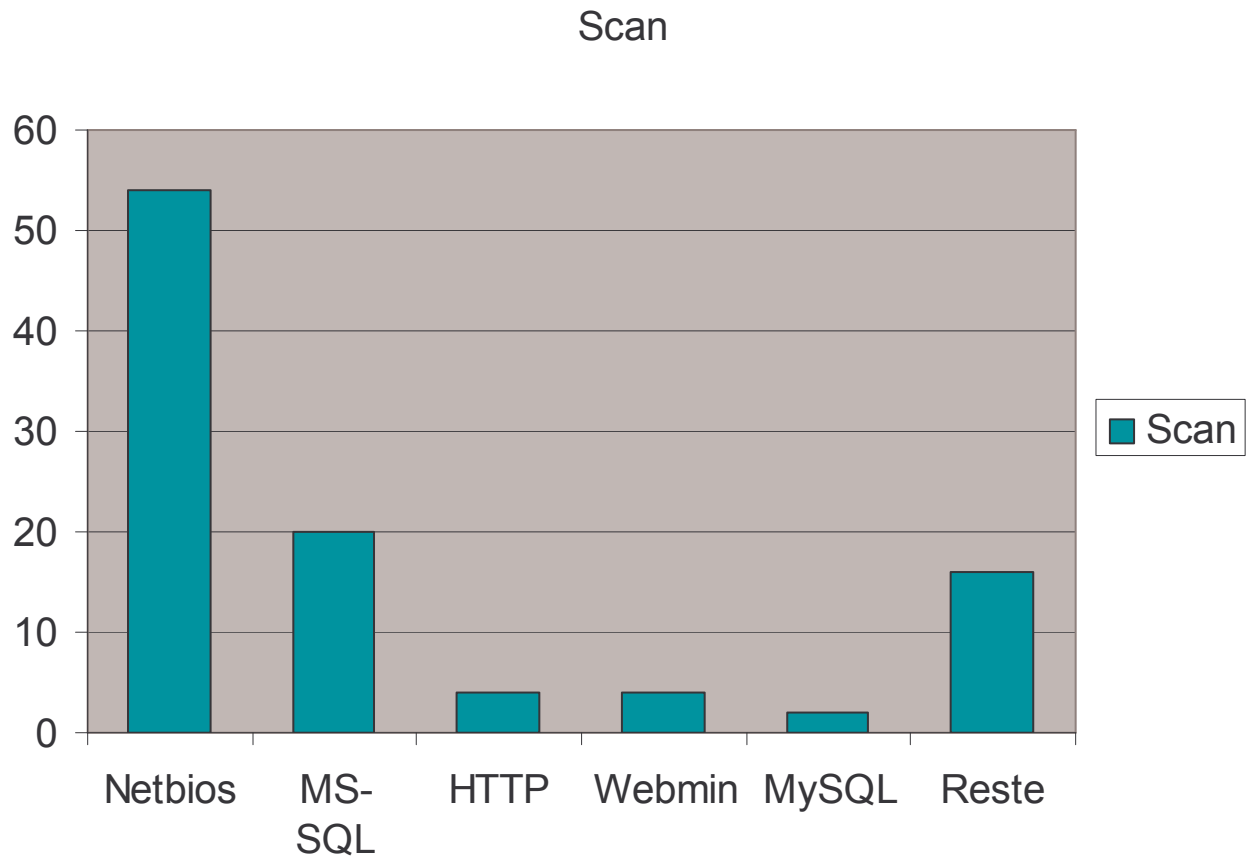
RéSIST

Tour d ’horizon

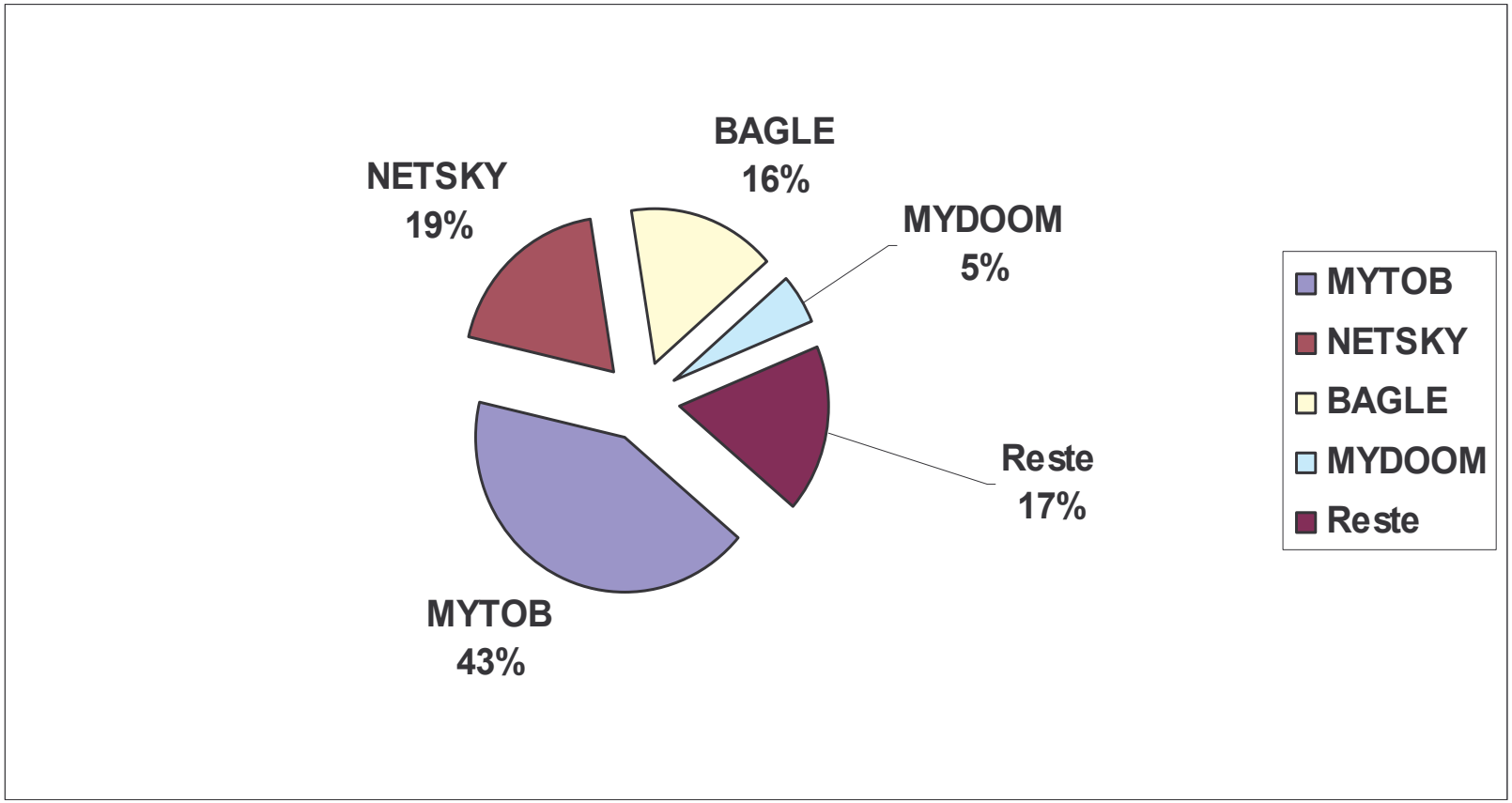
- Statistiques
- Faille
- Virus
- Utiles
  - Outil
  - Site Web
  - Actualités

Top des scans : juin 2005



RéSIST

Statistiques Juin: virus



RéSIST

Les scans SSH

- Mois de juin
- 28 attaquants différents
  - de 2 à 4652 tentatives
- 1905 utilisateurs (existants ou non)
  - root : 7490
  - admin : 106
  - mihai : 12

RéSIST

Les scans awstats

- Mois de juin
- 14 attaquants différents
  - de 2 à 519 tentatives (emplacement de awstats)
- sur 14 serveurs

RéSIST

Faille : Signature électronique

- Collision dans le hash MD5
  - Pour un hash MD5 donné on peut créer un fichier
- Jusqu'à présent : le fichier était « aléatoire »
- Idée de 2 chercheurs allemands :
  - Signature d'un fichier postscript, avec 2 « documents » internes
  - La signature est sur le nom du document qui devra s'afficher
- Revenir à ce propos à l'attaque Word/WordPad

RéSIST

Virus : MyToB

- Fils MyDoom et SpyBot
- Plus de 195 Variantes
- SMTP embarqué
- Annexe souvent en .zip (parfois en CMD, BAT)
- Orienté prise de contrôle

RéSIST

Virus : MyToB

- Propagation
  - Par email
  - Partage microsoft
  - Faille LSASS
- Désactive
  - Antivirus
  - Firewall
  - AntiSpyware
- Installe une backdoor (IRC)
- Remplit le fichier hosts avec de fausses entrées

RéSIST

Outil : rope

- http://www.lowth.com/rope
- Permet de créer un langage style inspect pour Iptables.
- Utilisable pour bloquer réellement du P2P, ouvrir du SIP.
- Utilisable uniquement en kernel 2.4.x, pas encore en 2.6.x
- Soumis aux mêmes difficultés qu'inspect.

RéSIST

Outil: Rope (2)

- iptables –A FORWARD –m rope - -rope-script gnutella –j drop
- script gnutella
  - `expect_str ('GNUTELLA CONNECT /')`
  - `expect_while( {isdigit} )`
  - `expect_str('.')`
  - `expect_while( {isdigit} )`
  - `expect_str( chr(13) chr(10) )`
  - `yes`

RéSIST

Economie, Loi & Presse

- SenderID : Microsoft refusera les messages non marqués en Novembre.