E-CoAT

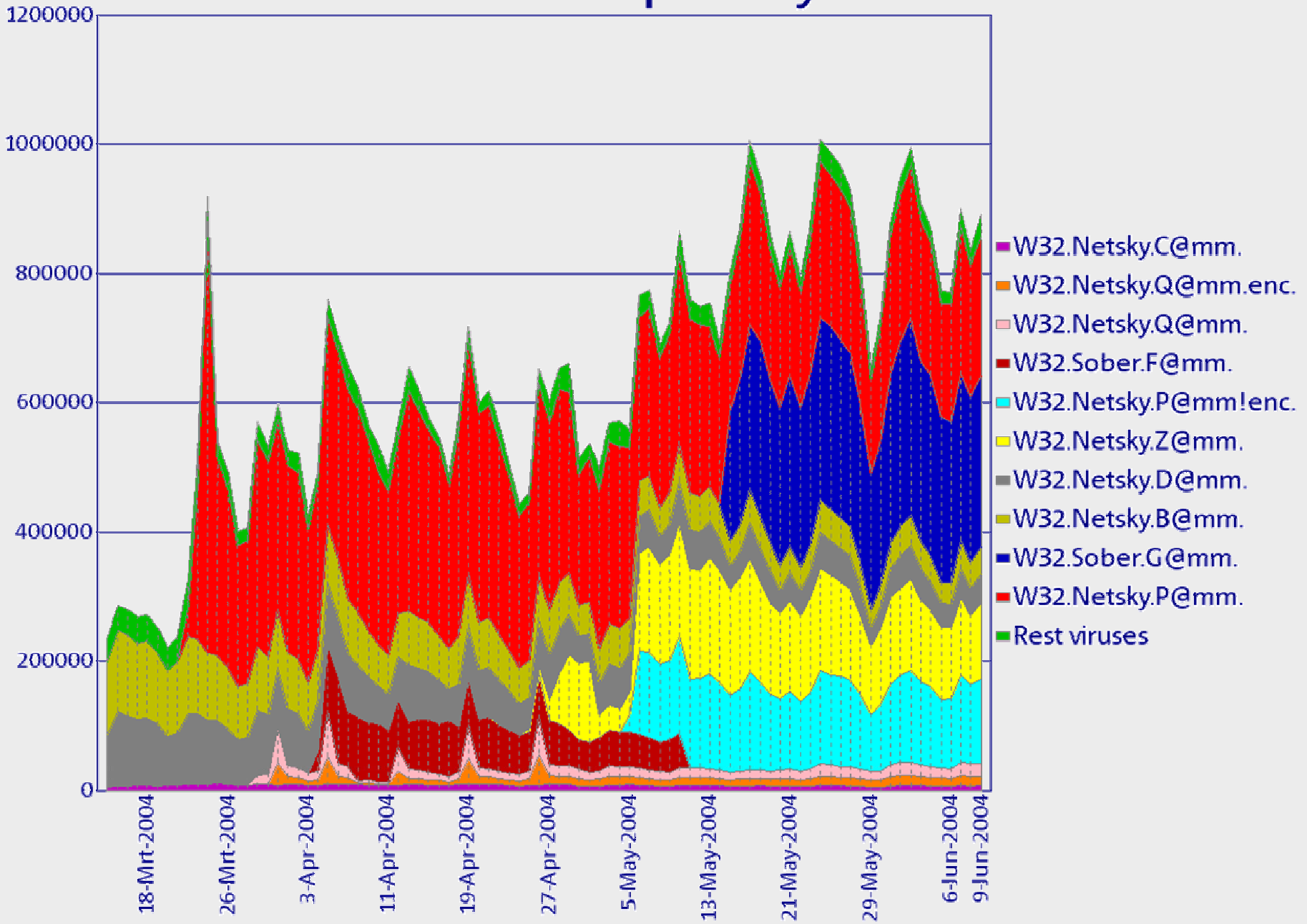
European Cooperation of Abuse fighting Teams

Remarks on E-CoAT

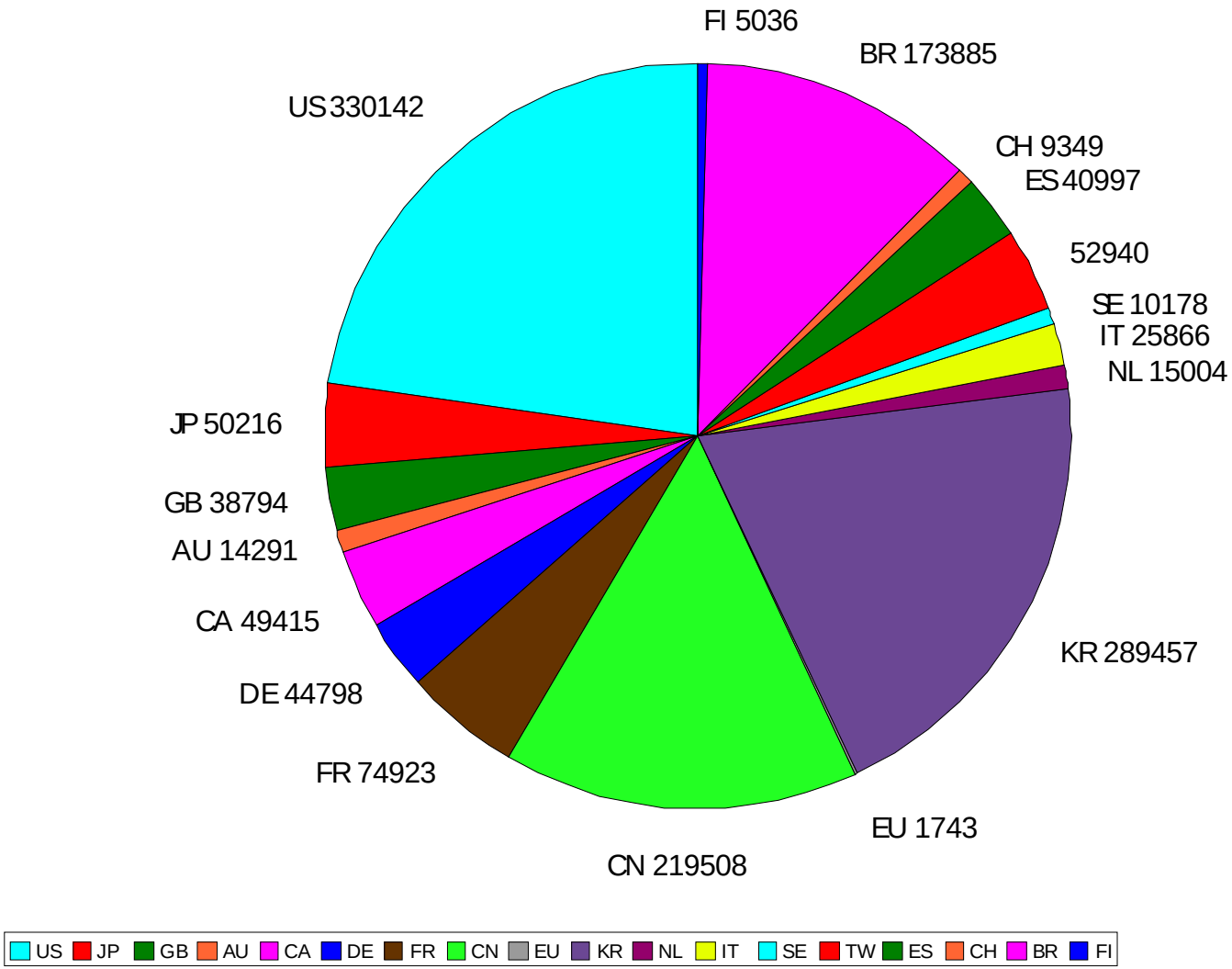
TF-CSIRT/FIRST joint event
Amsterdam, January 2006

Don Stikvoort
(e-coat workshop chair)

Total Virus Kills per day



SORBS blacklist entries



Abuse *you know it's massive ..*

- Example
  - Major North-European ISP / telecom provider
  - 700 to 1000 complaints per day
- Blacklisting out of control at times
  - Whitelisting as a patch
- Phishing increasing
- Botnets
- … … …

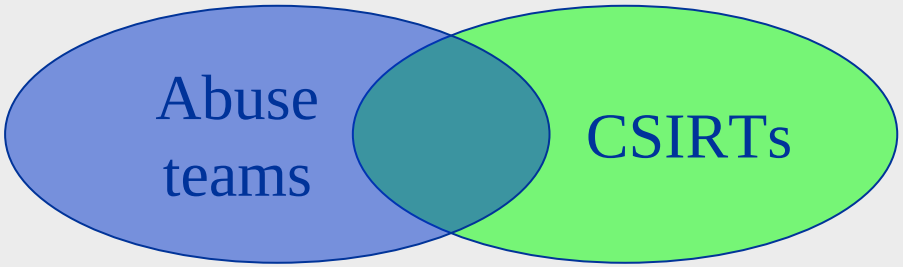
THE PROBLEM IS HARDLY GETTING ANY SMALLER …

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

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 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 projects

- Noc-to-noc contacts for E-CoAT members
  - IRC server
    - Courtesy KPN-CERT & XS4ALL (Scott McIntyre)
  - Mailing lists
- Whitelisting / blacklisting
  - Discussions with blacklisters/whitelisters started (sorbs … , bit.nl initiatives like nl whitelist & others)
    - Mainly blocking of (individual) IP numbers or SMTP servers
  - eu-whitelist, or ?? Will be investigated
- Tooling
  - Group started on tooling (e.g. incident handling, forensics, whitelisting)
- Awareness raising
  - ENISA: role of national fora, inspire regulation
- A.o.b. – up to members

E-CoAT factsheet (i)

- Volunteer driven
- Minimum overhead
  - 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)
  - Intent to create FIRST Special Interest Group together with similar efforts in other regions (like AAA in AP region)
    - Propose BoF session at FIRST conference in Baltimore

E-CoAT factsheet (ii)

- Next workshop (*tentative*):
  - Helsinki 20 September 2006
  - Preceding TF-CSIRT
- Website
  - http://www.e-coat.org/
- E-mail
  - sc@e-coat.org
  - sc = elected “Support Coordination” group – organises the efforts