# VIRUS

- Tags
  obsolète, enchantier

  à détruire

Les virus informatiques sont des programmes qui sont exécutés à l'insu des utilisateurs et qui ont la propriété de se propager d'une machine à une autre.

- Objet : Manuel virus
- Niveau requis : DÉBUTANT
- Commentaires : *Quoi? un anti virus sous Linux? !*
- Débutant, à savoir :

## Introduction

### Virus

#### Cet article étant bourré d'âneries, il doit être considéré comme en travaux :)

Un **virus** est un programme qui a un comportement malsain sur le système d'exploitation (SE) (on voit aussi OS pour Operating System).
Un virus s'auto-réplique.

#### Exemple d'attaque très simple : Les Fork Bomb

Une boucle infinie générant des processus *zombies*, parasitant à terme le système et provoquant son plantage (**Fork Bomb**).
exemple à ne surtout pas tester sur sa machine sous peine d'être obligé de faire un reboot

```
:(){ :|:& };:
```

Les fork bombs sont une forme de deni de service, la ligne de commande indigeste ci dessus est une fonction utilisant la récursivité, c'est à dire que la sortie du programme est redirigée dans lui même à l'aide d'un pipe ⇒ | , Le programme est éxécuté en tache de fond ⇒ &
Le programme appelle donc une instance de lui même qui appelle une instance de lui même, etc... la consequence c'est que toutes les ressources de la machines vont être saturée et l'utilisateur n'aura même plus assez de ressources pour tuer le processus
Pour comprendre le fonctionnement, le programme suivant fait exactement la même chose que le précédent mais sa syntaxe est plus facilement compréhensible

```
forkBomb() {
 forkBomb | forkBomb &
```

```
}; forkBomb
```

=== Se proteger des forks bomb ===
Se proteger des fork bombs est assez simple, il suffit d'ajouter les noms, les groupes ou tous les utilisateurs au fichier /etc/security/limits.conf et d'y mettre une limitation du nombre de processus.


La syntaxe utilisée dans ce fichier sera bientôt expliquée,

### Malware

Un **malware** est un logiciel malveillant.

Ce sont de petits programmes conçus pour vous nuire, ou vous surveiller, vous traquer, et qu'il vaut mieux pourchasser et détruire.

- Les malwares ne sont pas conçus pour se reproduire eux-mêmes.
- Un malware peut contenir un virus sans rapport avec son programme.




Un virus est un logiciel conçu pour vous nuire et qui a la faculté de se répliquer en contaminant d'autres programmes, c'est donc une forme de malware ;)

On distingue plusieurs catégorie de logiciels malveillant :

- Les virus
- Les vers qui ont la facultés de de s'autorepliquer et n'ont, à la différence des virus pas besoin de “parasiter” d'autres programmes
- Les chevaux de Troie (trojan) et les portes dérobées (backdoor)
- Les rogues, les spyware, keyloggers, exploits, outils de DOS et DDOS, etc…


Donc une attaque sous GNU/Linux c'est possible !

## 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 documents à des clients sous Windows et je ne peux pas me permettre de les contaminer.


Également, il existe des **virus** sous GNU/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 contaminé par un virus.

A ma connaissance, les seuls virus ayant existés sous GNU/Linux ne sont que des Proof of Concept. Un virus ayant besoin d'exploiter une faille de sécurité et les failles exploitées par ces virus ayant été patchées depuis longtemps, il n'y a actuellement aucun virus actifs répertoriés sous GNU/Linux. Ce qui ne veut pas dire qu'il ne peux jamais en avoir, de plus les virus ne sont pas la seule menace pour la sécurité

## Linux et Windows face aux virus :

Les avantages de Linux par rapport à Windows :

Il n'y a pas de virus à l'encontre de **Linux** (ainsi que de Mac OS/X) car l'architecture de leurs logiciels est conçue pour ne leur permettre :

1. ni de pénétrer,
2. ni de se répliquer,
3. ni de se propager.

Les virus contre **Linux** ou **Unix** sont des campagnes de désinformation destinées à discréditer les logiciels libres et à vendre des anti-virus à des gens qui n'en ont pas besoin avec le libre.

Il est même dangereux d'utiliser un **logiciel anti-virus privateur** (même **gratuit**) sous Linux, surtout si on en a pas le code, car ce serait une énorme faille dans la sécurité.

Ces systèmes d'exploitation font partie de la famille des **Unix**. C'est sur **Unix** que sont apparus les premiers virus vers 1975.
Tout de suite, les concepteurs d'Unix ont mis en place les barrières qui ont sécurisé Unix.

*Ainsi, il y a* des lustres *qu'on ne parle plus de virus sur **Unix***.

A contrario, Microsoft n'a pas pris les mêmes précautions pour des raisons historiques.
Pour faire le DOS il lui a fallu faire des simplifications considérables et la notion de sécurité a été complètement éludée.
Dans toutes les versions qui ont suivi, la sécurité est un emplâtre que l'on rajoute et non une caractéristique intrinsèque du système.

La **légende** comme quoi l'inexistence actuelle de virus contre Mac OS/X et Linux repose sur leur faible nombre est dénuée de fondement.
*Elle est cependant soigneusement entretenue par les privateurs et les marchands d'anti-virus qui y voient un manque à gagner.*

La perfection n'existe pas, il arrive que des informaticiens trouvent des *failles potentielles de sécurité*

dans le code source du libre.
Les corrections sont aussitôt réalisées puis les mises à jour de sécurité sont livrées aux utilisateurs dans les heures qui suivent.

## Administration

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

Autrement dit : Une bonne administration sous GNU/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 mots de passe root d'envergure et n'hésitez pas à les renouveler annuellement! Un bon mot de passe root se compose de 20 caractères alpha-numériques!
- Installez : clamav logiciel linux d'anti-virus libre pour tous vos systèmes.

## Lien

- http://pjarillon.free.fr/redac/virus.html
- http://fr.wikipedia.org/wiki/Logiciel_malveillant

From:
http://debian-facile.org/ - **Documentation - Wiki**

Permanent link:
**http://debian-facile.org/atelier:chantier:virus**

Last update: **26/01/2016 22:57**