LES VIRUS

Jean-Michel COSTE

Évoqué en France en Octobre 1989 à l'occasion d'une grand-messe télévisuelle et dans quelques articles à sensation souvent mal documentés, le problème des VIRUS informatiques éveilla l'inquiétude de l'opinion publique. L'alerte fut provoquée le 11 Octobre 1989 par une note du secrétariat général de la défense nationale expédiée au CNRS et faisant état d'une probable attaque de VIRUS le vendredi 13 suivant.

En fait les Virus existent depuis l'apparition de l'informatique (sous des formes diverses). Les informaticiens se sont souvent amusés à pousser le système sur lequel ils travaillent jusqu'à ses limites, L'apparition massive de VIRUS sur compatibles PC date de 1987 (Pakistani BRAIN, LEHIGH, OLP). En 1988, les VIRUS étaient environ une douzaine (à l'époque on parlait aux US de DIRTY DOZEN, en français les DOUZE SALOPARDS). L'introduction massive de micro-ordinateurs dans les universités et les établissements scolaires, le nombre grandissant d'ordinateurs personnels, les réseaux de communication ont favorisé la création et la diffusion des VIRUS, maintenant au nombre de plusieurs centaines.

Aucun type de machine n'est épargné, APPLE, COMMODORE, ATARI, compatibles IBM ont tous leur lot de VIRUS. Nous allons décrire dans la suite l'anatomie d'un VIRUS sur compatible PC, les principes étant certainement valables pour tout autre type de micro-ordinateur.

I. LES GAGS

Ce sont de "petits" programmes que l'on peut trouver amusants ou non, selon son humeur. Qui n'a pas encore vu les effets de DRAIN, FACE, EGAGAG, RADIO ? Le premier vous dit qu'il a trouvé de l'eau dans votre disque dur et fait entendre un bruit de pompe dans le haut-parleur de votre PC. Le second reste résident et déclenche l'apparition d'un petit bonhomme (code ASCII 1 ou 2) à chaque pression sur la touche INS. Effet garanti dans WORD, les bonhommes se heurtent aux lignes de

texte (j'ai même vu des élèves tenter de les capturer en dessinant des cadres !). Le troisième reprogramme la matrice de caractères de la carte vidéo (EGA ou VGA) et les caractères apparaissent en gothique, en italique ou à l'envers. Quant au quatrième, il donne l'impression de transformer votre PC en récepteur radio (voix et musique digitalisées).

Ces programmes n'ont bien entendu rien à voir avec des VIRUS. A la rigueur, FACE pourrait être considéré comme un pré-VER, puisqu'une fois lancé, il reste résident jusqu'à l'extinction de la machine, comme le font certains utilitaires de bureau (SIDEKICK, GRAPH-IN-THE-BOX par exemple).

Si vous êtes victime de l'un de ces gags, ne criez pas au VIRUS, examinez plutôt votre fichier de lancement AUTOEXEC.BAT (ou autre) dans lequel un petit plaisantin a intercalé le nom du programme en question.

La liste que j'en donne n'est pas exhaustive, ils sont souvent distribués par les clubs d'utilisateurs.

II. LES VERS

A. Softwar

Je recommande la lecture de ce livre, histoire romancée, peu probable mais parfaitement possible, du logiciel de météo vendu par les USA à l'Inde, récupéré par l'URSS, qui contenait un VER dont le but était de bloquer le système sur lequel il fonctionnait dès qu'apparaissait une certaine pression atmosphérique sur une île perdue du pacifique.

B. La banque

Une autre anecdote qui circule : un programmeur, employé dans une banque, avait introduit dans le programme général de gestion quelques instructions qui avaient pour but de vérifier si son nom faisait figurait parmi les clients de la banque. Dans le cas contraire, il provoquait des dégâts en effaçant des fichiers. Le jour ou il fut "remercié", il ferma son compte. On imagine facilement la suite : il fallut récupérer la dernière sauvegarde, et mettre plusieurs programmeurs à traquer l'intrus dans les milliers de lignes du programme.

C. Principes d'installation d'un ver

1. à la conception

Dans les deux cas précédents, le VER était constitué de quelques instructions introduites *par le programmeur* dans le texte *source* du programme, donc au moment de la conception du logiciel.

2. greffage

Il est possible d'installer un VER dans un programme exécutable. C'est une opération délicate si l'on procède "à la main". Nous allons examiner le principe d'installation d'un VER dans un exécutable de type "EXE". Pour cela, quelques prérequis sont nécessaires.

Un fichier de type EXE est constitué d'un entête (au minimum 512 octets) contenant des renseignements pour le DOS. Parmi ceux-ci, l'adresse de démarrage du programme (de la première instruction à exécuter). La figure 1a illustre cette structure.

Figure 1a

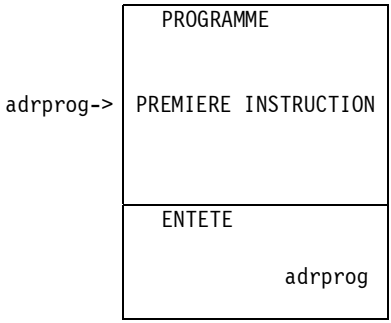
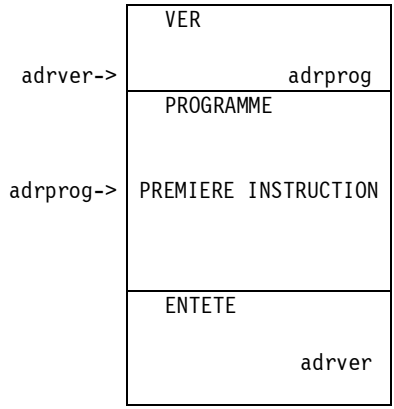


Figure 1b



L'installation se fait en trois temps (voir figure 1b).

1). Recopier le VER à la suite de programme (la commande COPY, bien utilisée, devrait suffire),

2). Récupérer l'adresse de démarrage pour la stocker dans le VER,

3). Remplacer l'adresse de démarrage du programme par l'adresse de la première instruction du VER.

Au lancement du programme, le système d'exploitation cherche l'adresse de démarrage dans l'entête, exécute les instructions du VER, lequel (s'il est bien programmé) passe la main au programme original.

Lorsque ce programme se termine, la mémoire qu'il occupait est libérée par le DOS, et le VER disparaît avec lui jusqu'à la prochaine utilisation du programme hôte. Le VER peut aussi être programmé pour rester résident (voir plus loin) et se manifester de manière périodique. Je nommerais ce type de programme MICROBE ou pré-VIRUS.

L'action du VER est à la mesure de l'imagination et de la méchanceté du programmeur, cela peut aller du simple "COUCOU" sur l'écran jusqu'à l'effacement de fichiers sur le disque, tout cela avant le lancement de votre dernier jeu favori qui semble fonctionner parfaitement.

On a vu circuler aux USA une grande quantité de copies (illicites) de jeux porteurs de VERS.

Le traitement en est simple : il suffit d'effacer le programme porteur. Contrairement aux VIRUS, les VERS ne se reproduisent pas. Un VER n'est exécuté que si on lance son programme porteur.

III. LES INTERRUPTIONS

Le processus de fonctionnement des VIRUS est lié à l'architecture des machines : Les principes d'interruption et de programme résidents.

Le système de gestion des événements (PC ou MAC) est une conséquence du principe d'interruption dont sont dotés leurs processeurs (80xxx ou 68000). Le PC est équipé d'un contrôleur d'interruption programmable (le PIC 8259). Son but est de percevoir les événements extérieurs. Chaque événement est transmis au PIC dont le rôle est d'informer le processeur. Pour simplifier, ces événements sont numérotés, nous allons en décrire quelques uns.

08 TIMER	Interruption due au TIMER (voir plus loin)
09 CLAVIER	Une touche a été pressée
12 COMMUNICATIONS	Octet reçu sur COM1

Le TIMER est un circuit qui envoie une interruption 18 fois par seconde (environ). Cela permet la mise à jour des date et heure.

Le processeur, recevant une demande d'interruption, et connaissant son numéro (c'est le 8259 qui le lui transmet), cesse son activité courante et lance le programme approprié à la gestion de l'événement. Il reprendra le traitement en cours lorsque cette gestion

sera terminée. Pour déterminer l'adresse du programme d'interruption, il consulte une table (située dans le premier Ko de mémoire RAM,) qui contient ces adresses. Elles sont mises en place par le BIOS au démarrage de la machine. (On appelle aussi ces adresses les VECTEURS d'interruption). Il y a 256 vecteurs possibles, chacun d'eux occupant 4 octets.

Ce que l'on vient de décrire représente la gestion des événements extérieurs, dûs à des périphériques, on les nomme interruptions matérielles. La table des vecteurs contient aussi les adresses d'autres programmes de service. On les appelle interruptions logicielles. Elles sont demandées par programme.

16 VIDEO	Ecriture/Lecture en mémoire vidéo,
19 ACCES DISQUE	Ecriture/lecture sur disque,
23 IMPRIMANTE	Communication port parallèle.

Cela a été conçu pour faciliter le travail du programmeur. Par exemple, au lieu de calculer le numéro de la case mémoire dans laquelle il doit déposer un caractère pour le voir s'afficher sur l'écran, il lui suffira de placer dans un registre du processeur les numéros de ligne et de colonne, et de demander une interruption 16 (en simplifiant à outrance !).

Ces vecteurs se trouvant en RAM, ils sont donc modifiables. Les VIRUS modifient (ou "détournent") certains de ces vecteurs. D'autres programmes le font, pour la bonne cause. Il existe même une fonction du DOS qui permet d'obtenir et de modifier la valeur d'un vecteur, quelle tentation !

A. Un pré-VIRUS : KEYBFR

Un compatible PC, quel que soit le pays où il est livré, est équipé d'un clavier US (QWERTY). On a simplement changé quelques touches, mais les circuits sont absolument identiques. Beaucoup s'en sont rendus compte pour avoir oublié le magique KEYBFR (ou KEYB FR). Le BIOS de la machine gère le clavier par l'INT 9.

KEYBFR est composé de deux parties : une partie installation, une partie traitement. Seule la partie traitement reste résidente.

L'installation est simple : (voir figures 2a et 2b)

IX. Lire le vecteur 9 et conserver cette adresse.
X. Remplacer le Vecteur 9 par l'adresse de son propre programme de traitement.

XI. demander à rester résident

Une fois installé, le fonctionnement est évident : A chaque pression sur une touche, une INT 9 est déclenchée, le processeur lit le vecteur 9 et lance l'exécution du programme se trouvant à l'adresse "nouvclav". Ce programme a pour but de tester si la touche fait partie de celles qu'il doit transformer (A,Q,W,Z,...). Si oui, il la traite et "rend la main". Si non, il passe la main au programme se trouvant à l'adresse "adrclav" (qu'il a soigneusement mémorisée) lequel se chargera de toutes les autres (E,R,T,ESC, ENTREE, ...) et "rendra la main". Ce traitement terminé, Le processeur reprendra le travail interrompu.

Figure 2a

(Avant KEYBFR)

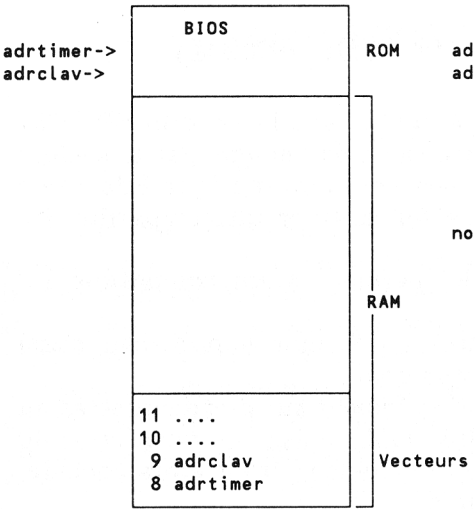
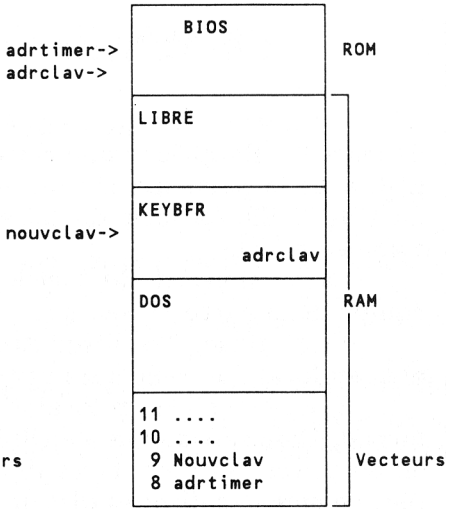


Figure 2b

(Avant KEYBFR)



Vous trouverez la suite de cet article dans le prochain bulletin :

IV. Principe de fonctionnement d'un VIRUS

V. Les virus "programme"

VI. Les VIRUS "boot"

VII. Protection

VII. Détection et Traitement

Jean-Michel COSTE
Formateur MAFPEN-Créteil