

# MARC BLANCHARD VIRUS DOCTEUR

## [Définition&Explications] Un Trojan, trojen, cheval de troie

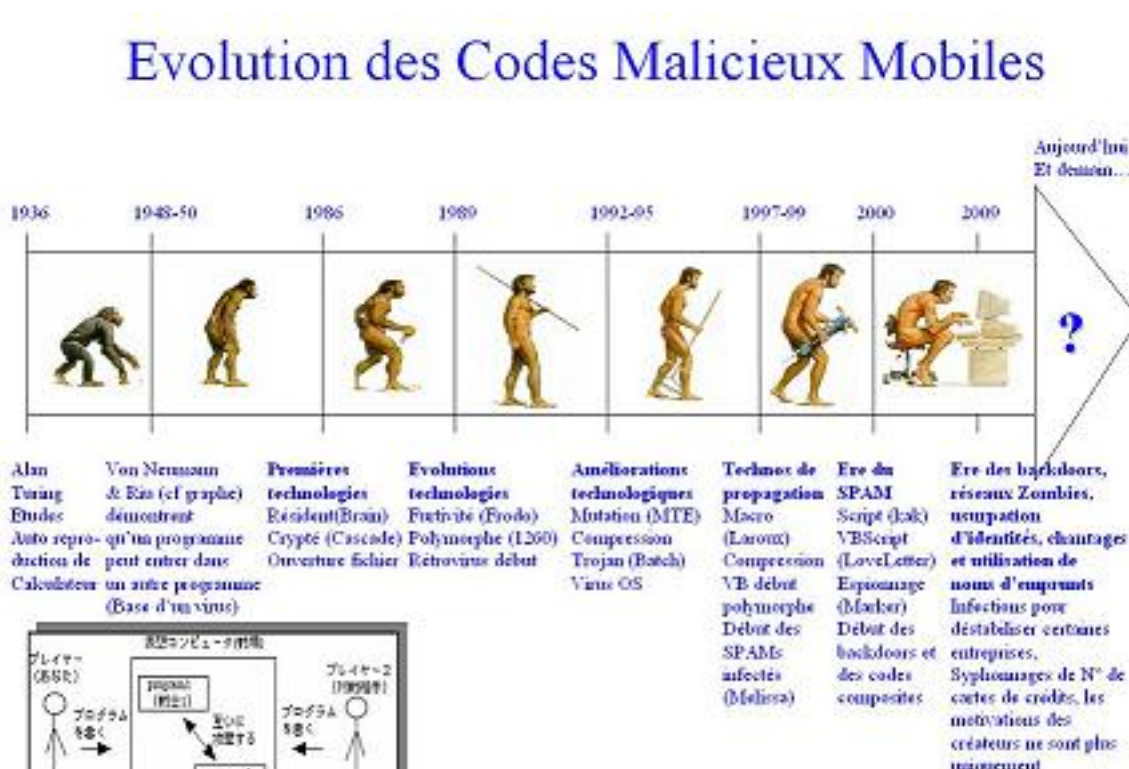
Dans cette section pour tout public, je vais essayer d'aborder de manière la plus compréhensible un certain nombre de termes que nous utilisons dans notre métier, nos laboratoires et que, peut-être, vous rencontrerez dans les différents compte-rendus scientifiques sur ce site.

Dans ce post, voici une petite explication sur le mot TROJAN (Cheval de Troie).

La nomination du mot TROJAN est utilisée pour tout ce qui a une relation avec une attaque d'un ordinateur, serveur, perturbation informatique. Cette utilisation est incorrecte, mais elle est comprise par tous et toutes. C'est pourquoi, je vais vous expliquer le terme générique TROJAN qui est aujourd'hui utilisé dans notre métier.

### Définition :

Les premiers trojans ont été développés par le mathématicien Alan Turing en 1936, qui avait comme mission d'appliquer le même programme sur différents calculateurs.



Un Trojan est un code malicieux dont la totalité de son code programme EST le code malicieux.

Contrairement aux techniques utilisées par les virus (concaténation du code malicieux dans le code programme original d'un fichier existant (fichier hôte)), les trojans sont complètement indépendant au niveau de leurs codes.

Les trojans sont généralement des programmes en tant que tel, comme des outils freeware ou shareware, téléchargés par un utilisateur ou arrivant via une technologie de Worm ou StormWorm par le biais du mail, web, MSN, IRC, etc ou sous forme de lien HTML.

### **Technologies embarquées :**

Les Trojans peuvent embarqués de nombreuses technologies pour effectuer leurs process malicieux :

-Technologies de rootkit

- Technologies de Backdoors (portes dérobées) : ouverture d'un port TCP permettant au pirate d'entrer sur la machine victime pour lui faire faire des actions malicieuses

- Technologies de BotNet (robot internet) : permet d'envoyer l'adresse IP en temps réel de la victime au pirate, lui permettant ainsi d'avoir les coordonnées de ses victimes pour entrer via la backdoor

-Technologies de programmations telles que MUTEX

-Technologies de Compétences transversales pour une attaque sans incident !

-Technologies d'hébergement de WORMS (vers) permettant ainsi une durée de vie de ce code malicieux la plus longue possible

### **Perception de la contamination**

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

Ensuite, la perception de la contamination dépendra des actions pré-programmées du trojan.

### **Méthodes de détection**

Les trojans sont détectés et éradiqués par des logiciels antivirus.

### **Méthode d'erradication**

Il est possible de rencontrer des problèmes d'erradication des Trojans, car ils utilisent très fréquemment la technique MUTEX.

On essaiera, dans ce cas, de rebooter en mode sans echec, et de scanner tous les fichiers de la machine avec un antivirus à jour.

Pour certains egenes trojans, il est parfois nécessaire de procéder à un nettoyage manuel ou par le biais d'un cleaner.

## Commentaires

2007-11-27 17:20:55 - Alexandre - sorak92@hotmail.fr

C'est parfait !  
vous avez répondu à mes questions.  
je vous remercie.

Copyright : Blanchard [Virus Docteur] Marc - 2007-11-27 11:29:58  
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/>