Infections informatiques : virus et vers

Yves Deswarte
deswarte@laas.fr

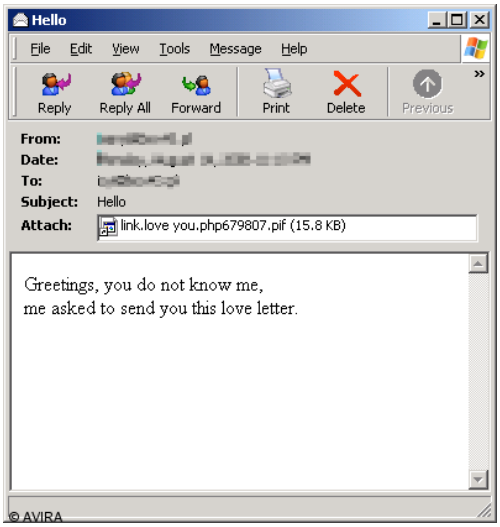
LAAS-CNRS

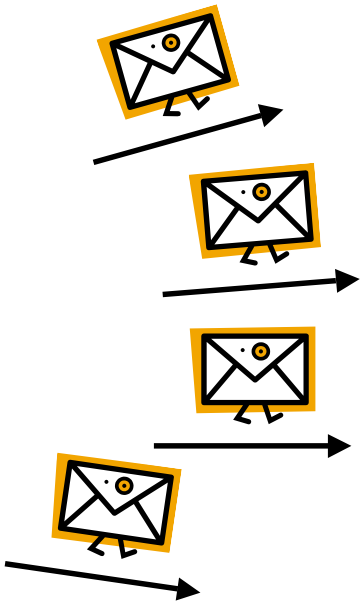
Virus informatique

- C'est un segment de programme qui se propage en insérant une copie dans un programme existant (par exemple sur disquette)

Vers informatiques

- Programme autonome, qui propage des copies de lui-même à d'autres machines
  - Ex. Le ver "I love you"





Dégâts liés à l'infection

- Propagation : période d'*incubation*
  - Rester aussi discret que possible : propagation lente, sans perturbation du fonctionnement normal
- Après la période d'incubation : bombe logique (facultative)
  - Effets visuels "amusants"
  - Modification/destruction de programmes, ou de données
  - Dégâts matériels

Prévention

- Isolation
  - Isolation totale : difficile aujourd'hui
  - Pare-feux : assez inefficaces pour les vers
- Utiliser des systèmes moins vulnérables
  - Moins courants : Unix, Macinstosh, …
  - Mieux protégés : par matériel (ex. TPM)
- Être prudent
  - Ne pas ouvrir de documents attachés
  - Ne pas télécharger des logiciels douteux…

Détection (anti-virus)

Deux types de détection :

- Détection par "signature" : rechercher (dans la mémoire, sur les disques, …) des suites d'octets caractéristiques d'un virus ou ver
  - Pas de détection de nouveaux virus
  - Difficulté : virus furtifs ou mutants ?
  - Nécessité de mises à jour fréquentes
- Détection par analyse du comportement :
  --> observer des symptômes
  (ex. modification d'un programme)
  - Rapport entre fausses alarmes et non-détection

Traitement ?

- Réparation automatique parfois possible si le virus ou ver est bien identifié (et qu'il n'y a pas d'autre problème)
- Solution générale (mais pénible !) :
  - [si possible : sauvegarder des données]
  - Reformater les disques (avec précaution)
  - Réinstaller tous les logiciels
  - Restaurer toutes les données (qu'il faut donc sauvegarder souvent)
  - Rétablir les différents paramètres…

Infection "utile" ?

- Le premier "ver informatique" était utile … Xerox 1980
- Les premiers virus aussi ! (du point de vue de leurs auteurs…)
  - Creeper/Reaper (~1970) : tester les réseaux
  - F.Cohen (1983) : démontrer des failles de sécurité
  - Brain (1986) : protection du copyright (???)
- Un ver "correcteur" peut supprimer les vulnérabilités qui lui permettent de se propager (vers Welchia, Natchia)
- Les moyens automatiques de protection peuvent être détournés pour des attaques
  - Sony, Symantec, ISS, Microsoft …
- Certains attaquants protègent leurs victimes contre d'autres attaquants !
  - vers Netsky, Sasser.E, …