E-CoAT

European Cooperation of Abuse fighting Teams

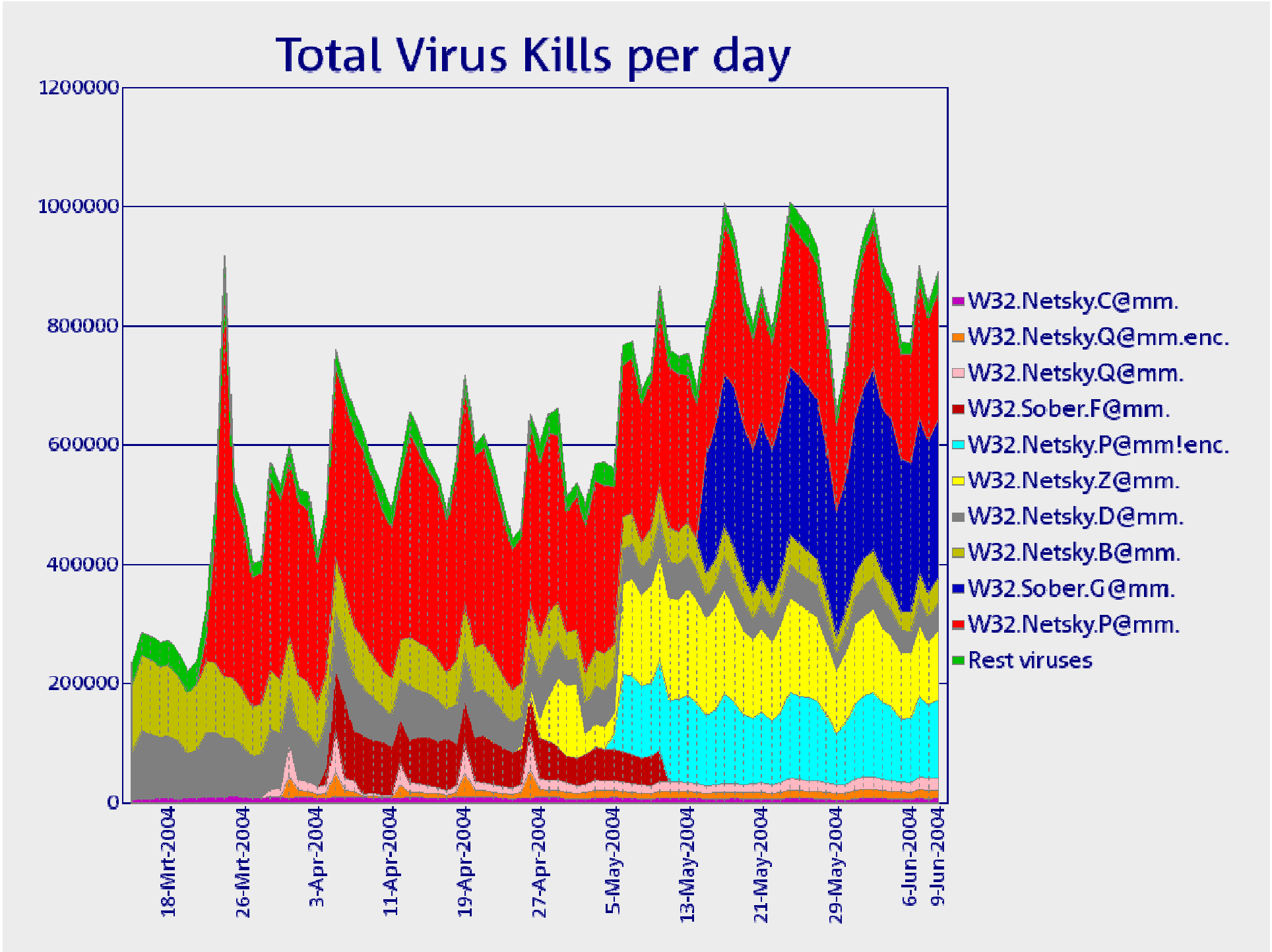
Lessons learnt and a pragmatic way forward

ENISA Gathering in Brussels, December 2005

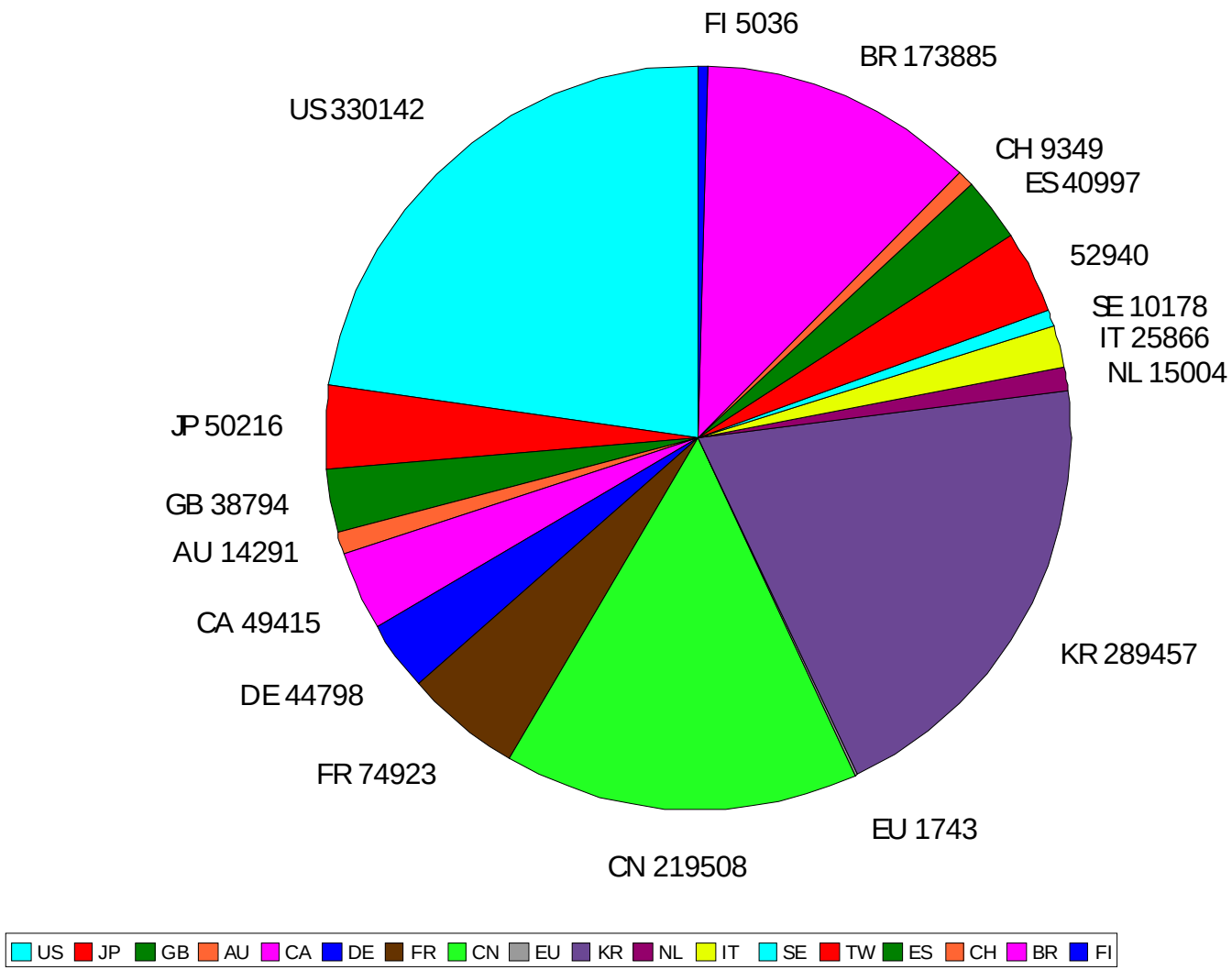
Don Stikvoort
(e-coat workshop chair)

Abuse *a massive problem (i)*

- Computer/network abuse incidents
  - Worms, viruses, trojans, botnets
  - Phishing
  - Copyright issues
  - Denial of service attacks
  - Result-incidents like blacklisting


Total Virus Kills per day
1200000
1000000
800000
600000
400000
200000
0
18-Mrt-2004
26-Mrt-2004
3-Apr-2004
11-Apr-2004
19-Apr-2004
27-Apr-2004
5-May-2004
13-May-2004
21-May-2004
29-May-2004
6-Jun-2004
9-Jun-2004
W32.Netsky.C@mm.
W32.Netsky.Q@mm.enc.
W32.Netsky.Q@mm.
W32.Sober.F@mm.
W32.Netsky.P@mm!enc.
W32.Netsky.Z@mm.
W32.Netsky.D@mm.
W32.Netsky.B@mm.
W32.Sober.G@mm.
W32.Netsky.P@mm.
Rest viruses

SORBS blacklist entries



Abuse *a massive problem (ii)*

- Example
  - Major North-European ISP / telecom provider
  - 700 to 1000 complaints per day
- Dealing with abuse
  - Low number of customers
    - → classical CERT team
  - High numbers of customers (big ISPs)
    - → separate Abuse Team next to CERT
- THE PROBLEM IS NOT GETTING ANY SMALLER !!!

Massive Abuse *who cares ?*

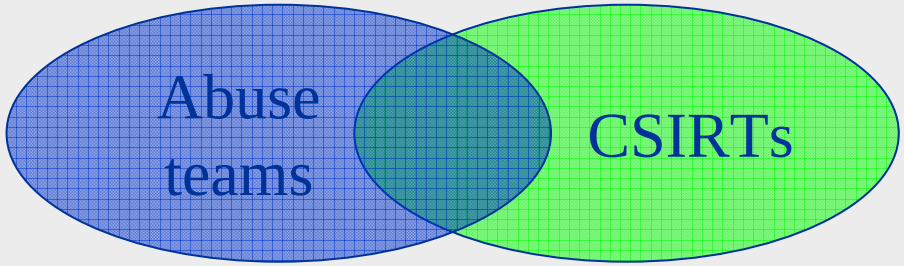
- TF-CSIRT and FIRST concentrate on classical CERT issues
  - lacking focus on mass aspects of abuse
- ETNO and FIINA concentrate on higher level issues
  - Not well suited for collaborative hands-on approach
- MAAWG concentrates on messaging
  - No clear focus on abuse yet

What then?

- European abuse teams felt the need for direct cooperation on issues of (massive) abuse handling & prevention
- At FIRST conference in Ottawa, June 2003, decided to go for it
  - Low-overhead, hands-on, collaborative approach
  - Focus on Europe for pragmatical reasons
  - Open eye to rest of world
  - Collaborate closely with TF-CSIRT
  - Liaise with FIRST, FIINA, ETNO, MAAWG, ...

E-CoAT initiative

- Initiative of large European ISPs abuse teams



- Workshops organised on volunteer base
  - Madrid Jan 2004
  - Hamburg May 2004
  - Amsterdam November 2004
  - Zürich May 2005
  - Amsterdam, 12 January 2006

E-CoAT *founding members*

- DFN-CERT
- DK-CERT
- IRIS-CERT
- KPN-CERT
- Telia Abuse
- T-Com Abuse Team
- T-Online Abuse Team
- Don Stikvoort (individual member)

E-CoAT goals & interests

- Goals
  - Discussion of shared problems
  - Sharing of solutions
  - Establishing best practices and common standards (e.g. reporting)
  - Awareness raising outside E-CoAT
- Interests
  - Fighting (massive) abuse together
  - Direct NOC-to-NOC contacts
  - Whitelisting/blacklisting
  - Other issues as initiated by members

E-CoAT road ahead (i)

- Road ahead decided in Zürich workshop last May →
- Proposed operational framework agreed to
  - Membership structure:
    - Abuse-teams
    - Individual members
  - System of checks and balances guaranteeing member rights
- Support Coordination group elected:
    - Maria Rådström, TeliaSonera abuse team
    - Markus Weyrich, T-Online
    - Martijn van der Heide, KPN-CERT
    - Peter Quick, T-COM
    - Francisco Monserrat, IRIS-CERT

E-CoAT road ahead (ii)

- SC group is organising:
  - Legal entity for E-CoAT due 1st quarter 2006
    - Association for
      - minimum overhead
      - maximum member rights
  - Membership directly following association set-up
  - Next workshops (Amsterdam. 12 January 2006)
  - Activities & Liaisons
  - E-CoAT public presence

E-CoAT factsheet (i)

- Volunteer driven
- Minimum overhead
  - Membership fee initially set at € 300 per year
  - Members do !
- Maximum efficiency through collaboration:
  - Optimal cooperation with internal/external CERTs
  - Explicitly recognised by TF-CSIRT (co-locating, reporting)
  - Liaison with relevant groups/institutions (ENISA, MAAWG, FIINA, ETNO)
  - Maybe create FIRST Special Interest Group together with similar efforts in other regions

E-CoAT factsheet (ii)

- Next workshop:
  - Amsterdam 12 January 2006
  - Register NOW
  - http://www.e-coat.org/5th-workshop.html
- Website
  - http://www.e-coat.org/
- E-mail
  - sc@e-coat.org
  - reaches all SC members plus workshop chair

E-CoAT pragmatic focus (i)

- Phishing is hot
  - Abuse teams cooperate with banks
  - Role of national CERT/abuse-team for a
- Blacklisting (block the bad guys) and whitelisting (keep the good guys from being blocked)
  - Collaborate with blacklisting initiatives like sorbs

- Awareness raising
  - Assist existing fora like ENISA !
    - role of national for a / member states
    - Guidelines / best practices
    - Inspire regulation

E-CoAT pragmatic focus (ii)

- NOC-to-NOC contacts
  - IRC server established
  - Mailing lists
  - Alerting system?
- More and more of the usual
  - Trojans, worms, viruses, etc.
  - Focus on tools (reporting & handling)

E-CoAT

Questions?

- On the floor, in the corridors …
- don.stikvoort@s-cure.nl

- sc@e-coat.org to reach the coordinating group plus the workshop chair

Thank you for your attention!