SPAM - État des lieux

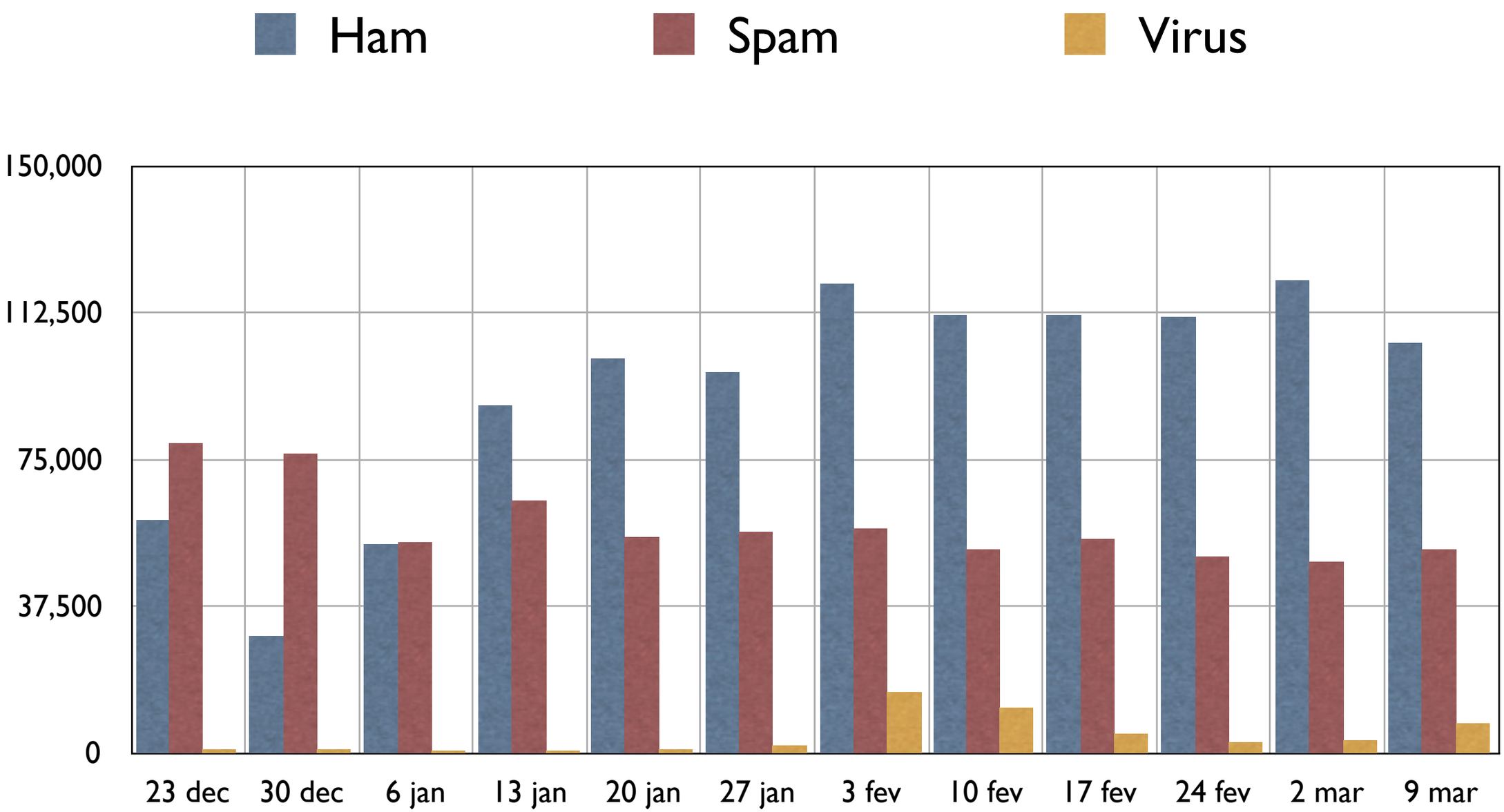
Matthieu Herrb

17 mars 2004

Rappels

- SPAM (pourriels, pollupostage,...) : courriers électroniques non sollicités.
- Activité plus ou moins illégale mais lucrative.
- Abus de relais SMTP ouverts ou machines mal sécurisées pour cacher l'identité du spammeur.

Évolution du problème



Anti-anti-spam

- Variations sur les mots clés :V|agra...
- Saturation des bases d'apprentissage bayésiennes.
- Collusion entre spammeurs et auteurs de virus/vers : utilisation de machines infectées comme relais.
- De plus en plus de spam mal détecté.

Vers la fin du mail ?

- Utilisateurs exaspérés !
- De plus en plus de messages perdus indirectement à cause du SPAM :
  - → faux-positifs,
  - → destruction accidentelle.
- Perte de confiance dans l'outil.
- Retour au papier.

Évolution des anti-spams

- Mots-clés restent efficaces
- Filtres bayésiens (Mozilla, Apple Mail,...) efficaces pour le reste (pour l'instant).
- Listes blanches.
- Accepter inconditionnellement les messages signés par S/MIME

Les 3 lois de l'anti-spam

- Ne pas altérer les messages valides

  (signature électronique)

- Respecter la vie privée et la législation

  (rapports de la CNIL, jurisprudence...)

- Ne pas ajouter de bruit dans le système

  (messages de rejet, délais, etc.)

Greylisting

- Nouvelle technique

`http://projects.puremagic.com/greylisting`

- Principe :

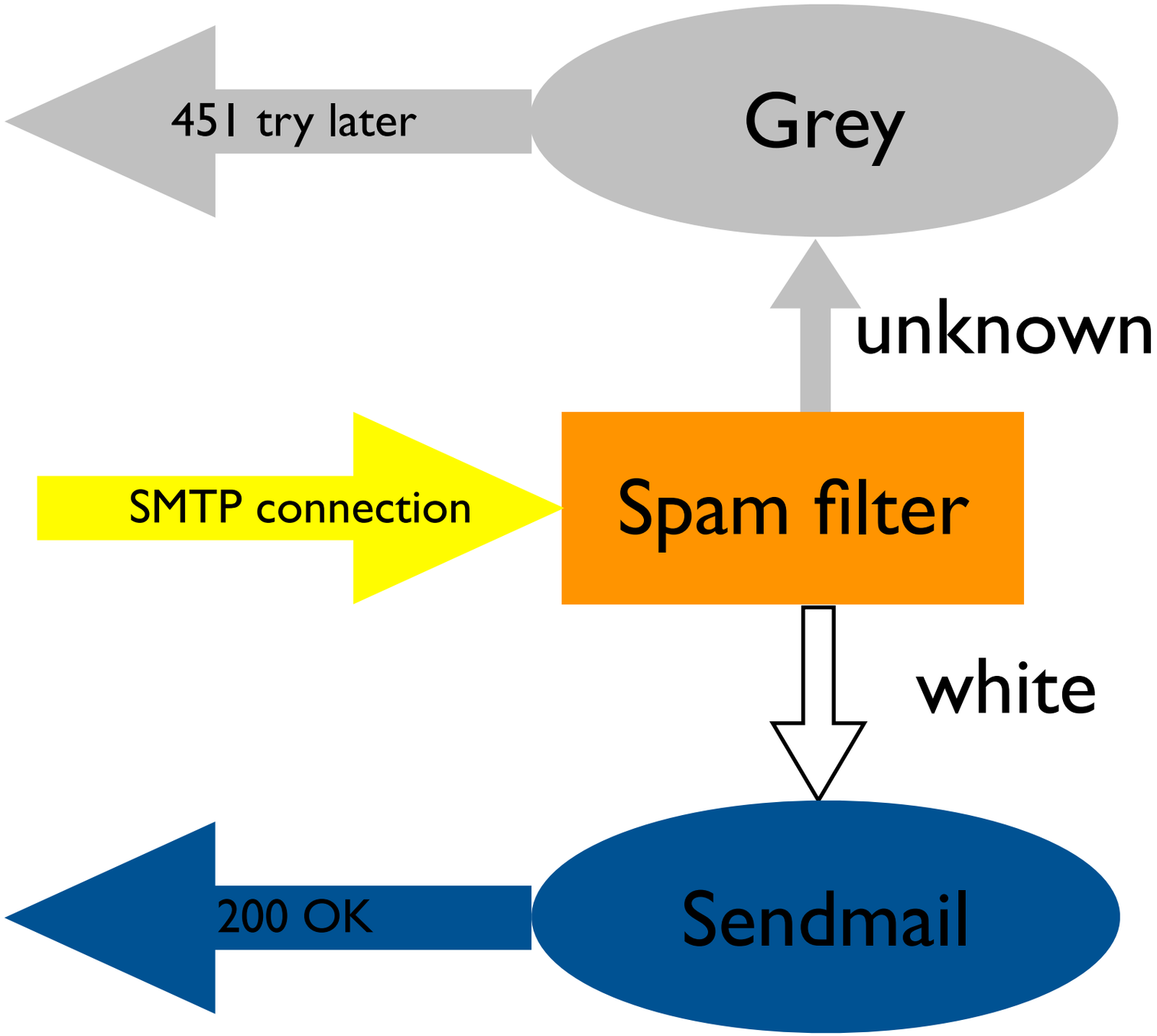
→ les spammeurs n'ont pas les moyens de traiter les ré-émissions

→ refuser avec un code 4xx (erreur temporaire) les triplets (expéditeur, destinataire, relais) inconnus. Enregistrer le triplet dans la liste "grise".

Greylisting (II)

- Si nouvelle soumission du même triplet dans un certain délai → accepter et mettre en liste blanche.
- Si pas de nouvelle soumission dans ce délai: probablement Spam. On peut :
  - ne rien faire (message pas reçu),
  - black-lister le relais en question.

Greylisting : principe



Greylisting : en pratique

- Implémentation dans spamd (OpenBSD).
- Combinaison possible avec le ralentissement des spammeurs.
- D'autres implémentations en cours de développement.

  → `<ftp://ftp.espci.fr/pub/milter-greylist/milter-greylist-0.18.tgz>`

- Plus difficile à contourner (nécessite des ressources persistantes : files d'attente,...).

Greylisting : conclusion

- Mis en place sur un site “moyen” (20 000 messages/jour):

  → Charge CPU négligeable (beaucoup plus faible que SpamAssassin).

  → En pratique très peu de messages retardés (quelques %).

- “La” solution ? (sans doute pas ☹)

Questions ?