DHA támadás elleni védekezés központosított szűréssel

SZABÓ GÉZA, BENCSÁTH BOLDIZSÁR

BME Híradástechnikai Tanszék, CrySyS Adatbiztonsági Laboratórium
{szabog, boldi}@crysys.hu

Lektorált

Kulcsszavak: DHA, címkinyerő támadás, feketelista, DNS, központosított védekezés

Cikkünkben a spamvédelmi módszerek területén végzett kutatásainkat és fejlesztési terveinket, eredményeinket kívánjuk vázolni. A tervezett védekezési módszerek komponens alapú fejlesztések, egymással szorosan összefüggő módszerek, melyek egymás szoftverelemeit is jelentős mértékben felhasználják. Elemezzük a rendszerünk által összegyűjtött adatokat és bemutatjuk, hogy milyen tipikus DHA támadók vannak, illetve hogy ezeket egyértelműen meg lehet-e különböztetni egymástól pusztán a támadási statisztikák alapján.

Az elektronikus levelező-szerverek által karbantartott levélcímek megszerzésének egyik lehetséges módja a címkinyerő támadás (Directory Harvest Attack), melynek során egy támadó létező e-mail címeket kísérel meg összegyűjteni címek próbálgatásának segítségével. A levelező szerverek, amennyiben egy érkező levél nem az általuk karbantartott felhasználók címére lett küldve, úgy vagy azonnali, vagy későbbi visszajelzést adhatnak arra nézve, hogy a kapott levélben szereplő felhasználó postafiókja nem létezik a nyilvántartásukban. Ez a folyamat információval szolgál a levelező-szerver által karbantartott e-mail címekről. A támadók ezt az információt használják ki, nagy számú levelet küldve az adott e-mail szervernek. Azokról a címekről, amelyekről nem érkezik válasz, azaz 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 DHA támadás lehetősége ismert volt eddig is, ám a sok alternatív levélcím összegyűjtési lehetőség miatt eddig nem kapott kiemelt fontosságot a kéretlen levélküldők által célpont összegyűjtés során használt eszközök között. Ahogy a felhasználók egyre jobban vigyáznak e-mail címeikre, a DHA előtérbe került és a támadók elkezdték előszeretettel alkalmazni.

A cikkben számba vesszük a lehetséges védelmi megoldásokat és ezen alapelveket felhasználva bemutatjuk az általunk implementált több programkomponensből álló, hálózaton keresztül együttműködő rendszert. A rendszer egy feketelistát felhasználó megoldás, ahol a feketelista a támadók IP-címeit tartalmazza egy központi adatbázisban. A levelezőszerverek védelmét egy támadást bejelentő modul és a támadó levélküldését megakadályozó front-end modul látja el. A feketelista szerver tulajdonképpen egy DNS kiszolgáló, ahova a kliensektől érkező bejelentések és lekérdezések is DNS lekérdezés formájában utaznak. A DNS lekérdezésre a szerver egy IP-címmel válaszol, ami a kliens oldalon jelentheti akár azt, hogy a kérdezett IP támadóhoz tartozik, akár azt, hogy ártatlan. A meglevő rendszerek mellé beépítve, azoknál erőforrás megtakarítást lehet elérni, mivel a DHA támadók levelei nem kerülnek a lassabb, erőforrás igényesebb tartalomszűrő mechanizmusok rostája alá, korábban ki lehet tiltani őket a rendszerből. A rendszer valós környezetben való helytállása bizonyítja, hogy megfelelően működik és az alkalmazott védelemi módszer eredményes. A cikkben ezen valós rendszer által összegyűjtött eredményeket elemezzük és rendszerezzük, bemutatva, hogy milyen lehetőségek vannak a támadások csoportosítására az összegyűjtött információk alapján.

1. Bevezetés

Az emberek az egyre növekvő kéretlen levelek áradatának, 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 használják címüket, vagy akár azt is, hogy a weblapjukon rajta hagyják-e ezt a fontos személyi adatukat. Mindkét esetben ugyanattól kell tartani: a keresőrobotok képesek összegyűjteni a `mailto:user@levelcim` alakú hivatkozásokat. A cél sajnos már minden Internet-felhasználó számára nyilvánvaló: a címeket kéretlen levelek, spamek kiküldésére kívánják felhasználni. A fórumok ilyen szempontból kiemelten veszélyesek, hiszen ha kifejezetten nem korlátozzuk az e-mail címünk szerepeltetését, akkor minden hozzászólásunk mellé odakerülhet.

Egy alternatív e-mail címgyűjtési lehetőség az emberi hiszékenységet kihasználó támadási forma: a hamis oldalak és kérdőívek módszere *(phishing)*. Egy népszerű, látogatócsalogatónak tűnő oldalon valamilyen ügyes fogással (például nyereményjátékok, reklámajándékok) ráveszik az áldozatot, hogy beírja az adatait. Így garantáltan működő címeket tudnak a támadók összegyűjteni.

Ha a felhasználó a fent említett e-mail cím gyűjtési lehetőségeket kizárta, ám gondosan kezelt e-mail címére egyszer csak kéretlen levelek kezdenek el özönleni, akkor e-mail szolgáltatója nagy valószínűséggel egy címkinyerő, azaz *directory harvest attack (DHA)* támadásnak esett áldozatul.

A DHA témája sokszor előkerül, és a kereskedelmi antispam termékek egy hirtelen mozdulattal ki is pipálják az általuk nyújtott szolgáltatások listáján, elfelejtvén megemlíteni, hogy milyen módszert is használnak a támadás kivédésére. A továbbiakban a lehetséges módszereket foglaljuk össze és javaslatot teszünk egy hatékony védelmi mechanizmusra.

1.1. Miért lehetséges a címkinyerő támadás?

A DHA problémája a levéltovábbítási protokollban *(simple mail transport protocol, SMTP)* [1] gyökeredzik: az e-mail szerverek, azaz az SMTP kiszolgálók, vagy más kifejezéssel élve levéltovábbító ügynökök *(mail transport agents, MTA)*, ha megfelelő e-mail címre kapták a levelet, úgy nem adnak semmilyen visszajelzést, egyszerűen csak elfogadják azt. Azonban a szerver, ha egy nem létező címre kap levelet, úgy vagy azonnali, vagy későbbi visszajelzést adhat arra nézve, hogy a felhasználó postafiókja nem létezik.

A címkijutás 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 szolgáltatás megtagadási *(denial of service, DoS),* azaz a hardver vagy szoftver megbénításával, illetve működésének zavarásával a felhasználót elérhetetlenné tevő támadást eredményez.

1.2. A támadás fajtái

A DHA támadást, azaz a címlista-kinyerő támadást, két típusba sorolhatjuk: az egyik „brute force” jelleggel az összes lehetséges karakter, illetve szótag kombinációt kipróbálja, mint e-mail címet. A másik jóval szofisztikáltabb: tipikusan előforduló e-mail címeket generál vagy gyűjt emberek vezeték és keresztnevéből, gyakran előforduló szavakból, szóösszetételekből, továbbá ismert e-mail azonosítókból.

Másik lehetséges csoportosítása a DHA támadásnak a felhasznált IP-címek száma alapján történhet: az „alap” változatban a támadó ugyanarról az IP címről próbálkozik, a másik esetben több IP címmel rendelkezik és ezeket felváltva használja a támadáshoz, és ezzel egy eloszott címlista-kinyerő támadást hozva létre *(Distributed DHA)*.

2. DHA-val kapcsolatos munkák

A DHA problémája többnyire ismert, a védekezés viszont jelen pillanatban meglehetősen rendezetlen, mivel mindenki a saját maga által kifejlesztett eszközét próbálja használni. Azon cégek, amelyeket DHA nem ér, többnyire nem is védekeznek. A kereskedelmi termékek funkciójukat tekintve inkább antispam termékek, és nem a DHA támadás ellen vannak kihegyezve. Nagyrészt a valós időben frissített fekete lista *(Real-time Black/Block List, RBL)* alapú megoldásokat támogatják levél érkezésekor, azaz nyilvános RBL-listákon ellenőrzik a feladó címét, hogy támadónak minősítették-e már korábban.

A specifikusan DHA elleni védekezésre felkészített termékek közül az egyik legegyszerűbb megoldást választotta a *Kerio MailServer* [16]: felfigyel a nem létező postafiókoknak küldött levelekre és egy bizonyos szám felett elkezdi szűrni a lehetséges támadókat. A *Secluda Inboxmaster* [17] már konfigurálható SMTP hibaüzenetek beállítását teszi lehetővé, így ha egy spamet detektálnak a levél kézbesítés közben, a szerver egy válaszüzenetet küld a feladónak, hogy nem létező e-mailre próbált levelet küldeni. Ezzel a megoldással az a legfőbb probléma, hogy a DHA támadást nehezen szűri ki, hiszen az ebben a támadásban részvevő e-mailek általában nem tartalmaznak spamet, amit a spamszűrő módszerek így nem jeleznek.

Komolyabb védelmet jelent a jól bevált elemek egybeépítésével operáló a *Styx Mail Filter* [14]: itt egy hardver-szoftver együttest kap a vásárló, ami a kéretlen reklám levelek és vírusos tartalmak szűrését végzi a levelek levelező rendszerbe jutása előtt. Az alapkivitel szabad szoftvereket használ, így megtalálható benne a *ClamAV* [11] víruskereső és *SpamAssasin* [10] spamszűrő. Ez utóbbi egy RBL-alapú megoldást foglal magában, amely kiegészül egy Bayes szabály-tanuló rendszerrel, *Razor*[1] és *DCC*[2] komponensekkel, ami a levelek szűrését elvégzi, de DHA támadást nem jelent az RBL-szerverek felé. Az is előfordul, hogy a termék dokumentációja alapján nem tudni, hogyan működik, de a hatékonyság miatt, nagy valószínűséggel RBL-alapú, ilyen például az *eSafe Advanced Anti-spam Software* [15].

Az egyszer használatos e-mail címek szükségessége esetén egy lehetséges megoldást nyújthat a *mailinator* [9]. Egy azonosítás nélküli e-mail szervert valósítanak meg, ami semmi másra nem jó, mint hogy levelet fogadjon. Bármilyen címzettnek erre a címtartományára érkező levelet elfogad, aminek a postaládáját meg lehet tekinteni belépve az oldalra. A leveleket és az ideiglenes postaládákat óránként ürítik, így arra is jó lehet, hogy például egy fórumra való bejelentkezéshez szükséges megerősítő e-mailt elküldenek erre a helyre, amit megnézünk egyből, és megerősítjük belépésünket. Mivel semmilyen azonosítás nincs, ezért bárki meg

1 Vipul's Razor [12] – egy elosztott, kollaboratív, spamfelismerő és -szűrő hálózat. A rendszernek állandóan frissülő adatbázisa van a felhasználók és a rendszert használó kliensek által beküldött spamek ujjlenyomatáról, azaz azokról a levelekről, amit a felhasználók spamnek ítéltek. Egy levél vizsgálata úgy történik, hogy ellenőrzik a levél ujjlenyomatát, nem szerepel-e a Razor feketelistáján.

2 Distributed Checksum Clearinghouse [13] – A Razor-hoz nagyban hasonló megoldás, de a kliensek itt minden e-mail hash lenyomatát átküldik, és a rendszer azt a lenyomatot ítéli egy kéretlen reklám levél lenyomatának, amit nagyon gyakran jelentenek neki.

tudja nézni bármelyik postafiókot. Ezzel a módszerrel egyben egy *honeypot*[3]-ot is megvalósítanak, és egy órára visszamenőleg meg tudják mutatni, hogy ki az, aki a legaktívabban küldözget nekik levelet.

3. A lehetséges védekezések

A DHA támadás ellen szóba jöhető védekezési mechanizmusok kerülnek bemutatásra a következő részben.

3.1. Új programelemet nem igénylő módszerek

A védekezés egyik lehetséges formája, ha nem telepítünk új programokat a meglévő levelező rendszer mellé, hanem a következő pontokban bemutatott módszerek valamelyikét használjuk.

3.1.1. Egyszer használatos e-mail cím

A védekezés a DHA támadás ellen történhet egyszerűen bonyolultra választott e-mail címekkel, ami a szótáras támadás ellen ideig-óráig véd, de a környezetünk nehezen fogja tudni megjegyezni új e-mail címünket. A védekezés ezen formája brute-force támadások ellen haszontalan lehet, továbbá nem véd a cím kiszivárgásának más lehetőségei ellen.

Az e-mail címmel való védekezés másik lehetséges módja, ha egyszer használatos e-mail címet használunk. A megoldás hibája, hogy a kommunikáció elég egyoldalú lehetőségét teremti csak meg, mivel küldeni gond nélkül fogunk tudni levelet bárkinek, de ha választ is várunk egy levelünkre, akkor a válaszcímeknek léteznie kell mindenképpen. A levelezésünk tehát nem teljesen egyszer használatos, így jelentős karbantartást, adminisztrációt igényel. Teljesen egyszer használatos e-mail esetében válaszra nem számíthatunk.

3.1.2. Különleges szerver konfiguráció

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. Ez több problémát vet fel: 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?

3.2. Új program elemet igénylő módszerek

Ebben az esetben már valamilyen aktív komponens kerül az eddig használt levelező-rendszer mellé. Két eltérő megoldást lehet alkalmazni, illetve ezek együttesét, növelve egymás hatékonyságát.

3.2.1. Egyénileg védekező rendszer

Az egyik megoldás az egyénileg védekező rendszerek. Ekkor minden résztvevőnek van egy saját önműködő rendszere, amely a döntéseit egyéb rendszerektől függetlenül hozza. A támadásszűrést a levéltovábbítás során keletkező hibaüzenetek alapján lehet elvégezni.

Ha a támadó DHA támadás során levelet küld, akkor téves címzettnek küld e-mailt egy adott IP címről, majd később újra fog próbálkozni ugyanarról az IP címről másik tévesen címzett levéllel. Elosztott 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. A támadás elosztottsága függhet a detektált szűrési módszertől és a támadó által várt haszontól. Felmerülhet az a kérdés, hogy mennyire bízhatunk meg a feladó IP-címének valódiságában. Ha tudjuk, hogy a levelet végül egy megbízható levelező szerver továbbította felénk, akkor a szerverrel fel kellett tudnia építeni a kapcsolatot a levélküldőnek, így a címe nem lehet hamis, ha pedig nem megy keresztül több levelező szerveren, akkor velünk is képesnek kell lennie kapcsolatot kiépíteni, ami publikus cím tartományok esetén csak úgy lehetséges, ha legalább a címtartománya (subnet-je) valós (részletes vizsgálat [5]).

3.2.2. Hálózaton alapuló védelem – a javasolt rendszerünk

Másik lehetséges védelmi mechanizmus a hálózaton alapuló védelem. Ekkor a rendszer a hálózat egyéb résztvevőivel együttműködve próbál védekezni a DHA támadás ellen. Javasolt megoldásunk a következő:

Ha egy támadó egy ismeretlen címre küld egy e-mailt a megtámadott szerveren, a megtámadott szerver küld egy hibajelentést a központi szervernek. Ez a hibajelentés tartalmazza a támadó IP-címét, a kipróbált e-mail címet, és a támadás idejét. A központi szerver gyűjti ezeket a jelentéseket, és ha túllép egy küszöböt az ezen IP-ről jövő próbálkozások száma, akkor behelyezi a támadó IP-címét a feketelistára. A szerver a listára kerülés után is jegyzi a támadó kísérleteit, így nem hagyja elévülni a bejegyzést. A feketelista tartalmát csak konkrét cím vonatkozásában lehet lekérdezni a szervertől, azaz a szerver egy igen-nem választ ad arra a kérdésre, hogy egy e-mail feketelistás-e vagy sem.

A feketelistákról (Black Lists) röviden:

Eredetileg a kéretlen leveleket küldőik saját e-mail címükről küldték szét, mintha csak rendes levelet küldenének. Ezeket a felhasználókat (számítógépeket) könnyen azonosítani lehetett, majd kitiltani őket viselkedésük miatt, így a levélküldők elkezdtek levél közvetítőket *(open relay*[4]*)* használni, melyek átvették a levéltovábbítás terhét. Legújabban kompromittált kliens gépeket használnak *(zombie*[5]*)*. Ezzel elérhetik, hogy kevés

3 Általában egy, vagy több hálózati csatlakozással bíró, valamilyen sebezhető operációs rendszert és szolgáltatást emuláló rendszer. A támadók könnyű célpontnak vélik és felfedik ezáltal magukat és szándékukat, így tőlük már az éles rendszer védhetővé válik.

4 Olyan levéltovábbító szerver, mely hajlandó olyan levelek továbbítását is átvenni, hol sem a feladó, sem a címzett nem helyi felhasználó.

5 Valamilyen módon trójai programot juttatnak a felhasználóhoz, mellyel számítógépét irányítani lehet. Ezzel tudta nélkül rávehetik naponta akár több száz levél elküldésére is.

erőforrás lefoglalásával, amit egy-egy felhasználó úgysem vesz észre, összességében nagy mennyiségű kéretlen levelet küldjenek szét. Az ismert spamforrás e-mail címeket, spam küldő gépre vonatkozó IP-címeket feketelistákon szokták összegyűjteni.

Az RBL-listákból több fajta van: van ami e-mail címeket, DNS neveket, DSL címeket, open-relay szervereket, open proxy-kat [7] gyűjt. Ezek teljesen naprakészek és ugyanolyan típusú RBL szerverből több is létezik a világon elszórtan más-más szervezetek által üzemeltetve és esetleg egymástól kicsit eltérően megvalósítva. Az, hogy adott céllal és módszerrel is akár több RBL szerver létezik hasznos lehet védelmi szempontból, mert nem olyan könnyű megtámadni, kiiktatni a szervereket. Az is igaz azonban, hogy az RBL szerverek egy része lassan frissül, pontatlan adatokat tartalmaz. A rendszergazda (illetve esetleg a szoftverfejlesztő) feladata lehet, hogy az RBL listák használata során olyan kombinációt dolgozzon ki, amely megfelelően hatékony a szervezet számára (például pontozás alapú heurisztika).

A feketelistás megoldások több szempontból is szerencsések [6]: technikai szempontból segítik megakadályozni a spam bejutását, másrészt képes társadalmi nyomás kifejtésére, megalapozására a kéretlen levelekért felelős gépek, illetve szolgáltatók irányában, hiszen a letiltott berendezéseket használó legitim felhasználók kénytelenek fellépni szolgáltatójukkal szemben a rendszer megfelelő müködésének visszaállítása érdekében.

4. A javasolt rendszer működésének leírása

A javasolt rendszer egy rendszernapló-elemzőből, és egy ennek eredményét később felhasználó front-end modulból áll. Az eredményeket központi nyilvántartásban összegezzük, azaz nyilvántartjuk azokat a gépeket, amelyek DHA támadásban érintettek. A feketelistán IP-címeket tárolunk, és passzív monitorozást végzünk [2].

Ha a DHA támadó küld levelet a rendszernek, akkor a működés a következő: az első levél átmegy az ellenőrzésen, mivel az IP-címe még nem került be a szerver adatbázisába, hiszen még nem volt olyan résztvevő, aki támadást jelentett volna erről a címről. Az üzenet továbbmegy a levelező-szerverbe, ami egyfelől ellenőrzi, hogy kézbesíteni tudja-e a helyi postafiókokba a levelet. Mivel támadás esetén sikertelen a kézbesítés, a jelentés bekerül a rendszernaplóba. A rendszernapló elemző rendszere az e-mail kiszolgáló jelentéseiből valós időben megnézi, hogy a téves címzéssel rendelkező e-mailek honnan jönnek (milyen IP-címről), és ezekről részletes jelentést tesz a központi adatbázisnak.

A rendszer a DNS protokollt használja a lekérdezésekre és jelentés küldésére a védett szerverek és a RBL-szerver között. A DNS protokoll előnyei közé tartozik a robosztusság. A DNS szervere cache-mechanizmusa növeli a rendszer stabilitását, mivel ideiglenes hiba esetén is tudhat megfelelő választ adni lekérdezésekre. A DNS protokoll többnyire a tűzfal konfigurációkon is átjut, nem igényel újabb nyitott portokat. (A DNS teljesítményének részletes vizsgálatát [3]-ban lehet megtalálni.)

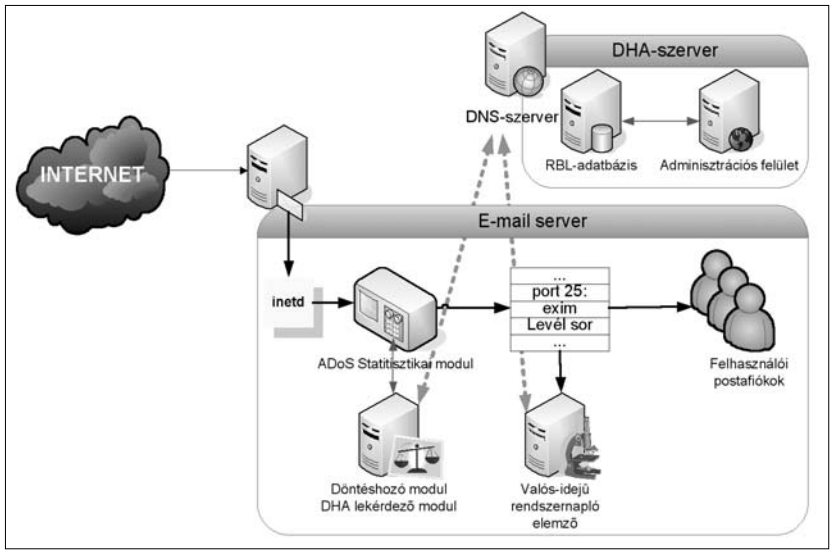
Csökkenthető azon IP-címek támadó adatbázisba kerülésének esélye, akik egyszer-egyszer csak véletlenül elgépelik a címet. A központi adatbázisban nem kerülnek be egyből a bejelentett IP-címek a támadók közé, hanem előtte az előző bejelentéseket is alapul véve a bejelentési időközök gyakoriságát kiszámolja a szerver. Ha ez egy bizonyos értéket átlép, akkor teszi át a bejelentett IP-címet a támadók listájára.

5. A javasolt megoldás implementációja

A rendszer prototípusát *(1. ábra)* linux rendszer felhasználásával hoztuk létre, standard levelezést lebonyolító megoldásokkal. Új levél érkezése esetén az *inetd* rendszerprogram működésbe hozza a levelező szervert. Ez hagyományosan a 25-ös TCP portra érkező kérésekre figyel, és elindít hozzá egy MTA-t (pl. sendmail, postfix, exim stb.) Ám a mi esetünkben nem közvetlenül adjuk át a kérést a levelező szervernek, hanem egyik modulunkon keresztül átvezetjük a kérést. Ez a modul felelős a DHA támadások kiszűréséért, azaz az ismert támadók kitiltásáért.

A DoS frontend [4] előbb statisztikai módszerekkel ellenőrzi, hogy az adott IP címről nem hajtanak-e végre DoS támadást a levelező szerver ellen, és ha ezen a szűrésen átment az IP, akkor kerül sor a DHA támadással kapcsolatos ellenőrzésre. DoS támadás érzékelése esetén a DoS frontend modul eldobja az adott támadó felől jövő TCP kapcsolatokat. A DHA támadó fe-

1. ábra A rendszer prototípusa



lől jövő levél ezután nem megy tovább a levelező rendszer felé, tehát nem kerül kézbesítésre és így nem keletkezik újabb bejelenteni való a szerver felé.

A szűrésen átment TCP kapcsolatot továbbadjuk a levelező szervernek, ami a teszt környezetekben *exim4* levelező szerver. A rendszernapló elemző a linux *syslog* naplóállományában valós időben keresi a levelező rendszer által generált jelentéseket. A különböző levelező szervereknek a rendszernapló bejegyzései eltérőek, így más-más bejegyzések vizsgálatára is fel kellett készíteni az elemző modult. A naplófájl típusát egy külső konfigurációs fájlban lehet beállítani a modul regisztrálásakor használt azonosító és titkos kóddal együtt. Az RBL-adatbázis *MySQL*-ben lett megvalósítva. Az adminisztrációs felület Apache és PHP futtató környezetet igényel. A rendszernapló elemző modult és a RBL-szerver Perl-ben lett implementálva. A rendszer működés közben is megtekinthető [18], illetve a kliens és szerver prototípus is letölthető.

6. A javasolt rendszer vizsgálata

Az alábbiakban a megvalósított rendszer más megoldásokkal kerül összevetésre, illetve a védekezési eljárás és a védett rendszerek támadhatóságát vizsgáljuk meg.

6.1. A rendszer előnyei

Több rendszer az egyéni védekezés módszerét, a gépek önálló védelmét valósítja meg, amivel az a nyilvánvaló baj, hogy ha egyetlen gépet védenek és nem egy központot használnak, akkor egy széles körben elosztott támadás ellen nem véd. Az általunk javasolt központosított megoldás a központ leállása esetén hasonló módon képes önálló döntést végrehajtani.

Több komplett antispam rendszer állítja magáról, hogy védelmet biztosít a DHA támadások ellen, de a megoldás által használt módszert nem ismerteti. Érdekes, hogy a kereskedelmi szoftvergyártók az RBL-szerverekkel együttműködnek egy levél érkezésekor, azaz kiszűrik az ismert támadók IP-címeit, de támadás esetén többnyire nem járulnak hozzá ezen listák automatikus bővítéséhez.

A rendszerünk támadást bejelentő megvalósítása is RBL-alapú és integrálható más rendszerekbe. 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 tudni károkat okozni, amennyiben a támadást a szűrést végző rendszeren bejelentik központunknak. A rendszer kliens oldalának megvalósítása komponens-alapú, aminek több előnyös következménye is van:

– a támadók bejelentési és a tiltási mechanizmusa különválasztható;
– egy már meglevő rendszer is kiegészíthető vele, illetve akár csak bizonyos komponenseivel, így növelve a meglévő hatékonyságát is, nem kell a teljes rendszert átalakítani;
– a komponensek transzparensek kívülről, így a kiesésük esetén nem teszik a rendszert használhatatlanná;
– a DHA védelmi komponens segíti, hogy a gépek védelme komplex, átfogó legyen és a meglévő vírus és spamszűrőket kiegészítve nyújtson védelmet.

6.2. Téves riasztások kezelése

A rendszer támadóknak tekinthet olyan levélküldőket is, akik csak véletlenül elgépelik a címet és így nem létező postafióknak küldenek levelet. A központi adatbázisba sajnos ilyen esetben is támadóként kerül bele a felhasználó által használt SMTP kiszolgáló. A téves riasztások alacsonyan tartása érdekében több módszer használható, hogy az egyedi téves levelek elválaszthatóvá váljanak a valódi támadóktól: 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.

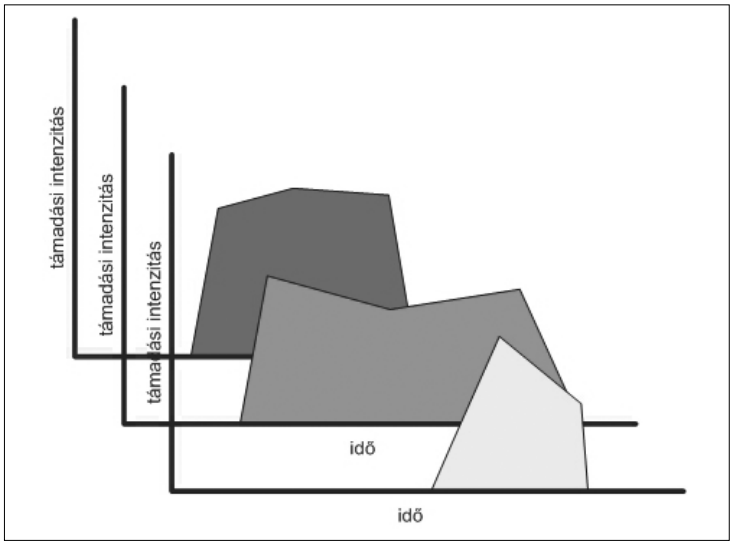
Másrészt alkalmazható öregítés *(aging)* a központi adatbázisban. Az öregítés, azaz az adat eltávolítása adott idő elteltével nagyon fontos szerepet játszik a rendszerben, ezért jól kell megválasztani a használt metódust: ha egy támadót eltávolítunk a listáról, akkor tovább támadhat, ha viszont túl sokáig van rajta, akkor akár a rendes felhasználók forgalmát is megakadályozhatja (például olyan IP címek esetén, amikor a felhasználók gyakran cserélődnek ugyanazon IP cím mögött).

A téves riasztások a rendszer legnagyobb gyengeségét jelenthetik, hiszen a nagy számú téves riasztásból adódóan előfordulhat, hogy a rendszergazda inkább kikapcsolja a védelmet. A téves riasztások problémájának megoldása emiatt a rendszer működésének szempontjából kulcsfontosságú.

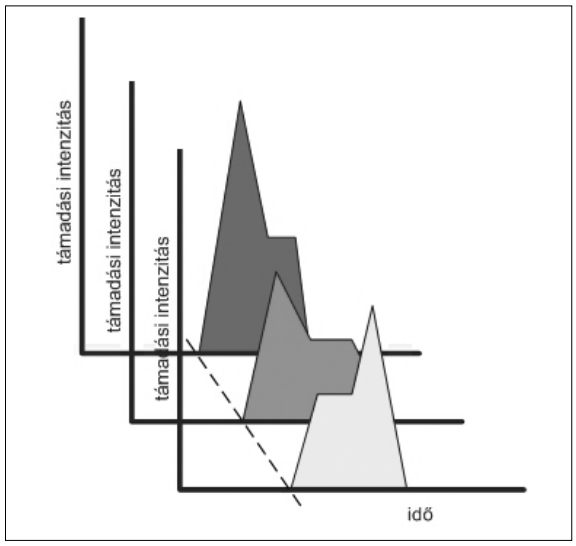
6.3. A védelem eredményessége

A központosított szűrés eredményeképpen a támadó csak nagyon korlátozott számú próbát tehet a védett címtartományokon. A tipikus támadás során sok emailt küldenek ki rövid idő alatt, így a rendszer hamar besorolja a támadókat a tiltólistára. A tiltás után a támadónak ki kell várnia az öregítést, azaz azt az időt, amíg a rendszer kiszedi az IP-t az ismert támadók listájáról, majd a folyamat újrakezdődhet. A támadó gépe egy bizonytalan végeredménnyel záródó próbálkozás alapján tiltólistára kerülhet, és utána azt nem tudja használni nagyobb haszonnal kecsegtető támadásokra sem, például spam kiküldésére. A támadónak tehát védelmünk alkalmazása esetén nem lesz érdeke a DHA támadás mindaddig, míg az abból származó haszon meg nem haladja az alternatív módszerekkel elérhető hasznot.

Természetesen a rendszerünk nem nyújt védelmet a nem védett rendszereknek, így azokon korlátlanul próbálkozhat a támadó. A védelem csökkentheti a támadó nyereségét, gazdaságtalanná téve a DHA támadást, ezáltal a nem védett rendszereknek közvetve okozhat hasznot.



2. ábra
Tudatos támadók jellemző viselkedése



4. ábra
Több vírussal fertőzött gép, mint támadók jellemző viselkedése egymáshoz képest

7. A támadók csoportosítása támadási intenzitás alapján

A DHA támadókról feltételezzük, hogy megkülönböztethetőek. Egyik ilyen megkülönböztető jegyük a támadási statisztikájuk. Megvizsgáltuk a valós rendszerekből gyűjtött támadási statisztikákat, és megpróbáltunk tipikus támadó modelleket kialakítani.

Az egyik tipikus támadó modell a tudatos támadók *(3. ábra)*, akiknek a viselkedésén látszik, hogy nem véletlenül küldenek néha egy-egy levelet, hanem nagy intenzitású, alkalmi támadást indítanak.

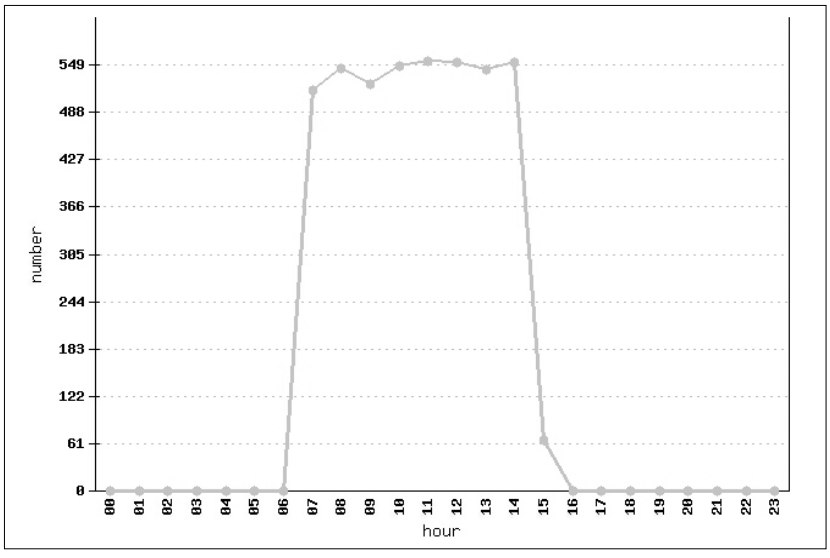
Az időpontokat megvizsgálva azt látjuk, hogy a támadók otthoni számítógépüket bekapcsolva hagyva, tipikusan munkanapokon támadnak. Hétvégén a támadások általában szünetelnek. Ekkor az internet-elérést nyílván másra is használják. Jellemző rájuk egy állandó levélküldési sebesség, mivel a sávszélességüknek egy fix hányadát használják a támadásra. Ez általában nem nagyon ingadozik, félgázzal sohasem támadnak, ha más dolguk van, akkor teljesen leállnak és akkor kezdik újra, amikor megint meg van hozzá az erőforrásuk.

Megvizsgáltunk egy-két ebbe a „tudatos” kategóriába sorolható magyarországi támadót. Az IP számhoz tartozó, úgynevezett RIPE bejegyzés alapján fix című kábelnetes és változó című, ám egy ADSL-poolba (tartományba) tartozó címekről volt szó.

Ezek nem nagyvállalatok által bérelt IP-tartományokból jöttek, és a sávszélességüknek is csak kis hányadát használták a DHA-ra. A sávszélesség kis része is elegendő volt azonban napi 5-6 ezer levél küldésére, ami körülbelül 500 levél/óra sebességet feltételez. Több tudatos támadó között a támadás időpontját illetően általában nincs kapcsolat, ez látható a *3. ábrán* (jelentősége főként a többi ábrával összevetve érthető meg.)

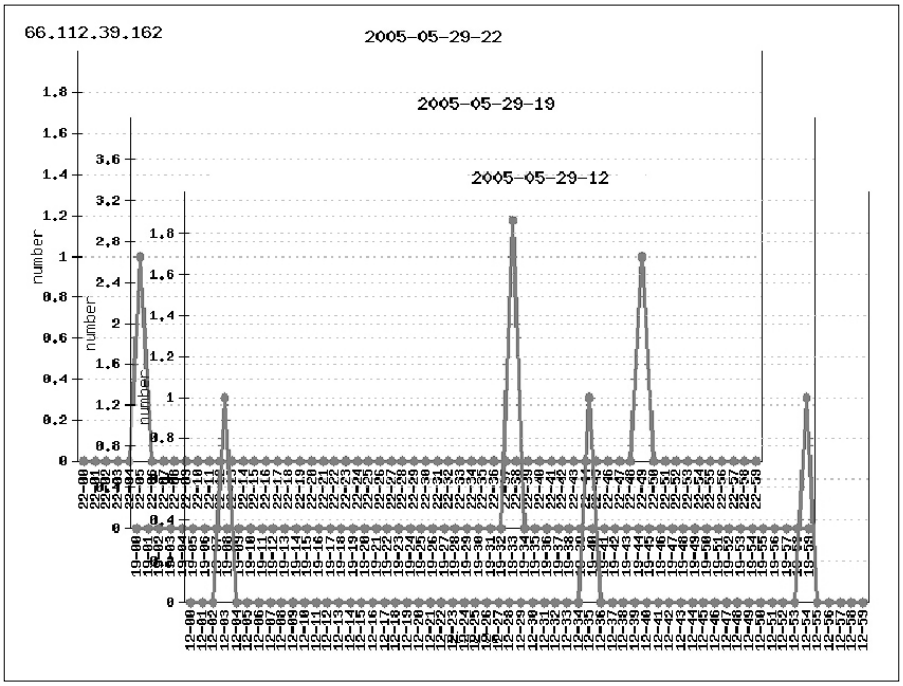
A *vírusokkal fertőzött, így a vírus által támadó gépek* és a trójaiakon keresztül távirányított gépek (ún. zombie-k) levélküldési sebessége kategorizálásunk szerint nagyon ingadozó *(4. ábra)*.

3. ábra Egy tudatos támadó napi statisztikája



Ennek egyik oka, hogy nagyon elterjedtek, valamint hogy hatalmas mennyiségű zombie-gép áll a támadók rendelkezésére, amelyek sávszélességei elég változóak. A támadó nagy mennyiségű gépet irányít, ezeket úgy próbálja meg felhasználni, hogy igyekszik jól kiaknázni azok erőforrásait, ugyanakkor a támadás a lehető legnagyobb mértékben elosztott legyen.

A támadás viszonylag szabályos időközönkénti felbukkanása védett rendszerünkben belső időzítő, illetve koordináció meglétét sugallja. Az időzítés alapján feltételezhető, hogy azonos vírusok azonos időpontban indíthatnak támadást a rendszer ellen. Ezt szemlélteti a következő oldali *5. ábra*.

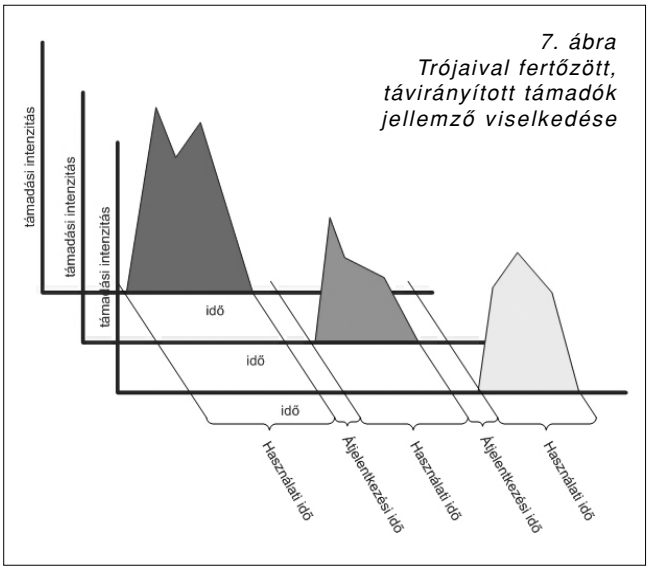


5. ábra
Ugyanazon támadó 3 különböző órában mutatott aktivitása

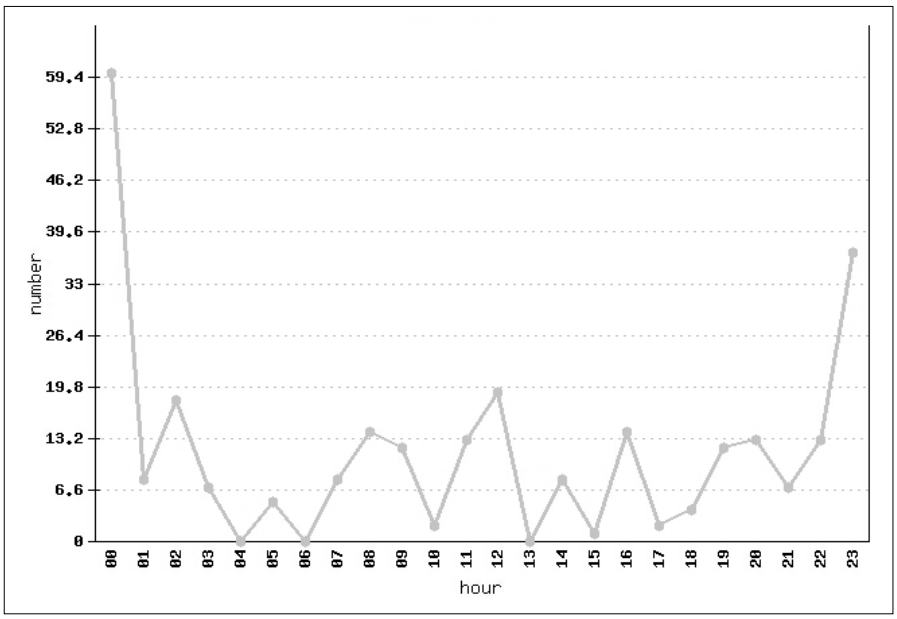
A másik oka a levélküldési sebesség ingadozásának az a cél, hogy jelenlétük rejtve maradjon a tulajdonos gépén, így célszerűen ne zavarja a rendes munkája során a felhasználót, hanem az amúgy is rengeteg szabadidőben használjon mind számítási, mind hálózati erőforrásokat. Egy feltehetőleg vírussal fertőzött gép napi támadási statisztikáját mutatja a *6. ábra*, ahol jól látszik az ingadozó levél küldési sebesség.

A *trójain keresztül távirányított gépek* is főleg napközben aktívak, azonban a távirányító ismeretlen, ezért nem tudni milyen időzónában tartózkodik, így a távirányított gépek időzónáinak összevetése nem sok információval szolgálhatna. Mivel az azonos időzónában levő gépek nagy valószínűséggel egyszerre aktívak, ezért nem célszerű a támadóknak teljesen más időzónában levő gépeket irányítani. Egy támadó feltételezhető aktivitását a zombie-gépein szemlélteti a *7. ábra*.

Eddig a trójaiak egy nagyon kezdő szintű felhasználásáról volt szó, sajnos azonban ezen a területen is vannak *professzionális támadók,* akik az általuk irányított zombie-számítógépeket nagyfokú, jól kialakított koordinációs rendszeren keresztül működtetik, amit az irodalomban többnyire „botnet”-nek, azaz robotok hálózatának hívnak. Ez a támadási módszer lehetővé teszi a támadóknak, hogy egyszerre ne csak egy trójait irányítsanak, hanem rengetegnek adjanak parancsot, ez tehát egy alternatív megoldás egy elosztott DHA támadás indítására az időkoordinációs módszer mellett.



7. ábra
Trójaival fertőzött, távirányított támadók jellemző viselkedése



6. ábra
Vírussal fertőzött gép támadásának napi statisztikája

Távirányított elosztott DHA-ra jó példa a rendszerünket ért egyik nagy arányú támadás, ami a *8. ábrán* látható. Az azt megelőző, illetve rákövetkező órákban átlagosan 1000 támadó szándékú levél érkezett, míg aztán 3 órakor hirtelen majdnem 9000! A támadások vizsgálatához a rendszerünk szűrési funkcióját kiiktattuk, hogy az ne befolyásolja a megfigyelés folyamatát (a támadó ne észlelje levelei szűrését). A támadók jellemzőinek összefoglalását láthatjuk az *1. táblázatban*.

Támadó típusa	Időpont	Relatív aktivitás	Intenzitás	Támadás sebessége	Jellemző aktivitás
tudatos támadó	napközben	nincs összefüggés	egyenletes egy támadót tekintve	akár 500 óránként	*3. ábra*
vírus okozta támadás	bármikor	egy időzónából egyszerre/ nincs összefüggés	még egy támadót tekintve is ingadozik	1-2 óránként	*4. ábra*
távirányított támadó	napközben	időben egymáshoz képest eltoltan	még egy támadót tekintve is ingadozik	10-20 óránként	*7. ábra*

1. táblázat A támadók lehetséges besorolása és jellemzőik

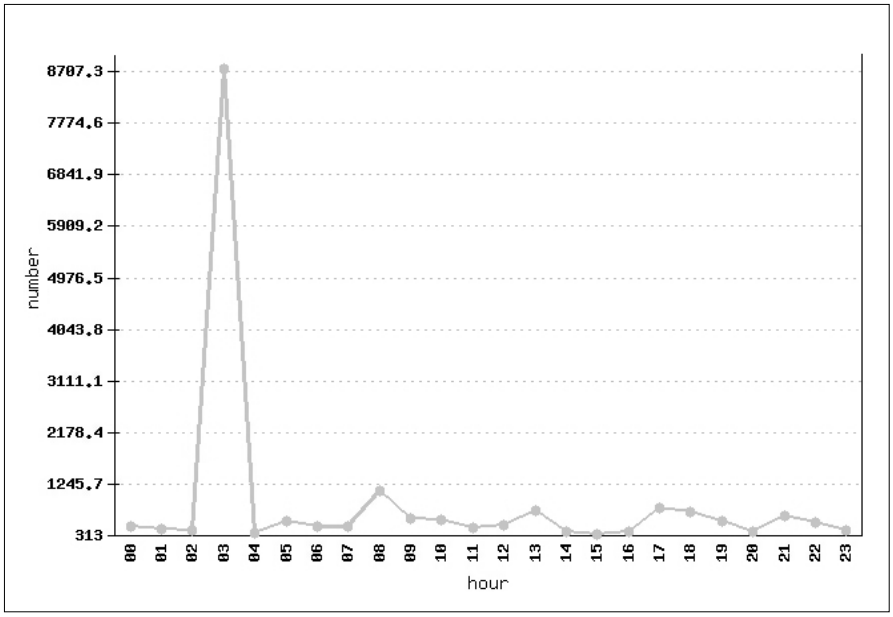
8. Összefoglalás

A cikkben megvizsgáltuk a DHA támadásokat, melyek brute-force jellegű támadások egy levelező-szerver által karbantartott e-mail címek kinyerésére. Számba vettük a lehetséges védekezési technikákat és javasoltunk egy új megoldást a támadások kiszűrésére.

A javasolt megoldásnál a rendszerünk a hálózat egyéb résztvevőivel együttműködve védekezik a DHA támadás ellen, úgy hogy az egyes e-mail kiszolgálók egy központi szerver által karbantartott RBL-listát töltenek fel feltételezett támadókról, valamint ezt a listát kérdezik le új kapcsolatfelépítés engedélyezése előtt. Ezek figyelembevételével bemutattuk az általunk kialakított komponensekből felépülő védelmi mechanizmust, és elemeztük azt.

A rendszerünk felépítése a következő: egyrészt áll egy rendszernapló elemzőből és egy SMTP szervereken működő szűrő komponensből. Másik része egy szerver alkalmazás, ami a szűrők által szolgáltatott eredményeket központi nyilvántartásban összegzi, azaz nyilvántartja azokat a gépeket, amelyek DHA támadásban érintettek. A rendszer által szolgáltatott adatokat alapul véve csoportosítottuk a támadókat és a fenyegetettségeket, amit a levelező szerverekre jelentenek.

8. ábra DHA eredménye egyik rendszerünk ellen



Irodalom

[1] J. Klensin: Simple Mail Transfer Protocol 2001, RFC 2821.

[2] Jaeyon Jung, Emil Sit: An Emprical Study of Spam Traffic and the Use of DNS Black Lists 2004.

[3] Jaeyon Jung, Emil Sit, Hari Balakrishnan, Robert Morris: DNS performance and the effectiveness of caching IEEE/ACM Transactions on Networking, 10(5), October 2002.

[4] Bencsáth Boldizsár, Vajda István: Ados frontend 2005. január

[5] Joshua Goodman: IP Addresses in Email Clients, Microsoft Research, Redmond, WA 98052.

[6] Terri Oda, Tony White: Developing an Immunity to Spam, Carleton University

[7] Open Relay Database, http://www.ordb.org

[8] Distributed Sender Blackhole List, http://dsbl.org

[9] Mailinator, http://www.mailinator.com/mailinator/index.jsp

[10] The Apache SpamAssassin Project, http://spamassassin.apache.org/

[11] Clam AntiVirus, http://www.clamav.net/

[12] Vipul's Razor, http://razor.sourceforge.net/

[13] Distributed Checksum Clearinghouse, http://www.rhyolite.com/anti-spam/dcc/

[14] Styx Mail Filter – vállalati levelezőszerverek védelmére kifejlesztett integrált hardver- és szoftver megoldás, http://www.albacomp.hu/sajtokozlemeny.asp?szam=25 (2005. január)

[15] eSafe Advanced Anti-spam Software, ftp://ftp.ealaddin.com/pub/Marketing/eSafe/White_paper%/WP_eSafe_Anti_Spam/esafe_antispam_whitepaper.pdf

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

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

[18] VIRUSFLAGS (a rendszer működő prototípusa), http://www.virusflags.org