Budapesti Műszaki Egyetem

▷ Híradástechnikai Tanszék

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

Szabó Géza (szabog@crysys.hu)

Szabó Gábor (szaboga@crysys.hu)

Bevezető

▷ E-mail cím őrzése

- egyre növekvő mennyiségű kéretlen levél - SPAM
- levélben terjedő vírusok
- más kártékony kódok

Kinek is adjuk oda az e-mail címünket?

- valamilyen online fórumon
- weblapunkon: mailto:szabog@crysys.hu helyette <szabog at crysys dot hu> vagy képként
- névjegyünkön

⟼ cím-kinyerő (DHA) támadás

Cím-kinyerő támadás

▷ Általános problémák

SMTP protokoll röviden:

- jó levél: nincs visszajelzés az e-mail szerver felől
- nem létező felhasználó címére: azonnali vagy későbbi visszajelzés

A DHA támadás alapgondolata:

- rengeteg levelet küldeni az adott e-mail szervernek
- Azokról a címekről, amelyekről nem érkezik válasz, nyilvántartást felvenni.
- érvényes cím $\mapsto$ címlista

A cím kijutás mellett: DoS

Cím-kinyerő támadás

▷ Támadás fajtái

- felhasznált levél cél-cím alapján
  - “brute force”
  - tipikusan előforduló e-mail címek
- felhasznált forrás IP-cím alapján
  - a támadó ugyanarról az IP címről próbálkozik
  - több IP címmel rendelkezik (disztributív DHA)

Támadás fajtái

▷ “brute force”

```
Mar 30 06:56:49 shamir sm-mta[19028]: j2U4umVY019028: <ujubi@ebizlab.hit.bme.hu>... User
Mar 30 06:57:21 shamir sm-mta[1385]: j2U4vKFx001385: <akuh@ebizlab.hit.bme.hu>... User u
Mar 30 06:57:48 shamir sm-mta[9917]: j2U4vmQ8009917: <puugun@ebizlab.hit.bme.hu>... User
Mar 30 06:58:16 shamir sm-mta[24614]: j2U4wFwZ024614: <rije@ebizlab.hit.bme.hu>... User
Mar 30 06:58:44 shamir sm-mta[6924]: j2U4wijv006924: <baji@ebizlab.hit.bme.hu>... User u
Mar 30 06:59:08 shamir sm-mta[15334]: j2U4x8Sj015334: <wigelu@ebizlab.hit.bme.hu>... Use
Mar 30 06:59:37 shamir sm-mta[18230]: j2U4xbQ4018230: <umez@ebizlab.hit.bme.hu>... User
Mar 30 07:00:04 shamir sm-mta[1665]: j2U504UO001665: <rupuru@ebizlab.hit.bme.hu>... User
Mar 30 07:00:41 shamir sm-mta[24998]: j2U50f1K024998: <dazazu@ebizlab.hit.bme.hu>... Use
Mar 30 07:01:12 shamir sm-mta[6332]: j2U51CbY006332: <feno@ebizlab.hit.bme.hu>... User u
Mar 30 07:01:47 shamir sm-mta[20374]: j2U51l0O020374: <zile@ebizlab.hit.bme.hu>... User
Mar 30 07:02:21 shamir sm-mta[3755]: j2U52LFT003755: <jinofa@ebizlab.hit.bme.hu>... User
Mar 30 07:02:56 shamir sm-mta[19705]: j2U52uGo019705: <peno@ebizlab.hit.bme.hu>... User
Mar 30 07:03:27 shamir sm-mta[14252]: j2U53QhE014252: <ridus@ebizlab.hit.bme.hu>... User
Mar 30 07:04:02 shamir sm-mta[20525]: j2U542Ma020525: <ropa@ebizlab.hit.bme.hu>... User
Mar 30 07:04:35 shamir sm-mta[16265]: j2U54Zhc016265: <efihika@ebizlab.hit.bme.hu>... Us
Mar 30 07:05:09 shamir sm-mta[22642]: j2U558OR022642: <izew@ebizlab.hit.bme.hu>... User
```

Támadás fajtái

▷ Tipikusan előforduló e-mail címek

```
Feb  8 08:04:18 shamir sm-mta[7594]: j1874Hl5007594: <Vulcan@ebizlab.hit.bme.hu>... User
Feb  8 08:18:09 shamir sm-mta[14063]: j187I9Es014063: <snowman@ebizlab.hit.bme.hu>... Us
Feb  8 08:34:22 shamir sm-mta[1441]: j187YLJS001441: <Ricardo@ebizlab.hit.bme.hu>... Use
Feb  8 08:36:15 shamir sm-mta[14478]: j187YLJS001451: <Rambo@ebizlab.hit.bme.hu>... User
```

Lehetséges védekezések

▷ Új program elemet nem igénylő módszerek

- E-mail cím választással
  - bonyolultra választott e-mail címek: brute-force támadások ellen haszontalan
  - egyszer használatos e-mail cím
- Szerver konfi gurálással
  - fogadjon el minden e-mailt és ne jelezzen vissza róla senkinek, a téves leveleket eldobjuk
    A megoldás problémái:
    - a levélküldők nem tudják meg, hogy a cím nem létezik: elárasztathatják a szervert téves levelekkel
    - legitim felhasználók sem kapnak visszajelzést a tévesen címzett levelekről

Lehetséges védekezések

▷ Kitudódott, majd megszűntetett postafiók...

```
Feb  1 00:02:53 shamir sm-mta[19185]: j0VN2U1v019185: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:03:07 shamir sm-mta[17881]: j0VN368V017881: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:06:48 shamir sm-mta[22743]: j0VN6ikZ022743: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:08:03 shamir sm-mta[32292]: j0VN80QC032292: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:13:52 shamir sm-mta[28568]: j0VNDolb028568: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:23:21 shamir sm-mta[4271]: j0VNNKVD004271: <boldi@ebizlab.hit.bme.hu>... No su
Feb  1 00:27:37 shamir sm-mta[20856]: j0VNRN4N020856: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:43:38 shamir sm-mta[19782]: j0VNhbtD019782: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:44:26 shamir sm-mta[17623]: j0VNiPtO017623: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 00:49:26 shamir sm-mta[9012]: j0VNnPPZ009012: <boldi@ebizlab.hit.bme.hu>... No su
Feb  1 01:00:52 shamir sm-mta[19872]: j1100m3T019872: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 01:03:47 shamir sm-mta[25275]: j1103k9e025275: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 01:04:09 shamir sm-mta[2484]: j11048SF002484: <boldi@ebizlab.hit.bme.hu>... No su
Feb  1 01:23:34 shamir sm-mta[16822]: j110NWR6016822: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 01:25:48 shamir sm-mta[3599]: j110PNes003599: <boldi@ebizlab.hit.bme.hu>... No su
Feb  1 01:37:50 shamir sm-mta[30723]: j110blEQ030723: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 01:37:56 shamir sm-mta[25189]: j110br66025189: <boldi@ebizlab.hit.bme.hu>... No s
Feb  1 01:52:01 shamir sm-mta[32132]: j110pxfN032132: <boldi@ebizlab.hit.bme.hu>... No s
```

Lehetséges védekezések

▷ Új program elemet igénylő módszerek

Hoszt alapú védelem.

- Minden résztvevőnek saját önműködő rendszere van, amely a döntéseit egyéb rendszerektől függetlenül hozza.
- A támadás szűrését a levéltovábbítás során keletkező hibaüzenetek alapján lehet elvégezni.

Hálózaton alapuló védelem.

- A rendszer a hálózat egyéb résztvevőivel együttműködve próbál védekezeni a DHA támadás ellen.
- Olyan rendszer is védhető, akit még meg sem támadtak.

A mi megoldásunk

▷ Felépítés

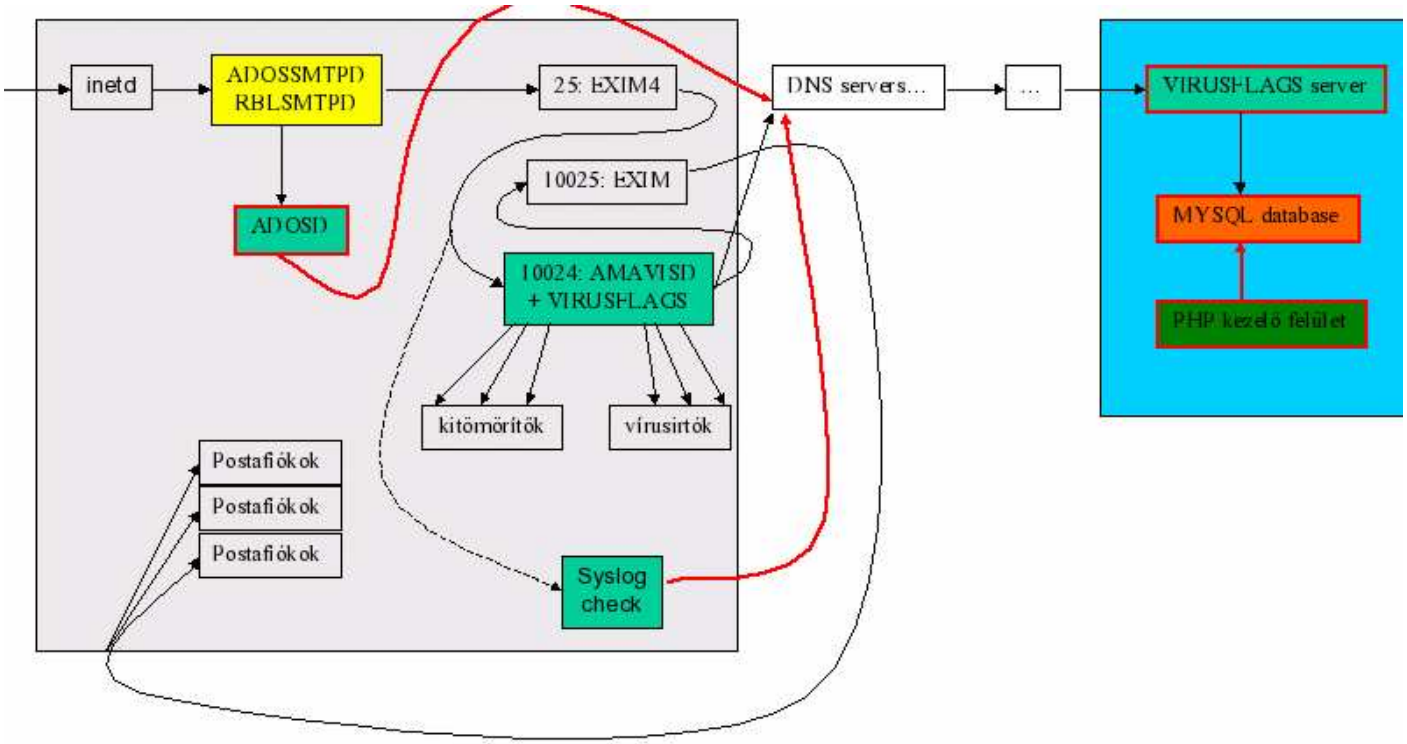
Hálózaton alapuló védelmet valósítja meg.
Felépítés:

- egy syslog elemző
- egy spam detektor
- víruskereső rész

A jelentések és lekérdezések DNS query-ként utaznak a hálózaton.

A mi megoldásunk

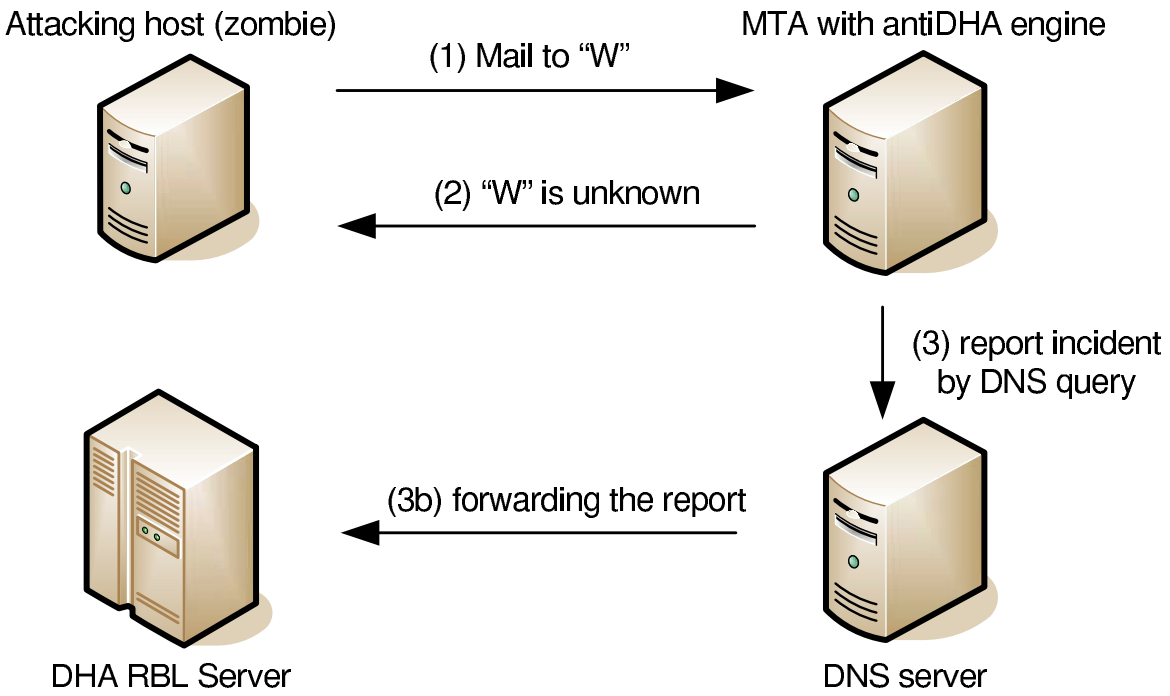
▷ A rendszer működése



1. ábra. A komponensek kapcsolata

A prototípus

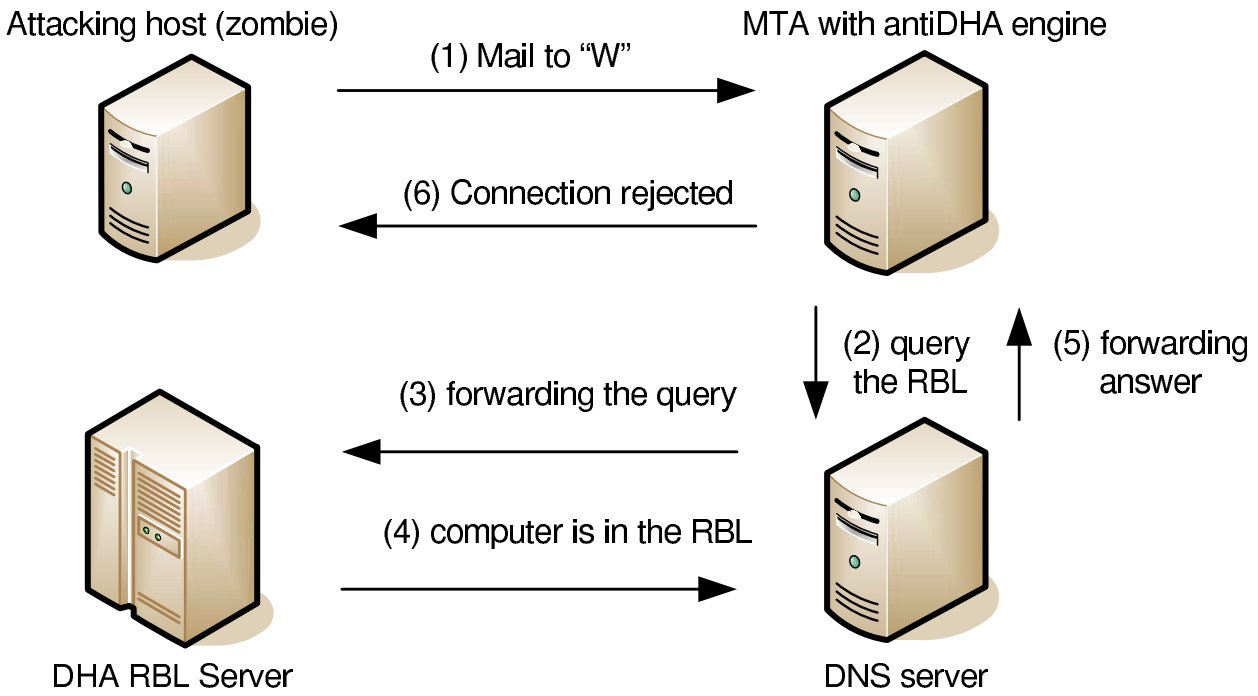
▷ Jelentés generálás



2. ábra. A jelentés generálás

A prototípus

▷ Szűrés



3. ábra. A szűrés menete

Téves riasztások kezelése

▷ Öregítés

„véletlen cím elgépelés” $\mapsto$ öregítés

- adminisztrátor vezérelt öregítés
- egyszerű öregítés
- több-fázisú öregítés

A rendszerünk vizsgálata

▷ Előnyei

- A rendszer szerver oldalának megvalósítása is RBL-alapú és integrálható más rendszerekbe.
- A rendszerünk komponens-alapú:
  - a riportolás és a tiltás különválasztható
  - egy már meglevő rendszer is kiegészíthető vele, illetve akár csak bizonyos komponenseivel, így növelve a meglévő hatékonyságát is
  - a komponensek transzparensek kívülről, így a kiesésük esetén nem teszik a rendszert használhatatlanná
  - a DHA komponenssel együttműködnek vírus és spamszűrő modulok is

A rendszerünk vizsgálata

▷ Támadás a rendszer ellen

DoS támadás az RBL-szerver ellen.

- Alacsony szinten detektálja a szerver a támadó lekérdezéseket és nem kezd erőforrás igényes adatbázis műveletekbe.
- Lekérdezések helyességéről meggyőződünk

Hibás adatok bevitele.

- Korlátozott számú adminisztrátor
- A módosításokról napló készül
- Támogatja a rendszer egy korábbi állapotra való visszaállást.

A rendszerünk vizsgálata

▷ A védelem eredményessége

A központosított szűrés eredményeképpen a támadó csak egy nagyon korlátozott számú próbát tehet a védett domain-eken.

- A támadó címeit sorban feljegyzi, így azt a többi védett domain-en sem tudja felhasználni támadásra.
- A zombie gépeit is elveszti ezáltal.
- A támadó által kiküldendő e-mailek számát is megnöveli
- Nyeresége csökken jelentősen

A rendszerünk vizsgálata

▷ A védelem eredményessége (folyt.)

Dinamikus IP címek. Log fájl vizsgálat valós-időben: újra és újra bekerül a központi adatbázisba a támadó a címcsere esetén is.

Figyelmeztetés küldése. Terveinkben szerepel, hogy a rendszer automatikusan vagy adminisztrátor segítségével jelentést küldjön a támadó ISP-jének, vagy a zombie tulajdonosának.

A mi megoldásunk

▷ A rendszer további szolgáltatásai

Rendszerünk összeköthető spam-felismerő szoftverekkel is.
Erőforrások megtakarítása

Vírusos levél tartalom esetén is jelentés készül. Korábban ismertetett virusflags-server motorját kombinálja. (Tavaly került részletesebben ismertetésre...)
Ha a támadó egyszer DHA-zik, spam-el vagy vírusokat küld, akkor már mást nem fog tudni a védett hálózaton.

A mi megoldásunk

▷ Konklúzió

- Bemutatásra került egy hálózaton alapuló védekezési mechanizmus a DHA támadók ellen.
- A rendszerünket használva csökkenteni lehet a levelező szerver terheltségét megszűntetve a DHA támadásokat, és elkerülni a kitudódott e-mail címeinkre érkező spam-ek áradatát.

A mi megoldásunk

▷ Eddigi eredmények

Helyi illetőségű címek, amikről eddig DHA támadták a levelező szerverünket:

- 217.65.98.75:
  (Tiszanet, fi x IP) naponta több min 4000 (!) levél
- 82.131.136.226:
  (Invitel, ADSL-pool) naponta kb. 400 levél
- 82.131.138.24:
  valószínűleg ugyanaz a valaki
- 82.131.137.65:
  valószínűleg ugyanaz a valaki
- 62.77.226.136:
  (Vivendi, ADSL-pool) naponta kb. 200 levél
- ...

A mi megoldásunk

▷ Megtalálható...

Egyelőre adatokat gyűjtünk.
Mások csatlakozásást is szívesen vesszük:

- http://pics.etl.hu/ szabog/ados/html/index.html a statisztikai interface
- syslog analyzer is letölthető CVS-ből a pics-etl.hu-ról
- a DHA front-end is letölthető CVS-ből a pics-etl.hu-ról