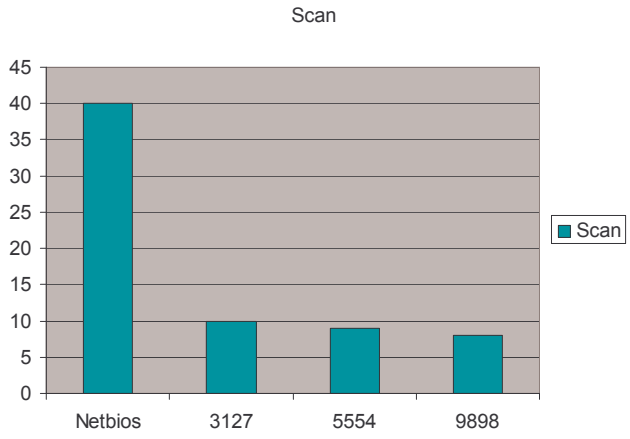
# Tour d ’horizon

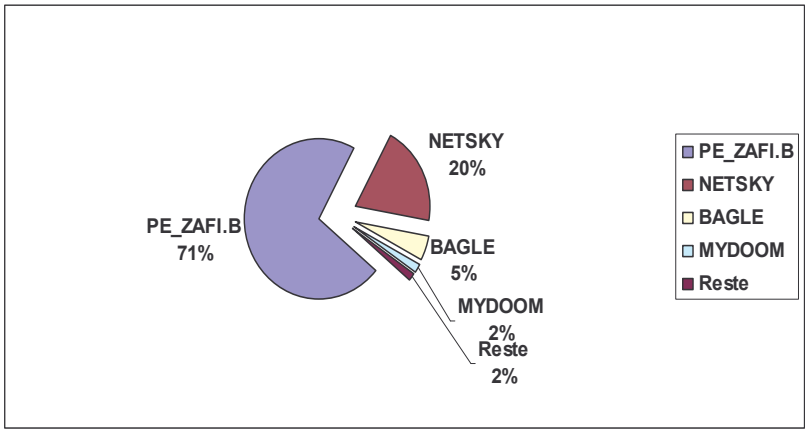
- Statistiques
- Faille
- Utiles
  - Outil, service WWW, Presse
- Actualités

# Top des scans : été 2004



RéSIST

# Statistiques été 2004: virus




RéSIST

# Faille Winamp

- Faille 0day (exploitée avant sa découverte officielle)
- Ajout automatique d'un habillage (skin) à Winamp.
- Le skin peut alors exécuter en local des html et par la même n'importe quel programme.
- Corrigée par la version 5.05 de Winamp.

RéSIST

# Utiles

- Outil : rootkit hunter
- Evénements : Microsoft & Anti-Spam
- Economie, Loi & Presse

RéSIST

# Outil : pads

- Détection passive de version de serveur
- http://passive.sourceforge.net
- GPL
- Unix
- Ne détecte que 107 versions logicielles
  - Facilement upgradables (fichiers texte)
- Exemple :
  - Port 25 / Host 193.49.48.250 / Service – smtp / Application – Postfix SMTP (dns-ut1.univ-tlse1.fr)

## Evénements

- Sortie du SP2 pour Windows XP.
  - Protection par défaut.
  - Quelques problèmes avec plus de 200 logiciels (y compris microsoft)
  - Problèmes souvent réglables par une configuration fine du pare-feu de windows XP
  - De nombreuses entreprises attendent de voir.

## Evénements

- Le temps de correction d'un Windows dépasse le temps moyen d'infection (20 minutes).
  - http://isc.sans.org/survivalhistory.php
  - Le modus operandi existe sur cette même page :
    - Survivre le premier jour avec windows XP

## Evénements

- Nouvelles méthodes anti-spam
  - Algorithme de chung-kwei utilisé en recherche génétique. Serait plus efficace que les bayésiens.
  - Normalisation en cours du protocole SPF à travers le protocole Sender-ID du « MARID group » de l'IETF.

## Economie, Loi & Presse

- Augmentation des débits ADSL
  - 10Mbit/s / 800 Kbit/s… Que de DDoS !
- Site d'information
  - http://isc.sans.org/diary.php