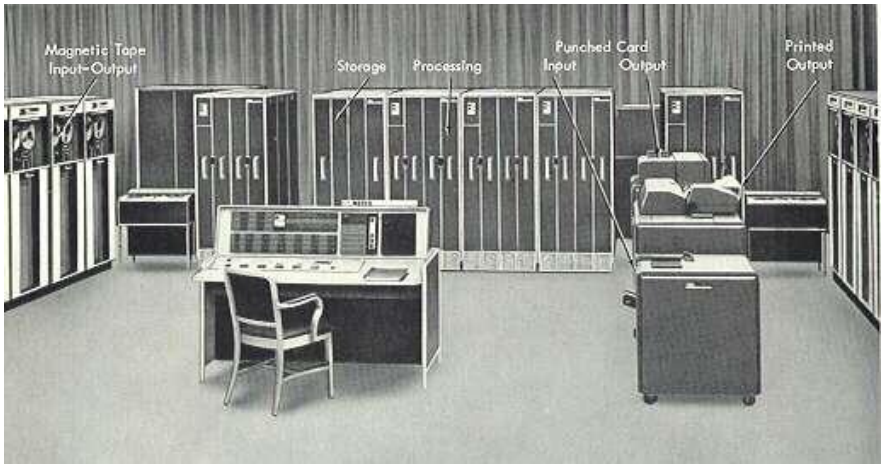
LES MALWARES

HISTORIQUE, TYPOLOGIE, DEFENSE

HISTORIQUE

La genèse: 1960 -1984

- **Au départ, un concept de jeu entre informaticiens: écrire un programme auto-reproducteur qui élimine les programmes adverses (sur IBM 7090)**
- **Dans le même temps, premiers programmes pour réaliser des tâches répétitives sur plusieurs machines d'un même réseau**
- **Aucune malveillance**



HISTORIQUE

1984-1995: les ennuis commencent

- **Le terme de « virus informatique » a été employé par Fred Cohen pour la première fois en 1984**
- **1986: premiers cas de PC infectés, réseau des universités en première ligne**
- **1988: Le vers « RTM » (Robert Tappan Morris): 5% du réseau qui deviendra Internet touché. A l'origine de la création des CERT (Computer Emergency Response Team) aux Etats-Unis**
- **1989: 50 virus répertoriés, propagation par disquette**
- **1990: Apparition de virus polymorphes, changeant d'apparence à chaque copie**

HISTORIQUE

- **1991: 1000 virus**
- **1991: les grands éditeurs tels que Symantec, McAfee déjà présents sur le marché**
- **1992: apparition des premiers serveurs dédiés à l'échange de virus (Europe de l'Est, Dark Avenger)**
- **1992: premier virus pour Windows**
- **80% des virus sont des virus systèmes**

HISTORIQUE

1995 à 2000: virus en masse, changement de typologie

- **1995: apparition des virus de macro**
- **1996: premier virus pour Excel (XM/Laroux). Acharnement sur Microsoft commence**
- **1997: 15 000 virus dont 1000 de macro**
- **1998: 40 000 virus, dont 80% de macro**
- **-> Disparition des virus systèmes**
- **1999-2000: diffusion par mail prend le pas sur diffusion par disquette: les « mass-mailers »**

HISTORIQUE

- **Janvier 99: Premier virus à utiliser la messagerie électronique: W32/Ska@M. 6 mois pour faire le tour du monde**
- **Mars 99: W97M/Melissa@MM met 2 jours!**
- **Mai 2000: VBS/Loveletter@MM met quelques heures…**
- **Apparition des virus utilisant VBS et JS**
- **2000: 56 000 virus**

HISTORIQUE

2001-…: nouveaux objectifs

- **Antivirus deviennent efficaces contre virus de macro**
- **Retour des vers, colportant backdoor et des outils de collecte d'information**
- **Un même ver peut se propager par la messagerie, les serveurs Web, les partages réseaux… infection des serveurs et des PC**
- **Les virus utilisent Internet pour se mettre à jour**
- **2004: 100 000 virus**

HISTORIQUE

- **Utilisation des réseaux peer-to-peer**
- **Virus à usage frauduleux et non plus ludique**
- **Exploitation immédiate des vulnérabilités publiées (Zero Day Attack)**
- **PDA puis mobiles touchés (bluetooth, MMS…)**

TYPOLOGIE

Par grandes familles d'infection:

- **Les bombes logiques**
- **Les chevaux de Troie**
- **Les portes dérobées**
- **Les outils de capture d'information**
- **Les outils d'attaque réseau**
- **Les outils d'appropriation de ressource**

TYPOLOGIE

Par cible:

- **Virus programme**
- **Virus système**
- **Virus interprété**
- **Vers**

- **www.wildlist.org**

TYPOLOGIE

Différence entre un virus et un vers?

- Le ver (définition de Peter Denning, 1990): programme capable de fonctionner de manière indépendante. Il se propage de machine en machine au travers des connexions réseau. Un ver ne modifie aucun programme, il peut cependant transporter des portions de code qui pourront effectuer une telle activité.

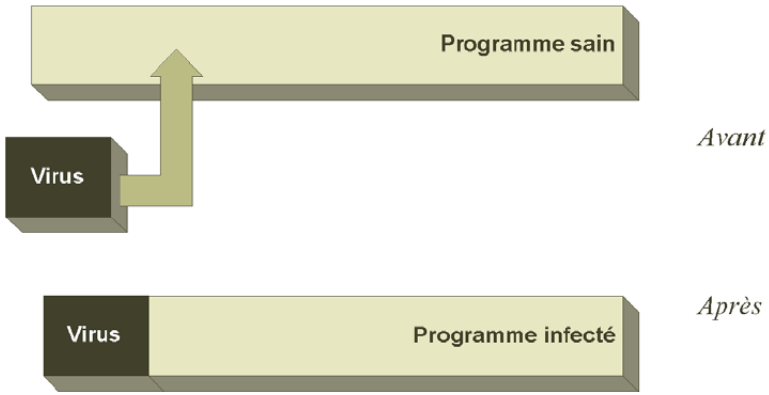
- Le virus (définition de Fred Cohen, 1984): programme capable d'infecter d'autres programmes en les modifiant pour y inclure une copie de lui-même qui pourra avoir légèrement évolué. Le virus ne peut pas fonctionner d'une manière indépendante. L'exécution du programme hôte est nécessaire à son activation.

- Les vers sont un sous-ensemble de la famille de virus.

TYPOLOGIE

Par mode d'infection:

- **recouvrement**

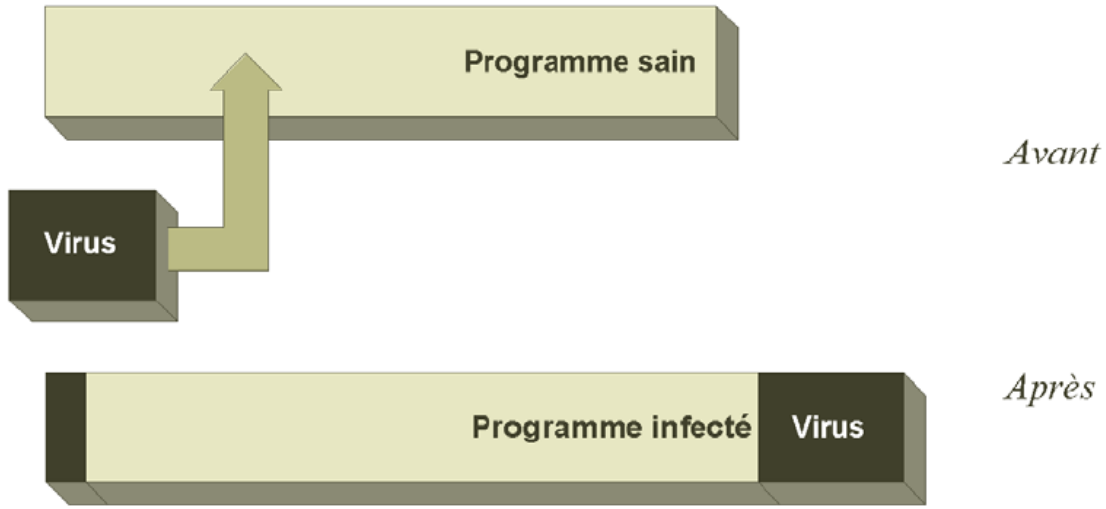


Le virus écrase une partie du code du programme hôte

TYPOLOGIE

Par mode d'infection:

- **ajout**

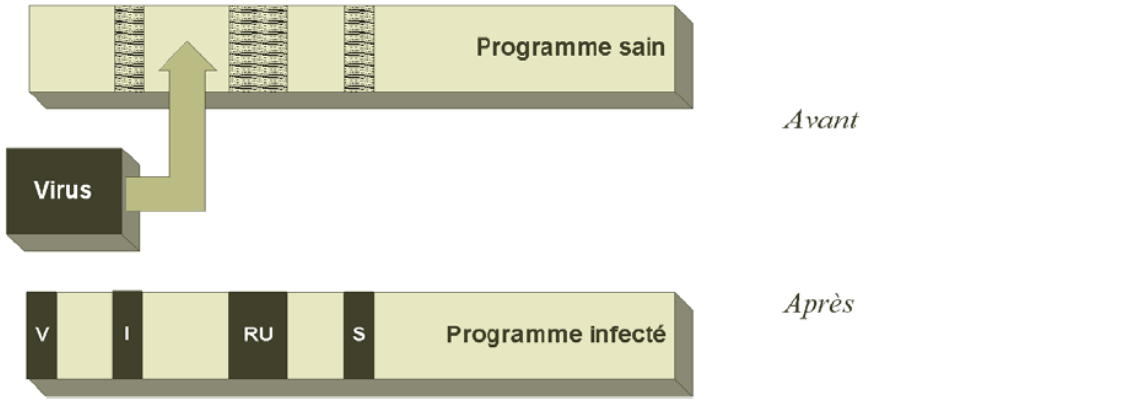


Le virus greffe son code sur le programme hôte

TYPOLOGIE

Par mode d'infection:

- **cavité**



Le virus morcelle son code en modules insérés dans les espaces inoccupés du programme hôte

TYPOLOGIE

Par mode d'infection:

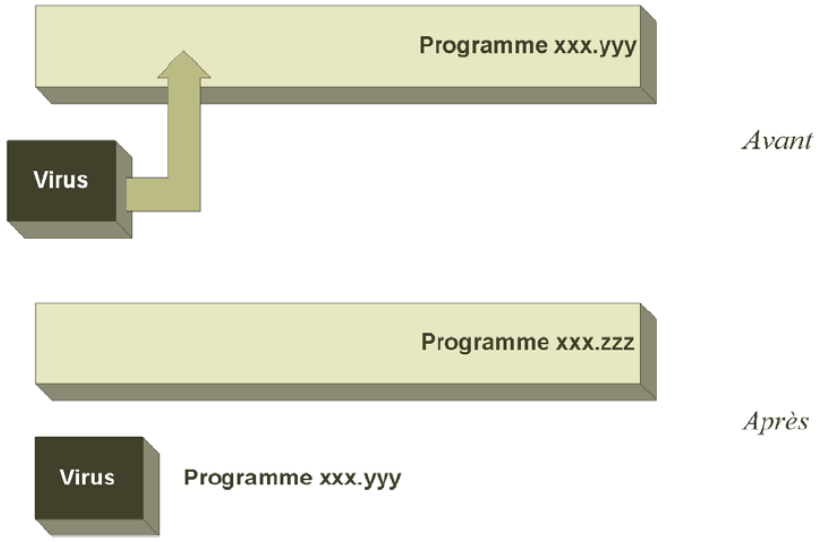
- **Point d'entrée obscur**

Le virus place son point d'entrée dans un endroit variable du programme hôte

TYPOLOGIE

Par mode d'infection:

- **Par virus compagnon**



Le programme hôte est inchangé, un programme de même nom est ajouté sur le disque

DEFENSE

Produits antivirus:

- **Détection: 4 méthodes**
  - Recherche par signature
  - Contrôle d’intégrité
  - Recherche heuristique
  - Le monitoring de programme

DEFENSE

Produits antivirus:

- **Eradiction:**
  - Étude du code viral
  - Comparaison des fichiers sains et infectés
  - Localisation des données déplacées et sauvegardées
  - Marquage des fichiers nouvellement créées
  - Recherches des modifications annexes induites sur le système (base de registre…)