Le CERT Renater

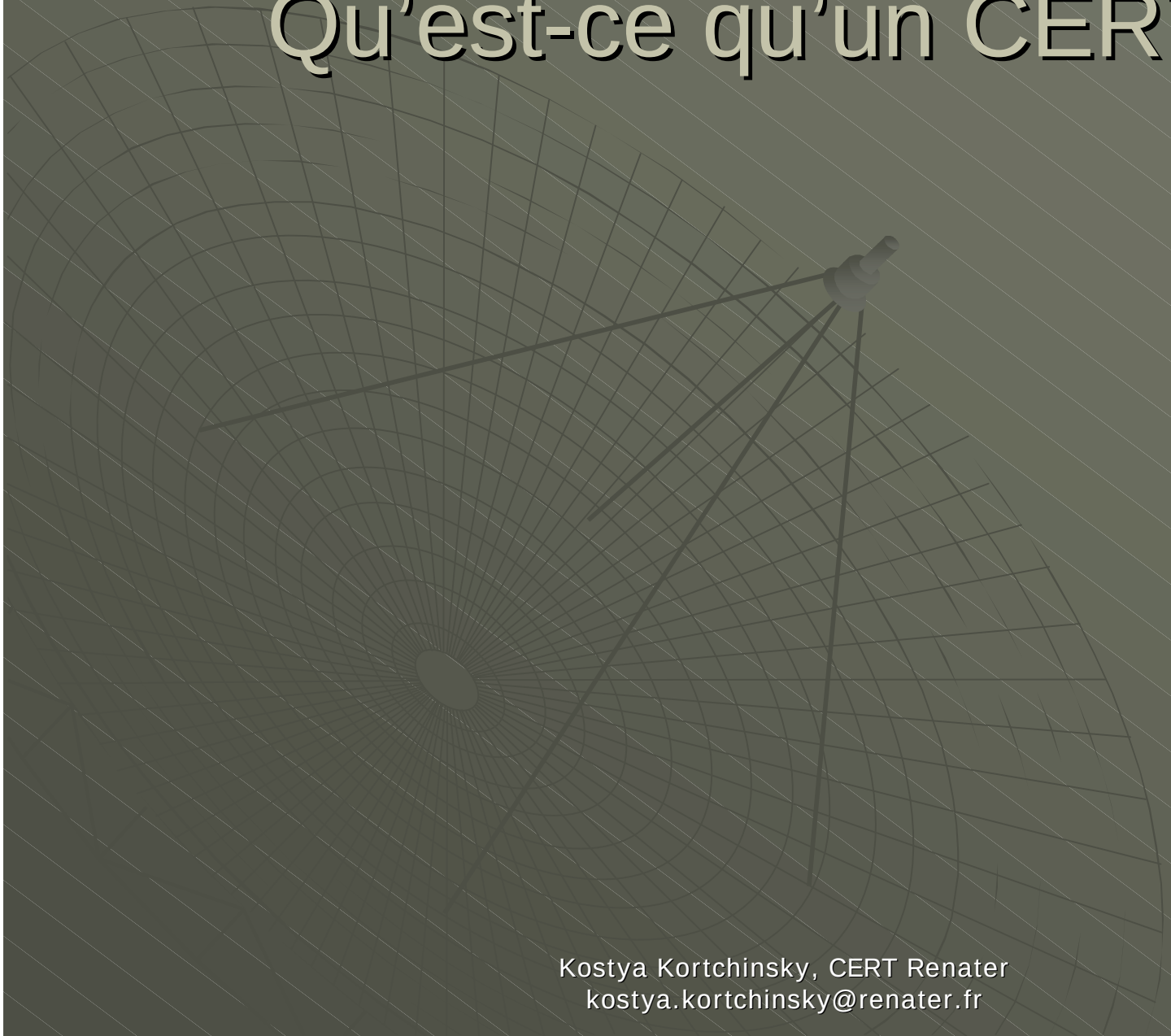
Journées Techniques de l'Ouest
Mercredi 18 Décembre 2002

Kostya Kortchinsky, CERT Renater
kostya.kortchinsky@renater.fr

Sommaire

- Qu’est-ce qu’un CERT ?
- Le CERT Renater
  - Rôle préventif
  - Rôle curatif
  - Coopération
- Action du CERT Renater en 2002

Qu’est-ce qu’un CERT ?



Qu’est-ce qu’un CERT ? (1)

- Historique
  - Novembre 1988
    - Ver MORRIS
    - Création du CERT/CC (Computer Emergency Response Team Coordination Center)

Qu’est-ce qu’un CERT ? (2)

- Rôle et mission (1)
  - Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations
    - réception des demandes
    - analyse des symptômes
    - éventuelle corrélation des incidents

Qu’est-ce qu’un CERT ? (3)

- Rôle et mission (2)
  - Traitement des alertes et réaction aux attaques informatiques
    - analyse technique
    - échange d'informations avec d'autres CERTs
    - contribution à des études techniques spécifiques
  - Établissement et maintenance d'une base de donnée des vulnérabilités

Qu’est-ce qu’un CERT ? (4)

- Rôle et mission (3)
  - Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences
  - Coordination éventuelle avec les autres entités (hors du domaine d'action)
    - Centres de compétence réseaux
    - Fournisseurs d'accès à Internet
    - CERTs nationaux et internationaux

Le CERT Renater

Le CERT Renater (1)

- Rôle préventif (1)
  - Sources d'information externes
    - Bulletins
      - Listes de diffusion des vendeurs (RedHat, ...)
      - Autres CERTs (CERT/CC, AusCERT, ...)
    - Sites WEB
      - Archives d' « exploits » (PacketStorm, ...)
    - Listes de diffusion et de discussion
    - Internet Relay Chat (IRC)

Le CERT Renater (2)

- Rôle préventif (2)
  - Sources d'information internes
    - Réseau de test (Pot de Miel)
    - [Audit de sécurité distant]

Le CERT Renater (3)

- Rôle préventif (3)
  - Bulletins d'information
    - VULN : vulnérabilités des systèmes d'exploitation et des applications
    - STAT : résumé des incidents de la semaine
    - INFO : description détaillée de phénomènes liés à la sécurité
    - ALER : alerte sur un problème de sécurité menaçant de se répandre largement

Le CERT Renater (4)

- Rôle curatif (1)
  - Détection de machines compromises
    - Point de contact pour la communauté académique française
    - Remonté des résumés des scans
      - Detescan, Anapirate, Vigilog
    - Métrologie
      - Attaques (scans, déni de service, ...)
      - Trafic contraire à la charte (P2P, FTP Warez, ...)

Le CERT Renater (5)

- Rôle curatif (2)
  - Expertise technique
    - Analyses de compromissions
      - Analyses d'images de disques
      - Analyses distantes de disques
    - Reverse-engineering d'outils
    - Développement d'outils
    - Recommandations en cas de compromission

Le CERT Renater (6)

- Coopération (1)
  - Nationale
    - Autres CERTs
      - CERTA : Administration
      - CERT-IST : Industrie, Services et Tertiaire (Alcatel, CNES, Elf et France Télécom)
    - Fournisseurs d’accès Internet

Le CERT Renater (7)

- Coopération (2)
  - Internationale (1)
    - FIRST (Forum of Incident Response and Security Teams)
      - Favoriser la coopération entre les équipes
      - Fournir un moyen de communication commun
      - Aider au développement des activités des ses membres
      - Faciliter le partage des informations relatives à la sécurité

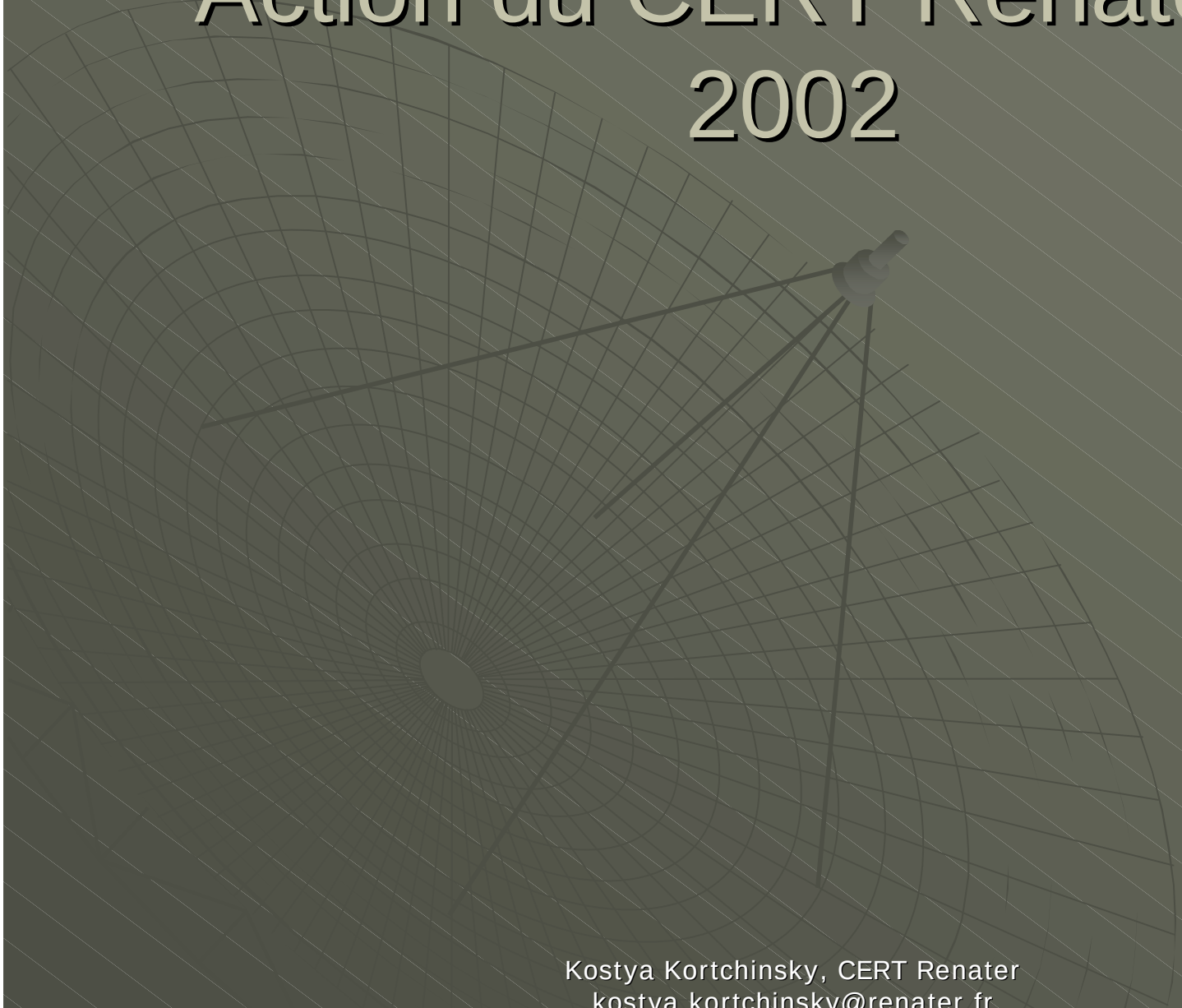
Le CERT Renater (8)

- Coopération (3)
  - Internationale (2)
    - TF-CSIRT (Task Force CSIRT)
      - Encourager et soutenir la coopération entre les CSIRTs européens

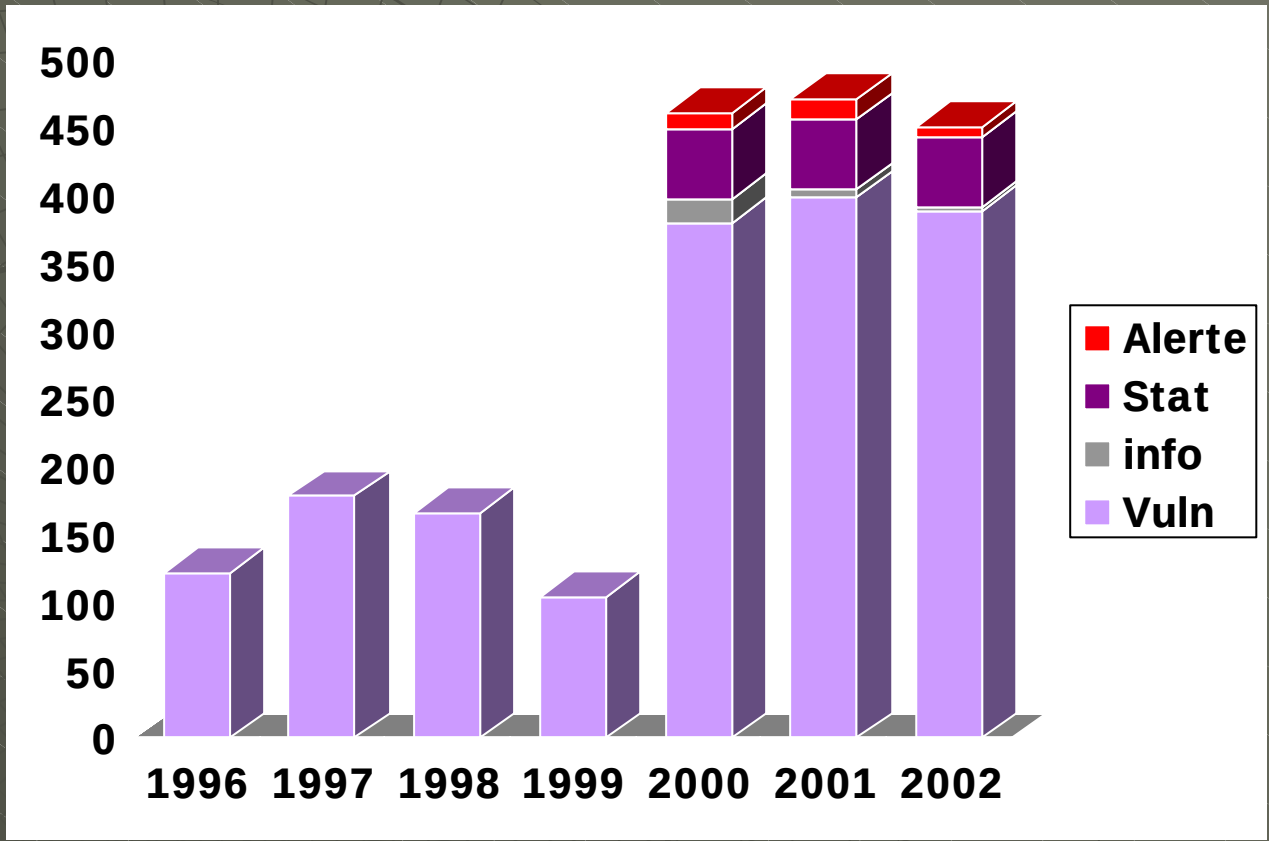
Le CERT Renater (9)

- Coopération (4)
  - Internationale (3)
    - eCSIRT.net
      - Améliorer la sécurité de l'infrastructure européenne des technologies de l'information
      - Permettre une réponse appropriée et rapide aux attaques visant cette même infrastructure
      - Augmenter la prise de conscience des problèmes de sécurité en documentant le travail des CSIRTs et en publiant des statistiques

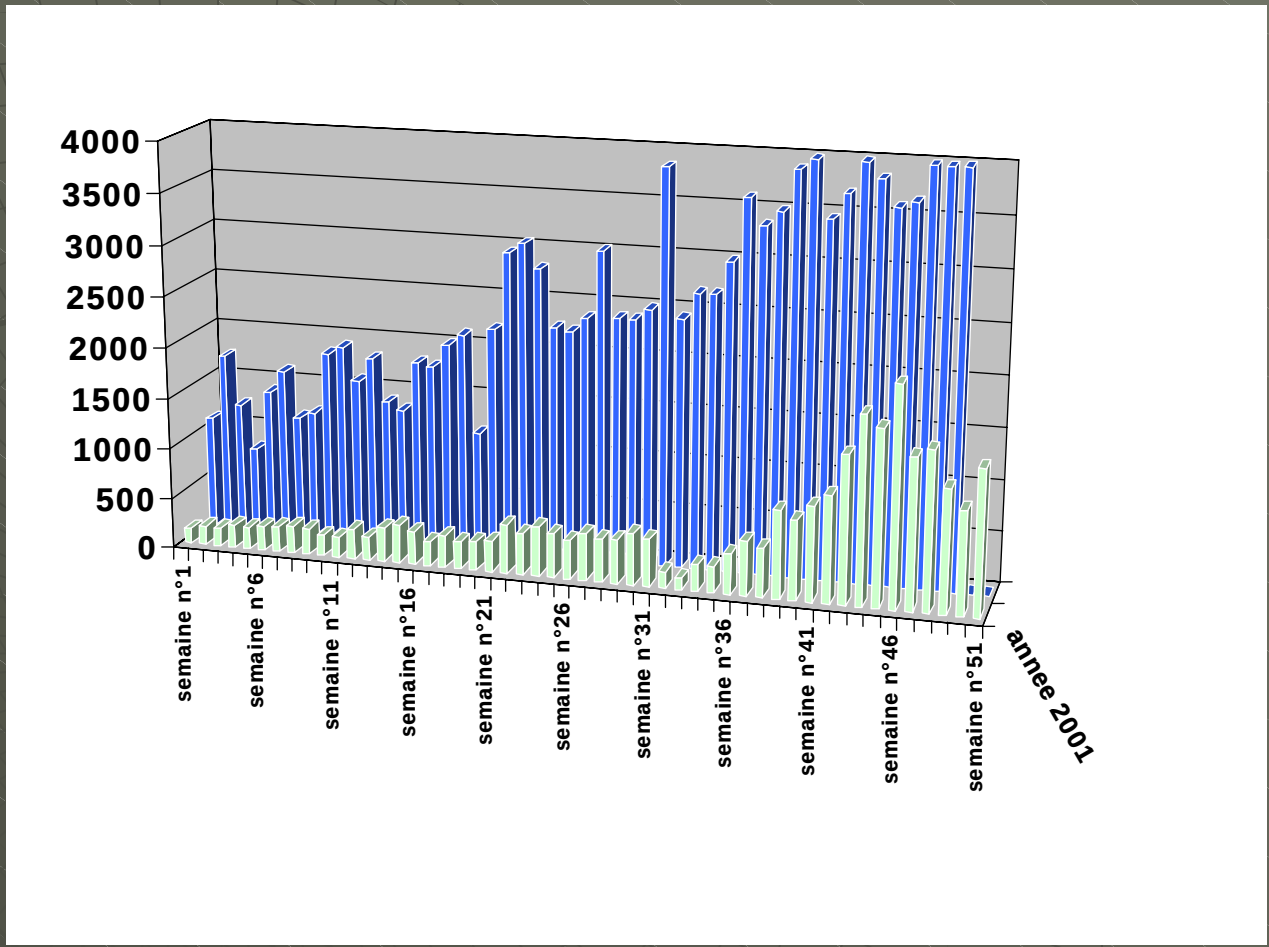
Action du CERT Renater en 2002



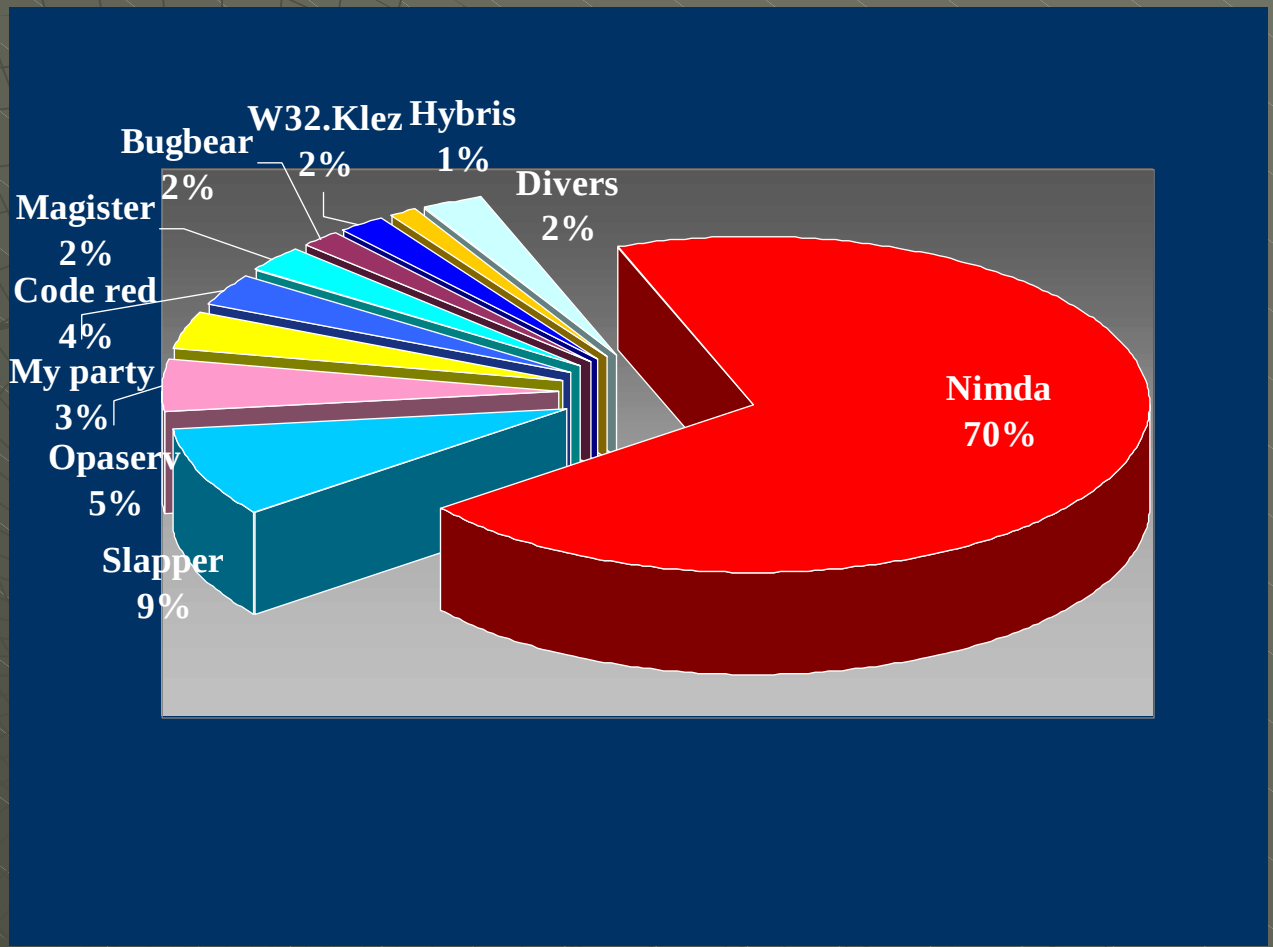
Statistiques (1)



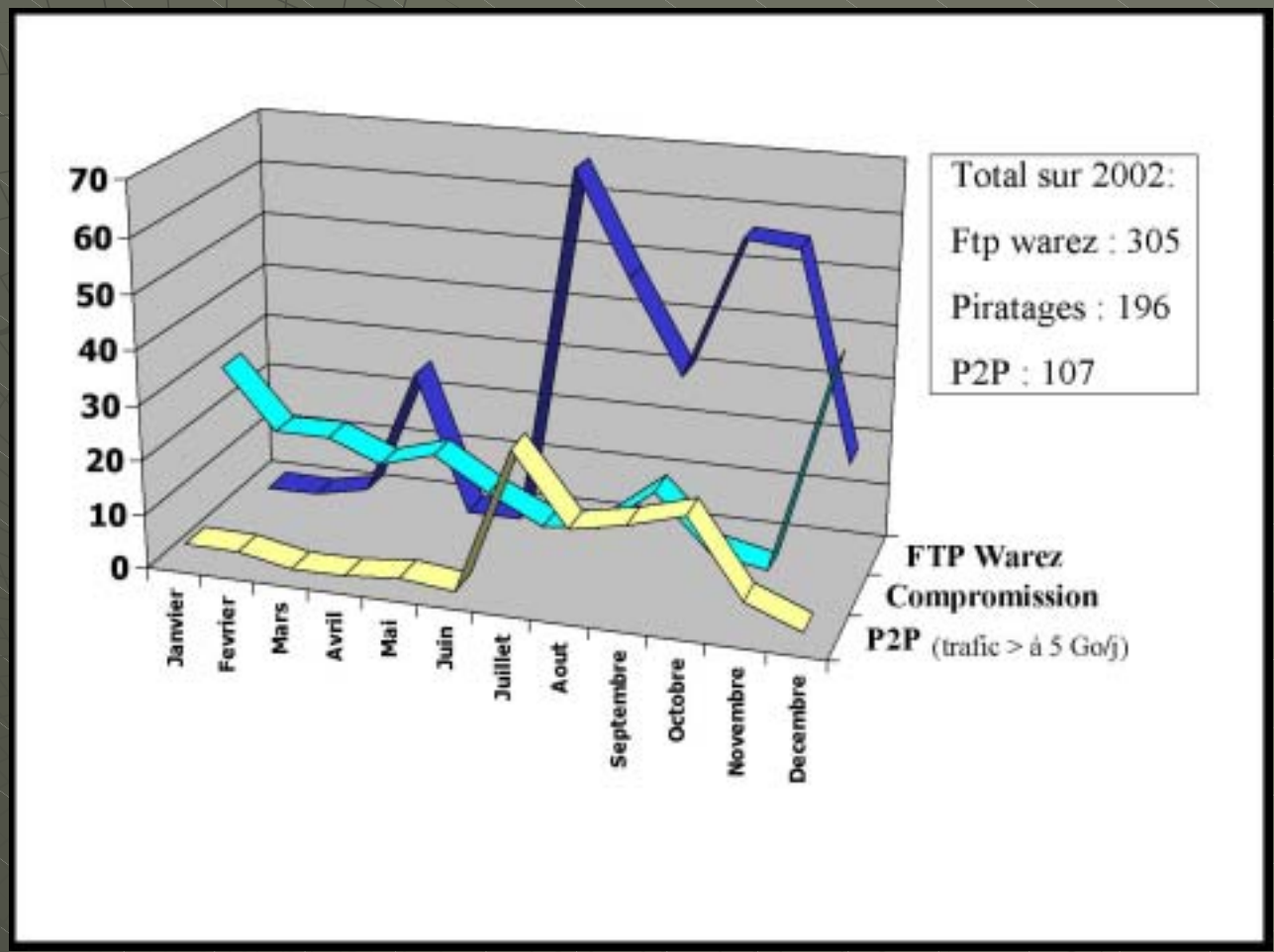
Statistiques (2)



Statistiques (3)



Statistiques (4)



Présentations en Région

- En 2002, le CERT Renater a effectué des présentations à :
  - Toulouse le 19 mars 2002 (24 personnes)
  - Lyon le 4 Avril 2002 (21 personnes)
  - Bordeaux le 14 Mai 2002 (23 personnes)
  - Nancy le 30 Mai 2002 (34 personnes)
  - Paris le 8 Octobre, dans le cadre des "Journées Sécurité" IN2P3
  - Besançon, le 5 Décembre (18 personnes)