LES « VIRUS » ET QUELQUES PRÉCAUTIONS À PRENDRE...

A. TABLE DES MATIÈRES

B. QUELQUES DÉFINITIONS

1. un virus est un programme informatique :

1. c'est en général un "***morceau de code***" écrit souvent en **code binaire** ou en **assembleur** pour assurer une petite taille, dissimulé
   - dans un fichier exécutable
   - ou le plus souvent dans les secteurs de démarrage
   - ou dans les secteurs de partition
   - ou dans les macro-instructions des applications bureautiques...
2. il est difficile à déceler, notamment
   - car il se niche souvent au coeur d'un autre programme, dans des places vacantes
   - ou parce qu'il reprend le même nom que d'autres programmes
   - ou parce qu'il est « ***furtif*** » (***stealth***) : capable de s'adapter et de se camoufler, capable de repérer une attaque anti-virus et d'y remédier...

- ou parce qu'il est « ***crypté*** » : sa signature n'apparaît pas en clair
- ou « ***polymorphe*** » : un moteur de mutation procède à des cryptages différents et aléatoires

3. son apparition est souvent aléatoire, ou différée : c'est surtout le cas des « ***virus latents »*** qui n'apparaissent qu'à une certaine date ou après la n^{ième} manipulation d'un programme ou d'une instruction...
4. sa manifestation est très diversifiée donc pas facilement identifiable :
   - apparition de logos, dessins, messages, sons... insolites,
   - impossibilité de « ***booter*** » (démarrer) un disque, qui s'est notamment rempli de secteurs défectueux (les « ***virus de boot*** » sont très répandus),
   - modifications de logiciels ou d'instructions... Par exemple, modification fréquente de la date.
   - ou même modification des éléments matériels (disque, électronique, normes vidéo...)
   - voire parfois destruction du **BIOS** si celui-ci est en mémoire flash (ce qui de plus en plus fréquent en 1999)
   - ralentissement du système, des logiciels...
   - et parfois il entraîne la destruction des fichiers de données...

==> Définition de **Pamela KANE** : « ***Vital Information Resources Under Siege »***, c'est à dire programme menaçant les ressources d'information vitale

==> D'une manière générale le terme VIRUS est utilisé pour désigner **tout programme malveillant**

2. ce programme a la capacité de s'auto-reproduire :

On parle souvent de logiciel **auto-modifiant** ou **auto-reproducteur.**

==> sa capacité de « ***muter*** » lors de sa « ***reproduction*** » limite encore la possibilité de l'identifier.

3. son auteur est un informaticien ou un programmeur amateur :

a) souvent appelé "***hacker***" :
   - ce nom désignait au départ (années 70) d'habiles programmeurs ou « ***bidouilleurs »*** du **TMRC** (**Tech Model Railroad Club**) du **MIT** ; le terme était alors assez souvent élogieux,
   - aujourd'hui terme péjoratif, souvent synonyme de « ***fraudeur »*** ou de « ***pirate ».***

b) le ***cracker*** désigne plutôt celui qui s'introduit frauduleusement dans un système.

C. QUELQUES TYPES DE VIRUS...

1. le "*virus*" proprement dit :

programme qui introduit « ***des copies exécutables de lui-même dans d'autres programmes »*** qui ne sont pas encore ***infectés*** (c'est à dire ne comportant pas ***l'empreinte*** du virus)

1. un ***virus dit bénin*** ne ferait que se reproduire sans dommage (immédiat en tout cas ?).
2. un ***virus résident*** se place en mémoire vive.
3. un ***virus furtif*** utilise une partie de son code pour échapper aux diverses détections :
   - en détournant les interruptions du DOS,
   - en changeant de signature à chaque propagation : ***virus polymorphe***,
   - par mutation de son code : ***virus polymorphe*** également,
   - en contournant les antivirus lancés à sa poursuite et en jouant lui même le rôle de l'antivirus en contrôlant toute modification des registres qui le menaceraient... = ***virus tunnel***
4. un ***rétrovirus*** est un virus s'en prenant directement aux outils de surveillance des antivirus

2. le « *ver* » :

c'est un programme qui se reproduit très vite dans n'importe quelle zone du système informatique. À l'inverse du virus, il n'a pas besoin d'un programme hôte spécifique et n'est pas forcément destructeur. un « ***virus ver »*** se reproduit comme tout virus, puis attend le déclic avant de s'exécuter.

3. le « *virus ou bombe logique* » :

programme qui détruit complètement (ou tout simplement renomme) d'autres programmes ; en général, il ne se reproduit pas.
il se développe souvent de manière aléatoire et presque toujours différée (selon une date, une donnée ou une absence de donnée particulière...).

4. le « *cheval de Troie* » :

c'est un **programme exécutable** ou une **DLL** (fichier catalogue) dissimulant sa fonction destructrice.
le programme « ***tueur »*** s'active en profitant du lancement d'une application-hôte qui détourne momentanément l'attention (jeu ou utilitaire, souvent ***freeware*** ou ***shareware***) ; il est souvent porté par un virus qui le lance lors de sa duplication...
il a le plus souvent une action destructrice immédiate mais il se reproduit rarement, ce n'est donc pas un virus au sens propre.
Actuellement de nombreux **chevaux de Troie** ne seraient que des « ***espions*** » dissimulés dans des ordinateurs, pas des programmes destructeurs. Le développement d'Internet accentue cette fonction (Cf. **Partie I.E**.), notamment dans les ***chats*** (discussions en direct). L'objectif principal est de récupérer des données confidentielles et essentielles (Nom, Mot de passe, code bancaire...) dans l'ordinateur cible.
le "***virus de Troie***" quant à lui se détruit après s'être reproduit n fois et la plupart du temps après avoir eu une action néfaste.

5. le macrovirus :

Depuis le milieu des années 90, les virus se nichent le plus souvent dans les macro-commandes des applications bureautiques surtout celles d'**Office** (**Word**, **Excel**...). Leur transmission se fait donc dans des documents, pas dans des programmes, ce qui les rend plus dangereux car en général on ne contrôle que les fichiers exécutables !

Ces virus sont en fait des instructions parasites ou destructrices, écrits dans le macro-langage utilisé dans l'application qu'ils parasitent.

D. QUELQUES EXEMPLES « HISTORIQUES » DE « VRAIS » VIRUS...

DATE	NOM et AUTEUR	REMARQUES
1970	**CREEPER de Bob THOMAS**	· sur réseau **ARPANET** (ancêtre d'Internet)
1970	**REAPER**	· anti-**CREEPER**
1974	**RABBIT**	· s'introduit dans le SED **ASP** d'IBM
	ANIMAL	· virus dans un jeu sur **UNIVAC**
1980	**ARPANET REDUX**	· blocage du système **ARPANET**
1981	**ELK CLONER**	· sur **APPLE II**
1982	**virus dans le jeu CONGO**	· sur **DOS 3.3 - APPLE II**
1985	**virus BURLESON**	· contamine la société **USPA**
1985	**EGABTR**	· 1° virus sur **PC** (***un cheval de Troie***)
	SURPRISE	· destruction des fichiers du répertoire courant
	FILER, SEEFREE...	· faux logiciels utilitaires...
1987	**LEHIGH**	· à l'Université **Lehigh,** infectant **COMMAND.COM**
1987	**C(BRAIN)=PAKISTANAIS**	· apparu à l'Université du **Delaware**
1987	**PLO ou VENDREDI 13**	· apparu à l'Université de **Jerusalem**
1987	**CHRISMAS.EXE**	· sur logiciel **PROF's d'IBM**
...		
vers 97	**CAP**	· macrovirus dans les fichiers WORD !

199 8	**BACK ORIFICE**	· Cheval de Troie adapté à Internet

l'inflation !
- 1988 : environ 50 virus recensés
- 1990 : près de 250
- 1992 : près de 1000, avec une dizaine de nouvelles souches par mois !

E. QUELLES PROTECTIONS OU PRÉVENTIONS POSSIBLES CONTRE LES VIRUS ?

1. acheter exclusivement des logiciels originaux :

mais même les grandes firmes ne sont pas à l'abri d'un ancien employé qui cherche à se venger
même acheté en magasin, on n'est sûr de rien : Cf. l'histoire rocambolesque du **Pakistanais Brain**, virus présent sur des copies à bas prix de grands logiciels vendus en toute légalité au **Pakistan**, pour punir ces pingres d'acquéreurs occidentaux !

2. activer la surveillance du BIOS

Dans le **BIOS**, rendre active (***Enabled***) la fonction de contrôle (**Virus Warning**) en général située dans **Bios Features Setup** du **SETUP**.

3. éviter de démarrer à partir d'une disquette

il faut démarrer systématiquement depuis le disque dur. Il peut être alors prudent dans le **SETUP** d'obliger l'ordinateur à démarrer en C: au lieu de A: (Option **Boot Sequence** de **Bios Features Setup**).
sinon démarrer avec un DOS original ou une disquette système **protégée en écriture !**

4. contrôler toute nouvelle disquette :

1. s'assurer de son origine : ne pas ***lancer*** un programme non testé ou sûr.
2. se méfier particulièrement :
   - des logiciels trop attractifs, notamment érotiques, ils sont parfois ***piégés,***
   - des jeux d'origine incertaine,
   - des logiciels de recopie : l'antique ***Copywrite*** serait à l'origine du Virus du **Vendredi 13** ?
   - des logiciels utilitaires d'origine inconnue,
   - des logiciels trop bon marché : Cf. le **Pakistanais** sur des premières versions de **Lotus 123**
3. utiliser les "***antivirus***" ou logiciels de détection, mais il faut des versions récentes, sinon la recherche de "***signature***" est parfois inopérante pour :
   - des virus furtifs,
   - des fichiers compactés type .**ARC** ou .**ZIP,**
   - des virus nouveaux ou ***mutants***, donc non encore identifiés...

   Rappel : **ces soins ne servent souvent à rien si le virus est déjà présent**, surtout dans le cas de « ***virus dormant ou latent »*** qui ne se déclare que longtemps après...
4. si possible comparer
   - la disquette nouvelle ou le logiciel qu'elle contient,
   - avec une disquette sure qui sert "***d'étalon***", de référence.

5. utiliser le moins possible le téléchargement ou les fichiers joints:

le ***téléchargeur*** (logiciel **FTP** notamment) en lui-même n'est pas dangereux, mais le logiciel ou fichier qu'il fournit peut contenir un virus, actif seulement au moment où on exécute le programme.
choisir autant que possible des sites de téléchargement officiels, connus...
pour les fichiers joints dans le **courrier électronique**, il faut adopter la même prudence : certaines listes pour des raisons de sécurité refusent systématiquement les fichiers joints.
Si le courrier électronique classique est en lui-même sans danger, les courriers en **html** peuvent être source de contamination car ils contiennent des principes actifs (**javascript**...)
Utiliser éventuellement **Netstat** (utilitaire **Windows**) pour contrôler les transferts.

6. protéger physiquement les disquettes :

MALHEUREUSEMENT des programmes exigent l'accès libre à la disquette pour y écrire des fichiers temporaires, ou pour y reconnaître la marque de l'original (disquettes dites « ***Clé*** »), ou pour procéder à une initialisation ou personnalisation du produit.

7. protéger les fichiers :

RAPPEL : **seuls les fichiers exécutables** peuvent être cause de contamination, les fichiers de données, même infectés, ne peuvent pas être une source directe de contamination.
Quelques méthodes assez simples :
1- ajouter les attributs « ***caché »*** et « ***lecture seule »*** à ses fichiers : par exemple en utilisant la commande DOS **ATTRIB** de la manière suivante : **ATTRIB+R *.COM/S** qui n'autorise dans ce cas que la lecture des fichiers **COM** dans tous les répertoires...
2- utiliser des mots de passe dans des fichiers ***batch*** (commande **SET** du **DOS**),
3- créer des répertoires difficilement reconnus : par exemple en utilisant des caractères « ***invisibles »*** comme **le Alt 255** dans les noms choisis pour certains répertoires (dossiers),
4. Protéger l'interpréteur de commande : par exemple le mettre dans un sous-répertoire (ex. NOUVEAU) au lieu de la racine habituelle, puis dans **CONFIG.SYS**, insérer : **SHELL C:\NOUVEAU\COMMAND.COM/P** et dans **AUTOEXEC.BAT** insérer : **SET COMSPEC=C:\NOUVEAU\COMMAND.COM**

Remarques : toutes ces démarches sont facilement découvertes et contrées avec un connaissance moyenne du système d'exploitation ou SED, ce qui rend la protection illusoire.
Mais les $^4/_5$ au moins des utilisateurs n'ont pas cette connaissance approfondie, ce qui met à l'abri de leur maladresse, ou de leur malveillance.

8. Empêcher le lancement des macro-virus : exemples avec Winword

Il y a différentes méthodes pour empêcher l'exécution de macro-commandes sous **WORD**, la principale et la plus simple étant simplement d'ajouter l'option **/m** après **winword.exe** dans le chemin du raccourci de **Word**.
Avec **Winword 97**, vérifiez que l'option **Protection contre les virus de macro** soit activée dans l'onglet **Général** de **Outils/Options.**
Vérifiez que le dossier **DÉMARRAGE** dans le dossier **Program Files\Microsoft Office\Office** ne contient pas de documents « irréguliers » ou inconnus.
Vérifiez (avec la commande **Démarrer/Rechercher**) que des fichiers ne contiennent pas la commande **MacroCopie** (**Windows 95**) ou **OrganizerCopy** (version **1997**), car elle est indispensable pour répandre ce type de virus.

9. contrôler/filtrer les accès aux ordinateurs :

1. les salles en « libre-service » seraient à limiter, contrôler plus systématiquement...
2. les ordinateurs centraux, de gestion, de trésorerie, de gros fichiers...
   - doivent être utilisés par un minimum de personnes
   - pour un minimum de tâches
   - être peu accessibles physiquement : salles fermées, codes d'accès...
3. généraliser la technique des mots de passe
   - avec le **SETUP** (possibilité de configurer son ordinateur, présente sur de nombreux systèmes)
   - utiliser tout simplement la commande **SET** du **DOS** pour entrer une variable personnelle et faire un fichier ***batch*** qui la teste afin de pouvoir utiliser les logiciels les plus courants ; celui qui connaît le **DOS** découvrira la clé, mais c'est au moins une protection vis à vis des « ***amateurs ».***
4. utiliser des logiciels spécialisés de protection d'accès...

MAIS on rentre vite dans une psychose policière dangereuse. Et si on devient paranoïaque, on ne se servira plus de son ordinateur !

10. comparer des fichiers importants avec les originaux conservés

a) les fichiers exécutables de type ***texte*** ou ***batch*** : dès leur création, en faire une copie sur papier et comparer de temps en temps avec le contenu des fichiers du disque : on peut utiliser la commande **TYPE** de MSDOS pour l'impression : exemple : **TYPE AUTOEXEC.BAT > PRN:**
b) les fichiers en langage machine (.**EXE, .COM...**) :
--> comparer ceux du disque avec les originaux sur disquette au moyen de la commande DOS : **COMP :**

exemple pour les fichiers .EXE : **COMP *.EXE a:*.EXE**
--> dès l'installation d'un nouveau programme, il est bon de conserver le catalogue des fichiers exécutables pour d'ultérieures comparaisons = exemple : **DIR *.COM > PRN:**

11. choix d'un ordinateur test :

pour les grands services, 2 possibilités peuvent permettre de contrer les virus :
*** cas 1 :** n'utiliser le nouveau programme que sur un seul ordinateur, mis volontairement en quarantaine, pour tester le logiciel.
*** cas 2 :** avancer la date et l'heure d'un ordinateur ; s'il est atteint on peut ainsi prévenir les dégâts pour les autres si le virus est lié à l'horloge interne.

12. sauvegarder régulièrement les données notamment:

1. il faudrait :
   --> tout sauvegarder,
   --> à intervalle régulier, au moins une fois par jour pour les gros utilisateurs,
   --> et si possible sur 2 supports différents.
2. exemple de rotation : « ***méthode des générations successives*** » :
   - la 1° sauvegarde est conservée sur la disquette I
   - la 2° sur la disquette II
   - la 3° sur la disquette III
   - la 4° sur la disquette I et ainsi de suite en recommençant...
   = si le virus s'est introduit entre 2 sauvegardes, ET QU'ON S'EN SOIT RENDU COMPTE, une des disquettes contient forcément des données saines...
3. Mais la sauvegarde n'est jamais sure :
   --> certains virus ne détruisent pas les données, mais les infectent; au bout d'un certain temps toutes les sauvegardes sont alors également infectées... et ne seront réutilisables qu'avec un programme spécial,
   --> une recopie suffit souvent à reproduire le virus,
   --> elle ne vaut vraiment que pour les virus destructeurs de disque. On a ainsi au moins préservé ses propres données, pas forcément les programmes : mais à la longue un programme se retrouve, rarement le temps passé à saisir ses propres documents !

F. COMMENT LES COMBATTRE ?

1. repérer des fonctionnements inhabituels ou répétitifs :

plantages répétitifs, blocage d'un périphérique...
dates des fichiers modifiées ou incongrues
lenteur étonnante d'un programme,
messages, logos, bruits... suspects ou délirants (mais **Windows** non habitue parfois au pire sans raison ! avec des messages mal traduits ou très alarmistes),
présence de fichiers inconnus,
pertes de données,
modifications dans la structure arborescente et diminution de la place mémoire disponible,
activité imprévue d'un lecteur ou autre périphérique...

2. démarche immédiate :

1. il faut arrêter immédiatement l'appareil.
2. vérifier toutes les connections, fils, prises, interfaces...
3. relancer l'ordinateur depuis le lecteur de disquette avec une **disquette système *propre*** et protégée.
4. tout contrôler,
   - la mémoire (par exemple avec la commande DOS **MEM** qui permet une bonne analyse des programmes chargés en mémoire),
   - votre disque par exemple avec l'option ***Master Boot Recovery*** : commande **FDISK /mbr** qui analyses et parfoit répare le secteur d'amorçage...
   - et vos sauvegardes...
5. utiliser un programme de détection et de « ***nettoyage*** »

3. quelques soins préalables :

Parfois le problème n'est pas viral, tenter alors ces 2 démarches :

1. les problèmes peuvent provenir d'une simple erreur dans les "***chaînages***" entre fichiers ou au sein d'un même fichier ; un utilitaire du DOS fait souvent des merveilles :
   - **CHKDSK /F**
   - ou **SCANDISK** surtout avec l'option **Type d'analyse : Minutieuse**. Il ya possibilité avec **SCANDISK** de contrôler les dates incongrues **(Options-Dates et heures non valides)**
2. les erreurs ou lenteurs peuvent provenir d'un disque saturé : utiliser un outil de **défragmentation**

4. en cas de problème persistant :

1. réinitialiser le disque avec la disquette (ou le Cédérom) programme originale.
2. formater **complètement** le disque :
   - préparation avec **FDISK**
   - utilisation de **FORMAT**
3. réinstaller les programmes seulement à partir des **originaux.**
4. Remarque : si le **BIOS** a été modifié, il faut parfois essayer de récupérer les parmètres d'usine, dans le **SETUP**, en validant l'option **Load BIOS Defaults**

G. RUMEURS ET VIRUS IMAGINAIRES... ET AUTRES CANULARS.

1. le principe :

1. un message bien construit, référencé, d'apparence rationnelle... nous informe
   - soit d'un danger de propagation virale sur Internet (le plus souvent par les services de **messagerie** - **fichiers joints** - et par tous ceux utilisant également le **téléchargement** - **FTP** surtout),
   - soit d'un message urgent, de détresse, à communiquer rapidement à d'autres personnes.
2. Le destinataire, humaniste ou apeuré, pense bien faire en communiquant rapidement ce message à d'autres personnes, sans en vérifier la véracité.
3. « ***L'intoxication*** » triomphe, le résultat est évident : il y a engorgement du réseau par des messages répétitifs dont la plupart ne sont que des canulards. L'aspect nocif a triomphé : embouteillages, ralentissement des communications, vérifications sur les mêmes sites, interventions parfois fort hargneuses des ***postmasters*** et responsables des serveurs...
4. Remarque : parfois certains internautes se demandent si toutes ces mauvaises nouvelles n'ont pas aussi pour but de nous amener à consulter certains sites spécialisés ? comme on disait autrefois que des nouveaux virus permettaient de faire vivre les sociétés produisant les logiciels antivirus...

2. deux types principaux :

1. le faux virus ou virus imaginaire : de multiples appellations sur Internet : ***hoax***, ***virus virtuel***, ***virus myth***, ***rumor***, ***urban legend***... La liste en est donnée notamment par le service de veille de la société SYMANTEC.
2. le principe traditionnel de la « ***chaîne de lettres*** » : un message de détresse ou de solidarité à transmettre. Le Ministère américain de l'énergie les traque. (Cf. Sites en annexe).

H. ANNEXES : QUELQUES RÉFÉRENCES :

1. quelques sites concernant surtout virus imaginaires et fausses nouvelles :

sur les ***légendes urbaines***...	***http://urbanlegends.miningco.com/*** ***http://www.snopes.com***
sur les ***virus myths...***	***http://www.kumite.com/myths/*** ***http://www.umich.edu/~virus-busters/hoaxes/***
Atoutmicro, revue québéquoise, listes, conseils...	***http://www.atoutmicro.ca***
HOAXBUSTER : que sont les ***hoaxes*** et comment les combattre	***http://Hoaxbuster.com***
McAFEE : liste...	***http://www.mcafee.com/support/hoax.html***
Ministère US de l'Énergie : chaînes de lettres et ***hoaxes***...	***http://ciac.llnl.gov/ciac/CIACChainLetters.html*** ***http://ciac.llnl.gov/ciac/CIACHoaxes.html***
SYMANTEC : liste, conseils...	***http://www.symantec.com/avcenter/hoax.html***
YAHOO	***http://www.yahoo.com/Society_and_Culture/Mythology_and_Folklore/Uraban_Legends/Computer_Viruses***

2. quelques sites sur les virus en général

AVP - services et encyclopédie des virus	***http://www.avp.com***
Computer Virus information -F-SECURE	***http://www.europe.datafellows.com/vir-info***
Encyclopédies des virus...	***http://www.antivirus.com*** ***http://www.attac.net/techvirfl.html*** ***http://www.avpve.ru/avp_ve.eng/index.htm***
McAFEE avec contrôle en ligne de votre disque dur !	***http://www.mcafee.com***
NETWORK ASSOCIATES	***http://www.nai.com/virinfo***
SYMANTEC : général et bouclier contre attaques virales	***http://www.symantec.com/region/fr/*** ***http://www.symantec.com/region/fr/press/n970117.fr.html***
WORDinfo-WEBindex	***http://www.wordinfo.com/links/macvirus.htm***

Michel ANTONY- Michel.Antony@ac-besancon.fr - Mise à jour le 08/09/2000