DHA VÉDELMI RENDSZER EREDMÉNYEINEK STATISZTIKAI VIZSGÁLATA

Laboratory of Cryptography and System Security (CrySyS)
Híradástechnika Tanszék
Budapesti Műszaki és Gazdaságtudományi Egyetem

Szabó Géza (szabog@crysys.hu)
Bencsáth Boldizsár (bencsath.boldizsar@crysys.hu)

Bevezető

E-mail cím veszélyben

Mindennapi problémák:

- Állandóan növekvő számú kéretlen levél – SPAM
- E-mailben terjedő vírusok
- Más kártevők (pl. trójaiak, kémprogramok)

Mit tehetünk ez ellen?

- E-mail címhez való hozzáférés korlátozása
  - Honlapokon **`mailto:szabog@crysys.hu`** helyett: **`<szabog at crysys dot hu>`** vagy képként
  - Fórumokon megfelelő beállítások
- Még akad megoldatlan probléma: Directory Harvest Attack (DHA)

Directory Harvest Attack

Támadás leírása

SMTP protokoll röviden:

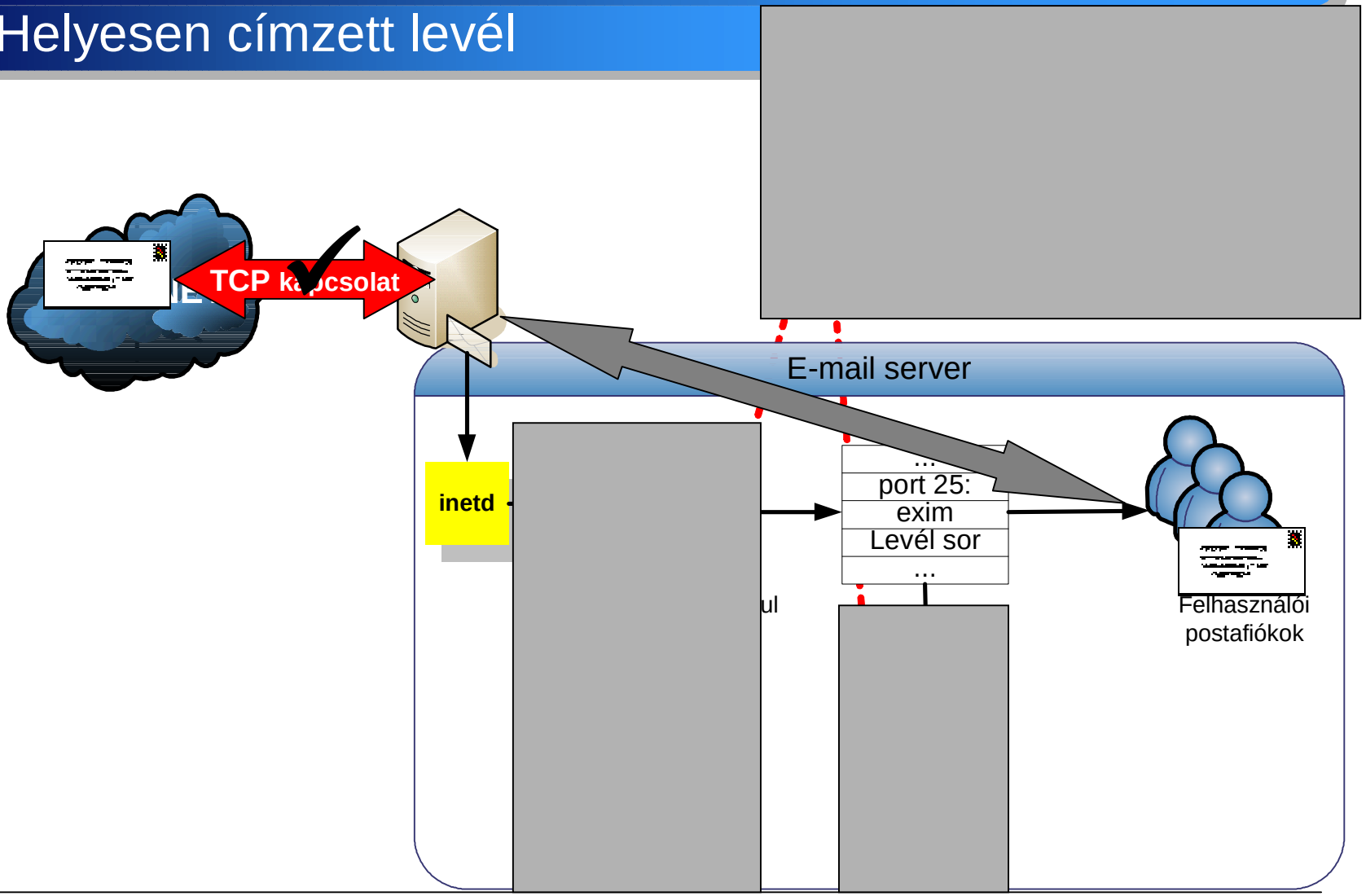
- Rendes levél érkezik:
  a levelező szervertől nincs jelzés
- Nem létező címzettnek küldött levél:
  azonnali vagy késleltetett visszajelzés a szerver felől

A támadás alapgondolata:

- A támadott levelező szervernek sok levelet küldeni
- Azokat a címeket megjegyezni amikről nem jött visszajelzés
- Létező címek $\Rightarrow$ cím-lista

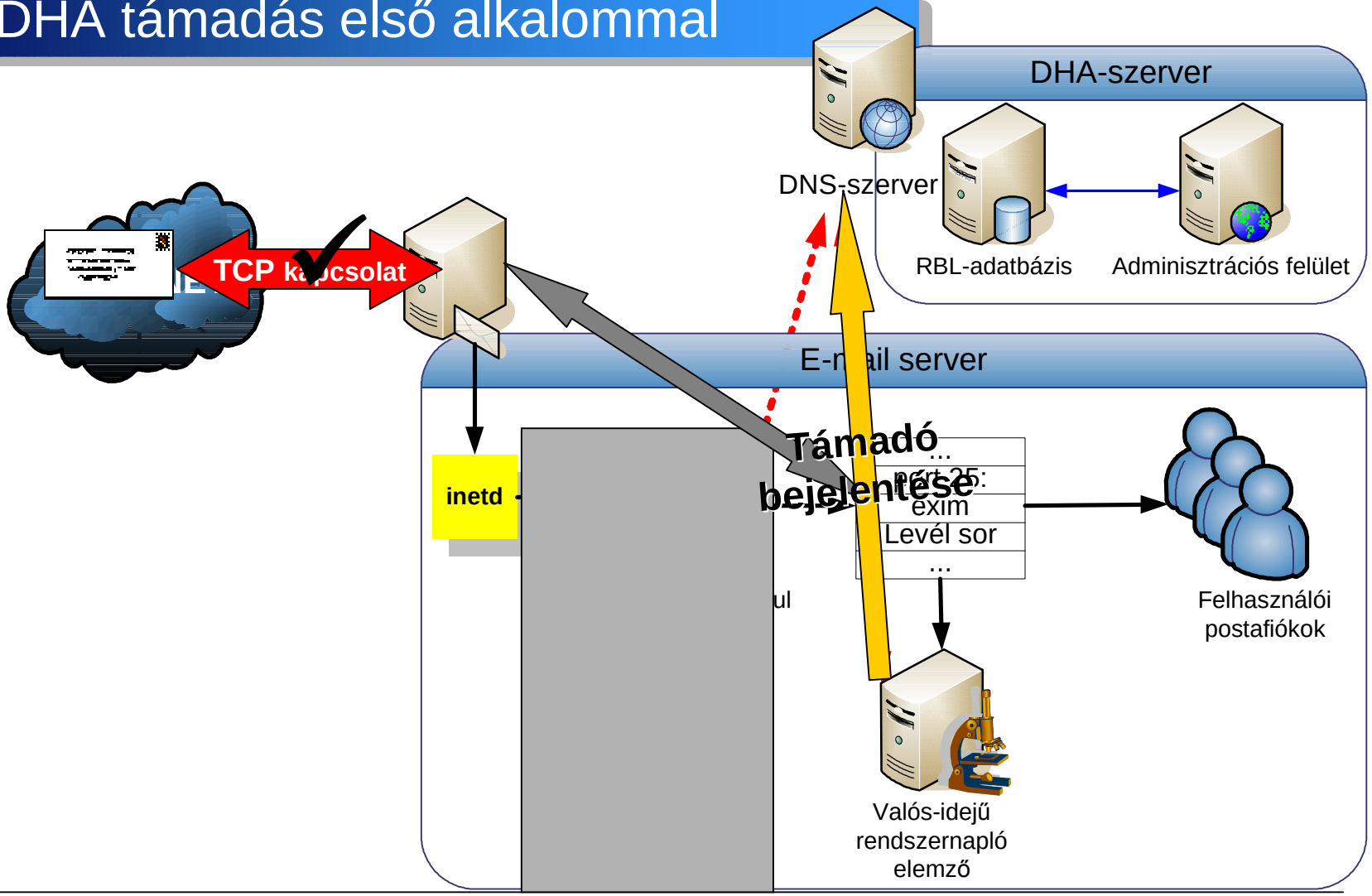
Rendszer működése

Helyesen címzett levél



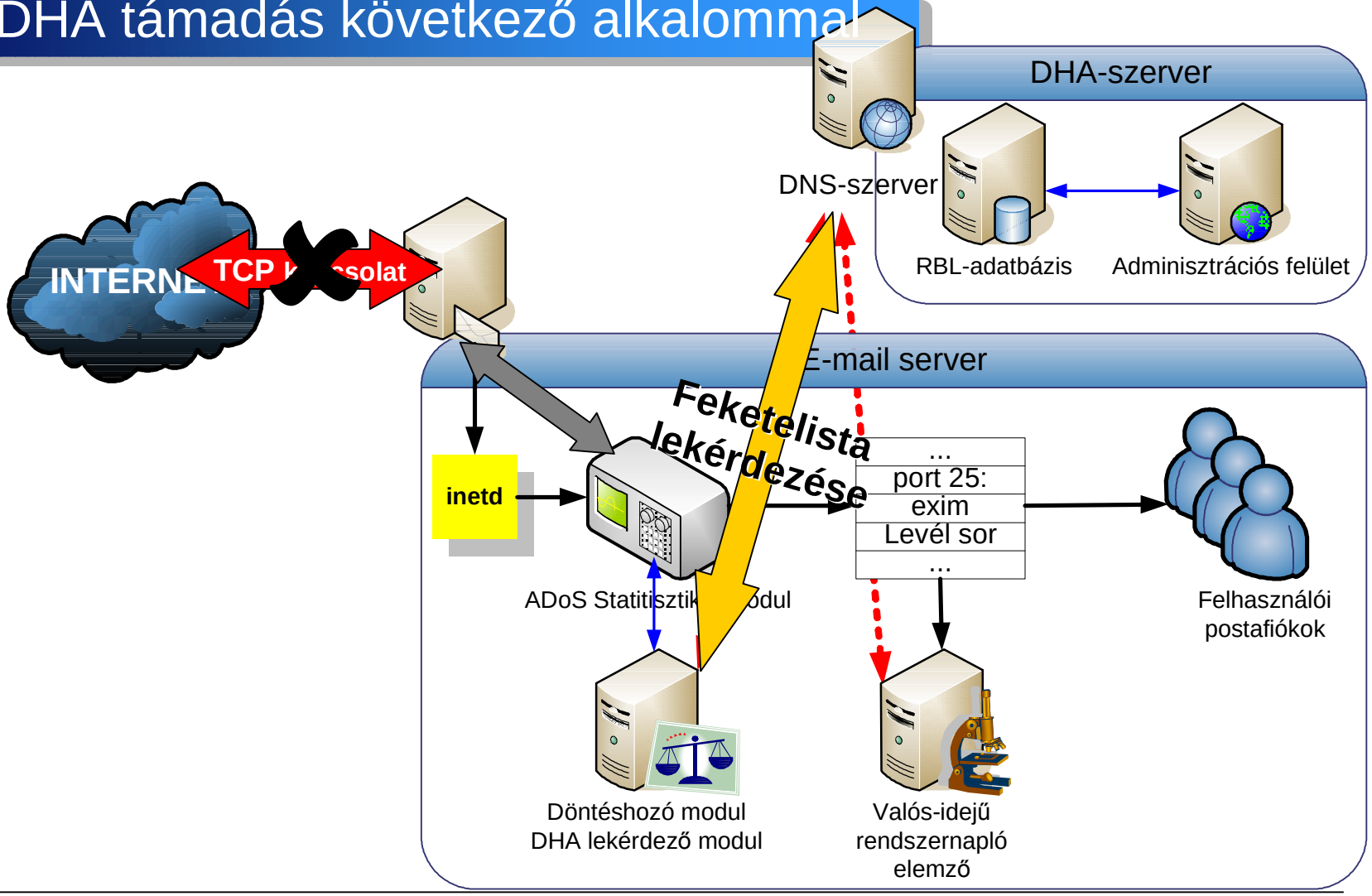
Rendszer működése

DHA támadás első alkalommal



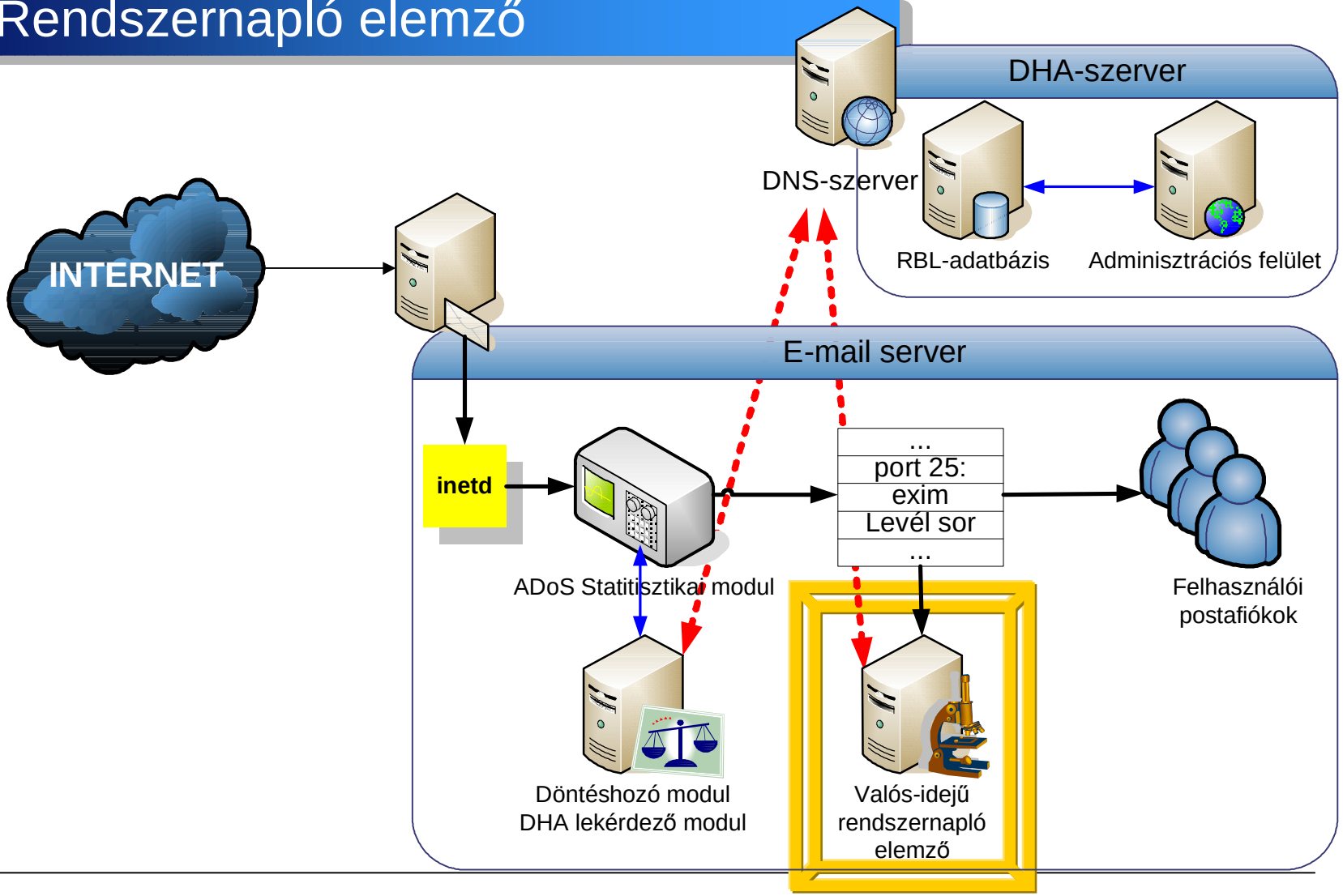
Rendszer működése

DHA támadás következő alkalommal



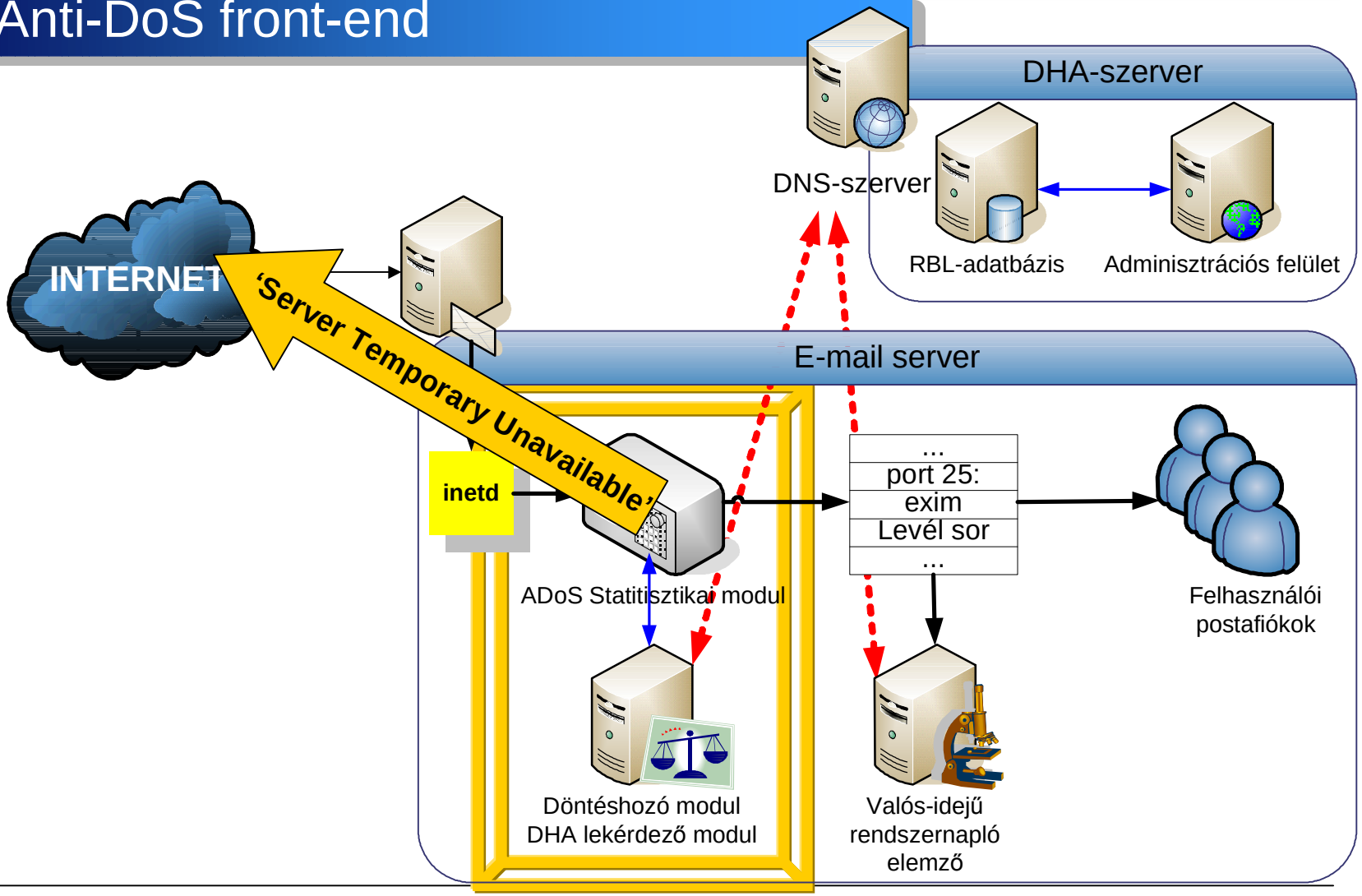
Védelem a DHA ellen

Rendszernapló elemző



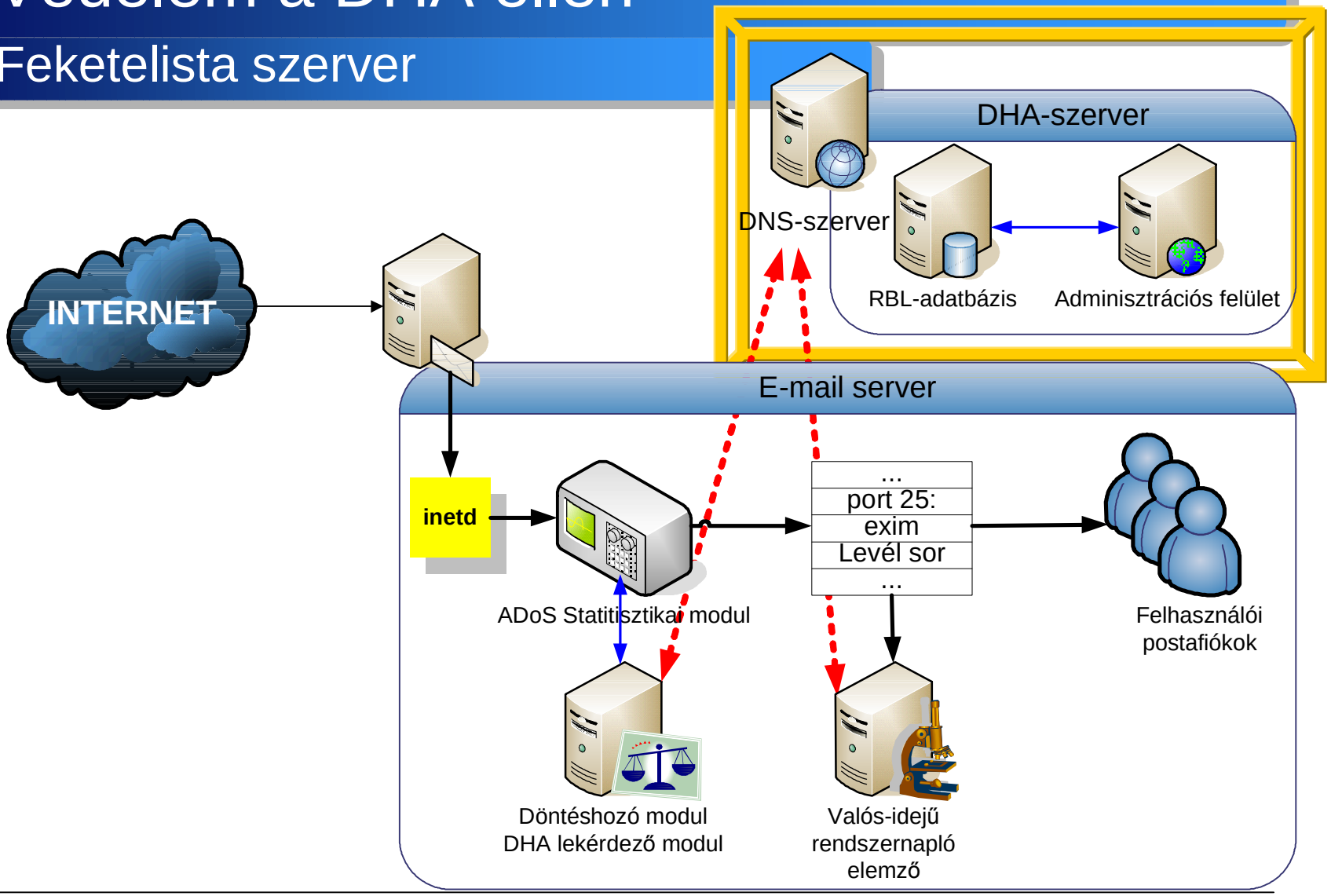
Védelem a DHA ellen

Anti-DoS front-end



Védelem a DHA ellen

Feketelista szerver



Védelem a DHA ellen

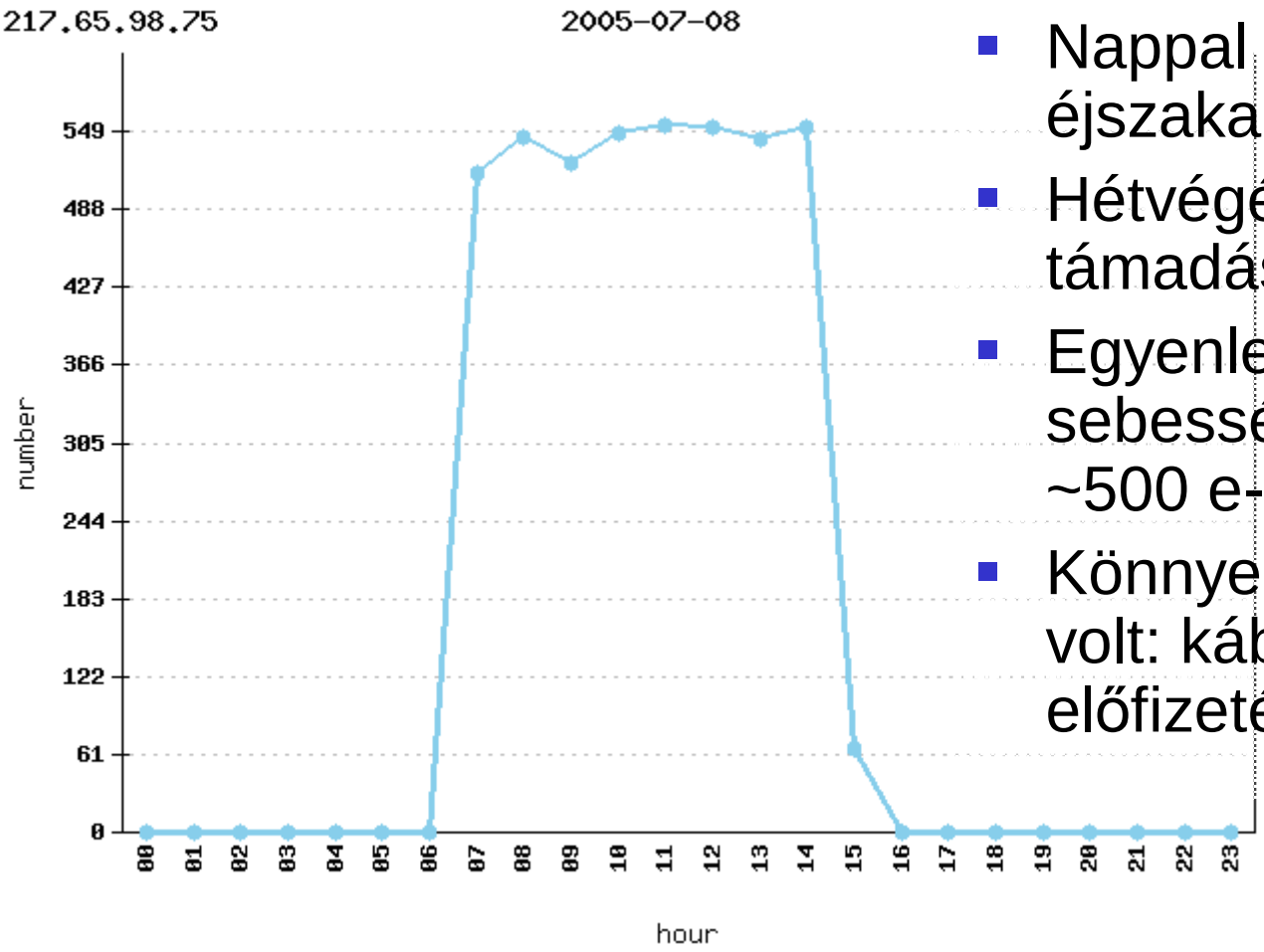
A védelem eredményessége

- A rendszer védelmet nyújt a DHA ellen
- Nem a meglévő protokollokat vagy rendszereket módosítottunk: beépülő komponensek meglévő rendszerek mellé
- Támadó levélből a megengedett félrecímzett levél érkezési intenzitás értékétől függően is csak 1-1 csúszhat át a védelmen
- A komponensek transzparensek kívülről: meghibásodásuk esetén a teljes rendszer viselkedése nem lesz rosszabb, mint nélkülük

Támadók típusai

…a rendszerünkből származó adatok analízise alapján

Tudatos támadó

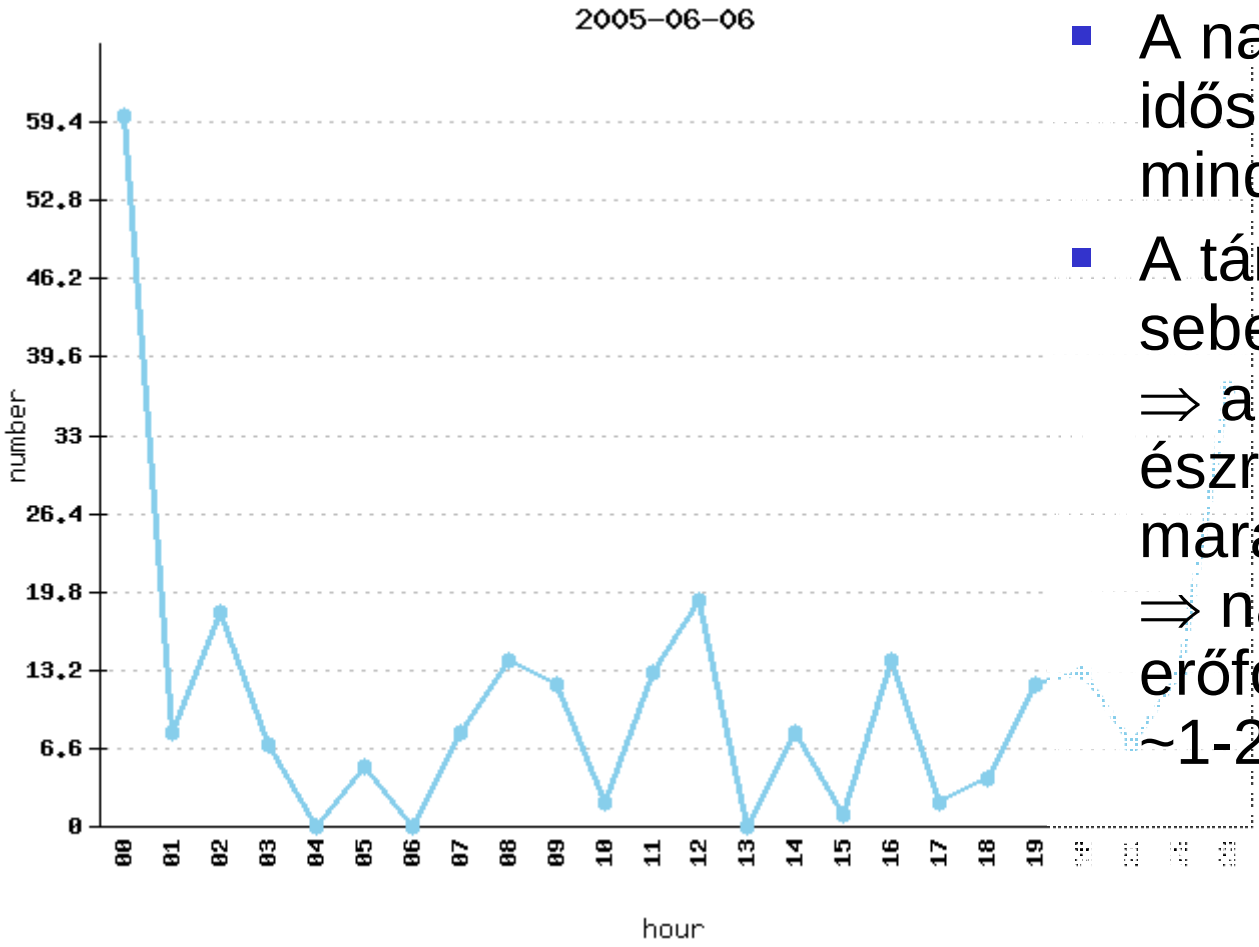


- Nappal aktív, éjszaka nem
- Hétvégén nincs támadás
- Egyenletes sebességgel támad: ~500 e-mail/óra
- Könnyen követhető volt: kábelnetes előfizetés, fix IP-cím

Támadók típusai

…a rendszerünkből származó adatok analízise alapján

Vírussal fertőzött gépek

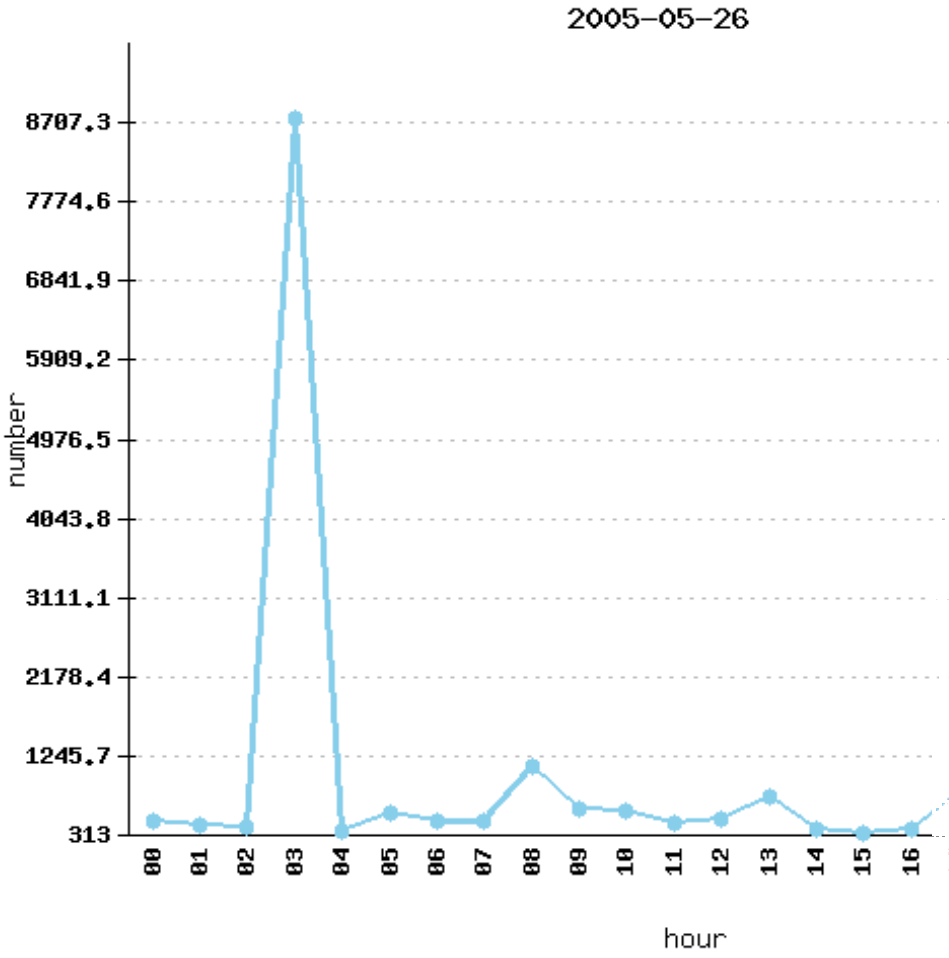


- A nap bármely időszakában aktív, minden nap
- A támadási sebesség változó
  ⇒ a céluk, hogy észrevétlenek maradjanak
  ⇒ nagyon alacsony erőforrás használat: ~1-2 e-mail/óra

Támadók típusai

…a rendszerünkből származó adatok analízise alapján

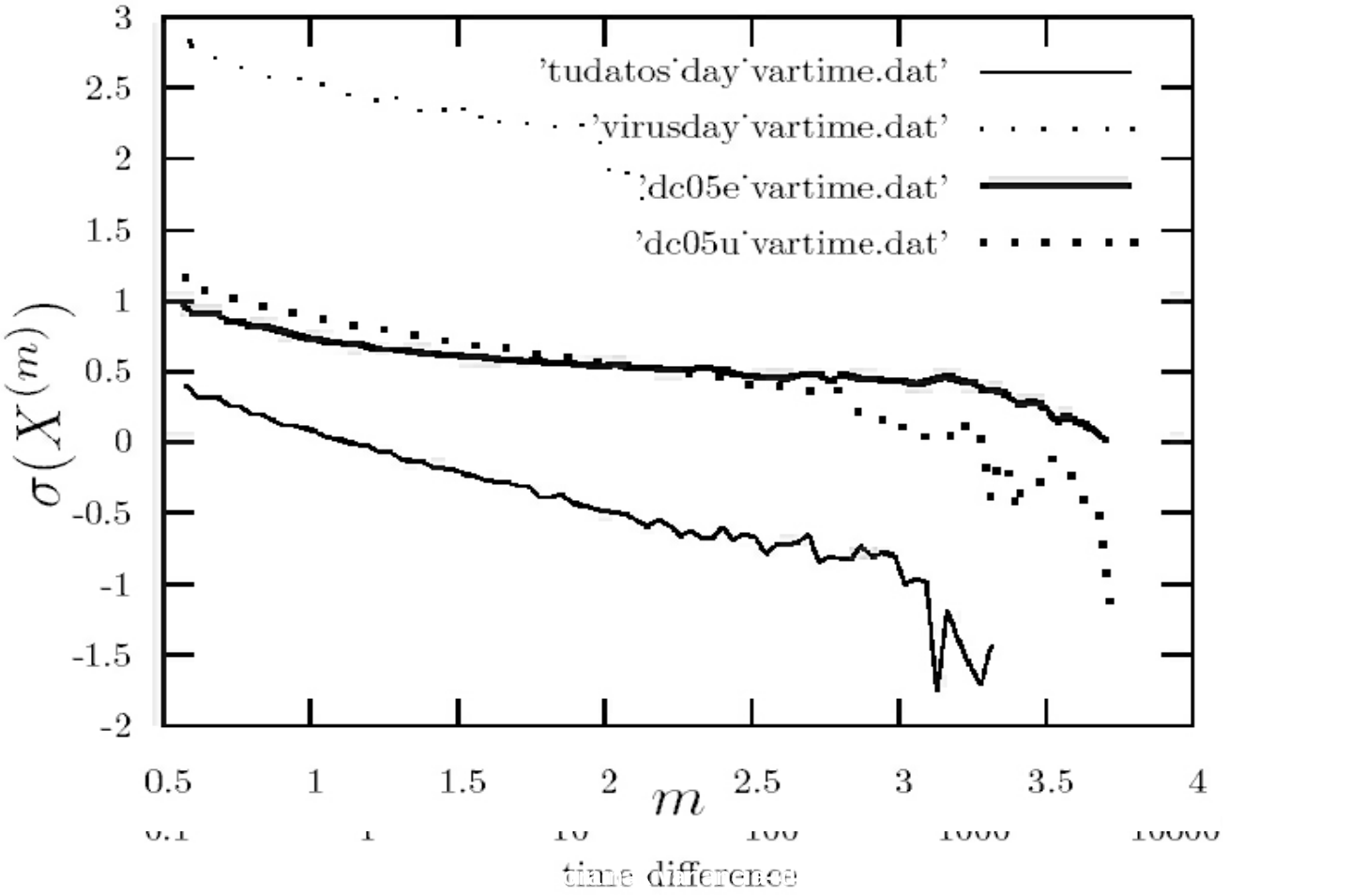
Távirányított zombiek



- Gyanúsan egybeeső támadási időszak
- Előtte és utána nincs támadás: támadó belép a zombiehoz, DHA támadási parancs, kijelentkezik
- Trójaiak párhuzamos irányítása: botnetek
- Hatalmas erőforrások állnak a botnetes támadók rendelkezésére

Támadási adatok

Statisztikai vizsgálata



Összefoglaló

- Hálózaton alapuló védelem

  Egy hálózaton alapuló védelmi rendszert alakítottam ki ami védelmet jelent a DHA támadások ellen.

- A rendszert akkor is meg lehet védeni, ha még meg sem támadták

  A központi feketelista segítségével a rendszert használó összes kliens információt szolgáltat egymásnak, így egy támadó nem csak egy védett rendszert nem tud megtámadni, hanem a többieknek sem okozhat kárt.

- Erőforrás megtakarítás

  A rendszer használatával az e-mail szerver terhelése csökkenthető, a DHA megállítható, és elkerülhető, hogy az e-mail címek spam küldők listájára kerüljön.

A rendszer elérhető

Az adminisztrációs felület címe

www.virusflags.org

Különleges DHA támadó aki egyáltalán nem terheli a levelező szervert