Sécurité

Édition au 18-nov.-16 ATTENTION CETTE VERSION EST EN TRAVAUX et la mise à jour est limitée

L'emploi de l'ordinateur facilite considérablement le travail du biologiste mais sans précautions élémentaires devient un enfer. Les données doivent en effet impérativement être « sécurisées » contre la perte d'une part, les attaques virales d'autre part.

Enregistrement et sauvegardes

Ne pas oublier d'abord qu'une **panne de courant** anéantit tout travail non enregistré… Des enregistrements périodiques, parfois proposés par certains logiciels, s'imposent donc. Il faut pourtant prendre garde à ne pas éliminer des versions anciennes pouvant contenir des données intéressantes… ce que l'on évite en enregistrant le fichier sous un autre nom. La gestion des différents fichiers doit être rigoureuse : il faut aussi éliminer pour pouvoir se retrouver dans les différentes versions.

Mais le support d'enregistrement est exposé à la destruction physique (disquette écrasée, démagnétisée, disque dur en panne, attaque par cryptage des données contre rançon…), la perte ou le vol… **Il faut donc absolument avoir des sauvegardes récentes de vos fichiers importants c'est à dire des copies réalisées sur un autre support.** On peut par exemple conseiller :

- De garder le fichier maître sur disque dur.
- D'effectuer des copies sur clés USB et/ou disques externes (éventuellement conservées dans des lieux différents).
- D'effectuer des copies sur un serveur informatique… le nuage ! (*cloud*). Des services gratuits ou payants le permettent comme *Dropbox*, Owncloud… On ne peut malheureusement pas exclure un piratage des données sur les serveurs distants ou durant le transfert.

Des logiciels appropriés se chargent de copie totale (*back up*) du disque dur, certains permettant de plus de n'effectuer que les copies des derniers fichiers modifiés sur une précédente sauvegarde (*back up*).

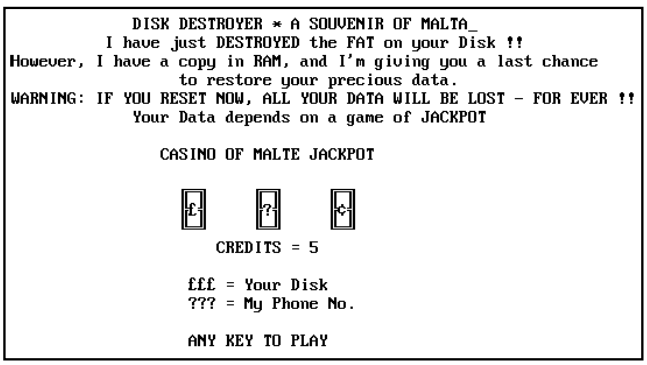
En cas d'incident, y compris une mise à la corbeille intempestive suivi d'un vidage de la corbeille, il reste encore possible de récupérer les données : il convient de trouver un spécialiste et de n'effectuer aucune opération disque avant son intervention. Des utilitaires de réparation se chargent de la récupération des données d'un disque dur ou d'une clé.

Pour des données très sensibles, un cryptage peut permettre une protection contre une lecture non autorisée.

Virus informatiques et autres logiciels malveillants (*malwares*)

Jeux d'ingénieurs consistant à créer des programmes capables de détruire les programmes adverses dans les années 1960, les virus sont devenus un véritable fléau, la contamination s'étant multipliée au rythme du développement de la micro-informatique. Pas moins de plusieurs dizaines de milliers de variétés de virus sont à l'affût pour infester les machines, affichant des messages tour à tour farfelus, inquiétants, jouant de la musique tel *Berlioz* exécutant les premières mesures de la *marche funèbre*, diminuant les performances des machines, ou pire, détruisant irréversiblement des données du disque dur.

Un exemple d'exécution :



Ces logiciels malveillants ne sont que des programmes informatiques. L'analogie avec les virus biologiques permet de disposer d'un vocabulaire porteur d'images fortes, mais l'analogie s'arrête là.

Actions des logiciels malveillants

Les actions possibles des logiciels malveillants peuvent être nombreuses :

- Transmission par tout support numérique, avec ou non autoreproduction.
- Affichage d'un message…
- Formatage du disque dur.
- Destruction de données.
- Transmission de données vers un ordinateur extérieur. On parle alors souvent de logiciel espion ou **espiogiciel** (spyware).
- Ouverture d'une porte dérobée (ouverture d'un port fermé – voir réseaux)

- Attaque d'un site web par saturation (*Denial of service*) quand un ensemble important d'ordinateurs se connectent simultanément.
- …

Ces actions peuvent être déclenchées en fonction de paramètres comme la date…

Un exemple célèbre est l'action de virus pour déséquilibrer les centrifugeuses permettant l'enrichissement de l'uranium en Iran…

Logiciels malveillants non autoreproducteurs

Les deux premiers types de logiciels malveillants, bombe logique et cheval de Troie, ne se diffusent que si quelqu'un décide de les recopier ou de les télécharger à partir d'un serveur

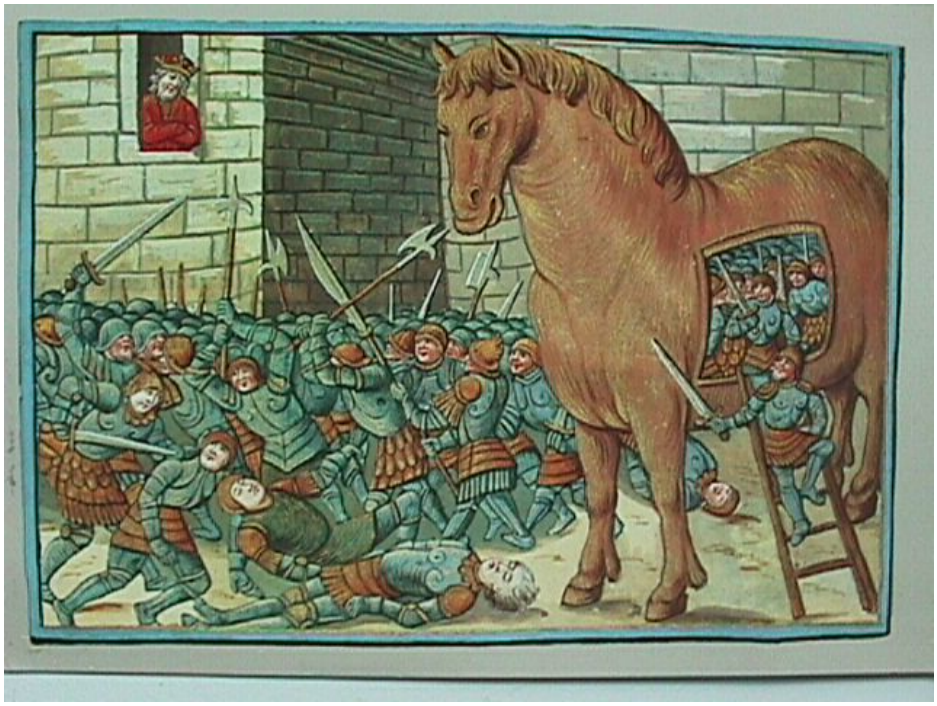
Bombe logique (logic bomb)

Une bombe logique est constituée d'une simple fonction destructrice au sein d'un programme d'intérêt général, la fonction ne s'exécutant que lors d'un événement particulier (déclenchement différé). On cite le cas d'un programme de paie au sein duquel un programmeur avait placé une bombe logique qui ne se déclenchait que si son nom était supprimé du fichier du personnel, entraînant la destruction des données sur les disques durs.

Ces bombes logiques sont indétectables, mais peu diffusées car elles n'affectent qu'un seul logiciel, elles ne résultent pas d'une infection.

Cheval de Troie (Trojan horse)

Un cheval de Troie dissimule sa fonction sous l'apparence d'un logiciel apparemment inoffensif, un jeu, un utilitaire… Quand il est activé par l'utilisateur, il exécute ses fonctions par exemple l'ouverture d'une porte dérobée comme le fameux cheval de Troie. On cite l'exemple d'un antivirus diffusé avec un utilitaire (à l'insu de l'auteur de l'antivirus) pour lire la documentation jointe et qui en profitait pour effacer des programmes sur le disque dur.



http://www.mondialisation.ca/un-cheval-de-troie-isra-lien/10498

Logiciels malveillants autoreproducteurs

Ces logiciels malveillants, vers et virus, sont doués de **capacités d'autoreproduction**, ce qui explique la contamination rapide de millions d'ordinateurs en peu de temps. Deux types sont distingués mais il existe des intermédiaires, les virus vrais et les vers.

Ver (*worm*)

Les vers ne contaminent pas d'autres programmes et utilisent les ressources de l'ordinateur pour s'autoreproduire. Ils se propagent surtout par les réseaux.

C'est le ver *Christmas Tree* qui se propagea sur le réseau interne d'IBM en décembre 1987 et afficha sur les écrans un arbre de Noël. Le 2 novembre 1988 un ver inoffensif paralysa pendant plusieurs jours le réseau américain Internet.

Virus (proprement dits)

Les virus sont capables d'autoreproduction, utilisant les autres programmes dans lesquels ils incluent leur code comme vecteur de transmission. Ils sont parasites des programmes hébergeurs. Pour reprendre une terminologie médicale, ces virus passent par une phase d'incubation durant laquelle les porteurs sont contagieux sans le savoir, puis par une phase aiguë qui met en évidence la maladie contractée.

Lors de l'exécution du programme, le logiciel viral lui-même s'exécute : inséré dans le fichier du logiciel (au début ou à la fin) il détourne la première instruction, déroule les siennes et rend la main au logiciel pour passer inaperçu. Lors de son exécution il commence par se dupliquer dans la mémoire vive, et, comme tout programme, peut enclencher une action. De la mémoire vive, le virus peut infecter par reproduction d'autres programmes au cours de leur exécution. Si ces programmes sont situés sur d'autres supports non verrouillés ou sur le réseau, ils seront infectés comme ils le seront en cas de copie du programme infecté. La recopie peut d'ailleurs endommager des données.

On peut identifier :

- Des virus de fichiers exécutables (*File virus*) , les plus communs, qui ajoutent leur code à une application, s'activent à son lancement et contaminent d'autres exécutables.
- Des virus de secteur d'amorçage (*Boot sector virus*) ou de secteur de partition des disques durs (*Partition sector virus*) qui sont transférés en mémoire et actifs avant même le chargement du système d'exploitation et donc des logiciels antivirus. Le virus peut ensuite infecter toutes les disquettes non protégées en écriture qui seront introduites dans l'ordinateur.
- Des virus mixtes (Multi-partite virus) qui infectent exécutables et boot/partition.
- L'ingéniosité des concepteurs de virus les a conduit à essayer de contourner les techniques de détection inaugurant ainsi de nouvelles formes virales sophistiquées :
- Les virus furtifs (*Stealth virus*) qui interceptent les interruptions sytème pour induire en erreur les détecteurs de virus, à l'image de l'avion F-117 trompant les radars de détection
- Les virus polymorphes (*Polymorphic viruses*) dotés d'un véritable « moteur de mutation » qui leur permet de modifier par un encryptage sophistiqué leur code à chaque infection rendant inopérant certains anti-virus.
- Certains virus comme Edv sont capables en testant les registres du microprocesseur de s'assurer qu'un détecteur de virus ne pointe pas vers son espace mémoire !!
- Les macrovirus comme WM Concept : derniers venus sont capables d'utiliser le langage de commande intégré à Word ou Excel et d'infecter des documents Word ou Excel en ajoutant des « macros » qui en s'exécutant vont introduire le virus dans le fichier Normal.dot et par la suite dans tous les documents Word. Les dernières versions de ces logiciels permettent, en cas de doute, d'inactiver l'exécution des macro-instructions. Il faut noter que ces macrovirus sont actifs tant sur un PC que sur un Macintosh, le macro langage étant commun.

Que faire en cas d'attaque virale ?

Il faut soupçonner l'action d'un virus dès qu'un dysfonctionnement apparaît : ralentissement anormal, *beep* intempestifs, anomalies sur l'écran, apparition de messages explicites, prolifération de mauvais secteurs sur le disque dur … (attention, certains dysfonctionnements peuvent être provoqués par des bogues dans une application).

Lancer alors l'antivirus pour scanner tout le disque afin de détecter la présence éventuelle d'un virus et suivre la procédure que le logiciel propose.

Dans certains cas il peut être nécessaire de redémarrer l'ordinateur avec la disquette de secours saine que tout bon antivirus propose de construire lors de sa première utilisation.

Comment les détecter et se protéger ?

En dehors des macrovirus qui peuvent infecter toutes les machines sur lesquels Word et Excel sont disponibles (PC et Macintosh) les virus sont spécifiques de chaque famille d'ordinateurs parce ce qu'ils sont codés à l'aide du langage de programmation du microprocesseur différent sur les deux types de machines. Ainsi aucun risque de voir un PC infecté par nVir (propre au Macintosh) ni un Macintosh infecté par Frodo (redoutable pour le PC).

Pour limiter les risques d'infection virale il faut :

- Installer un **programme antivirus résident**, pour tester tout support introduit, pour scanner périodiquement et en fond de tâche le disque dur. Il faut aussi ne pas oublier d'effectuer des mises à jour de la base de reconnaissance des virus afin de prendre en compte les virus apparus récemment.
- Limiter au maximum l'introduction de supports d'origine inconnue ou douteuse. Faire particulièrement attention aux logiciels piratés en particulier les jeux.
- Verrouiller les supports originaux avant tout usage : ils ne peuvent alors pas être infectés même si l'ordinateur est contaminé.
- Sauvegarder les fichiers importants fréquemment sur des supports sûrs.
- Avoir un support de secours sain pour pouvoir redémarrer l'ordinateur.
- Installer un PAREFEU, dispositif qui trie les données à l'entrée de l'ordinateur et peut donc éliminer l'intrusion.

Notons enfin que le matériel ne peut pas être abîmé par un virus. Encore que…

Se documenter

La plupart des éditeurs de logiciels antivirus disposent de sites Internet sur lesquels il est possible de télécharger des mises à jour ou d'obtenir des informations fiables sur les virus détectés en consultant une **base de données**.

Corrélats :

Réseaux