LES VIRUS
(SUITE)

Jean-Michel COSTE

IV. PRINCIPE DE FONCTIONNEMENT D'UN VIRUS

A. Structure d'un VIRUS.

La terminologie employée m'est tout à fait personnelle, mais correspond parfaitement aux virus qu'il m'a été donné d'étudier. Un "bon" VIRUS est structuré en quatre parties comme le montre le schéma suivant (Figure 3a) :

Nous allons détailler ces quatre parties.

B. Installation

C'est ce programme qui est exécuté en premier, au lancement de son programme hôte. Quel que soit son mode de lancement (voir plus loin les deux types de VIRUS), le programme doit laisser une partie de son code résident, (à la manière de KEYBFR) pour pouvoir agir pendant tout le temps d'activité de la machine. Le programme d'installation s'occupe de "brancher" les trois autres parties sur les interruptions les plus appropriées. Le VIRUS, pour s'activer (de manière régulière), peut détourner le vecteur TIMER vers le sous-programme d'activation. Pour pouvoir se reproduire (fréquemment, mais sans ralentir la machine de manière visible) il peut détourner le vecteur "accès disque" vers le sous-programme de propagation, de telle manière qu'un accès disque inoffensif (DIR A:, par exemple) déclenche la reproduction du VIRUS sur le lecteur A:. Les deux vecteurs originaux sont bien entendu recopiés dans le code du VIRUS, de manière à ce que les programmes d'activation et de propagation rendent la main aux programmes d'interruption originaux (les opérations détournées doivent se dérouler "normalement")

Une fois l'installation terminée, le programme donne la main à son programme hôte, comme le ferait un VER. L'utilisateur n'a rien vu.

La figure 3b montre l'état des vecteurs d'interruption après l'installation du VIRUS.

Figure 3a

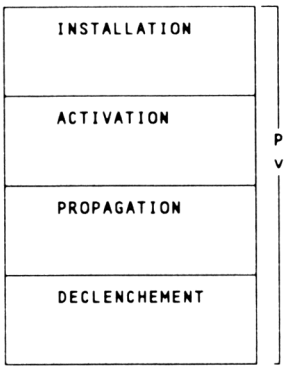
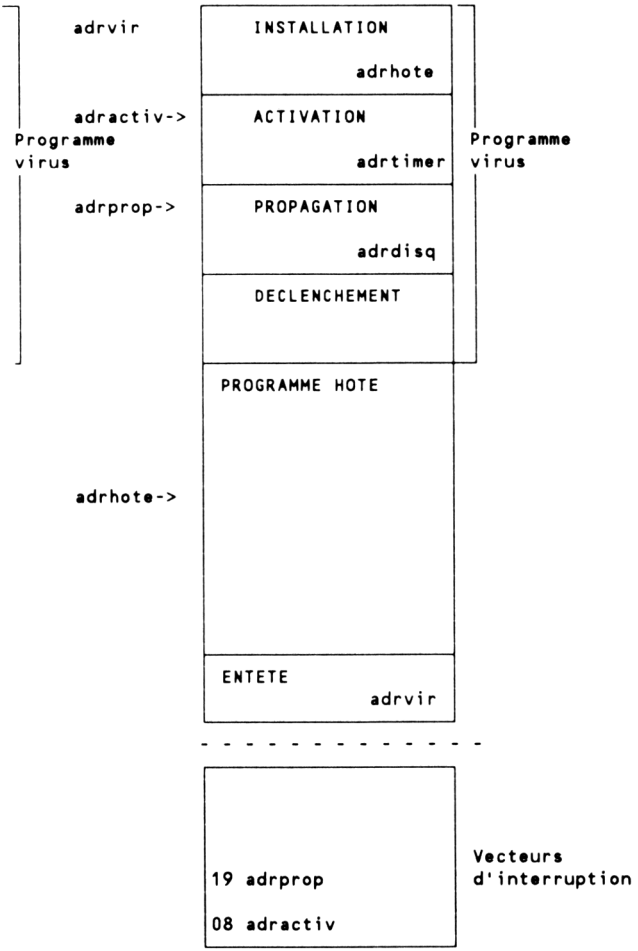


Figure 3b



C. Activation

C'est la partie la plus courte du programme VIRUS. Son travail est de répondre à la question suivante : est-il temps de se déclencher ? Par exemple : sommes nous le Vendredi 13 ? ou bien : suis-je installé depuis suffisamment longtemps dans cette machine ? Dans le cas d'une réponse

positive, le programme d'activation passe la main au programme de déclenchement.

Dans mon exemple, le programme d'activation est exécuté à chaque "clic" du TIMER, ce qui permet au VIRUS d'être activé de manière régulière. Il aurait aussi bien pu être "branché" sur l'interruption clavier (n'ayant pas beaucoup de choses à faire, le ralentissement produit n'est pas perceptible). Le programme d'installation ayant conservé l'adresse originale du programme d'interruption "détourné", le programme d'activation passe la main à celui-ci à la fin de son exécution (l'activité du virus doit être indécelable !).

D. Propagation

C'est la partie la plus importante du VIRUS, et qui le différencie du VER. Elle assure la fonction de "reproduction" du VIRUS. Sa tâche est de transférer le VIRUS sur un autre support que celui qui a permis son installation. Son activité devant être indécelable, on trouvera souvent ce sous-programme "branché" sur le programme d'écriture-lecture disque (vecteur de l'INT 19) comme dans la figure 3b. En effet, à chaque appel disque, ce programme est activé, la lampe-témoin de l'activité du disque s'allume, l'utilisateur ne s'aperçoit pas que son innocente commande DOS (DIR A: par exemple) a permis au VIRUS de se reproduire.

Ce programme n'est que l'automatisation de l'installation d'un VER décrite plus haut. Selon l'imagination du programmeur, on trouve dans cette partie une ou plusieurs méthodes de reproduction. C'est la méthode de reproduction qui caractérise les VIRUS. Ils peuvent s'installer à la place, ou en plus d'un programme exécutable. S'installer dans un fichier de données serait suicidaire, puisque cela donnerait l'alarme à l'utilisateur (données erronées) et qu'un fichier de données ne contient pas de code exécutable.

Une fois la reproduction terminée, ce programme passe la main au programme original de traitement de l'interruption (dont l'adresse a été soigneusement conservée), car l'utilisateur doit obtenir le résultat de sa commande.

E. Déclenchement

C'est là que l'on trouve les qualités destructrices des virus. Ce sous-programme est appelé par le programme d'activation lorsque

certaines conditions sont réunies. Les effets sont divers et plus ou moins méchants. Les plus sympathiques sont ceux qui vous écrivent un message (quelquefois comique, ou bien demandant de légaliser la Marijuana), qui font de la musique ou des bruits bizarres. Un effet un peu moins agréable est l'apparition inopinée d'une balle ricochant sur les bords de l'écran, le ralentissement outrancier de l'activité de votre PC favori, l'augmentation exubérante de la taille des fichiers ou l'installation d'une quantité invraisemblable de (faux) secteurs défectueux. De plus en plus désagréable, la destruction de la piste 0 du disque dur (par lectures-écritures exagérément répétées), le cryptage des fichiers de données (illisibles le jour où le virus s'auto-détruit) etc..

Voyons maintenant les deux formes principales de VIRUS (selon leur mode de transmission).

V. LES VIRUS "PROGRAMME"

Ils s'installent dans les fichiers COM ou EXE (ou les deux), selon le schéma de la figure 3b. Leur programme de reproduction répond à l'algorithme suivant :

- choisir le programme à infecter
- se recopier à la fin du programme
- changer l'adresse de lancement
- conserver l'adresse de lancement originale

exemple : Jerusalem

Ils peuvent en plus vérifier si le programme choisi contient déjà une "souche" du VIRUS, pour éviter de le contaminer une seconde fois.

Un cas particulier : Jerusalem.

Ce VIRUS (lorsqu'il est résident), s'installe dans les fichiers exécutables de type EXE au moment où on les exécute. De plus, comme il ne vérifie pas si le programme en question est déjà contaminé, on peut trouver plusieurs fois le code du VIRUS dans le même programme ! Ce qui signifie qu'au lancement du programme infecté, vous installez résidents autant de VIRUS que le nombre de fois où il est reproduit. Chacun s'installe en conservant l'adresse du suivant, le dernier rendant la main aux interruptions originales. Imaginez le temps perdu à chaque

appel du TIMER ! (c'est pourquoi certains disent que son effet est de ralentir la machine, alors qu'il ne s'agit que d'un effet induit).

VI. LES VIRUS "BOOT"

Pour pouvoir s'installer en mémoire, un VIRUS doit donc se cacher dans un programme exécutable. Rien ne garantit pourtant que le programme infecté sera exécuté fréquement, c'est pour cela que le virus LEHIGH, un des premiers VIRUS connus, s'installait dans le fichier COMMAND.COM, garantissant ainsi une installation à chaque mise sous tension. Le traitement en est relativement simple : démarrer avec une disquette DOS saine et recopier un COMMAND.COM original.

Il existe cependant un autre programme qui est exécuté à la mise sous tension, et qui est présent sur tout support magnétique (disque ou disquette) : le programme BOOT. Il peut être bon de rappeler l'organisation des supports pour bien comprendre la suite.

A. Structure disquette

Une disquette (360 Ko) est constituée de deux faces (0 et 1), quarante pistes (0 à 39), chaque piste contenant 9 secteurs (1 à 9) de 512 octets chacun. Par commodité, le DOS numérote ses secteurs de manière consécutive, de 0 à 719. On obtient donc la table de correspondance suivante :

Face	Secteurs physiques	Secteurs Logiques
0	1 à 9	0 à 8
1	1 à 9	9 à 17
0	1 à 9	18 à 26

etc..

Les disquettes de capacité plus importante possèdent un nombre de secteurs et de pistes plus importants mais la numérotation logique est effectuée de manière similaire.

Certains de ces secteurs sont réservés :

0 : BOOT
1 à 4 : FAT (File Allocation Table)
5 à 12 : Directory (répertoire principal)

Le BOOT est un bloc de 512 octets contenant deux types d'information :

- une table décrivant le support (nombre de faces, pistes, nombre de secteurs réservés,...)
- un programme (lu et exécuté par le BIOS à la mise en service) qui détecte la présence (ou l'absence) des fichiers système (IO.SYS et MSDOS.SYS), les charge et les exécute. S'ils ne sont pas présents, on obtient un message du genre :

  Disque non-système ou erreur disque

  Changez-le et appuyez sur une touche.

La table d'allocation est un descriptif pour chaque granule (groupe de secteurs) qui indique si le groupe est libre, occupé ou défectueux.

Le directory contient la liste des fichiers, leur date et heure de création, longueur etc..

B. Implantation d'un "BOOT VIRUS"

Le secteur logique 0 d'une disquette (ou d'un disque dur) est donc l'endroit le plus approprié pour l'installation d'un VIRUS. Les 512 octets du premier secteur n'étant pas toujours suffisants pour contenir le code complet du VIRUS, il faudra écrire la suite dans un endroit que l'utilisateur ne pourra pas déceler aisément (sans créer de fichier supplémentaire, ce qui donnerait l'alerte immédiatement). L'astuce consiste à utiliser un groupe qui sera ensuite marqué comme défectueux (le DOS ne l'utilisera pour aucune écriture) ou une piste jamais utilisée (la piste 40 d'une disquette par exemple). De plus, pour que l'implantation du VIRUS soit invisible, il faudra (après l'installation) redonner la main au programme BOOT original que l'on aura pris soin de réécrire lui aussi, à l'abri.

Le mode de reproduction répond à l'algorithme suivant :

- lire le secteur logique 0 (BOOT original)
- écrire le début du code dans le boot (secteur 0)
- puis la suite du code dans le premier secteur libre
- réécrire le secteur boot original (à la suite)
- marquer les secteurs utilisés comme défectueux

Exemple : PING-PONG

Il est possible de visualiser ce secteur avec DEBUG, PCTOOLS, NORTON. Si les messages d'erreur habituels ont disparu ou sont remplacés par d'autres, méfiance.

C. Les VIRUS "PARTITION".

Le VIRUS cité en exemple (Ping-Pong) s'installe sur toutes les partitions d'un disque dur. Chaque partition étant vue comme un disque et possédant la structure BOOT, FAT, DIRECTORY. On peut partitionner un disque pour deux raisons. Premièrement, pour utiliser deux systèmes d'exploitation différents (DOS et UNIX, DOS et PROLOG, DOS et NOVELL, et, pourquoi pas DOS primaire ET DOS étendu !), deuxièmement pour répartir les applications par genre, ou bien ranger les applications sur une partition et les fichiers sur une autre (accès plus rapide, usure uniforme du disque). Pour que le système s'y retrouve, il faut avoir décrit quelque part le nombre de cylindres utilisés par chaque partition et l'endroit où elle commence (il faut pouvoir charger le secteur BOOT de chaque système d'exploitation). Ensuite il faut aussi déterminer sur quelle partition le système d'exploitation sera chargé. Ces deux fonctions sont assurées par une table (appelée table de partition). La lecture de ces informations est assurée par un programme, couramment appelé MASTER BOOT. Ce programme, ainsi que la table, se trouvent sous la tête 0, piste 0, et occupent une piste complète. Ce programme est lu par le BIOS, exécuté, et c'est lui qui lancera le BOOT de la partition active.

Cet endroit est un refuge privilégié pour certains VIRUS (STONE par exemple), plus difficiles à détecter car cette zone ne peut être décrite par un numéro de secteur logique.

VII. PROTECTION

Il n'y a pas de protection universelle contre les VIRUS. La meilleure protection est une grande méfiance. Il faut être très soupçonneux, toute disquette provenant de l'extérieur sera déclarée suspecte. Mon travail de formateur m'amenant à visiter de nombreux établissements scolaires, j'examine à mon retour toutes les disquettes utilisées pendant la formation. Avant de commencer une formation, je passe toutes les machines à l'antivirus. Ce doit être une pratique courante du responsable informatique.

Certains VIRUS sont faciles à détecter, Ping-Pong par exemple. Jerusalem, installé dans le programme WORKS, empêche son fonctionnement (on reçoit le message : impossible d'exécuter WORKS). La plupart restent indécelables jusqu'au jour où ils se déclenchent, et peuvent polluer toutes les disquettes qui passent à leur portée pendant ce temps. Le vieux proverbe est donc plus que jamais d'actualité : il vaut mieux prévenir que guérir. C'est par une prévention efficace que les VIRUS disparaîtront.

La rumeur populaire cite des cas d'infection par connexion d'ordinateurs à un serveur. La seule manière de "contracter" un VIRUS est de télécharger un programme et de l'exécuter sur la machine réceptrice. La simple connexion à une messagerie ne peut en aucun cas transmettre un VIRUS.

De même, la copie d'un fichier de données (texte ou autre), la consultation d'un répertoire, la copie d'une disquette contenant un VIRUS ne transmettent pas de VIRUS.

Les VIRUS "programme" s'installent en lançant le programme infecté et les VIRUS "BOOT" en démarrant la machine avec une disquette dans le lecteur, porte fermée. Ce sont les deux seules méthodes de contamination possibles.

Il existe des logiciels de protection, qui empêchent l'écriture sur certaines zones de disque définies par l'utilisateur (au détriment des performances de la machine). D'autres détectent les tentatives d'installation de VIRUS connus (l'utilisateur est obligé de suivre les mises à jour régulières).

VIII. DÉTECTION ET TRAITEMENT

A. Détection

On peut détecter la présence de VIRUS "à la main". Pour les VIRUS de type BOOT, en lisant le secteur BOOT avec DEBUG ou un utilitaire approprié (avec un peu d'habitude, on reconnaît facilement PING-PONG et STONE de cette manière). Pour les VIRUS de type PROGRAMME, on peut contrôler la longueur des fichiers programme (en éditant périodiquement sur imprimante les répertoires des supports, ou en comparant la longueur d'un programme suspect avec un original sans défaut). Ces méthodes rustiques ne peuvent être utilisées que ponctuellement, et les éditeurs de logiciels ayant flairé un marché

lucratif, on trouve actuellement une grande quantité de logiciels "antivirus" aux performances diverses (un VIRUS détecté et détruit par un antivirus ne le sera pas nécessairement par un autre).

Chaque VIRUS est constitué d'une suite d'instructions bien précises. En choisissant un nombre d'instructions suffisamment grand, une suite d'octets donnés caractérise un VIRUS (on a peu de chances de retrouver la même suite dans un autre programme, mais il existe tout de même une probabilité non nulle). Cette suite d'octets (choisie par le programmeur d'antivirus a été nommée "signature" du VIRUS. L'antivirus recherche dans les secteurs de démarrage et dans les fichiers exécutables toutes les signatures des VIRUS qu'il connaît. Si le test est positif, il déclenchera une procédure de traitement appropriée, si cela est prévu.

B. Traitement

Les méthodes d'implantation des VIRUS étant restreintes (puisque liées au fonctionnement du système) il suffit à l'antivirus de retrouver les paramètres originaux (soigneusement conservés par le VIRUS) et de les rétablir en annulant le lancement systématique du programme parasite. Une autre solution, plus destructrice mais aussi efficace, est d'effacer le fichier contaminé ou de reformater le support (c'est quelquefois la seule solution).

Dans tous les cas, il faut avoir caché (dans un endroit connu de vous seul) une disquette DOS "propre". Utiliser les originaux ou faites en une copie qui sera **protégée** (vous pourrez en profiter pour faire une copie de vos fichiers AUTOEXEC.BAT et CONFIG.SYS si longuement élaborés). Redémarrez le système avec cette disquette saine et ensuite lancez le logiciel antivirus (lui aussi sur une disquette protégée).

Vous pouvez lancer un logiciel antivirus de votre disque dur (au risque de polluer ce programme) pendant que le virus est actif, mais rien ne vous assure que le virus détruit ne se réinstallera pas aussitôt.

C. L'avenir

L'éradication d'un VIRUS connu ne pose pas de problème technique insurmontable, le point délicat est la phase d'identification. Pour produire des antivirus efficaces, il faut détecter les nouveaux VIRUS. Il existe un réseau d'utilisateurs (appuyé principalement sur les

messageries et les revues spécialisées en informatique individuelle) où circulent les informations sur les VIRUS.

Les logiciels deviennent de plus en plus performants, il y a de fortes (mal)chances pour que les VIRUS suivent la même voie. Les programmeurs de VIRUS vont donc maintenant essayer d'échapper à la détection.

Les auteurs de VIRUS ont déjà mis en oeuvre des camouflages efficaces : le changement de signature et le rétablissement temporaire des données erronées, par exemple.

Pour empêcher la détection de signature, on découpe le programme en petites procédures courtes (une dizaine d'octets), puis un programme qui appelle ces procédures. Il suffira d'arranger les sous programmes de manière aléatoire à chaque reproduction pour déjouer le détecteur de VIRUS, qui devra utiliser des signatures très courtes (avec des risques de confusion avec du code inoffensif) ou changer sa méthode de détection. Un des premiers VIRUS "camouflés" est EDV (ou CURSY), qui se reproduit par le BOOT, mais rétablit le secteur original dès qu'on essaie de le lire ! (la routine de camouflage est constituée d'une trentaine d'octets).

Les algorithmes de compactage sont de plus en plus connus, et seront donc utilisés pour masquer leur présence. En compactant une partie du programme avec son propre code, la taille du fichier infecté ne changera pas. Un VIRUS pourra même changer d'algorithme à chaque installation, changeant donc sa signature.

Le moins qu'on puisse dire est que l'avenir n'est pas rose. Les programmes "boucliers" ne sont pas infaillibles, les plus sûrs sont ceux qui détectent les tentatives d'installation. Certaines sociétés (encore alléchées par un marché à saisir) proposent une "maintenance antivirus". Un bouclier est installé sur la machine, subit des mises à jour régulières, et l'on vous garantit qu'en cas d'attaque par un VIRUS inconnu, vous serez dépanné dans les 72 heures ! Que d'énergie et de matière grise dépensés !

Je pense qu'il faudra malheureusement en passer par là, surtout en milieu scolaire où le nombre d'utilisateurs important (par rapport au nombre de postes) et l'utilisation en libre service favorisent la circulation des disquettes et l'implantation des VIRUS.

IX. LES ANTIVIRUS.

Il existe une grande quantité d'antivirus sur le marché, quasiment toutes les éditeurs de ce genre de produit proposent des mises à jour régulières.

FLUSHOT+ (Software Concepts Design)

Bouclier. Contrôle les tentatives d'intrusion et l'intégrité des fichiers définis par l'utilisateur. Disponible sous le nom de BIOSOFT (100F) chez Soft & Micro (15 avenue d'Eylau 75016 PARIS).

V-ANALYST

Détecte et supprime une centaine de virus parmi les plus courants (Ping-Pong, Jerusalem, ..). Disponible chez Infodidact (5 bis rue du Louvre 75001 PARIS ou CAMIF).

VIRUSCAN (McAfee Associates)

La version 75 détecte (et supprime) actuellement plus de 200 virus répertoriés. Disponible sur les serveurs. Constitué de deux programmes SCAN (détection) et CLEAN (éradication). Contient également deux autres programme: NETSCAN, qui permet d'examiner tous les lecteurs d'un réseau, et VSHIELD qui empêche l'installation des virus qu'il détecte. Gratuit pour une utilisation personnelle, la disquette contient une licence à renvoyer dans le cas d'une utilisation professionnelle.

Jean-Michel COSTE
Formateur MAFPEN-Créteil

BIBLIOGRAPHIE

Science & Vie Micro n°66 (novembre 1989)
- L'affaire des virus

La Revue de l'Utilisateur de l'IBM PC

- N°64 (septembre 1990) A Propos de Ping-pong.
- N°66 (novembre 1990) A propos de Jerusalem.
- N°70 (mai 91) Les virus partition.

VIRUS PROTECTION

Pamela KANE (éditions SYBEX). Ce livre est accompagné d'une disquette contenant quelques utilitaires (utilitaires du Dr PANDA).

LA PESTE INFORMATIQUE

Alain ACCO et Edmond ZUCCHELLI (éditions CALMANN-LEVY)

RAPPEL DE QUELQUES CONSEILS

Ne pas utiliser de programmes et de disquettes "douteux". Est suspect a priori tout ce qui vient de l'extérieur. (au besoin, montrer aux élèves l'utilisation d'un programme antivirus).

Ne jamais démarrer une machine avec une disquette dans le lecteur (c'est le mode de transmission des "BOOT virus").

Dans le cas d'une infection, après avoir décontaminé la machine, décontaminer TOUTES les disquettes susceptibles d'être passées sur cette machine.

Dans le cas de non-fonctionnement ou de fonctionnement douteux d'un logiciel, ne pas procéder à la réinstallation avant d'être sûr qu'un virus n'en est pas la cause.

Protéger les originaux (empêcher l'écriture).

Conserver en permanence une disquette système saine et protégée qui servira à redémarrer la machine avant une désinfection.

Procéder à des contrôles réguliers.

Ne pas accuser systématiquement les virus, un mauvais fonctionnement est souvent le fait d'une mauvaise utilisation.