

# MARC BLANCHARD VIRUS DOCTEUR

## [Définition&Explications] Un virus

Dans cette section pour tout public, je vais essayer d'aborder de manière la plus compréhensible un certain nombre de termes que nous utilisons dans notre métier, nos laboratoires et que, peut-être, vous rencontrerez dans les différents compte-rendus scientifiques sur ce site.

Dans ce post, voici une petite explication sur le mot VIRUS.

La nomination du mot virus est utilisé pour tout ce qui a une relation avec une attaque d'un ordinateur, serveur, épidémie sur internet ou une infection informatique. Cette utilisation est incorrecte, mais elle est comprise par tous et toutes. C'est pourquoi, je vais vous expliquer les différences entre tous ces codes qui, de par leurs formes, leurs techniques, leurs propagations et infections sont nommés différemment.

### **Que se passe-t-il lorsqu'un logiciel ou un programme est exécuté ?**

a. l'utilisateur clique sur une icône d'un programme, dans notre exemple Notepad :



b. Ce programme va se charger en mémoire RAM de l'ordinateur :

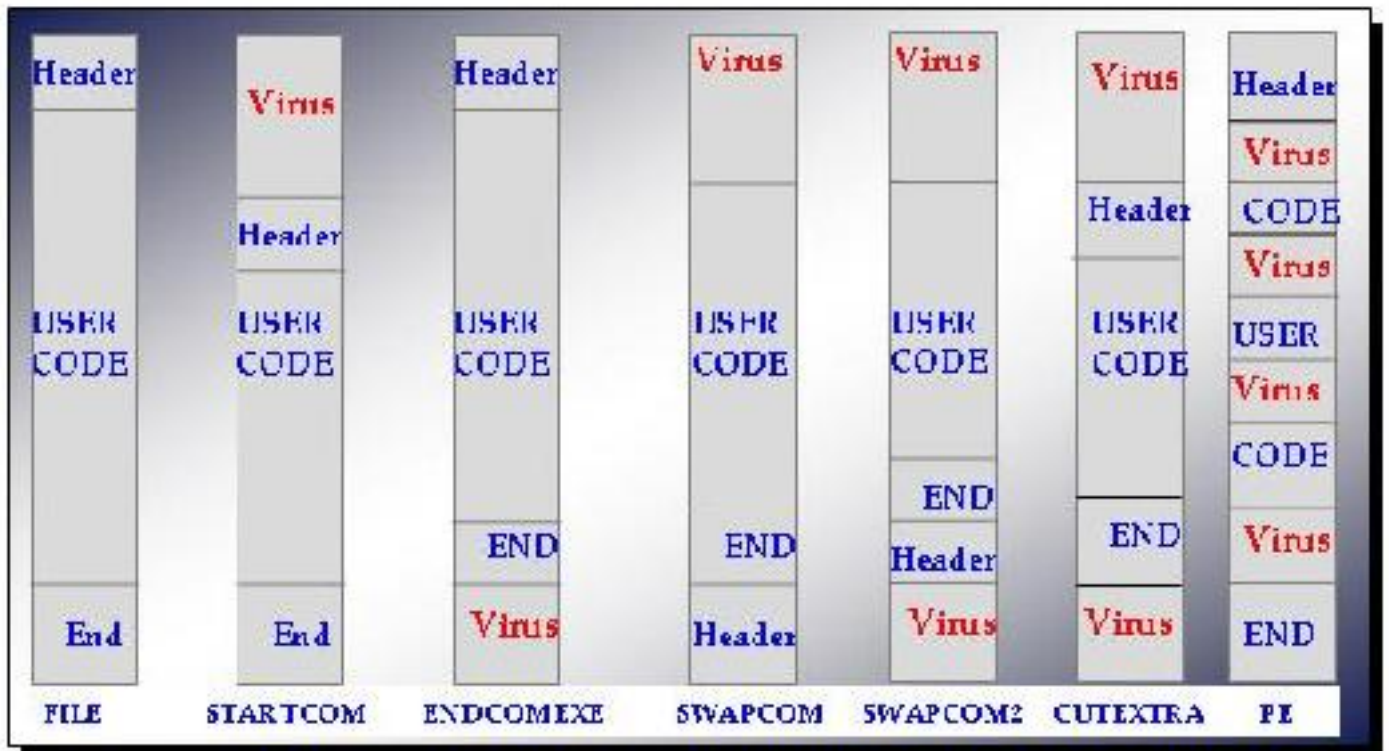


c. Le résultat après exécution apparaît sous forme de fenêtre ou dans une barre de tâches



### Que se passe-t-il lorsqu'un virus tente d'infecter un fichier ?

Un virus est en fait un micro-programme qui est dépendant d'un fichier utilisateur que nous appelons un fichier hôte. Le virus va effectuer plusieurs tentatives d'infections dans le fichier hôte en fonction de sa technologie. En d'autres termes, le virus s'auto-adapte selon les fichiers présents sur le disque dur de sa victime. Le but est d'infecter un maximum de fichier afin d'allonger sa durée de vie.



On constate sur la gauche, la structure schématique d'un fichier. De gauche à droite, représentent toutes les possibilités technologiques qu'un virus va tenter pour infecter un fichier hôte, afin qu'il puisse continuer de fonctionner nativement, mais également de lancer le virus de façon transparente.

### Constatation

On se retrouve alors avec un fichier qui a en fait deux programmes, le micro-programme du virus et le programme original !



### **Perception de la contamination**

En général, l'utilisateur ne s'aperçoit de rien, car un virus est si petit, si furtif, qu'il travaille en arriere plan à l'insu de l'utilisateur.

Un virus pénètre dans la machine de sa victime par le biais de téléchargement de programmes ou de logiciels comme des sharewares ou freewares proposés sur des forums, peer to peer, par des pièces jointes attachées aux messages, ou en cliquant sur un lien web contenu dans un courrier électronique, etc...

### **Méthodes de détection**

Les virus, utilisant ces techniques d'infections, sont généralement bien détectés et éradiqués par des logiciels antivirus.

### **Variantes technologiques**

Pour contrer les antivirus, certaines technologies incluent dans toutes les catégories de codes malicieux comme les virus, vers, chevaux de troie, portes dérobées, rootkits, etc, et sont utilisées afin de gagner du temps de durée de vie.

Pour un code malicieux, la durée de vie est capitale, puisque plus la durée de vie est longue, plus il sera virulent, et donc plus propagateur. Par conséquent, plus long à être éradiqué.

Dans cette rubrique, nous traiterons plus en détails de ces technologies.

## Commentaires

2007-10-08 16:17:26 - Thierry

Clair et accessible à tous !  
Merci ;)

2007-10-08 16:51:55 - cochontetram - <http://cochon.tetram.free.fr>

Sympa cette petite explication merci :)

Copyright : Blanchard [Virus Docteur] Marc - 2007-10-07 22:21:00  
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- \* de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

\* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

\* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>