A MAGYAR TUDOMÁNY ÜNNEPE

ÚJ SZÉCHENYI TERV

E(L)JÖVENDŐ

IKT kutatási eredmények a gazdaság és a társadalom szolgálatában

MŰEGYETEM 1782

MAGYAR TUDOMÁNYOS AKADÉMIA 1825

MAGYARORSZÁG MEGÚJUL

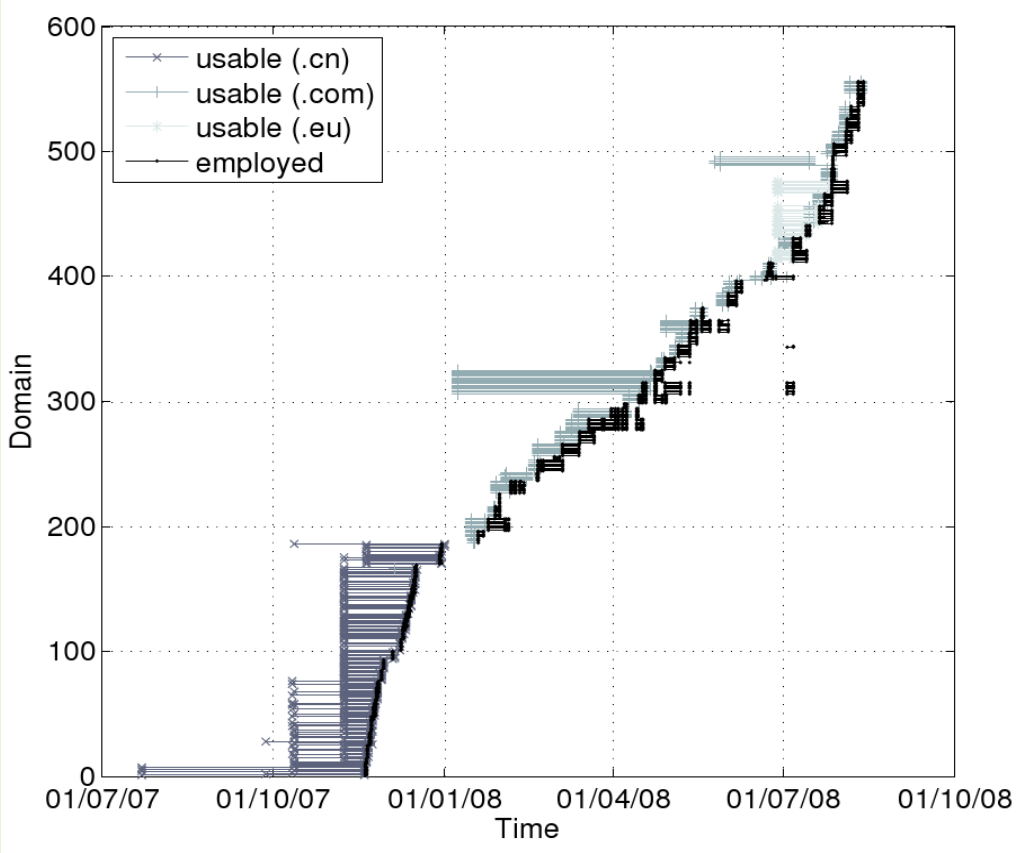
A projekt az Európai Unió támogatásával, az Európai Regionális Fejlesztési Alap társfinanszírozásával valósul meg.

Téma: Hírnévre épülő biztonsági megoldások a jövő Internet architektúrájában

Félegyházi Márk
CrySyS Adat- és Rendszerbiztonság Laboratórium (CrySyS Lab.)
Híradástechnikai Tanszék (HIT)
Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)

www.crysys.hu

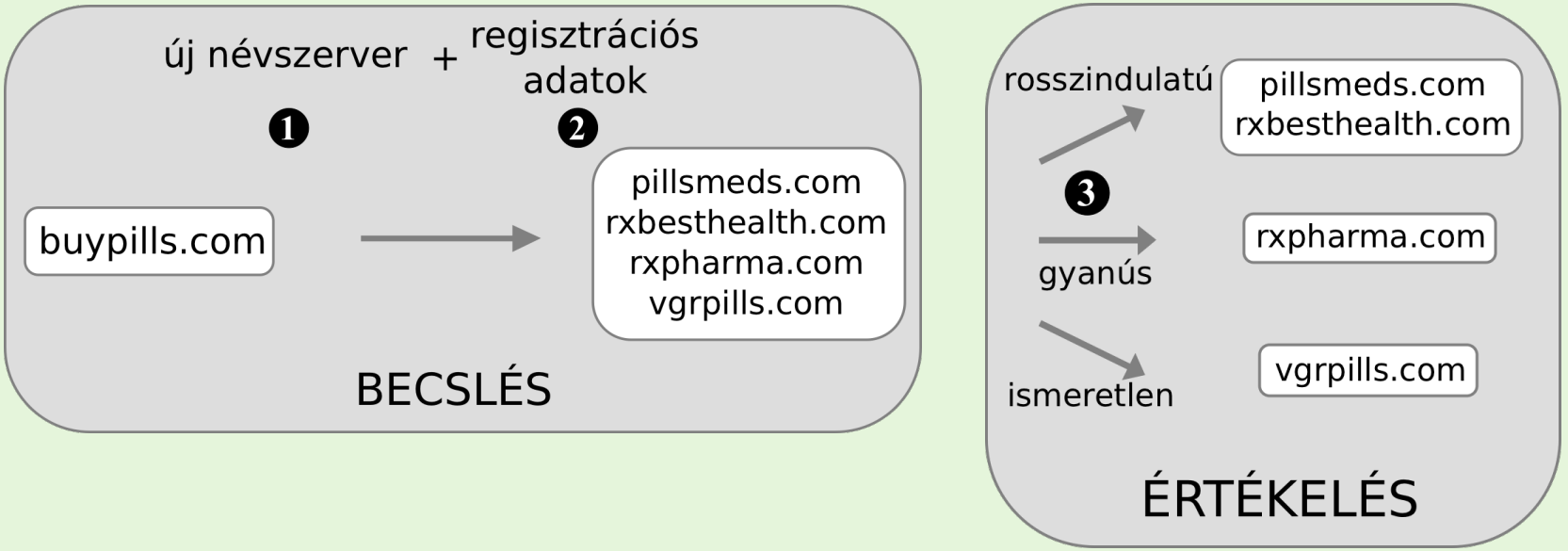
Spam domain regisztrációk



- domaineket feketelistázás után gyorsan eldobják
- csoportos domain regisztrációk

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009

Proaktív domain csoportosítás



Tesztelési szempontok

.COM zóna fájl - NS bejegyzések

WHOIS regisztrációs bejegyzések

buypills.com

2011-10-10

2011-09-01 - Enom

ÚJ

ns1.canadian.com
(utóbbi 1 évben regisztrálva)

pillsmeds.com

2011-09-01 - Enom

rxbesthealth.com

2011-09-01 - Enom

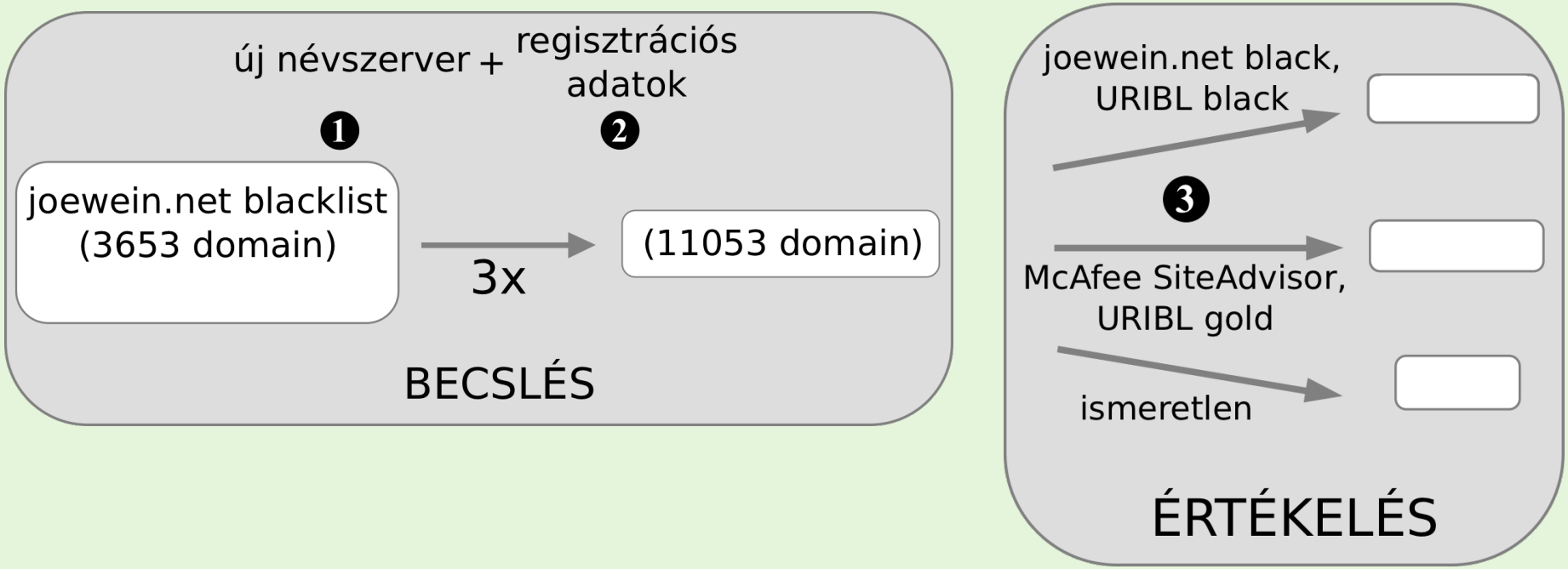
besthealthpills.com

2011-06-20 - Enom

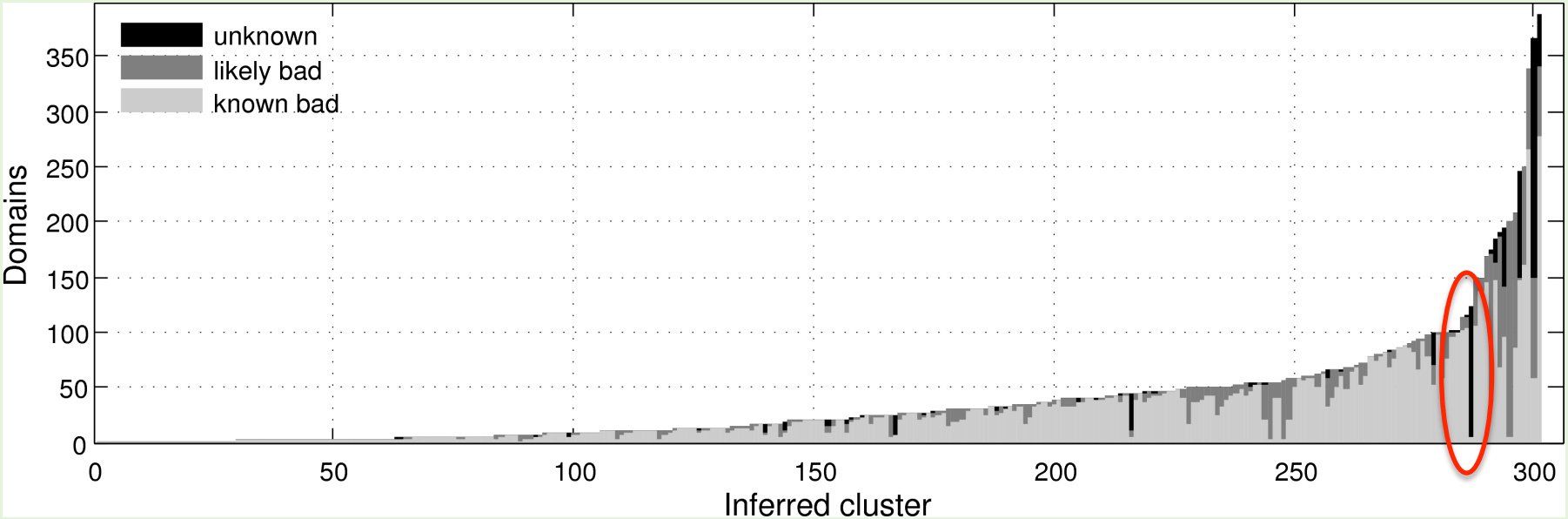
rxpharmacy.com

2011-09-01 -GoDaddy

Értékelés


új névszerver +
regisztrációs adatok
1
2
joewein.net blacklist (3653 domain)
3x
(11053 domain)
BECSLÉS
joewein.net black, URIBL black
3
McAfee SiteAdvisor, URIBL gold
ismeretlen
ÉRTÉKELÉS

Spam domain regisztrációk



- nagyon kevés álpozitív találat (FP)
- álpozitív találatok egyes csoportokra korlátozódnak
  - a csoportok 84%-a nem tartalmaz álpozitív domain neveket

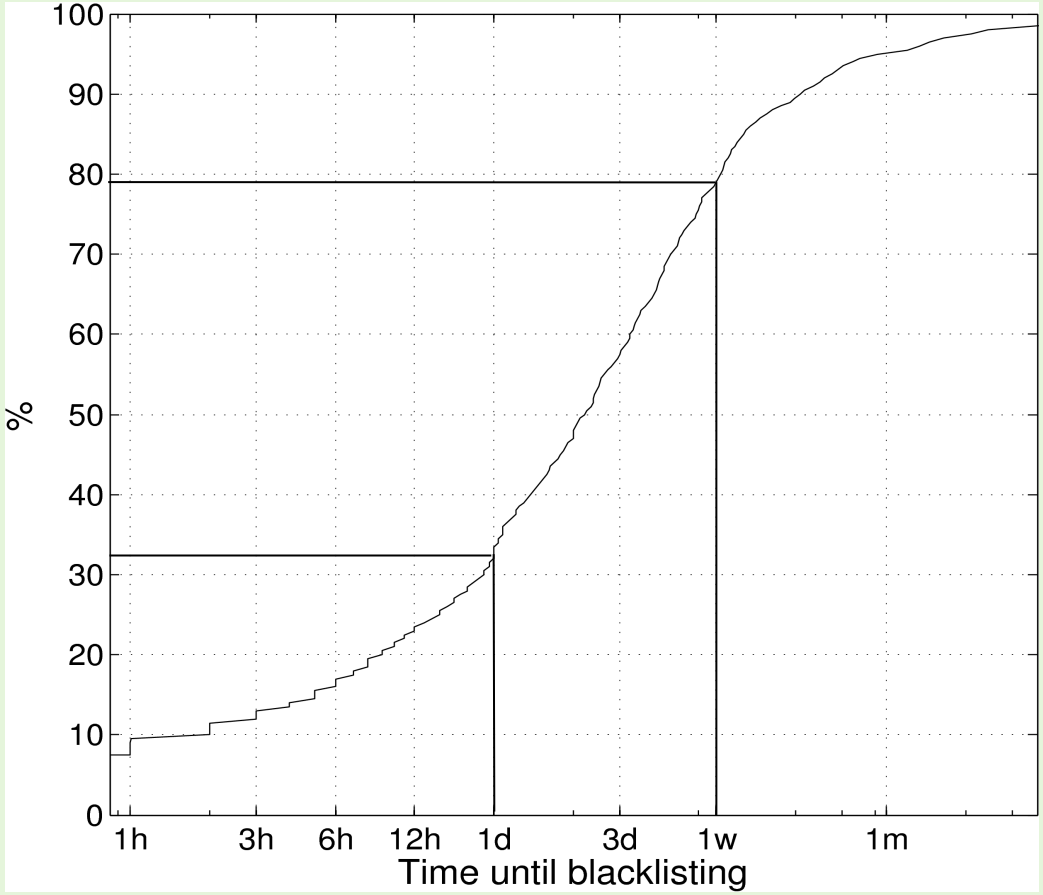
Álpozitívok?

- gyanús csoportok (pl: 123 domain, 119 FP)
  - nagyon sok főnév-főnév típusú

```
sodamonitor.com
sofapin.com
soulvisionmedia.com
suggestioneject.com
thrillcrash.com
thunderjudge.com
treeturn.com
wristprogram.com
dockundertake.com
wrenchimprove.com
queensnoop.com
(51 rows)
```

```
blue-towel.com
blue-trails.com
blue-trumpet.com
blue-tux.com
blue-twin.com
blue-up-parfum.com
blue-vet.com
blue-view-sak.com
blue-walking-stick.com
blue-skyblue.com
(72 rows)
```

Gyorsabb feketelistázás!



Összegzés

- rossz domaineket csoportokban regisztrálják és használják
- domain becslés kezdeti domainek és regisztrációs info alapján
- hatékony módszer
  - 73% becsült rossz domain később feketelistára került
  - 93% becsült domain “gyanús”
  - az álpozitívok sokszor valódiak
- a feketelistázott domainek 92%-a sokkal hamarabb előrejelezhető

gyors válasz spam-re

További kutatási tervek

- DNS biztonság és spam
  - domain regisztrációk vizsgálata
    - mi a domain regisztrációk célja? Jó, rossz, spekulatív?
  - typosquatting vizsgálata domaineknél
    - hasonló domainnevek forgalom elterelésére