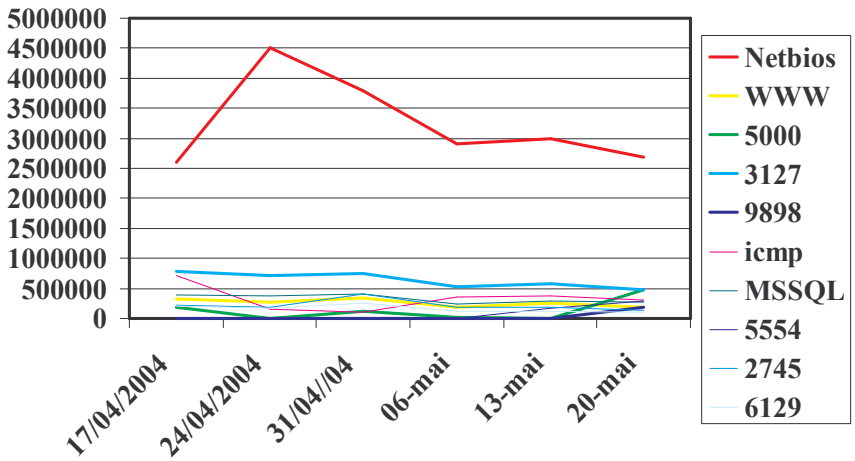
Tour d ’horizon

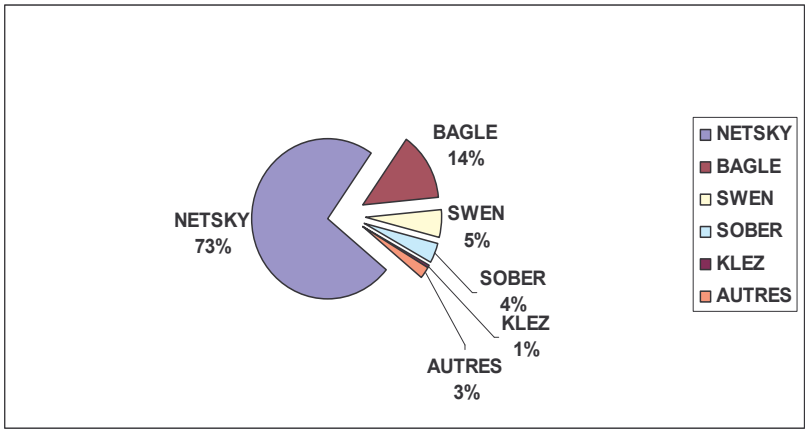
- Statistiques
- Agressions
  - Ver
- Utiles
  - Outil, service WWW, Presse
- Actualités

Top des scans : Avril/Mai



RéSIST

Statistiques Avril/Mai: virus



RéSIST

Agressions

Virus/Ver :
Sasser/Dabber/Bobax/Kibuv

Virus/Ver : LSASS

- Nom : Sasser/Bobax/Dabber/Kibuv
- Découvert : mai 2004
- Type : Ver
- Propagation par
  - réseaux (connexion TCP/IP) sur une faille LSASS
  - Ou faille RPC/DOM

Virus/Ver : LSASS

- Actions :
  - Utilisation de la faille LSASS
  - Buffer Overflow nécessitant parfois un reboot
  - Installation d'un troyen (3127, 6129, etc.)
  - Annonce sur un canal IRC
  - Attaque d 'autres machines (port 445/5000)
- Filiation nombreuse
- Clairement orienté Spammeurs/Pirates

Virus/Ver : LSASS

- Conclusions :
  - Importance d ’OS à jour
  - Importance du « interdit par défaut » sur les firewalls
  - et à minima : interdiction des protocoles Microsoft.
  - Et faire de même en interne

Utiles

Outil : clamwin

Evénements : vol de code source

Economie, Loi & Presse

RéSIST

Outil : clamwin

- Antivirus open source
- http://www.clamwin.com
- Gratuit
- Basé sur clamav
- Fonctionne en environnement windows
- Non résident

RéSIST

Evénements

- Vol de 600 Mo du code de Windows 2000
- Vol de 800 Mo de code CISCO IOS
- Arrêt de l'auteur de Sasser

RéSIST

Economie, Loi & Presse

- Vote de la LEN
  - Possession d'outils de « hacking » pour un motif légitime ?

RéSIST

Actualités

- JSSI
- SSTIC à Rennes (2 au 4 juin 2003)
  - Bientôt disponibles sur http://www.sstic.org