

# Virus

- Tags  
obsolète

à détruire

Un virus c'est un programme qui a un comportement malsain sur ton os.  
Donc un virus sous linux c'est possible !

Cette définition ne correspond pas à celle d'un virus. Cette définition se rapporte plus à la destination general de ce qu'est un malware. Un virus est un programme informatique qui a la particularité de se multiplier en infestant d'autres programmes, le terme de virus a été choisis à cause de ce comportement qui est semblable à celui d'un virus biologique

**Exemple de virus très simple :**

*Une boucle infinie qui provoque des zombies...*

Ce n'est pas un virus ce genre de malware se rapproche plus d'un forkbomb, s'est à dire un programme se dupliquant à l'infini, que ce programme génère des zombies ou non ne changera rien au problème

## Explications :

Il est totalement faux de croire qu'un **antivirus** ne se met que sur un dual-boot ou sur un serveur de fichiers.

*Personnellement, j'envoie des docs à des clients sous Windows et je ne peux pas me permettre de les contaminer.*

Egalement, il existe des **virus** sous Linux (si, si) et même si les dépôts sont tenus par des gens dignes de confiance, nous ne sommes pas à l'abri d'un paquet virusé.

## Linux et Windows face aux virus :

Les avantages de Linux par rapport à Windows sur ce point :

- Moins connus + politique de liberté du code

tsss... Je conteste vigoureusement se premier point qui est du bourrage de crâne insidieux contre les logiciels libres. Si les "desktops" sont moins nombreux, les serveurs eux sont bien représentés, et un serveur est par définition très exposé. J'en profite d'ailleurs pour rappeler que internet en lui même est une brillante réussite des logiciels open-source.

La "sécurité par l'obscurité", on sait ce que ça vaut, et le deuxième point vient d'ailleurs le rappeler

: On ne peut pas compter qu'une faille soit cachée pour assumer la sécurité, ce qui est un défaut général des logiciels propriétaires pour lesquels on est dépendant du bon vouloir de l'éditeur pour les combler (ou pas) avec une réactivité généralement bien plus faible qu'avec les logiciels libres ou l'on a accès à l'intégralité du code.

Une des principales raisons de la meilleure sécurité de Linux par rapport aux virus est la politique de sécurité plus stricte quand à l'installation et l'exécution des programmes (plus enquiquinante dirait un Windowsien, la sécurité est toujours contraignante). Comme pour une bijouterie, un bon mur et peu d'ouvertures offre une bonne protection pour beaucoup moins cher que beaucoup de gardiens (anti-machins Microsoft).

-

Haricophile

## Administration

Un virus ne peut pas s'installer sans l'accord (direct ou indirect) de l'admin du système.

Autrement dit, Une bonne administration sous linux ne prendra jamais de virus, une bonne administration sous M\$ si !

Ne transigez pas avec les droits d'administration de votre système.

- Tout ce qui n'est pas nécessaire à l'user doit être réservé à root !
- Ne vous baladez pas sur internet sous votre session **root** !
- Composez des passwd root d'envergure et n'hésitez pas à les renouveler annuellement !
- Un bon mot de passe root se compose de 20 caractères alpha-numériques !
- Utilisez [keepassx](#).

From:

<http://debian-facile.org/> - **Documentation - Wiki**

Permanent link:

<http://debian-facile.org/atelier:chantier:securite-virus>

Last update: **23/10/2015 05:32**

