Co je DDOS, jak to funguje a jak se tomu bránit

DDOS

DDOS co je to?

- Distribuovaný denial-of-service útok je pokus, aby se stroj nebo síťový zdroj k dispozici.
- Ačkoliv provedení, cíle a motivy se mohou lišit, obecně jde o cíle jednotlivce nebo skupiny lidí.
- Mohou na určitou dobu vyřadit služby, které jsou nějakou dobu buď mimo provoz nebo je obtížné se k nim přihlásit.
- Např. Internetové připojení, online služby atd.

DDOS cíle

- Webové servery Bank
- Webové servery Online služeb (Facebook, Twitter, atd.)
- Internetové stránky firem
- Vládní webové servery
- Útoky na infrastrukturu internetu
- A mnoho dalších

Způsoby útoků DDOS

- Jeden ze základních útoků typu DDOS je zahlcení cílového počítače extrémním počtem požadavků na komunikaci.
- Počítač tak není schopen reagovat na legitimní provoz, nebo reaguje pomalu až v podstatě je nedostupný.
- DDOS útok jednoduše řečeno útok, který má za úkol zahltit cílový server, aby nemohl poskytovat svoje služby.

Jaké jsou symptomy a projevy I

- Neobvyklý pomalý výkon sítě.
- Nedostupná konkrétní webová stránka
- Neschopnost přistoupit k jakékoliv webové stránce.
- Dramatický nárůst počtu nevyžádaných e-mailů.
- Odpojení bezdrátového nebo kabelového internetu.
- Termín „hit offline“ se používá k odpojení od internetu.

Jaké jsou symptomy a projevy II

- DDOS útoky mohou také vést k problémům se sítí. Např. mohou mezi router a Internetem zmenšovat šířku pásma, díky tomu mohou ohrožovat nejen počítač, ale i celou síť.
- Pokud je útok proved ve velkém měřítku, může být v celé oblasti ohroženo internetové připojení.

METODY ÚTOKU

Metody útoku

5 základních typů útoků

1. Spotřeba výpočetních zdrojů, jako je šířka pásma, msto na disku a procesorový čas
2. Narušen informací o konfiguraci, jako jsou směrovací informace.
3. Narušení informace o stavu, jako je nevyžádané resetování relace TCP.
4. Narušení fyzických síťových prvků.
5. Bránění komunikaci mezi uživatelem a obětí.

Metodika útoků

Útok DoS může zahrnovat výkonný malware určený pro

- Maximální procesorové vytížení
- Trigger chyby v mikrokódu zařízení
- Trigger chyby v rozpisů pokynů, aby se počítač dostal do nestabilního stavu.
- Exploitování chyb v operačním systému
- Crash Operačního systému

Jednotlivé typy útoků

ICPM Flood

- Útok šmoula je jeden konkrétní varianta zaplavení DoS útoku na veřejného Internetu. Opírá se o nesprávně nakonfigurovaných síťových zařízení, která umožňují pakety mají být zaslány na všechny počítače hostitelům v určité síti přes broadcast adresu sítě, spíše než konkrétní stroj. Síť pak slouží jako zesilovač smurf. V takovém útoku, budou pachatelé posílat velké množství IP paketů s zdrojovou adresu falešné zdají být adresa oběti. Síť je šířka pásma je rychle vyčerpána, brání oprávněné pakety dostat až na místo určení. V rámci boje proti popření servisních útoků na Internetu, služby, jako je registr Zesilovač Šmoula dali poskytovatelů síťových služeb schopnost identifikovat špatne sítě a přijmout odpovídající opatření, jako filtrování .
- Ping povodeň je založena na posílání oběť ohromující počet ping paketů, zpravidla pomocí "ping" příkazu z unix-jako hostitelé (-t vlajka na Windows systémech je mnohem méně zdatní přemáhat cíl, i-l (velikost) flag neumožňuje odeslaný paket velikost větší než 65500 v systému Windows). Je to velmi jednoduché zahájit, základním požadavkem je přístup k větší šířku pásma , než oběti.

SYN flood

- SYN Flood nastane, když hostitel pošle záplavu TCP / SYN paketů, často s kovanou adresou odesílatele. Každý z těchto paketů je zpracována jako požadavek na připojení, což je server, aby se třeli půl otevřené spojení , tím, že vrátí TCP / SYN-ACK paket (Potvrdit), a čeká na paketu v odpovědi ze adresu odesílatele (odpověď na ACK paketů). Nicméně, protože adresa odesílatele je kované, odpověď nikdy nepřijde. Tyto polovina-otevřených spojení saturovat počet dostupných připojení serveru je schopen dělat, držet to od reagovat na legitimní požadavky až po útoku skončí.

Slza útoky

- Slza útok zahrnuje zaslání pozměněny IP fragmenty s překrývajícími se, přes-velké užitečné zatížení na cílovém počítači. To může selhat různé operační systémy z důvodu chyby v jejich TCP / IP fragmentace re-montážní kód. Windows 3.1x , Windows 95 a Windows NT operační systémy, stejně jako verze Linux před verzí 2.0.32 až 2.1 a 0.63ar náchylné k tomuto útoku.
- Kolem září 2009 zranitelnost v systému Windows Vista byl odkazoval se na jako "kapkovitý útok", ale útok cílený SMB2 , která je vyšší vrstva než TCP pakety, které slza použít.

Low-rychlost Denial-of-Service útoků

- Low-rate DoS (LDOS) útok využívá TCP je pomalu čas měřítku dynamiku převzatého časového limitu (RTO) mechanismy ke snížení TCP propustnost. V podstatě, může útočník způsobit tok TCP opakovaně zadat stát RTO zasláním high-sazba, ale krátký-trvání záblesky, a opakující se pravidelně na pomalejších časových škálách-RTO. Propustnost TCP na napadení uzlu bude významně snížena, zatímco útočník bude mít nízký průměrný kurz, takže je obtížné zjistit.

Peer-to-peer útoky

- Útočníci našli způsob, jak zneužít množství chyb v peer-to-peer serverů zahájit DDoS útoky. Nejagresivnější těchto peer-to-peer-DDoS útoky exploitů DC + + .Peer-to-peer útoky se liší od běžných botnet útokům. S peer-to-peer není botnet a útočník nemusí komunikovat s klienty se podvrací. Místo toho, útočník se chová jako "Loutkář," nabádá klienty velkých peer-to-peer sdílení souborů uzlů odpojit od jejich peer-to-peer sítě a připojit se k oběti stránkách místo. V důsledku toho může být několik tisíc počítačů agresivně snaží připojit k cílové stránky. Zatímco typický webový server může zpracovat několik set spojení za sekundu před představením začne snižovat, většina internetových serverů selže téměř okamžitě do pěti nebo šesti tisíc spojení za sekundu. S mírně velkým peer-to-peer útoku, by mohla být potenciálně stránky hit až 750.000 spojení v krátké době. Cílená webový server bude připojen do které příchozí spojení.
- Zatímco peer-to-peer útoky jsou snadno identifikovat s podpisy, velké množství IP adres, které musí být blokováno (často přes 250.000 v průběhu jednoho rozsáhlého útoku), znamená to, že tento typ útoku může přemoci zmírnění obranu. I když zmírnění zařízení může vést blokování IP adres, existují další problémy, aby zvážila. Například, tam je krátký okamžik, kdy je otevřeno připojení na straně serveru před podpisem samotné projde. Jen jednou připojení je otevřen k serveru může určit podpis bude odeslán a zjistil, a připojení stržena.Dokonce i stržení připojení trvá serverové zdroje a může poškodit server.
- Tato metoda útoku lze zabránit tím, když v peer-to-peer protokolu, které porty jsou povolené nebo ne. Pokud port 80 není dovoleno, lze možnosti útoku na webových stránkách je velmi omezený.

Asymetrie využití zdrojů v hladovění útoků

- Útok, který je úspěšný v náročné zdrojů na oběti počítači musí být buď:
- provádí útočník s velkými zdroji, buď:
  - ovládání počítače s velkou výpočetní výkon nebo, více obyčejně, velké propustnosti sítě
  - ovládá velké množství počítačů a směrovat je k útoku jako skupina. DDoS je primární příkladem.
- s využitím vlastnost operačního systému nebo aplikací na oběti systému, který umožňuje útok náročné mnohem více oběti zdrojů, než útočník je (asymetrický útok). Šmoula útok , SYN flood , Sockstress a nafty jsou všechny asymetrické útoky.
- Útok může využít kombinaci těchto metod, aby se zvětšit jeho sílu.

Permanentní denial-of-service útokům

- Trvalé denial-of-service (PDO), také známý jako volně phlashing, je útok, který poškozuje systém tak špatně, že to vyžaduje výměnu nebo přeinstalování hardwaru. Na rozdíl od Distributed Denial-of-service útok , útok CHOP využívá bezpečnostní chyby, které umožňují vzdálenou správu na řídících rozhraní oběti hardwaru, jako jsou směrovače, tiskárny nebo jiného síťového hardwaru .Útočník používá tyto chyby Chcete-li nahradit přístroje firmware s upraveným, zkorumpované, nebo vadného firmware image-proces, který po dokončení oprávněně je známý jako *blikající.* To proto " cihly "zařízení, které je činí nepoužitelnými pro své původní účely, dokud nebude možné být opraveny nebo vyměněny.
- CHOP je čistě hardwarové cílený útok, který může být mnohem rychlejší a vyžaduje méně prostředků než pomocí botnetu v útoku DDoS. Protože těchto vlastností, a potenciální a vysoká pravděpodobnost bezpečnostních exploitů na Network Enabled Embedded Devices (potřeby), tato technika se přišel k pozornosti mnoha hackerů komunit. PhlashDance je nástroj vytvořený Rich Smith (zaměstnanec Systems společnosti Hewlett-Packard Security Lab) pro detekci a prokázání CHOP zranitelnosti v roce 2008 EUSecWest Aplikovaná bezpečnostní konferenci v Londýně.

Použití úrovni povodně

- Různé DoS způsobující využije jako přetečení bufferu může způsobit server-running software zmást a vyplnit místa na disku nebo konzumovat všechny dostupné paměti nebo CPU čas .
- Jiné druhy DoS spoléhat především na brutální sílu, zaplavení cíl s ohromující tokem paketů, oversaturating jeho připojení šířku pásma, nebo vyčerpání cílového systémové prostředky. Bandwidth-nasycení povodně spoléhat na útočníka má větší šířku pásma k dispozici, než oběti, obyčejný způsob, jak toho dosáhnout je dnes přes Distributed Denial of Service, zaměstnávat botnet . Další povodně mohou používat specifické typy paketů či žádosti o připojení k nasycení omezené zdroje, například, zabírat maximální počet otevřených spojení nebo vyplněním oběti disku s logy.
- "Banán útok" je další zvláštní typ DoS. Jedná se přesměrování odchozí zprávy z klienta zpět na klienta, prevence mimo přístup, stejně jako zaplavení klienta s odeslaných paketů.
- Útočník s shell úrovni přístup k oběti počítači může zpomalit, dokud to je nepoužitelný, nebo zhroucení pomocí vidlice bombu .
- Druh na úrovni aplikace DoS útoku je XDoS (nebo XML DoS), které lze ovládat pomocí moderních webových aplikací firewall (WAFS).

Nuke

- Nuke je stará denial-of-service útok proti počítačovým sítím se skládá z roztříštěných nebo jinak neplatné ICMP pakety odeslané do cíle, dosažené pomocí modifikovaného ping nástroj opakovaně Poslat tento poškozená data, a tak zpomaluje ohrožený počítač, dokud se do úplného zastavení.
- Konkrétním příkladem útoku atomovku to získalo nějakou důležitost je WinNuke , který využíval zranitelnost v NetBIOS handleru v systému Windows 95 . String out-of-band dat byl poslán k TCP port 139 z oběti stroj, přimět to, aby zamknout a zobrazí modrá obrazovka smrti (BSOD).

RU-Dead-Yet? (RUDY)

- Tento útok je jedním z mnoha nástrojů webových aplikací typu DoS jsou k dispozici přímo zaútočit webové aplikace hladem dostupných relací na webovém serveru. Stejně jako Slowloris , RUDY udržuje zasedá v zastávce pomocí nekončící POST přenosy a odeslání libovolně velkou hlavičku Content-Length hodnotu.

pomalého čtení útok

- Pomalé čtení útok odešle oprávněné požadavky na aplikační vrstvě, ale čte reakce velmi pomalu, a tak se snaží vyčerpat serveru připojení bazén. Pomalé čtení je dosaženo tím, reklamní velmi malém množství pro TCP velikost přijímaného okna a zároveň tím, že vyprázdní TCP klientů přijmout vyrovnávací paměť pomalu. To samozřejmě zajišťuje velmi nízkou dat průtoku

distribuovaného útoku I

- Distribuované odmítnutí služby útoku (DDoS) nastává, když více systémů zaplavit šířku pásma, nebo zdroje z cílené systému, obvykle jeden nebo více webových serverů. To je výsledek více napadených systémů (např. botnet) zaplavují cílené systém (y) s provozem. Pokud je server přetížen s připojením, lze nové připojení již nebudou akceptovány.
- Malware může nést DDoS útok mechanismy, jeden z dobře známých příkladů tohoto byl MyDoom . Jeho DoS Mechanismus byl spuštěn v určitý den a čas.Tento typ DDoS zúčastněných kódujete cílovou IP adresu před uvolněním malware a žádné další interakce bylo nutné zahájit útok.
- Systém může být také ohrožena s trojan , který umožňuje útočníkovi stáhnoutzombie agenta (nebo trojan může obsahovat jeden). Útočníci mohou také proniknout do systémů využívajících automatizované nástroje, které využívají chyby v programech, které poslouchají pro připojení vzdálených hostitelů. Tento scénář se týká především systémů fungujících jako servery na internetu.
- Stacheldraht je klasický příklad nástroje DDoS. Využívá vrstvami struktury, kde útočník používá klientský program pro připojení k rutiny, které jsou ohroženy systémy, které vydávají příkazy k zombie agentů , což usnadní DDoS útok.Agenti jsou ohroženy prostřednictvím manipulačních útočníkem, automatizované rutiny využít zranitelnosti v programech, které přijímají vzdálená připojení běží na cílových vzdálených hostitelů. Každý psovod může ovládat až tisíc agentů.

distribuovaného útoku II

- Tyto sbírky kompromisy systémů jsou známé jako botnety . DDoS nástroje jako Stacheldraht nadále používat klasické DoS útoku metody se soustředí na IP spoofing a zesílení jako útoky Šmoula a Fraggle útoky (ty jsou také známé jako útoky spotřebu šířky pásma). SYN záplavy (také známý jako útoky zdrojů hladovění), mohou být také použity. Novější nástroje lze použít DNS servery pro účely DoS. Viz další část.
- Jednoduché útoky, jako jsou záplavy SYN se mohou objevit s širokou škálou zdrojové IP adresy, což vzhled dobře distribuovaného DoS. Tyto povodňové útoky nevyžadují ukončení TCP třícestného handshake a pokusit se vyčerpat cílovou SYN fronty nebo serveru šířku pásma. Vzhledem k tomu, že zdrojové IP adresy lze triviálně falešné, by útok přišel z omezené sady zdrojů, nebo může dokonce pocházet z jediného hostitele. Stack příslušenství, jako například cookies, synmůže být účinná zmírňování před povodněmi fronty SYN, nicméně kompletní pásma vyčerpání vyžadují zapojení. Na rozdíl od mechanismu Mydoom je DDoS, může botnety být obrátila proti libovolné IP adresy. Script kiddies použít popírat dostupnost známých webových stránek oprávněným uživatelům. Více důmyslných útočníci použít DDoS nástroje pro účely vydírání - a to i proti jejich obchodních konkurentů .
- Pokud útočník připojí útok z jednoho hostitele by být kvalifikován jako útok DoS.Ve skutečnosti by byl jakýkoliv útok proti dostupnosti být kvalifikovány jako Denial of Service útok. Na druhé straně, jestliže útočník používá mnoho systémů současně zahájit útoky proti vzdáleného hostitele, by to být klasifikován jako DDoS.
- Mezi hlavní výhody útočníkovi použití distribuované typu denial-of-service útok je, že: více počítačů může generovat větší provoz, než útok jednoho stroje, více útoků stroje jsou těžší vypnout než jeden útok stroj, a že chování každého útoku Stroj může být stealthier, takže je těžší sledovat a vypnout. Tyto útočník výhody způsobit problémy pro obranné mechanismy. Například, pouze zakoupení více příchozích šířku pásma, než je aktuální objem útoku nepomůže, protože útočník mohl jednoduše přidat další útok strojů.
- V některých případech stroj může stát součástí DDoS útoku se souhlasem majitele. Příkladem toho je 2010 DDoS útok proti velkým společnostem kreditních karet příznivci WikiLeaks . V případech, jako je tento, příznivci hnutí (v tomto případě ty, které proti zatčení zakladatele WikiLeaks Juliana Assange) vybrat, stáhnout a spustit DDoS software.

Odráží / falešného útoku

- Distribuované odráží odmítnutí útoku služby (DRDoS) zahrnuje zaslání kované žádosti nějakého typu na velmi velký počet počítačů, které budou odpovědi na žádosti. Pomocí adresy internetového protokolu spoofing , je zdrojová adresa nastavena jako cílené oběti, což znamená, že všechny odpovědi budou jít do (a povodním) cíle.
- ICMP Echo Request útoky (Šmoula útok) mohou být považovány za jednu formu odraženého útoku, jak záplavy hostitele (y) zaslat Echo Request na vysílání adres mis-konfigurovaných sítí, což láká mnoho hostitelů posílat pakety Echo Reply oběti. Některé časné DDoS programy realizované distribuovanou formu tohoto útoku.
- Mnoho služeb může být využíván působit jako reflektory, někteří hůře zablokovat než ostatní. DNS zesílení útoků zahrnují nový mechanismus, který zvýšil amplifikační efekt, použití mnohem větší seznam serverů DNS, než viděl dříve.

neúmyslné odmítnutí služby I

- To popisuje situaci, kdy stránky skončí popřel, ne kvůli záměrnému útoku ze strany jednotlivce nebo skupiny jednotlivců, ale prostě kvůli náhlé obrovské bodcem v popularitě. To se může stát při extrémně populární stránky příspěvků viditelný odkaz na druhý, méně dobře připravené místě, například, jako součást reportáž. Výsledkem je, že významný podíl na primární webové stránky v pravidelných uživatelů - potenciálně stovek tisíc lidí - klikněte na tento odkaz v prostoru několika málo hodin, které mají stejný účinek na cílové stránky jako útok DDoS. VIPDoS je stejný, ale zejména tehdy, pokud se odkaz uloženy celebrity.
- Příklad tohoto nastal, když Michael Jackson zemřel v roce 2009. Webové stránky jako Google a Twitter zpomalil nebo dokonce havaroval. servery mnoha místech "si myslel, že žádosti byly z viru nebo spyware se snaží způsobit Denial of Service útok, varuje uživatele, že jejich dotazy vypadal jako" automatickým žádostem z počítače virus nebo spyware aplikace ".
- Novinky stránek a odkazů stránky - stránky, jejichž primární funkcí je poskytovat odkazy na zajímavý obsah jinde na internetu - se s největší pravděpodobností příčinou tohoto jevu. Kanonický příklad je efekt Slashdot , když přijímá data z Slashdot . Stránky jako je Reddit , Digg , na Drudge zpráva , Fark , něco hrozného , a webcomic Penny Arcade jste své odpovídající "účinky", známé jako "v tom smyslu, Digg", přičemž "drudged", "farking", "goonrushing" a "wanging"; resp.

neúmyslné odmítnutí služby II

- Směrovače byly také známo, že vytvoření neúmyslné DoS útoky, protože jak D-Link a Netgear routery vytvořili NTP vandalismu tím, že zaplaví NTP servery bez respektování omezení klientských typů nebo zeměpisných omezení.
- Podobné neúmyslné popírání doručování může dojít také prostřednictvím jiných médií, např. při URL je uvedeno v televizi. Pokud je server indexovány Google nebo jiný vyhledávač špičkách činnosti, nebo nemá mnoho dostupné šířky pásma, zatímco jsou indexovány, může také vyskytnout účinky DoS útoku.
- Právní byla přijata opatření v alespoň jednom takovém případě. V roce 2006,Universal Tube & Rollform Equipment Corporation žalován YouTube : masivní množství rádoby youtube.com uživatelů omylem zadali zkumavek společnosti URL, utube.com. Jako výsledek, trubka společnost nakonec museli utrácet velké částky peněz na modernizaci jejich šířku pásma.

Denial-of-Service Level II

- Cílem DoS L2 (případně DDoS) útok je způsobit zahájení obranný mechanismus, který blokuje síťový segment, ze kterého útok pochází. V případě distribuovaného útoku nebo IP hlavičky modifikace (která závisí na druhu bezpečnostního chování), že bude plně blokovat napadl sítě z internetu, ale bez pádu systému.

Reakce a Prevence

Prevence a reakce

- Obrana proti popření servisních útoků obvykle zahrnuje použití kombinace útoku detekce, klasifikace provozu a reakce nástrojů, jejichž cílem je blokovat provoz, že se identifikují jako nemanželské a umožňují provoz, že identifikovat jako legitimní. Seznam prevence a reakce nástrojů je uveden níže:

Firewally

- Firewally mohou být nastaven tak, aby se jednoduchých pravidel takové povolit nebo zakázat protokoly, porty nebo IP adresy. V případě jednoduchého útoku přichází z malého počtu neobvyklých IP adres například, jeden mohl dát do jednoduché pravidlo k poklesu veškeré příchozí přenosy z těchto útočníků.
- Složitější útoky však bude těžké blokovat s jednoduchými pravidly: například, pokud je pokračující útok na portu 80 (webová služba), není možné zahazovat veškeré příchozí přenosy na tomto portu, protože tím bude zabránit serveru slouží legitimní provoz. Kromě toho může firewally být příliš hluboká v hierarchii sítě. Směrovače mohou být ovlivněna ještě před dopravní dostane k firewallu. Nicméně, firewally mohou účinně zabránit uživatelům spouštění jednoduchých útoky záplav typu ze strojů za firewallem.
- Některé stavové firewally , jako OpenBSD pf paket filtru, mohou působit jako zástupce pro připojení: handshake je validován (s klientem) místo toho, aby prostě předání paketu k cíli. Je k dispozici pro další BSD stejně. V této souvislosti, to je nazýváno "synproxy".

Přepínače

- Většina spínače mají některé omezení rychlosti a ACL schopnost. Některé přepínače poskytují automatické a / nebo v rámci celého systému omezování rychlosti , traffic shaping , zpožděné vazby (TCP sestřih), hloubkovou inspekci paketů a filtrování Bogon (falešné IP adres) pro detekci a nápravě popření servisních útoků prostřednictvím automatické rychlosti filtrování a WAN Link selháním a vyvažování.
- Tyto režimy budou fungovat tak dlouho, dokud DoS útoky jsou něco, co může být zabráněno pomocí nich. Například může SYN flood být zabráněno pomocí odloženo vazbu nebo TCP sestřihu. Podobně obsahu založené DoS může být zabráněno pomocí hloubkového prověřování paketů. Útoky pocházející z temných adres nebo jít do tmavé adresy lze zabránit použitím Bogon filtrování . Automatické cena filtrování může fungovat tak dlouho, jak jste nastavili rychlost-prahy správně a granularly. Wan-link failover bude fungovat tak dlouho, dokud oba odkazy, DoS / DDoS mechanismus prevence.

routery

- Podobně jako přepínače, směrovače mají některé omezení rychlosti a ACL schopnost. Oni také jsou ručně nastavit. Většina směrovačů může být snadno přemožen pod útokem DoS. Cisco IOS má vlastnosti, které zabraňují zaplavení, tj. příklady nastavení.

Použití front end hardware

- Aplikace front end hardware je inteligentní hardware umístěny v síti předtím, než dopravní dosáhne servery. To může být použit v sítích ve spojení s směrovačů a přepínačů. Aplikace front end hardware analyzuje datové pakety, které vstoupí do systému, a pak identifikuje jako prioritu, pravidelné, nebo nebezpečné. Existuje více než 25 Bandwidth Management dodavatelů.

IPS prevence

- Prevence proti narušení systémů (IPS) jsou efektivnější, pokud útoky mají podpisy s nimi spojené. Nicméně, trend mezi útoků je mají legitimní obsah, ale špatný úmysl. Prevence proti narušení systémy, které pracují na obsah uznávání nemůže blokovat chování založené na DoS útoky. An ASIC založené IPS může detekovat a blokovat popření servisních útoků, protože mají výpočetní výkon a granularitu analyzovat útoky a chovat se jako jističe automatizovaným způsobem.
- A míra bázi IPS (RBIPS) musí analyzovat provoz granularly a průběžně sledovat dopravní vzor a zjistit, zda je provoz anomálie. Je třeba nechat legitimní plynulost provozu při blokování útoku DoS provoz

DDS based obrana

- Více zaměřeny na problém, než IPS, DoS obrany System (DDS) je schopen blokovat připojení na bázi DoS útoky a ty s legitimním obsahem, ale špatné záměry. DDS může také zabývat oběma protokolu útoky (např. slza a Ping of Death) a cena-založené útoky (například ICMP povodně a záplavy SYN).
- Stejně jako IPS, účelové systém, jako jsou dobře známé Top produkty vrstvy IPS, dokáže detekovat a blokovat popření servisních útoků na mnohem blíž traťové rychlosti, než softwarový systém založený.

Blackholing a sinkholing

- S blackholing, je vše provoz na napadených DNS nebo IP adresa odeslána do "černé díry" (null rozhraní, neexistující server, ...). Chcete-li být efektivnější a vyhnout ovlivnění připojení k síti, může být řízena ISP.
- Sinkholing trasy na platnou adresu IP, která analyzuje provoz a odmítá ty špatné.Sinkholing není efektivní pro většinu závažných útoků.

Čistý trubky

- Veškerý provoz je prošel "čištění centra" nebo "drhnutí centrum" prostřednictvím různých metod, jako proxy, tunelů nebo dokonce přímé obvody, které odděluje "špatné" komunikaci (DDoS a také další běžné internetové útoky) a odešle pouze dobrou dopravní rámec na serveru. Poskytovatel potřebuje centrální připojení k Internetu pro správu tohoto typu služeb, pokud se náhodou být umístěny ve stejném zařízení jako "čištění města" nebo "drhnutí centrum".