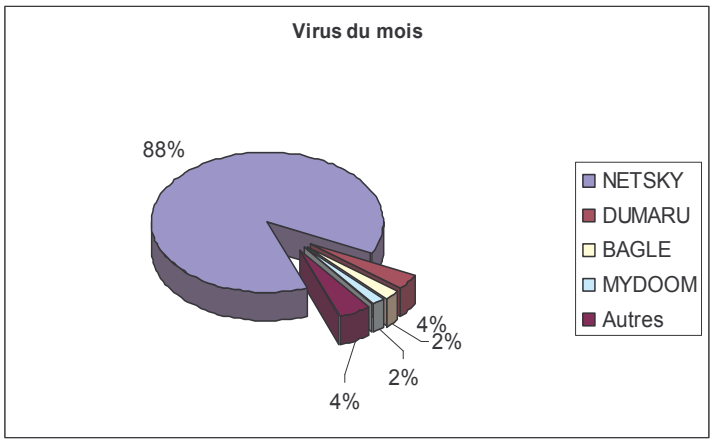
RéSIST

Tour d ’horizon

- Statistiques
- Agressions
- Utiles
  - Greylisting
- Actualités

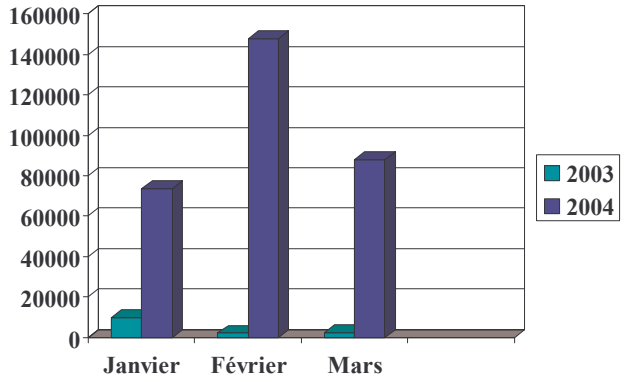
RéSIST

Statistiques : virus mars 2004



RéSIST

Statistiques : virus



RéSIST

Agressions

Virus/Ver : La nouvelle génération

Virus/Ver : La nouvelle génération

- Arrêt du bricolage
- Phase industrielle
- De l ’argent est à la clé
- Objectifs différents :
  - prise de contrôle : racket au DDOS
  - relais de spam :

Virus/Ver : La nouvelle génération

- Plus petits
  - 12 Ko pour un Bagle, 100Ko pour Subseven
- Plus rapides
  - 8 threads pour Bagle
  - 300 virus entre l ’apparition et la détection
- Plus mutants
  - Bagle : de .A à .U : 18 janvier au 26 Mars

RéSIST

Virus/Ver : La nouvelle génération

- Plus psychologues
  - FAI avec un zip crypté et explications
- Plus malins
  - Mot de passe dans le mail, puis dans image
- Plus furtifs
  - Sujet, origine, message, annexe aléatoires
  - Désactivent antivirus et firewall

RéSIST

Utiles

Méthode : greylisting

RéSIST

Méthode : greylisting

- Http://www.greylisting.org
- Méthode de lutte comportementale
- Constitution pour chaque mail du triplet
  - IP
  - @ de l 'expéditeur
  - @ du destinataire

RéSIST

Méthode : greylisting

- Si le triplet apparaît pour la première fois
  - Rejet 450 (refus temporaire)
- Si le triplet apparaît une seconde fois
  - Si le délai est > à X secondes : accepte
  - Sinon refus 450
- [Si le triplet n'apparaît plus au bout de 36 jours, on jette]

RéSIST

Méthode : greylisting

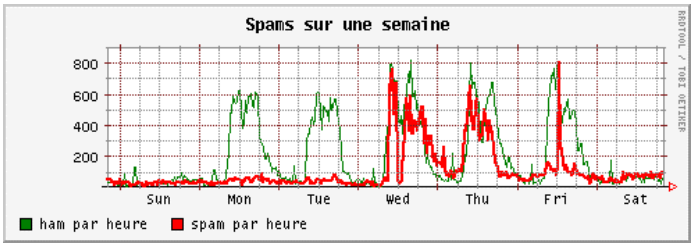
- Efficacité « brut de fonte »
  - Spam divisé par 10
  - Virus divisés par 20
- Génial !!! Mais
  - Problème avec l 'outil
  - Problème avec certains sites
  - Adaptation nécessaire

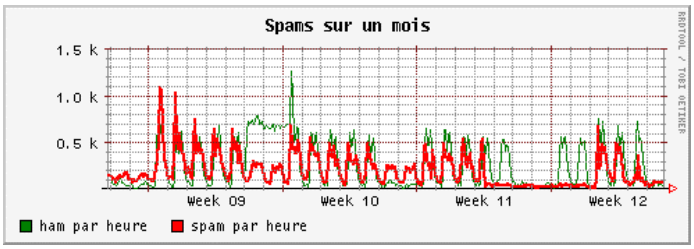
RéSIST

Méthode : greylisting

- Notion de liste grise
  - On n'applique le greylisting QUE sur la liste grise (360 domaines)
  - Celle-ci est constituée de clients de FAI, plus des unknown
- Résultats :
  - Virus divisé par 10
  - Spam divisé par 5

Méthode : greylisting





Méthode : greylisting

- Disponible sur
  - Sendmail par le biais d'un milter
  - Postfix en version 2.0.19-xxxxxx
    - Prendre DB_File::Lock
    - Gérer la notion de liste blanche
  - Exim
  - Un relais smtpd (greylisting.org)

RéSIST

Méthode : greylisting

- Exemple de greylisting pour postfix
  - http://cri.univ-tlse1.fr/resist/greylisting/