DHA támadás elleni védekezés lehetősége a támadók felismerése és központosított tiltása segítségével

Szabó Géza (szabog@crysys.hu)
Szabó Gábor (szaboga@crysys.hu)

2005. január 31.

Kivonat

Az alábbi cikkben a Directory Harvest Attack támadásokkal fogunk foglalkozni. Bepillantást nyújtunk a lehetséges védelmi mechanizmusokba. Számba vesszük a lehetséges védelmi megoldásokat és ezen alapelveket felhasználva bemutatunk egy általunk kidolgozott rendszert, ami hatékonyabb az eddigieknél.

1. Bevezető

Az emberek az egyre növekvő kéretlen levelek áradatának és levélben terjedő vírusok és más kártékony kódok hatására egyre jobban meggondolják azt, hogy kinek is adják oda az e-mail címüket. Átgondolják, hogy meg merjék-e kockáztatni, hogy valamilyen online fórumon címüket használják, vagy akár azt is, hogy egyáltalán a weblapjukon vagy névjegyükön rajta hagyják-e ezt a fontos személyi adatukat. A fenti okok miatt a felhasználók általában tartanak más, akár egyszer használatos e-mail címet, gyakran valamilyen ingyenes szolgáltatónál, ami ha "odavész", sem baj. Ha a címet elkezdik elárasztani kéretlen levelek, akkor a felhasználó rövid idő után átvált egy másik címre, a régit lemondja, vagy magára hagyja és később a szolgáltató is törli. Ha ennek ellenére egy általa gondosan vigyázott e-mail címre egyszer csak elkezdenek kéretlen levelek özönleni, akkor e-mail szolgáltatója nagy valószínűséggel egy címkinyerő (DHA) támadásnak esett áldozatul. A DHA témája sokszor előkerül, és a kereskedelmi anti-spam termékek egy hirtelen mozdulattal ki is pipálják az általuk nyújtott szolgáltatások listáján, elfelejtvén megemlíteni, hogy milyen megoldást is használnak a támadás kivédésére. Ezeket a módszereket szeretnénk összefoglalni és javaslatot tenni egy hatékony védelmi mechanizmusra.

1.1. Általános problémák

A DHA problémája az SMTP protokollban gyökeredzik: az e-mail szerverek, ha megfelelő e-mail címre kapták a levelet, úgy nem adnak visszajelzést, elfogadják a levelet. A szerver, ha nem létező felhasználó címére kap levelet, úgy vagy azonnali, vagy későbbi visszajelzést ad arra nézve, hogy a felhasználó postafiókja nem létezik. Ez a folyamat információval szolgál a levelező-szerver által karbantartott e-mail címekről. A támadók ezt az információt használják ki, rengeteg levelet küldve az adott e-mail szervernek. Azokról a címekről, amelyekről nem érkezik válasz (a szerver negatív visszajelzés nélkül elfogadja a levelet), nyilvántartást vesznek fel. Ezek a címek minden valószínűség szerint érvényes felhasználói azonosítókhoz tartoznak, így érdemes lehet rájuk a későbbiekben kéretlen leveleket küldeni.
A cím kijutás mellett problémát jelenthet a levelezést kiszolgáló szerver összeomlása. Az e-mail címek megszerzése érdekében a támadó rengeteg téves levelet küld a szervernek, amely így jelentősen, hosszú időre, és akár több támadótól is leterhelésre kerül. A leterhelés leköti a kiszolgáló hálózati kapacitását és processzorát is. Ez végeredményben egy DoS támadást eredményez.

1.2. A támadás fajtái

A DHA támadásnak, azaz a címlista kinyerő támadásnak, két típusa létezik: egyik "brute force" jelleggel az összes lehetséges karakterkombinációt kipróbálja, mint e-mail címet;
a másik jóval szofisztikáltabb: tipikusan előforduló e-mail címeket generál vagy gyűjt emberek vezeték és keresztnevéből, illetve gyakran előforduló szavakból, szóösszetételekből, továbbá ismert e-mail azonosítókból.

Más lehetséges csoportosítása a DHA támadásnak a felhasznált IP-címek száma alapján. Az „alap" változatban a támadó ugyanarról az IP címről próbálkozik, míg a másik esetben több IP címmel rendelkezik és ezeket rotálva választ ki mindig egyet a támadáshoz (disztributív DHA).

2. A lehetséges védekezések

2.1. Új program elemet *NEM* igénylő módszerek

2.1.1. E-mail cím választással

A védekezés a DHA támadás ellen történhet egyszerűen bonyolultra választott e-mail címekkel, ami a szó-

táras támadás ellen ideig-óráig véd, de a környezetünk nehezen fogja tudni megjegyezni új e-mail címünket.A védekezés brute-force támadások ellen haszontalan.
Az e-mail címmel való védekezés másik lehetséges módja, ha egyszer használatos e-mail címet használunk.

2.1.2. Szerver konfigurálással

Megoldás az is, ha a szervert úgy konfiguráljuk, hogy fogadjon el minden e-mailt és ne jelezzen vissza róla senkinek, a téves leveleket pedig egyszerűen eldobjuk.
A megoldás több okból is problémás: a levélküldők nem tudják meg, hogy a cím nem létezik, és elárasztathatják a szervert téves levelekkel. Fontos az is, hogy a legitim felhasználók sem kapnak visszajelzést a tévesen címzett levelekről. Mindezek miatt a visszajelzés letiltása nem javasolható.
A legmegfelelőbb természetesen az SMTP protokoll finomítása lenne, de mit tudunk addig is tenni, amíg ez nem következik be?

2.2. Új program elemet igénylő módszerek

2.2.1. Hoszt alapú védelem

Ebben az esetben minden résztvevőnek van egy saját önműködő rendszere, amely a döntéseit egyéb rendszerektől függetlenül hozza.
A támadás szűrését a levéltovábbítás során keletkező hibaüzenetek alapján lehet elvégezni.

Ha a támadó egy IP címről próbálkozik, akkor a következő módon detektálható a DHA.

- Ha téves címzettnek küld e-mailt egy adott IP címről.
- Később újra próbálkozik ugyanarról az IP címről.
- Az újabb cím is téves és a két téves cím között van valamiféle illesztési lehetőség.

Ha a támadó több IP címről próbálkozik, akkor így észlelhető (disztributív DHA).

- Ha téves címzettnek érkezik e-mail egy adott IP címről
- A következő téves címzettnek szóló e-mail másik IP-től jön ugyan, de a két téves e-mail cím között lehetséges valamiféle illesztés.

Disztributív DHA esetén is általában több e-mail címet próbál ki a támadó ugyanazon IP-címről még mielőtt IP-címet váltana. Azonban van olyanra is példa, hogy nem küldenek sok levelet egy címről. Ez valószínűleg attól függ, hogy észreveszik-e, hogy kitiltjuk támadás detektálása esetén az adott IP-címet, illetve, hogy mennyire fontos a támadónak a cím. Ésszerű csak a „hagyományos" DHA-val foglalkozni, a második esetben is be fog kerülni minden egyes IP cím az adatbázisba, amelyet felhasznál a támadás folyamán.
Érdekes eredményre vezethetne, ha nyilván tudnák azt tartani, hogy IP címek egy csoportját melyik támadó használja (például statisztikák készítése során, vagy az Internet-szolgáltatók felé jelenteni, stb.). Így egy-egy DHA támadás során összegyűlt e-mail címek eredeti szerzőjét a felhasználás idejének függvényében meg lehetne állapítani.

2.2.2. Hálózaton alapuló védelem

A rendszer a hálózat egyéb résztvevőivel együttműködve próbál védekezeni a DHA támadás ellen.
Ha egy támadó egy ismeretlen címre küld egy e-mailt a megtámadott szerveren, a megtámadott szerver küld egy hiba jelentést a központi DHA RBL szervernek. Ez a hiba jelentés tartalmazza a támadó IP-címét, a kipróbált e-mail címet, és a támadás idejét. A központi szerver gyűjti ezen jeletéseket, és ha túllép egy küszöböt ezen IP-ről jövő próbálkozások száma, akkor behelyezi a támadó IP-címét a fekete-listára. A szerver a listára kerülés után is jegyzi a támadó kísérleteit amennyiben tudja, így nem hagyja elévülni a bejegyzést. A fekete lista tartalmát le lehet kérdezni a szervertől, ami a feltett kérdésre, hogy egy e-mail fekete-listás-e vagy sem, egy igen-nem választ ad.
Az RBL (Real-time Black/Block List)-listákból több fajta van: van ami e-mail címeket, DNS neveket, DSL címeket, open-relay szervereket, open proxy-kat gyűjt. Ezek teljesen naprakészek és állandóan több is on-line, hogy egy esetleges támadás egyik-másik ellen az RBL-listás védelmi mechanizmusokat ne tegye használhatatlanná.

A RBL-listákat tárolni kell mindenképpen. Egy hoszt alapú védelmet tekintve a lokális adatbázis használata elkerülhetetlen. A hálózaton alapuló védelem esetén már a fejlesztő eldöntheti, hogy használni akar-e lokális adatbázist vagy nem. Ekkor a résztvevők cache-elhetik a lekérdezéseket így megszabadítva a szervert az állandó kérdés-felelet terhe alól. A lekérdezéseik eredményeit helyi adatbázisaikban tárolhatják. Az általunk javasolt megoldás is lokális adatbázist használna, hiszen nagy számú levél ellenőrzése esetén egy cache-mechanizmusra mindenképpen szükség van.

2.2.3. Lokális adatbázis használatával

A (nem elosztott) DHA-t tekintve a következő módon detektálható a támadás:
A DHA védelmi rendszer megvizsgálja a levelező szolgáltatás által generált log fájlt valós-időben. Ez azt jelenti, hogy nem utólagos vizsgálatra kerül sor (mondjuk a nagy terheltségű időszakot követően), hanem a levél beérkezésének pillanatában. Ez azért fontos, mert egy utólagos vizsgálat megtévesztő, esetleg hibás ered-

ménnyel szolgálhat (pl. a támadó addigra befejezte a támadást, már nem aktuális az így nyert dinamikus IP-cím lista).
Ha talál "Unknown User" bejegyzést, akkor megnézi a hozzátartozó IP-címet. Ellenőrzi, hogy szerepel-e az IP cím a helyi adatbázisban:

- Ha nem, bejegyzi a helyi adatbázisba (ez volt az első téves címzettnek küldött e-mail erről az IP címről).
- Ha igen és talál illeszthetőséget a két téves cím között, és még nem küldtünk róla jelentést akkor ez valószínűleg DHA támadás, így bejegyzi a helyi adatbázisba és elküldi a jelentést.

Azért vizsgál valamilyen fokú összefüggést a téves címek között, mert ezzel lehet csökkenteni annak a valószínűségét, hogy egy vétlen személyt jelentünk támadónak.
Előfordulhat így is az, hogy valaki többször, kis különbséggel elgépeli a címzettet. Mivel a helyi adatbázisban ennek nyoma van, így az illető bekerülhet a központi adatbázisba. Ennek a valószínűsége viszont elenyészően kicsi. Ha a felhasználó igazolja az ártatlanságát, akkor egyszerűen töröljük a központi adatbázisból. A helyi adatbázis használata a további kérdéseket veti fel:

- Ebben az adatbázisban is tárolni kell az összes olyan információt, ami a jelentés elküldéséhez szükséges.
- Ha egy IP címről elküldtük a jelentést, a rávonatkozó bejegyzés nem törölhető. Ha eltávolítanánk, akkor folyamatosan REPORTolnánk, amíg a támadó újra próbálkozik, ezáltal terhelve a központi adatbázist.
- A helyi adatbázisban érdemes jelezni, hogy már küldtünk jelentést. Ha egyszer már jelentettük a központ felé, akkor a rendszer többi része már tudja, hogy az adott IP-cím támadó.

2.2.4. Lokális adatbázis használata nélkül

Most tekintsük át azt az esetet, amikor minden egyes téves címre történő e-mail küldését bejelentjük a központi adatbázis felé. Ebben az esetben a felismerési algoritmus egyszerűsödik, a következő módon foglalható össze:
A rendszer megvizsgálja a log fájlt. Ha talál ismeretlen postafiókra küldés sikertelenségére vonatkozó bejegyzést, akkor elküldi a jelentést a központi adatbázis felé. Ebben az esetben nincsen szükség lokális adatbázisra, hiszen nem kell nyilvántartani az egyes IP címekhez tartozó próbálkozásokat.

3. DHA-val kapcsolatos munkák

A fent bemutatott védelmi módszerekre épülnek kereskedelmi termékek is. Ezek funkciójukat tekintve inkább anti-spam termékek, és nem a DHA támadás ellen vannak kihegyezve. Nagy részt a RBL-alapú megoldásokat támogatják levél érkezésekor, azaz nyílvános RBL-listákon ellenőrzik a feladó címét, hogy támadónak minősítették-e már korábban.
A Kerio MailServer [4] felfigyel a nem létező postafiókoknak küldött levelekre és egy bizonyos szám felett elkezdi szűrni a lehetséges támadókat.
A Secluda Inboxmaster [5] konfigurálható SMTP hibaüzenetek beállítását teszi lehetővé: ha egy spam-et detektálnak a levél kézbesítés közben, a szerver egy válasz üzenetet küld a feladónak, hogy nem létező e-mail-re próbált levelet küldeni. Ezzel a megoldással az a legfőbb probléma, hogy a DHA támadást nehezen szűri ki, hiszen az eben a támadásban részvevő e-mail-ek általában nem tartalmaznak spam-et, amit a spam-szűrő módszerek így nem jeleznek. A Styx Mail Filter [2] egy hardver-szoftver együttes, ami a kértelen reklám levelek és vírusos tartalmak szűrését végzi a levelek levelező rendszerbe jutása előtt. Az alapkivitel szabad szoftvereket használ, így megtalálható benne a ClamAV víruskereső és SpamAssasin spam-szűrő. Ez utóbbi egy RBL-alapú megoldást foglal magában(, amely kiegészül egy Bayes szabály-tanuló rendszerrel, Razor és DCC komponensekkel), ami a levelek szűrését elvégzi, de DHA támadást nem jelent az RBL-szerverek felé.
Egyes termékek dokumentációja alapján nem tudni, hogy működnek, de a hatékonyság miatt, nagy valószínűséggel RBL-alapúak, ilyen pl. az eSafe Advanced Anti-spam Software [3].

4. A mi megoldásunk

Egy olyan komponensekből álló rendszert javaslunk a probléma megoldására, ami a meglevő működő rendszerünk mellé beépül és megakadályozza a cím-kinyerési támadásokat. Javasolt rendszerünk felépítése a következő: egyrészt áll egy syslog elemzőből, egy spam detektorból és egy víruskereső részből. Az eredményeket központi nyilvántartásban összegezzük, azaz nyilvántartjuk azokat a gépeket, amelyek DHA támadásban érintettek. A központi nyilvántartás segítségével a komponenseinket használó összes résztvevő profitál egymás bajából is, azaz egy támadó nemcsak egy helyen lesz kitiltható, de másoknak sem fog károkat okozni.
A log-file elemzés módszere helyett felmerülhetnének más megoldások is:

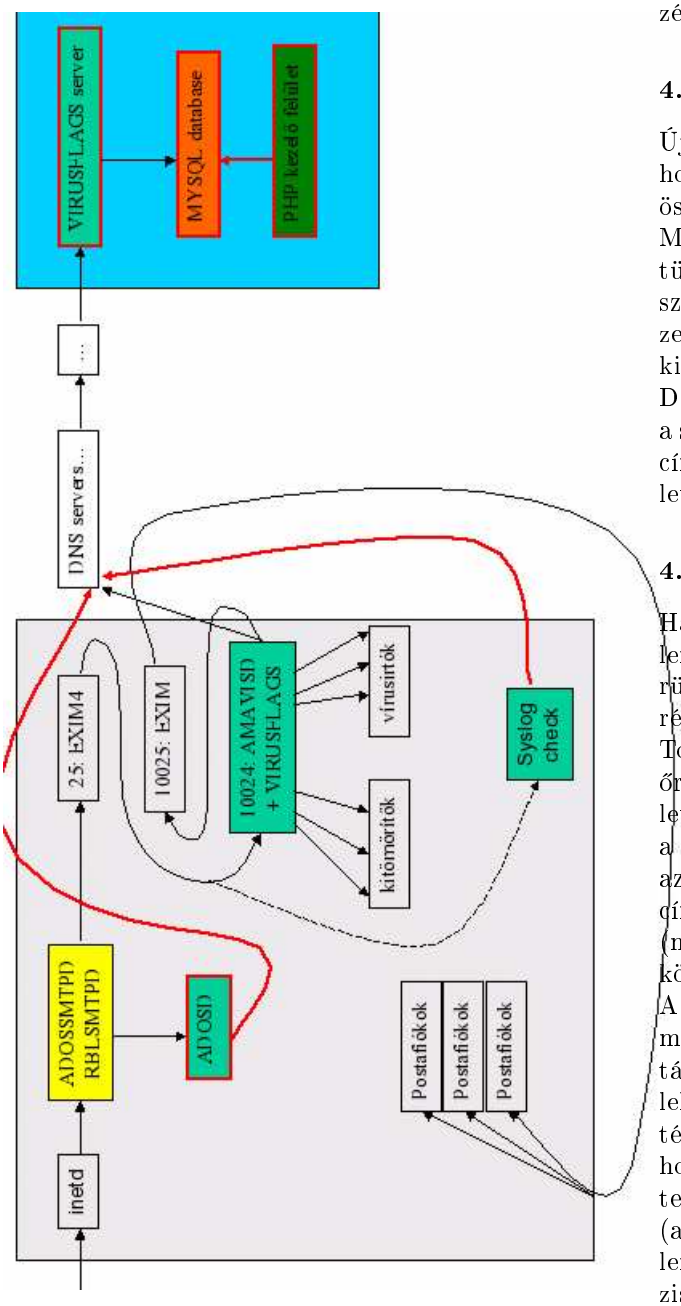
- a levelező-szerver előtt kialakíthatnánk egy front-end-et:
  A front-end még a levelező-szerverre kerülés előtt vizsgálhatná a DHA támadó leveleket. Ebben az esetben lényegében egy komplett levelező-szervert meg kellene valósítani.
- átírhatnánk a levelező-szervert

Azért választottuk a log-file elemzést a DHA támadó levelének levelező-szerveren átfutása után, mert így a

megoldás egyszerű, hatékony tud lenni és a meglévő jól működő elemeket nem kell helyettesíteni/újraírni.

4.1. A rendszer működése

A rendszer prototípusát a következő környezetben hoztuk létre: linux rendszert használunk,standard levelezést lebonyolító megoldásokkal. (lásd. 1. ábra)



1. ábra. A komponensek kapcsolata

4.1.1. DHA-elleni védelem folyamata

Új levél érkezése esetén az *inetd* démon működésbe hozza a levelező szervert. Ez hagyományosan a 25-ös portra érkező kérésekre figyel, és elindít hozzá egy MTA-t (sendmail, postfix, exim, ...). Ám a mi esetünkben, nem közvetelenül adjuk át a kérést a levelező szervernek, hanem egyik modulunkon keresztül átvezetjük a kérést. Ez a modul felelős a DHA támadások kivédéséért, azaz az ismert támadók kitiltásáért. Egy DNS lekérdezéssel frissíteni tudja a lokális adatbázisát a szerver adatbázisából, és egy korábban bejegyzett IP-címről jövő levelet már itt eldob, nem megy tovább a levelező-szerverekhez.

4.1.2. DHA támadás jelentése

Ha a támadó levele (valószínűleg első) átsiklik az ellenőrzésen, az azért volt, mert az IP-je még nem került be a szerver adatabázisába, még nem volt olyan résztvevő, aki támadást jelentett volna erről a címről. Továbbmegy a levelező-szerverbe, ami egyfelől ellenőrzi, hogy kézbesíteni tudja-e a helyi postafiókokba a levelet, ami támadás esetén mivel sikertelen, bekerül a jelentés róla a *syslog*-ba. A syslog elemző rendszer az e-mail kiszolgáló jelentéseiből megnézi, hogy a téves címzéssel rendelkező e-mailek honnan jönnek hozzánk (milyen IP címről), és ezekről részletes jelentést tesz a központi adatbázisnak.
A jelentés gyakorisága között lehet eltérés: minden támadást jelentsünk; vagy csak egyszer jelentsünk, egy támadást egy IP címről. Ezt egy lokális adatbázisban lehetne nyílvántartani. A központi adatbázis felé történő jelentésekkel kapcsolatban felmerül az a kérdés, hogy ha nem tartjuk nyilván mely támadásokat jelentettük már, akkor ha minden egyes újabb próbálkozást (ami szintén arról az IP címről jön) újra és újra lejelentenénk, ami feleslegesen terhelné a központi adatbázist. Szerencsére azonban ezzel nem kell törődni, hiszen a teljes rendszer úgy működik, hogy ha már egy IP cím be van jelentve, akkor a spam el sem jut a Sendmail-ig, a DoSFrontend-en fennakad (lásd. 5.2), így viszont már nem is fog bekerülni az újabb próbálkozás a log fájlba. Ezért döntöttünk úgy, hogy rendszerünk minden egyes próbálkozást jelent a központi adatbázis felé. Előnye a gyorsabb működés, egyszerűbb kezelhetősége, és nem kell lokális adatbázissal bajlódni.
A többszörös jelentés egyik különleges kihasználási módja az lehet, hogy elkülönített funkciójú védett

levelező-szervereket használunk a rendszerben: bizonyos résztvevők csak jelentenek a központ felé - ,ezek védtelennek tűnnek a támadónak - bizonyosak csak tiltanak támadó IP-címekről jövő kapcsolatokat, némelyik mindkettőt teszi. Ennek értelme a támadó számára hamar világos lesz: egy csak jelentést generáló gépről nem fogja tudni eldönteni, hogy oda érdemes-e próbálkoznia, mert nincs igazi visszacsatolás . A támadó gépe természetesen tiltva lesz.

4.2. Téves riasztások kezelése

A téves riasztások alacsonyan tartása érdekében a következő módszer használható, hogy az egyedi téves levelek elválaszthatóvá tehetők legyenek a valódi támadóktól. Az a probléma, hogy ha valaki csak „véletlenül elgépeli" a címet, tehát nem akar DHA támadást indítani, akkor is bekerül a központi adatbázisba. Ennek orvoslására több lehetőség is adódhat:

- Egyrészt a központi adatbázisban az is nyilvántartható, hogy az egyes IP címek mennyire „veszélyesek". Azaz pontozni lehet őket aszerint, hogy hány bejelentés érkezett arra az IP címre vonatkozóan.

- Másrészt alkalmazható öregítés (aging) a központi adatbázisban. Az öregítés nagyon fontos szerepet játszik a rendszerben, ezért jól kell megválasztani a használt metódust: ugyanis, ha egy támadót eltávolítunk a listáról, akkor tovább támadhat, ha viszont túl sokáig van rajta, akkor akár a rendes felhasználók forgalmát is megakadályozhatja.

4.3. Öregítés (aging)

Az öregítés az adat idővel való eltávolítása. Az öregítést /bővebben lásd. [1]/ itt a fekete listák tisztítására/frissítésére használjuk.
A lehetséges módszerek:

- adminisztrátor vezérelt öregítés:
  Egy adminisztrátor dönt egyes elemek további sorsáról. Rákerülhet valaki úgy is a listára, hogy egy támadó zombie-nak használta fel. Ezen gépek tulajdonosai kérhetik, hogy vegyék le a fekete listáról. Ezt akár automatizálni is lehet olyan módszerekkel, ahol bizonyossá válunk abban, hogy az e-mail cím használója ember (pl. egy bonyolult ábrán levő szöveg felismertetése a felhasználóval, amit egy számítógép nem tudna megcsinálni). Nagyon fontos, hogy a felhasználók címeinek listából kivétele esetén a postafiókuk üzemeltetőjét, esetleg az Internet Service Provider-t értesíteni kell, hogy intézkedjenek a felhasználóik védelmében.

- egyszerű öregítés:
  Egy időintervallum lejárta után a bejegyzések kikerülnek a fekete listáról. Ezt sajnos a támadó is bekalkulálhatja, és az adott idő lejárta után egyből újrakezdheti a támadást.

- több-fázisú öregítés:
  Az első támadás után a támadó bekerül a fekete listánkba. Ezután több sikertelen kézbesítési üzenet nem fog generálódni, mivel a szerverek egyből eldobják a támadó címről érkező leveleket. Pár számítógépet viszont meghagyunk a támadóknak, amelyeken nem végzünk szűrést. Ezeket statisztikai célra használjuk, illetve a központi szerveren tárolt lista friss információkkal való ellátására.

Az általunk javasolt megoldás végeredményben ennek a harmadik variációnak felel meg. Ezt úgy érjük el, hogy ugyan nem hagyunk meg gépeket a támadónak célpont gyanánt, viszont az összes résztvevő által szolgáltatott adatokból dolgozik a központi rendszer, így bár egy szerver csak egyszer fog jelenteni, de ha a támadó célpontot vált, korábbi aktivitásáról/inaktivitásáról már értesülhettek a résztvevők.

4.4. Pár probléma, amivel érdemes foglalkozni

4.4.1. Dinamikus IP-címek

Problémát jelenthetnek a dinamikus IP címek: egy támadónak meghatározott időnként (naponta) megváltozna az IP címe, így mindig újabb támadónak észlelve újra és újra bekerül a központi adatbázisba. A DSLRBL-ek megoldást jelentenek erre a problémára.

4.4.2. Központi adatbázis kiesése

Központi adatbázis kiesése a rendszer szempontjából kritikusnak tűnhet, de ekkor működése egy hoszt-alapú DHA védelmi rendszer működésére hasonlítana a legutoljára kapott információk alapján. Legrosszabb esetben a rendszer transzparens viselkedést mutatna, azaz nem lenne rosszab helyzet, mintha nem használnánk semmit (ez azért fontos, hogy megemlítsük, mert ekkor sem vesznek el fontos leveleink, legfeljebb a DHA támadásokat nem szűrjük ki).

4.5. A rendszer további szolgáltatásai

Rendszerünk összeköthető spam-felismerő szoftverekkel is. A megoldás lehetővé teheti erőforrások megtakarítását azáltal, hogy az ismert DHA támadó szerverekről érkező leveleket, vagy azok egy részét már nem vetjük alá erőforrásigényes tartalomszűrési eljárásoknak, hanem tiltjuk azokat. Rendszerünk más módszerekkel kombinálva azok hatékonyságát is jelentősen növelheti.
A rendszer másik funkciója, hogy akkor is jelentést küldünk a szervernek a levél feladójáról, ha vírusos volt annak tartalma. Ezt a levél tartalmának kibontásával, a megfelelő csomagoló program kiválasztásával, majd

a rendszer által használt valamelyik rendelkezésre álló víruskeresővel lehet megtenni.
Ha érvényes címre érkezett a levél, a vírusellenőrzésen is átment, akkor bekerül egy újabb levelező-sorba, ami már csak az ellenőrzéseken átesett, helyi postafiókokba szánt leveleket tartalmazza. Innen kézbesíthetők a levelek a felhasználóknak.

5. A rendszer vizsgálata

5.1. A rendszer előnyei

Több rendszer a hoszt-alapú védelmet valósítja meg, amivel az a nyílvánvaló baj, hogy ha egyetlen gépet védenek és nem egy központot használnak, akkor egy széles körben disztributív támadás ellen nem véd. Emellett meg kell említeni, hogy a javasolt megoldásunk a központi szerver kiesése esetén így működik, tehát ez a szolgáltatás integrálva van benne magasabb szinten.
A rendszerünk nagy előnye a kereskedelmi eszközökkel szemben a dokumentáltság. Pontosan lehet tudni, mi mit csinál benne. Ezzel a tulajdonsággal a kereskedelmi termékeket a gyártók nem szokták felruházni. (Ilyen pl. a [2], ami bár magyar termék, bár nyílt forráskódokat használ, mégis a működéséről nem találni egy sajtóközlemény mélységénél mélyebb leírást. Vagy másik példa lehet a [3], amelynek dokumentációja pontonként kitér mindenféle spam-védelmi mechanizmusra egyenként, de a DHA-elleni védekezésnél annyival intézi el, hogy "eSafe provides full protection against DHA" /eSafe teljes körű védelmet biztosít a DHA ellen/.)
Több komplett anti-spam rendszer állítja magáról, hogy védelmet biztosít a DHA támadások ellen. Nyílvánvaló a kapcsolat, ugyanis, egy DHA támadás ellen nem védett gépet sokkal nehezebb lesz később a spam ellen védeni, ha a helyi postafiókok kitudódnak. Az érdekes azonban az, hogy amíg az RBL-szerverekkel együttműködnek egy levél érkezésekor, azaz kiszűrik a támadók IP-címeit, addig támadás esetén nem járulnak hozzá ezen listák automatikus bővítéséhez. (Pl. [4]: "To fight directory harvest attacks, Kerio MailServer monitors any unusual change in SMTP activity and once this attack is recognized, it applies several defensive techniques such as slowing down responses, cutting off connections and faking responses." /A DHA ellen úgy küzd a rendszer, hogy amennyiben szokatlan változást észlel az SMTP tevékenységben, akkor lelassítja a válasz adást, a kapcsolatokat megszakítja és hamisan válaszol./)
Jelen cikk főleg az akadémiai szférának szól, saját mail-szerverekkel, ahol a kereskedelmi megoldás sokszor szóba sem jöhet.
A rendszer szerver oldalának megvalósítása is RBL-alapú és integrálható más rendszerekbe.
A rendszerünk komponens-alapú, aminek több előnyös következménye is van:

- a reportolás és a tiltás különválasztható, pl. rblsmtpd front-end segítségével
- egy már meglevő rendszer is kiegészíthető vele, illetve akár csak bizonyos komponenseivel, így növelve a meglévő hatékonyságát is ($\longleftrightarrow$ más megoldások esetében az egész rendszert meg kell vásárolni és egészében át kell térni az új rendszer használatára, ha a DHA ellen védelmet akarunk kapni)
- a komponensek transzparensek kívülről, így a kiesésük esetén nem teszik a rendszert használhatatlanná
- a DHA komponenssel együttműködnek vírus és spamszűrő modulok is:
  a DHA támadás alapja a haszon. Ha valaki egyetlen levéllel esetleg 'feldobja' a zombie-ját amiről DHA-t csinál, akkor később spam-et sem fog tudni küldeni arról a gépről a komponensek együttműködése miatt. Mivel egy adott DHA kísérlet esélye csekély (kb. 1/100 csak egy cím megtalálására még nagyobb rendszerben is) , ezért nem biztos hogy megéri a támadónak kockáztatni egy DHA miatt a zombie-ját, megéri inkább máshonnan címeket szereznie.
  A vírus jelentő modul, pedig megakadályozza, hogy ha az adott gépre olyan vírus került, ami trójai programot telepít, vagy saját maga nyit rajta backdoor-t, akkor a támadó nem fogja tudni használni, mint zombie-t, hiszen már a támadás előtt bejelentették.

5.2. Támadás a rendszer ellen

A megoldásunk új komponenst vezet be annak érdekében, hogy önmaga se váljon támadás áldozatává. Mi történik abban az esetben, ha a támadók a hoszt gépek helyett magát a szervert vennék célba, hogy kiiktassák az RBL-listáját?
A támadás történhet egy DoS támadással az RBL-szerverek ellen. A DoS támadás ellen úgy védekezhetünk, hogy még alacsony szinten detektálja a szerver a támadó lekérdezéseket és nem kezd erőforrás igényes adatbázis műveletekbe. Egy lekérdezés helyességéről egyrészt az üzenetek formátuma alapján, másrészt a kérdező hoszt címe alapján tudunk meggyőződni. Sajnos ezek az azonosítók hamisíthatóak a támadó által is, ezért tervezünk egy aláírást is belevenni az üzenetekbe. (A kulcs menedzselési folyamatot a szerver intézi az anti-DHA programunk regisztrációja során.)
Az RBL-lista használhatatlanná tétele történhet esetleg hibás adatok bevitelével is. A hibás adatok bevitelének megakadályozását úgy segíti elő a rendszer, hogy csak egy korlátozott számú adminisztrátori engedéllyel rendelkező felhasználó módosíthatja az adatokat szerverre történő bejelentkezés után. A módosításokról napló készül, így meg lehet tudni esetleg kinek

a nevében módosítottak adatokat, akinek a kulcsát így azonnal le kell cserélni, illetve támogatja a rendszer egy korábbi állapotra való visszaállást. Ezt az adatbázisának felépítése teszi lehetővé, ahol minden módosítást tárolunk.
A támadó megpróbálhatja csökkenteni költségeit, illetve eredményesebbé tenni támadását úgy hogy nem támad olyan zombie-król, amelyek IP-címe az RBL-listán van. Azaz megpróbálja eldönteni, hogy egy IP szűrve van-e vagy sem. A nyílvános RBL-listát le tudja kérdezni, tehát a szűrt gépek listájához hozzájuthat. Azt viszont meg tudjuk nehezíteni, hogy egy támadó a levelező szerverről el tudja dönteni, hogy védett-e. (A részletes működés fentebb: 4.1.2.)
Az mindenesetre jól látható, hogy a hangsúlyt a hibás adatok bevitelének megakadályozására kell fektetni, mivel az RBL-listánk lekérdezése, nem tesz kárt közvetlenül a rendszer működésében.

5.3. A védelem eredményessége

A központosított szűrés eredményeképpen a támadó csak egy nagyon korlátozott számú próbát tehet a védett domain-eken. Természetesen a rendszerünk nem nyújt védelmet a nem védett domain-eknek, így azokon korlátlanul próbálkozhat a támadó. A támadó pénzt nyer a megszerzett e-mail címek eladásából. Ennek a nyereségnek a maximalizálása az ő érdeke, amit a kiadások minimalizálásával, azaz a legkevesebb e-mail üzenet küldéssel, zombie gép feladással és a legnagyobb bevétellel, azaz a legtöbb e-mail cím összegyűjtésével próbál elérni. /bővebben [1]-ben/
A rendszerünk a támadó címeit sorban feljegyzi, így azt a többi védett domain-en sem tudja felhasználni támadásra (ezt hoszt alapúnál megteheti nyugodtan). A zombie gépeit is elveszti ezáltal, tehát a támadó költségeit megnöveli jelentősen. A támadó által kiküldendő e-mailek számát is megnöveli, mivel az nem tudja eldönteni, hogy csak késleltetődik a válasz és helyes a címzett, tehát folytatni érdemes a támadást, vagy hogy eldobáljuk a leveleit. A nyeresége pedig minimális lesz, mivel a lehetséges próbálkozásiból, amíg fel nem kerül az RBL-listára, majdnem biztos, hogy nem fog hozzájutni érvényes felhasználó névhez, azután, pedig a leveleit megszűrjük.
A védelem tehát csökkenti a támadó nyereségét, gazdaságtalanná téve a DHA támadást.

6. A prototípus

A rendszerünk prototípusa a DNS protokollt használja a lekérdezésekre és reportolásra a védett szerverek és a RBL-szerver között. A DNS protokoll előnyei közé tartozik a robosztusság, a cache-mechanizmusa a DNS szervereknek (ha egy kérés fennakad valahol, akkor sem veszik el jó ideig és a szerver terheltségét is lehet csökkenteni ezen cache-mechanizmus által, mivel így akár burst-ökben is ki lehet szolgálni a kéréseket), illetve a tűzfal konfigurációkon is átjut ez a mechanizmus, nem igényel újabb portokat.

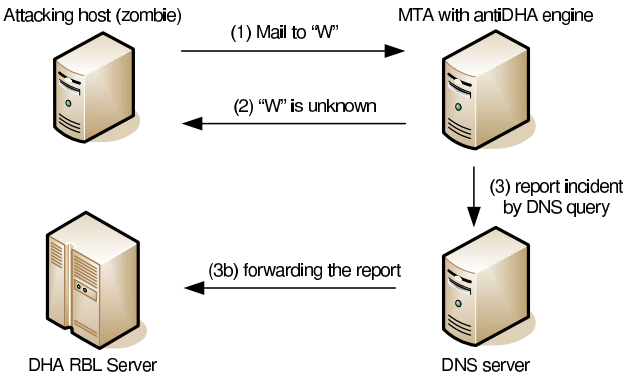
6.1. Jelentés generálás (report)

Egy támadás jelentése a következő módon hajtódik végre:

1. lépés:
   A támadó egy e-mailt küld egy internetes levelező-szervernek (MTA-nak).

2. lépés:
   A levelező-szerver egy SMTP protokoll szerinti választ ad, azaz, hogy a felhasználó ismeretlen a rendszer számára.

3. lépés:
   Az MTA küld egy jelentést a támadásról az RBL-szervernek. Ez egy meghatározott formátumú DNS név-feloldási kéréssel történik. A lekérdezés tartalmazza a támadó adatait. Ez lehet, hogy más DNS szervereken halad keresztül, ugyanúgy, mint a hagyományos DNS lekérdezések, míg el nem jut az RBL-szerverhez.



2. ábra. A jelentés generálás

6.2. Szűrés (filtering)

A szűrő rendszerünk prototípusa a következő egyszerű módon működik:
egy nem túl magas számú (jelenleg 10) nem létező címre küldött e-mail után hozzáadjuk a támadót a RBL-listához.
Nézzük mi történik, ha egy listán szereplő támadó egy új e-mailt akar küldeni egy védett hosztnak:

1. lépés:
   A támadó megpróbál egy e-mailt küldeni egy internetes levelező-szervernek (MTA-nak).

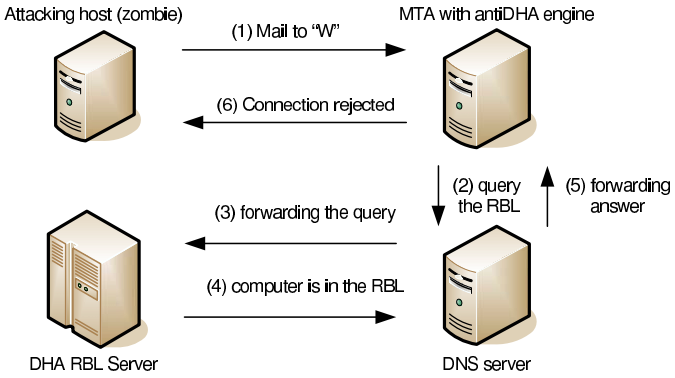
2. lépés:
   A védett hoszt egy DNS lekérdezéssel fordul az RBL-szerverhez, ami tartalmazza a támadó adatait.

3. lépés:
   Az MTA DNS-szervere továbbítja a DNS lekérést az RBL-szervernek.

4. lépés:
   Az RBL-szerver válaszol a DNS-lekérdezésre egy meghatározott IP-címmel, ami azt jelenti, hogy "Igen, ez a számítógép az RBL-listán szerepel". A DNS-szerver cache-elheti a választ egy bizonyos címre, aminek az intervallumát az RBL-szerver határozza meg.

5. lépés:
   A DNS-szerver visszaküldi a választ a védett hosztnak.

6. lépés:
   A védett hoszt elutasítja a kapcsolatot a támadóval. Ez az elutasítás történhet akár TCP szinten, akár a hagyományos SMTP protokoll szerinti hiba üzenettel.



3. ábra. A szűrés menete

7. Összefoglaló

A cikkben megvizsgáltuk a DHA támadásokat. A DHA támadás egy brute-force jellegű támadás egy levelező-szerver által karbantartott e-mail címek kinyeréséért. A lehetséges védekezési technikákat számba vettük. A javasolt hálózaton alapuló megoldásnál rendszer a hálózat egyéb résztvevőivel együttműködve próbál védekezeni a DHA támadás ellen. Ez tipikusan egy központi szerver által karbantartott RBL (Real-time Black List) -lista kérdezésével és feltöltésével működik.
Ezek figyelembevételével bemutattuk az általunk kialakított komponensekből felépülő védelmi mechanizmust, és elemeztük ezt. Javasolt rendszerünk felépítése a következő: egyrészt áll egy syslog elemzőből, egy spam detektorból és egy víruskereső részből. Az eredményeket központi nyilvántartásban összegezzük, azaz nyilvántartjuk azokat a gépeket, amelyek DHA támadásban érintettek. A támadó által kihasználható gyengeségeit is számbavettük a rendszernek és megoldást kerestünk a problémákra.
Majd a szűrési mechanizmus alapvető működését a rendszer prototípusán illusztráltuk egy támadás esetén.

Hivatkozások

[1] Bencsáth Boldizsár, Vajda István: *Efficient Directory Harvest Attack* /2005. január/

[2] Styx Mail Filter - vállalati levelező szerverek védelmére kifejlesztett integrált hardver- és szoftver megoldás, http://www.albacomp.hu/sajtokozlemeny.asp?szam=25 /2005. január 6./

[3] eSafe Advanced Anti-spam Software, ftp://ftp.ealaddin.com/pub/Marketing/eSafe/White_paper

[4] Kerio MailServer, http://www.kerio.com/kms_antispam.html

[5] Secluda Inboxmaster, http://press.arrivenet.com/tec/article.php/308157.html