Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

Védekezés a szolgáltatás megtagadásra irányuló támadás ellen

2012. január

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalomjegyzék

Egyre több olyan cikk jelenik meg a világsajtóban, amelyben arról lehet olvasni, hogy nagy hírnevű vállalatok, kormányzati szervek és/vagy intézmények weboldalait tették elérhetetlenné. A PTA CERT-Hungary (Nemzeti Hálózatbiztonsági Központ) az alábbi dokumentumban ismerteti a szolgáltatás megtagadásos (DoS) támadásokkal kapcsolatban a legfontosabb információkat, amivel segíthet felkészülni egy ilyen támadás megelőzésében, felismerésében és az esetleges károk enyhítésében. A dokumentum a

https://www.accessnow.org/page/-/docs/Defending_Against_Denial_of_Service.pdf alapján készült.

Bevezetés

A civil társadalom napjainkban jelentős kiber-fenyegetésekkel néz szembe. A lista csúcsán a szolgáltatás megtagadásra (DoS – Denial of Service) irányuló támadások állnak. Számos szervezet és magánszemély weboldala volt már célpontja ilyen támadásnak és a támadások gyakorisága egyre növekszik. A szervezetek gyakran nem rendelkeznek elegendő erőforrással, vagy megfelelő műszaki ismeretekkel a támadások kivédésére vagy a lehetséges károk enyhítésére, ezért a DoS támadások veszélye valószínűleg nem szűnik meg a közeljövőben.

DoS támadás minden olyan támadás, amely eláraszt egy webhelyet és ezáltal a normál körülmények között szolgáltatott tartalmat elérhetetlenné teszi a felhasználók számára.

Az elosztott szolgáltatás megtagadás támadások (DDoS – Distributed Denial of Service) azok a mennyiségen alapuló (rate-based) támadások, amelyek nagy számú számítógépről, - általában fertőzött munkaállomásokról - érkeznek. Ezek a „zombinak” nevezett munkaállomások széleskörűen elosztott támadó hálózatot, „botnet”-et alkotnak. A DoS támadások ellen könnyebb védekezni, ha a támadást okozó mechanizmus ismerete rendelkezésre áll, ezért kiemelkedően fontos a támadó szándékú forgalom megfelelő elemzése, amikor weboldal képtelenné válik normális funkcióinak ellátására.

Jelen útmutatónak két része van. Az első rész körvonalazza a szükséges lépeseket egy támadás esetén a weboldaluk rugalmasságának növelése érdekében. Tudható, hogy a legtöbb szervezet akkor találkozik először DoS támadással, amikor egyszerre csak önmaga válik egy ilyen támadás áldozatává. Jelen útmutató második része bemutatja azt a folyamatot, amely lépésről lépésre segíti a szervezeteket a helyzet hatékony kezelésében.

Stratégiák	Előkészítő szakasz	Kezdőszakasz	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.

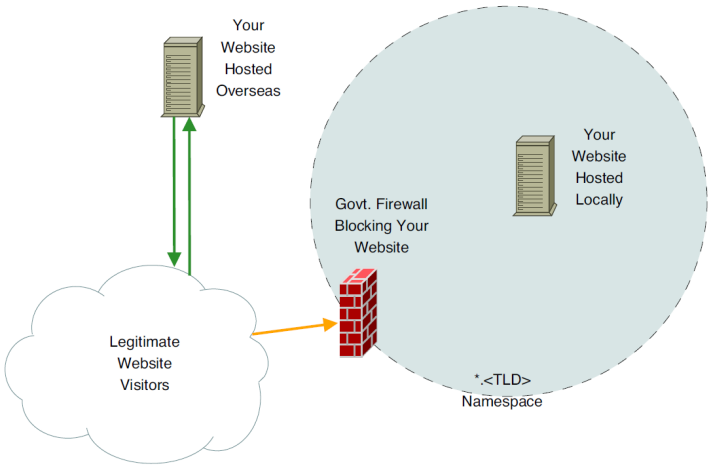
**Ha előre összeállításra került (az Előkészítő szakaszban), akkor ezt a rugalmassági stratégiát ebben a szakaszban kell érvénybe léptetni.

Első rész: előkészítő szakasz

A legtöbb DoS támadás hatásainak mérséklési stratégiáját célszerű jóval idő előtt érvényre léptetni. Néhány stratégiát, mint amilyenek a különféle oldal tükrözések (site mirroring) célszerű a normál működés részeként implementálni, függetlenül attól, hogy az oldal támadás alatt áll-e, vagy sem. Ezek a stratégiák olyan architektúrák, amelyek a weboldal elérése és teljesítménye szempontjából éppúgy jónak mondhatóak, mint a rugalmasság szempontja a DoS támadásokkal szemben. Többen más stratégiákat is megszerveznek, de azok „alvó” állapotban maradnak mindaddig, míg a weboldalt DoS támadás nem éri. A darknet-ek mindenképpen ebbe a kategóriába tartoznak éppúgy, mint a megosztott tartalomnak rugalmassági stratégiaként való használata (inkább, mint az elérést biztosító stratégia).

A hoszting helyszíne

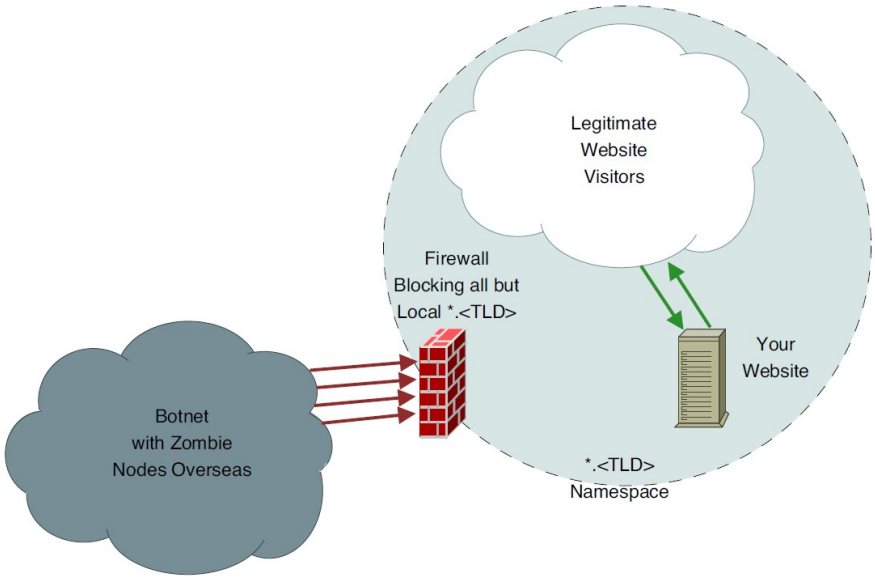
A weboldal elhelyezésének választott földrajzi helyszíne fontos tényező lehet a weboldal befolyásolására törekvő ellenfelek számára. Ezért ajánlott a weboldal elhelyezésére választandó helyszínt jó előre alaposan megfontolni.



Overseas Hosting Location Strategy

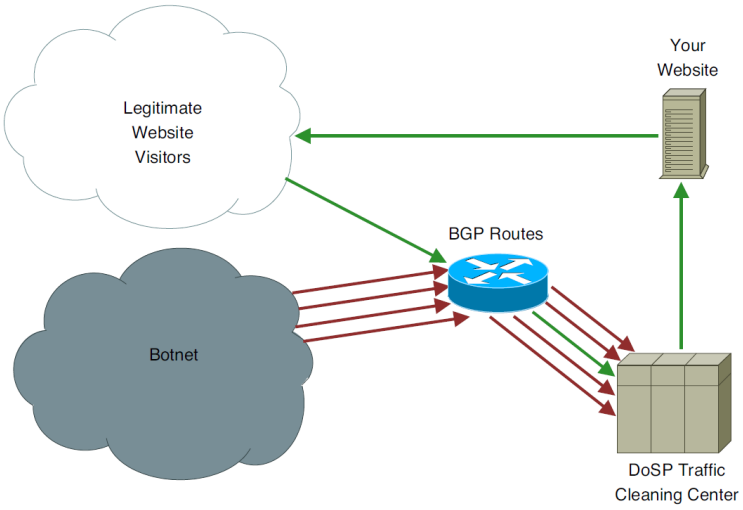
Helyi hoszting helyszínének stratégiája

Amennyiben a támadó a feketepiacon bérelhető botnet-ek szolgáltatásait veszi igénybe a weboldal támadásához, akkor igen valószínű, hogy a botnet-et felépítő „zombi” gépek túlnyomó többsége az ország legmagasabb szintű domain-jén (TLD) kívül helyezkednek el. Ezért lehetőség van arra, hogy a DDoS támadás hatásának mérséklése megoldódjon egyszerűen úgy, hogy a tűzfal segítségével eldobásra kerül minden upstream forgalom, ami nem az országon belüli számítógépektől származik. Ez nem befolyásolja a weboldal elérhetőségét a hazai látogatók számára.



Local Hosting Location Strategy

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



Third Party Denial of Service Protection Strategy

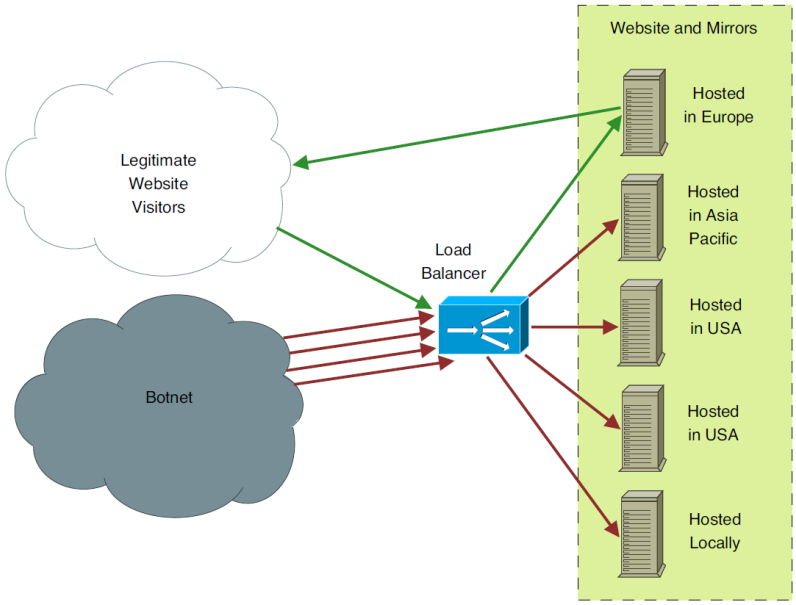
A hoszting szolgáltató kiválasztásakor figyelembe szükséges venni venni a kiválasztandó szolgáltató DoSP lehetőségeit és szolgáltatásait. A hoszting szolgáltató szintjén számos formája lehet a DoSP lehetőségének. Néhány alapvető DoSP opció lehet a sávszélesség rövid távú megnövelésére vonatkozó szolgáltatási garancia, ami által a weboldal meg tud birkózni a mennyiségen alapuló (rate-based) DoS támadásokkal. Azok a globális szolgáltatók, melyek megállapodást kötöttek a világ nagy telekommunikációs (Telco) cégeivel képesek lehetnek erősebb DoSP lehetőségeket nyújtani, mivel ezek a megállapodások lehetővé teszik számukra hogy „megtisztítsák” a bejövő forgalmat, vagy a forráshoz közelebb állítsák meg a támadást, semmint megvárnák, hogy a támadás elérje azt a hálózatot, melyben a weboldal hosztolva van. 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 nagy számú ügyfélnek. Ezek a közvetítők sok esetben képesek a legjobb DoS védelmet méltányos áron biztosítani. A DOSarrest például egy ilyen DoSP szolgáltató (http://www.dosarrest.com/).

Tükrök készítése

A weboldalak tükrözésének célja, hogy a tartalom több, különböző földrajzi elhelyezkedésű szolgáltatónál kerüljön megosztásra és megtöbbszörözésre. A sávszélesség elosztásával a weboldal tartalma megfelelő rugalmasságot nyerhet a romboló eseményekkel szemben, legyenek azok helyi természeti, vagy politikai jellegűek, vagy rosszindulatú tevékenység. Így felépítve a weboldalt az könnyen összecsomagolható, költöztethető, telepíthető és újratelepíthető, tehát a tükör oldalak létrehozása nagyszerű megoldás az esetleges DoS támadások hatásainak enyhítésére. Ahhoz, hogy a weboldal így épüljön fel, végig kell gondolni az oldal felépítésére és üzemeltetésére használt technológiákat. 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 kihívás a tükrözés előkészítésekor, hogy meg legyen határozva a módja annak, hogy hogyan legyen tesztelve a tükör olyan körülmények között, amilyenek egy folyamatos DoS támadás alatt tapasztalhatók. 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 annak működésképességét ellenőrizni.



Ez a mód megoldás lehet a problémára, mielőtt ezt egy valóságos támadás sokkal szélsőségesebb körülményei között kéne megtenni. Ezt a tesztet azonban nem szabad elfelejteni egyetlen próba után. A tesztnek egy rendszeresen ütemezett eseménynek kell lennie, mivel a környezet, a weboldalt felépítő összetevők és a háttérben tárolt adatok mind-mind gyakran változnak.

Kiegyenlített terhelésű 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 terhelésmegosztásos tükrözését lehetséges a DoS támadásokra való felkészülés keretein belül elvégezni, de tekintettel a terhelésmegosztó megvalósításából fakadó további bonyolultságra és a weboldal több példányának több szolgáltatónál való elhelyezésének költségeire, ezt gyakran elkerülik mindaddig, amíg egy tényleges DoS támadás meg nem nem indul a weboldal ellen. Az ilyen típusú tükrözés használatához meghatalmazás és a DNS rekordok módosításainak elvégzéséhez szükséges információk szükségesek. Ilyen például a rendszergazdai jogokkal üzemeltetett teljesítmény kiegyenlítő technológia, vagy ha konfigurációt az egyik szolgáltató által a szolgáltatás részeként biztosított terhelésmegosztó eszközéhez hozzáadjuk. Ilyen terhelésmegosztó eszközökre példa az F5 router és a „reverse proxy”.

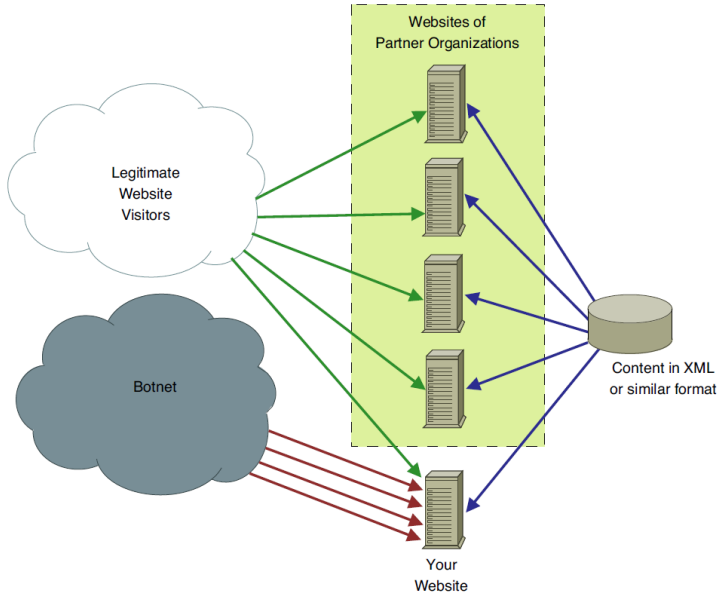
Nyílt szolgáltatói tükrök

Az egyik tényező, ami a nyílt szolgáltatókat olyan népszerűvé teszi a polgári társadalom számára a weboldalak tükrözésében az, hogy rendszerint ingyenesek vagy olcsóak. A nyílt szolgáltatói weboldal tükör lényegében a szolgáltatásként biztosított tartalom-közzétevő keret, mint amilyen például a Wordpress, vagy a Facebook. Ezek a szolgáltatók azért jók a DoS elleni védekezés szempontjából, mert tényleg hozzáférésük van teljes sávszélességben az erőforrásokhoz, amit érzékelhetően előszeretettel vesznek igénybe, ha a rendszerükben egy felhasználói fiók jelentős mennyiségen alapuló (rate-based) DoS támadás alá kerül. 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 szállításához. 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 DoS támadás.

Nagy sávszélességet nyújtó szolgáltatók

Van egy másik megoldás a nagy sávszélességet nyújtó szolgáltatók számára, ami felhasználható a DoS támadások hatásainak enyhítésére. Ezek a nagy sávszélességet nyújtó szolgáltatók sok esetben felhő (cloud) szolgáltatók is, amilyen például az Amazon és a Rackspace. Ezek a szolgáltatók 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 DoS támadás elleni védelemre való felhasználásakor a legfőbb megfontolás, hogy a kiválasztott felhő szolgáltató(k) olyan műszaki környezetet tud(nak) biztosítani, mely szükséges az adott weboldal tömörített változatának telepítéséhez és üzemeltetéséhez.

Megosztott tartalom

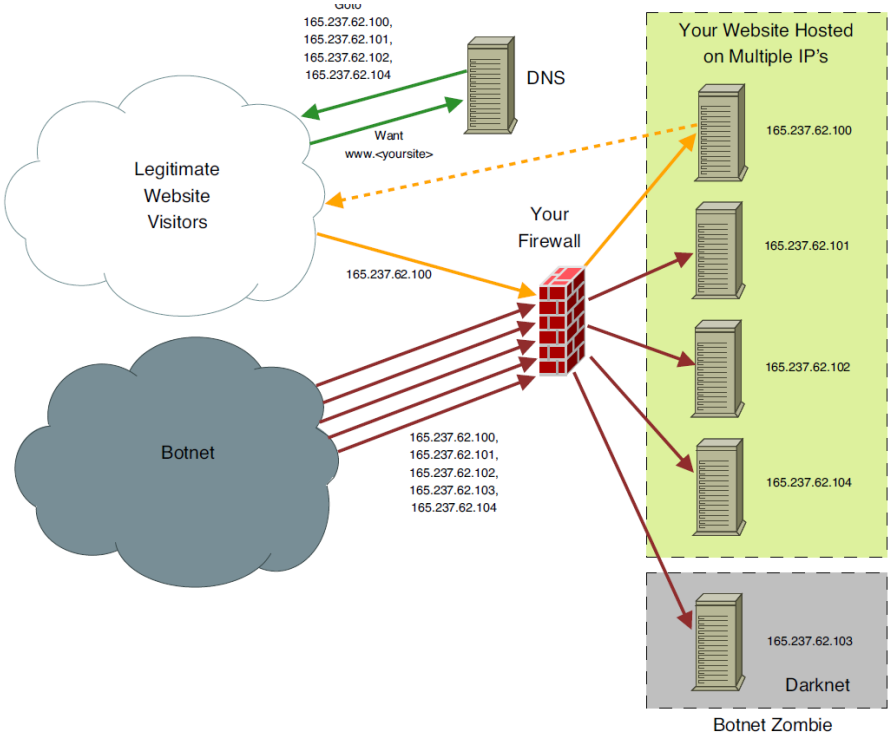


Distributed Content Strategy

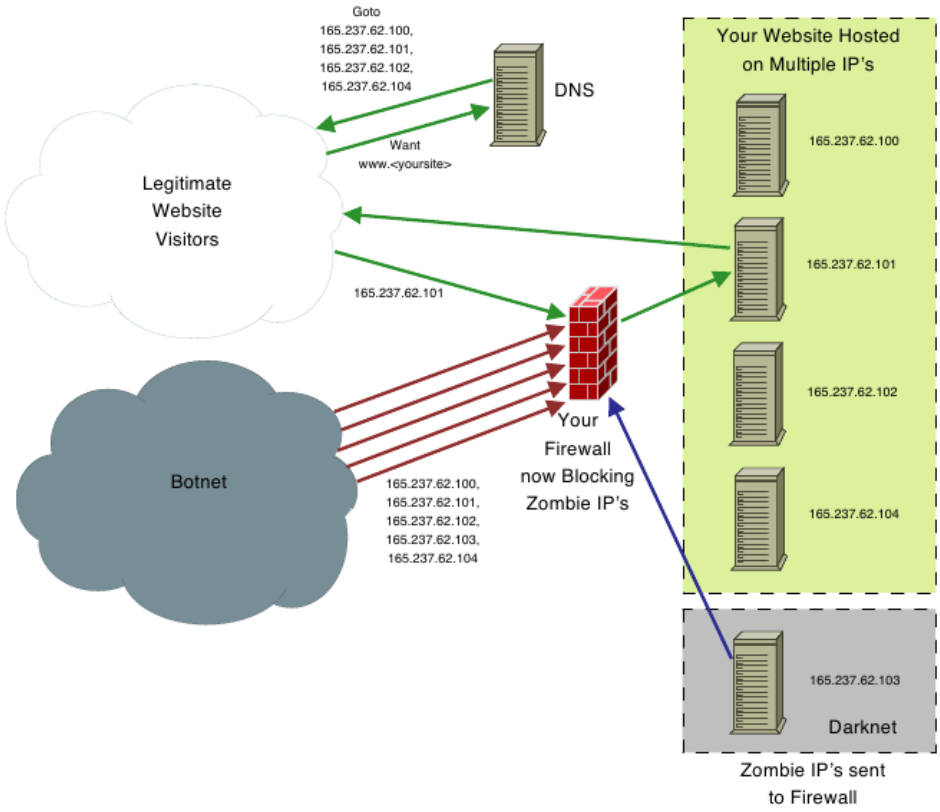
A DoS támadás hatásainak enyhítésének ez a formája arra törekszik, hogy a tartalmat olyan módon formázza meg, amely lehetővé teszi több különböző protokollon keresztül, és többféle alkalmazásokkal történő könnyű felhasználását. Fontos alkalmazni az MVC módszertant (modellezés, látvány, vezérlés - model, view, controller), mely az adatokat, az adatok feldolgozása és az adatok bemutatása szempontjából három különböző funkcióra választja. A DoS 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 ágyazza. Ezáltal a weboldal tulajdonosa képes lesz biztosítani, hogy oldalát a felhasználók akkor is elérjék, amikor az oldal egy DoS támadás miatt elérhetetlen. Az RSS-hez hasonló protokollok szabványosítása és egyszerűsége lehetővé teszi más weboldal tulajdonosok számára, hogy gyorsan közzétegyék az ilyen csatornán keresztül érkező tartalmakat.

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 darknet-nek. 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. „sajátweb.org”). A támadó számára nem lesz ismert, hogy a tartomány darknet-et tartalmaz, ezért amikor a támadást indít, 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 keresztül jutó támadó kliensek IP címeinek számát, ezáltal több erőforrást hagyva a webszervernek a tényleges felhasználók tartalommal való kiszolgálására.

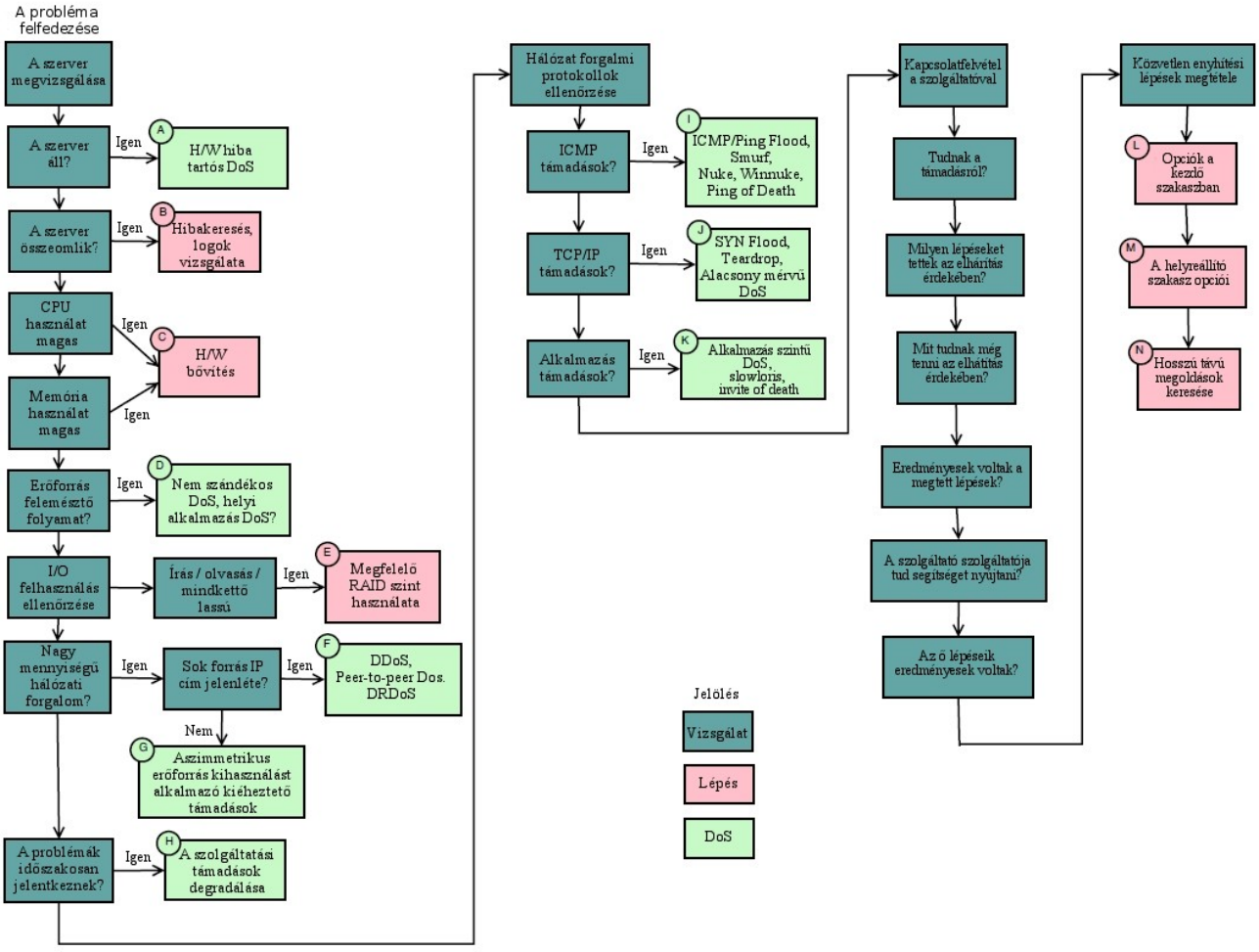


Második rész: reagálás egy DoS támadásra

A DoS támadások nyomasztóak. Nyomasztóak a weboldal látogatói számára, akik nem képesek elérni az oldal tartalmát. Nyomasztóak a szervezet személyzete számára, akik tudják, hogy üzenetük nem ér el a célközönség felé. Továbbá nyomasztóak a technikai személyzet számára is, akiknek az a feladata, hogy a weboldalt működőképes állapotban tartsák. Ezt szem előtt tartva a következőkben egy olyan könnyen követhető eljárás olvasható, amely segít a műszaki személyzetnek, hogy hatékonyan tudjon koncentrálni a weboldal látogatóinak számára az tartalom újból elérhetővé tételén.

Minden kék színű lépést végig kell csinálni és minden az azokban foglalt kérdésre kapott választ rögzíteni kell, mivel ezek a válaszok segíthetnek majd 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 DoS támadás hatásainak mérséklő stratégia bevezetése. A zöld lépések azokat a lehetséges DoS 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, amelyektől a szerver off-line 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 tönkretegyék - a hardvert (általában úgy, hogy egy utánzott (bogus) programot írnak a hardver eszköz ROM chip-jébe). Amennyiben a hibás hardver cseréje után az továbbra is hibásnak tűnik, akkor lehetséges, hogy az PDoS 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 enyhülést jelenthet. Néhány szolgáltatás megtagadó támadás nem mennyiségen alapuló (rate-based), hanem arra tesz kísérletet, hogy lokálisan eméssze fel az összetevők - például a CPU vagy a RAM - rendelkezésre álló erőforrásait.

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 (ami 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!). Tehát javasolt olyan jelek keresése, amelyeknek köszönhetően például a weboldal nem tervezett promóciójának hatására hirtelen megnőtt a jogszerű látogatók száma. Továbbá szükséges keresni a Helyi Alkalmazás DoS jeleit, mint amilyen például a „Fork bomb” (elágazó bomba). Amennyiben ilyen alkalmazás fellelhető, akkor ezt követően keresni kell a bizonyítékot a hacker betörésre. Lásd még (K) pont.

E. RAID alkalmazása a sebesség növelése céljából

A Redundant Array of Independent Disks (független merevlemezek redundáns tömbje - RAID) olyan technológia, mely szegmensekre bontja az adatokat, hogy azok több merevlemez között eloszthatóvá legyen, lehetővé téve a párhuzamos írást, vagy olvasást, ami növeli az I/O (input-output) sebességet. 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

Ezekből néhány mennyiségen alapuló (rate-based) szolgáltatás megtagadásos támadás. Ez lehet megosztott szolgáltatás megtagadás, SYN elárasztás, vagy hasonló; ADC protokollt, vagy hasonlót használó fájl megosztó hálózaton keresztüli peer-to-peer DoS, megosztott visszaverődő DoS (Distributed Reflected Denial of Service), mint például az ICMP visszhang-kérés/SMURF támadások, vagy a DNS amplifikációs támadások stb. A támadások természetétől függően az ezek ellen való védekezés az általuk használt portok egyszerű letiltásától a bonyolultabb intézkedésig terjedhet (például, ha a támadó forgalom nem különböztethető meg a jogszerűtől).

G. Aszimmetrikus erőforrás kihasználást alkalmazó kiéheztető (starvation) támadások

Az ilyen támadást általában nagyon erős, vagy nagy képességgel rendelkező géppel hajtják végre, amelyik elég ahhoz, hogy elnyomja a támadott webszerver teljesítményét. A kiválasztott képesség lehet a hálózati sávszélesség, a számítási teljesítmény, az egyidejű kapcsolatok maximális száma, vagy több más erőforrás.

H. A szolgáltatási támadások degradálása

A szolgáltatási támadások degradálása abból áll, hogy valamely DoS támadást szünet sorozatokkal 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 tűzfal segítségével.

J. SYN Flood, Teardrop, alacsony mérvű DoS

Ezek mind a TCP/IP protokoll elleni támadások. A legtöbb operációs rendszerben már van megoldás a SYN elárasztás és a teardrop (könnycsepp) támadások ellen, így tehát gondoskodni kell arról, hogy ezek mechanizmusok a kernel részét képezzék (ehhez a kernelt újra kell fordítani). Az alacsony mérvű (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 esetleg szükséges lehet a támadások hatásainak mérséklésére a lehető legjobban megtehető intézkedések végrehajtásával.

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

Az alkalmazásszintű 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 nehéz 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. Megjegyzendő, hogy a slowloris támadások megelőzésének egy egyszerű módja, ha a weboldalt Windows platformra kerül áthelyezésre, mivel a MS IIS nem érzékeny a támadásra. Az F5 terhelés-kiegyenlítő eszközök szintén enyhítik ezt a támadást, így tehát egy ilyen eszköz elhelyezése a hálózatban a weboldal elé hatásos lehet. A hálózat ellen lekövetett alkalmazás ellen irányuló támadások a teljes TCP handshake-et (kapcsolat létrejöttét) igénylik, ami azt jelenti, hogy a forrás IP címeket nem lehet hamisítani (spoof). Ez a tény

előnyként felhasználható, ha az adott forrás címeket naplózza és eljárások segítségével felveszi azokat a tűzfal szabályrendszerébe és ezt követően az adott címekről érkező minden forgalmat eldob.

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 DoS támadás alatt álló weboldal esetében érdemes az enyhítést 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 a DoS támadásokkal szembeni enyhítési szakaszától függetlenül, feltétlenül érdeke az enyhítésben való közreműködés a weboldal üzemeltetőjével. Amennyiben az adott hely mennyiségen alapuló (rate-based) támadás alatt áll, akkor az kihat a szolgáltató sávszélességére is és nem csak az adott weboldalt fogja érinteni, hanem más felhasználók weboldalait és hálózatait is. Ezért mindenkinek eminens érdeke, hogy együttműködően kommunikáljanak egymással. Gondoskodni kell arról, hogy az upstream szolgáltató tudjon erről. Tudatni szükséges, hogy a szolgáltatás előfizetőjének szándékában áll a szolgáltatóval együttműködni a probléma mielőbbi megoldása érdekében.

Kezdeti szakasz

A kezdeti szakasz célja, hogy a tartalomnak a lehetséges legnagyobb része vissza kerüljön 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 tartalmat kéréseken keresztül lekérdezhető és megkapható, így megtekinthető. Jelentheti, hogy a tartalom nem a szokásos formátumában, vagy a szokásos dinamikus formátumában érhető el. Az adatok lehetnek statikusak, egyszerűsítettek, vagy esztétikailag nem megfelelő 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 DoS 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 elfogása szükséges. Ezt olyan eszközökkel lehet megtenni, mint például a Wireshark (http://www.wireshark.org/). A szerverhez adminisztrátor szintű hozzáférésre lesz szükség, hogy a teljesítményét meg lehessen figyelni. A DoS 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 ellen védelmi eljárás kialakítása 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 az előző mondatban felvázolt kéréssel. Lehetséges, hogy egy nagyobb upstream szolgáltató képes a DoSP szolgáltatást alkalmazni. Minél „nagyobb" a szolgáltató, annál valószínűbb, hogy van kész megállapodása DoSP szolgáltatással történő munkára. Amennyiben kiderül, hogy ez a helyzet, akkor célravezető tárgyalásokat kezdeményezni, 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 mennyiségen alapuló (rate-based) DoS támadás éppen a saját hálózat előtt ér el egy eszközt. Amennyiben a tűzfalat lehet úgy konfigurálni, hogy a lehető legtöbb rosszindulatú forgalmat eldobja, akkor legalább maga a webszerver visszakaphatja kiszolgáló és feldolgozó teljesítményének egy részét, ami azt jelenti, hogy a továbbjutó szabályszerű lekérdezések ténylegesen kiszolgálhatók lehetnek. A szabályszerűen beérkező és kimenő forgalmaknak azért még meg kell majd „küzdeniük" a támadó forgalommal a sávszélességért, de csökkenteni lehet a változók számát a támadás egyenletében.

A tűzfal alkalmasságát a rosszindulatú forgalom a 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 igazolható.

Amennyiben a weboldalt a nemzeti TLD hosztolja és a látogatók túlnyomó része ugyanazon TLD-n belül található, akkor a helyi TLD kivételével minden más TLD-ről származó forgalom blokkolása egy újabb drasztikus intézkedés lehet. Ettől ez egy 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, különösen ha ez upstream ágban történik, a látogató közönség többségének elérhetővé teszi a tartalmat, míg a támadó forgalom nagy része számára nem.
Amikor a DoS támadás hatásainak enyhítésének taktikájaként tűzfalas megoldás kerül az előtérbe, akkor 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 DoS támadás alá kerülő weboldalak számára, mert igen hatékonyan lehet egy weboldal tartalmának formáját visszaállítani és azt tetszőleges sebességgel 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 rokon weboldalakon ez megjelenjen, akár csak részben is. Amennyiben nem történtek előzetes megállapodások a tartalom publikálását szolgáló csatornákat illetően, akkor a DoS 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 sem, 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 DoS támadás hatásainak enyhítésében. Ez a stratégia arra alapul, hogy a weboldalt vagy nem a megszokott domain névhez kapcsolódó IP címeken hosztolják, vagy azt más domain néven teszik meg. 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 weboldalt 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 DoS 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, függően a pillanatnyi hosztolási helyzettől vagy akár 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

Mennyiségen alapuló (rate-based) 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 teljesítményét teljes mértékben és legalább eredeti képességeinek megfelelően helyreállításra kerüljenek. E szakasz végére a weboldal képes lesz ellenállni bárminek, amit egy támadó a pillanatnyi támadás idején, vagy a jövőben ellene irányíthat.

Hosszú távú stratégiák a DoS támadások hatásainak enyhítésére

Külső fél által biztosított védelem a szolgáltatásmegtagadás ellen (DoSP)

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

Következtetés

A weboldalak elleni DoS támadás fenyegetése nagyon valós és a közel jövőben valószínűleg egyre hétköznapibb eszköz lesz. Amennyiben lehet, fel kell készülni a DoS támadásra, amennyire az erőforrások ezt megengedik. Amennyiben a weboldalt támadás éri, igyekezni kell a pánikot elkerülni. Amennyiben a személyzet követi jelen útmutatóban felvázolt lépéseket, bizonyosan képesek lesznek a reagálás szakaszain végighaladni, hogy szakaszosan helyreállítsák a látogatók számára értékes szolgáltatásokat.

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel.: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937