és megkezdeni a tartalom megküldését, annak érdekében, hogy a társ weboldalakon ez megjelenjen, akár csak részben is. Amennyiben nem történtek előzetes megállapodások a tartalom publikálását szolgáló csatornákat illetően, akkor a DDoS támadás idején meg kell kérni más weboldalak tulajdonosait és/vagy üzemeltetőit, hogy RSS csatornát használva ágyazzák be a tartalmat.

Darknet

Amennyiben a felkészülési szakaszban létrejött, akkor most szükséges aktiválni a mechanizmust. Ez vagy működik majd, vagy nem, attól függően, hogy a támadó által használt szoftver végez-e DNS lekérdezést a weboldal irányába, vagy sem.

Lemondás a domainről

Ez nagyon drasztikus intézkedés, és valószínűleg csak nagyon rövid ideig tartó előnyei lesznek a DDoS támadás hatásainak enyhítésében. A stratégia azon alapul, hogy a weboldalt vagy nem a megszokott domain névhez kapcsolódó IP címeken hosztolják, vagy azt más domain néven teszik elérhetővé. A támadó valószínűleg rövid idő után észreveszi, hogy a weboldalt áthelyezték és az új IP címet/címeket, vagy domain nevet/neveket hozzáadják a támadás konfigurációjához. Ez csak rövid idő-ablakot biztosít arra, hogy a látogatók hozzá tudjanak férni a tartalomhoz. Ennek a stratégiának a legnagyobb kihívása, hogy gyors és kreatív módszereket kell találni a látogatók tájékoztatására, hogy hol találják meg a tartalmat.

Helyreállító szakasz

A helyreállító szakasz célja, hogy a weboldal újra eredeti formájában és képességeinek teljességével legyen elérhető a felhasználók számára. Ebben a szakaszban a weboldal esetleg nagy válaszidővel érhető el, vagy szakaszosan működőképes, de a felhasználók számára már a teljes tartalom elérhető.

A helyreállító szakasz stratégiái a DoS támadások hatásainak enyhítésére

A hosztolás helye

Amennyiben a weboldal hosztolására választott földrajzi hely a túlterheléses támadások elleni védelem szempontjából rossz választásnak bizonyult, akkor célszerű lehet a weboldalt máshová költöztetni. Ez jelentheti az egyik szolgáltatótól egy másikhoz, vagy egy tengeren túli szolgáltatótól egy helyi szolgáltatóhoz való áthelyezést, a pillanatnyi hosztolási helyzet függvényében, vagy akár a látogatók többségének földrajzi elhelyezkedésétől.

Jelen dokumentum „Első rész: Felkészülési szakasz” részében olvasható további információ a hosztolás helyszínével kapcsolatban.

Terhelés megosztott tükrözés

Ahhoz, hogy a weboldalt a szokásos megjelenéssel és képességekkel jobban összhangban álló formában helyezzék ismét működésbe, elképzelhető, hogy gyorsan létre kell hozni egy terhelés megosztott tükör megoldást. Jelen dokumentum „Első rész: Felkészülési szakasz” részében olvasható további információ a terhelés megosztott tükrökkel kapcsolatban.

Nagy sávszélességű tükrök

Volumetrikus DoS támadás idején valószínűleg ez az egyik leggyorsabban megvalósítható, a helyreállítást célzó megoldás. Jelen dokumentum „Első rész: Felkészülési szakasz” részében olvasható további információ a nagy sávszélességű tükrökkel kapcsolatban.

Hosszú távú szakasz

A hossztávú szakasz célja, hogy a teljes funkcionalitású weboldal teljesítménye teljes mértékben és legalább eredeti képességeinek megfelelően helyreállításra kerüljön.

Hosszú távú stratégiák a DDoS támadások hatásainak enyhítésére

Külső fél által biztosított védelem a szolgáltatásmegtagadás ellen

Nem kérdéses, hogy az egyetlen valóban szilárd megoldás a DoS és DDoS támadások teljes spektruma elleni védelemre a külső féltől igényelhető szolgáltatás. Lehet, hogy az adott pillanatban ez drága, de ahhoz, hogy bármilyen túlterheléses támadáskor „vonalban maradhassunk”, ez az egyetlen, ami biztosíthatja a sikert. Ezért a hosszú távú stratégia célja a túlterheléses támadás elleni védelem bevezetése és alkalmazása.

Konklúzió

A weboldalak DDoS támadás fenyegetése nagyon valós és a közeljövőben valószínűleg egyre hétköznapibb eszköz lesz. Amennyiben lehet, fel kell készülni a DDoS támadásra az erőforrások és a kockázat függvényében. Amennyiben a weboldalt támadás éri, igyekezni kell a pánikot elkerülni. Ha a személyzet követi a jelen útmutatóban felvázolt lépéseket, bizonyosan képesek lesznek a reagálás szakaszain végighaladni, hogy szakaszosan helyreállítsák a látogatók számára értékes szolgáltatást.