

# Sõda või rahvaliikumine

Ükski asi ei ole päriselt nii nagu paistab...

Jaan Priisalu

# Mäss tänavatel

- Dirigendid
- Vene kodanik
- Maksu- ja tolliamet
- Turvaklaase oskaid nad lõhkuda
- Ka tavalised inimesed hakkasid massile vastu



# Planeerimine foorumites



**Я ПОМНЮ!  
Я ГОРЖУСЬ!**

**ДЕНЬ ПОБЕДЫ НАД ФАШИЗМОМ  
9 МАЯ 1945 ГОДА**



# Pankade ründamine

- Hansapanga vastu tehtud 6 DDoS-i, organiseerijad teada
- Arutlused foorumites
  - Sularahakriisi idee
  - Kohalikud venelased ei olnud ideestvaimustunud
    - Nad peavad siin elama, kardavad enda edu
    - Panku kardetakse
- Krediidipangal probleemid
- 10.05.07 9:42 algas DDoS Hansapanga vastu,
  - 90 minuti pärast kõik kanalid uuesti üleval
- 15.05.07 suurem ründekonfiguratsiooni muudatus
  - SEB-i rünnak hakkas 11:00
  - Hansa 14:15, downtime 5 min

# Vastasmõjud

- Ühes botnetis oli 82 000 arvutit
  - Sihtmärkide profileerimine
- Ei olnud mõtet filtrit allika lähedale panna
- Filtreerimise strateegia
  - Lubav nimekiri võrkude ja klientide kaupa, 70 boti sees
  - Keelav võrkude nimekiri (700 B klassi)
  - Keelav hostide nimekiri
  - Dünaamiline filtreerimine
- Mis on Rootsi internetis
- Cert.ee ja cert.fi olid üle koormatud
- Suurem rünnak kestis 3 nädalat, 300 IP-d veel juuni lõpus

Kõige olulisem oli inimeste suhtlus ja valmisolek

# Botide sõnumid

- &AnSSip=American\_WHORE
  - &AnSSip=ASSHOLE
  - &AnSSip=CHMO
  - &AnSSip=FUCK\_AMERICAN\_WHORE
  - &AnSSip=HUEPLET
  - &AnSSip=HUESOS
  - &AnSSip=PEZDOHUI
  - &AnSSip=PIDOR
  - &AnSSip=PIDORAZ
  - &AnSSip=PIZDA
- 
- Botid olid intelligentsed
  - Professionaalne relv – kanal täis 10 sekundiga,
  - Kui oleksid operatsiooni eest vastutav luureohvitser, siis mis mulje sobiks?

# Mida arvasid eksperdid

- Gadi Evron
  - The timing of the attacks, their scope and the sudden availability of botnets to aim at Estonian targets suggest that some level of organization was involved, Evron said. But there is no evidence to explain who was responsible. PCWorld
- Jose Nazario
  - Presented measurements
- Kaspersky
  - Alexander Gostev - Senior Virus Analyst at Kaspersky Lab - 15 August 2007.
    - many Russian Internet users who were not able to voice their protest in person used the only outlet they could: an online protest - in the form of DoS attacks.
    - Take another look at the attack statistics gathered by Arbor experts, and you can see that the overwhelming majority of attacks lasted less than one hour. How can one be sure that Russian special services “rented” botnets from hackers for these short periods of time?
    - Kew about defacements

Absloutely free movement in uncontrolled Russian Internet?

# Dr Jose Nazario meetod

<http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>

Korjas klientide käest netflow ja analüüsis seda

Mõõtevead:

- Netflow korjati osadelt arbori klientidelt
  - Netflow on ruuteri jaoks kõrvaltegevus – konfiguratsiooni vead
- Netflow ei vaata pakettide sisu
- Kuidas sihtmärk defineeriti? DNS?
  - Pangad ei olnud sihtmärgid
- Botid ei tekitanud liiklust pidevalt
  - Meie puhul oli ründeliiklus kaitsetegevuse jääk
- Kaitstes kasutati ka väljaspool eestit asuvaid lüüse
- Nazario's tipp oli 100Mbps, olen kuulnud 3Gbps

Järeldus: rünnet ta nägi aga ainult väikest osa sellest

# Peegelduste peegeldused

Economist, Washington Post, Wired jne saatsid reporterid

Mina -> Postimees

- Lapimaa suvilates on israeli satelliidiühendused
- Juuni lõpuks 300 keelatud IP-d
- “Küberrünnakuid tehti nii Lapimaalt kui israelist”

Gadi -> vene meedia

- Ei leidnud tõendeid vastutuse määramiseks
- Эстонское киберпространство атаквали простые пользователи Сети

Jose -> Kaspersky

- Mõõtis osa liiklust
- Botnetide rentimisel ei olnud mingit mõtet

Peegel on üsna udune

# Subjektiivne kokkuvõte

- Erinevad inimesed nägid mingit osa liiklusest
- Motivatsioon ja institutsioon määravad intsidendi klassi
  - Motivatsioon on subjektiivne
  - Kõik peale subjekti ainult oletavad
- Suurim muudatus oli poliitiline motivatsioon
- Kui vaippommitamine on rahvaliidumise normaalne osa, siis on maailm elamiseks kehv koht
- Me peame enda juhtmeid kaks aastat ette planeerima, täna tuleb “kübersõda” infosüsteemiks teisendada