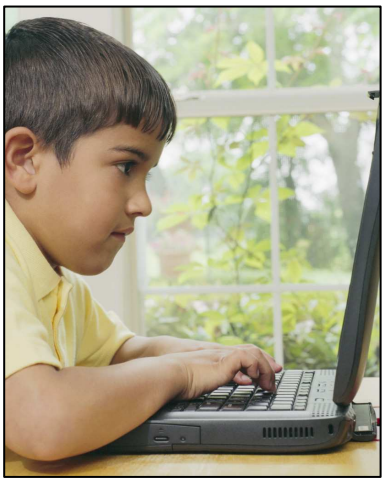
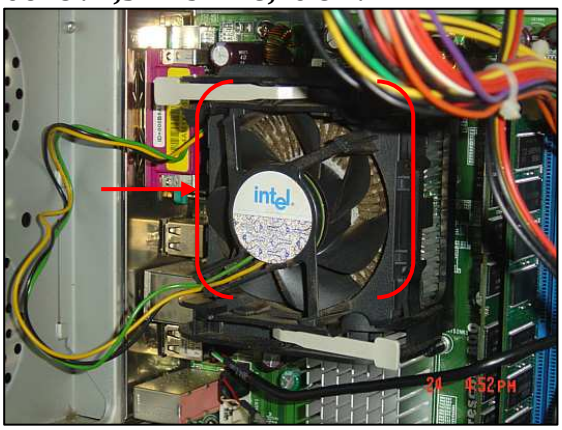


Risques d'un PC non protégé

Case study :

Examen en détail d'un ordinateur d'un jeune garçon de 12 ½ ans qui me confiait son ordinateur pour le contrôler gratuitement, un service gratuit pour les membres de notre **Internetstuff** (http://www.ettelbruck.lu/internetstuff).

Raison du contrôle : le jeune disait que son ordinateur était devenu tellement lent qu'il ne pouvait presque plus travailler avec et aussi une connexion à Internet était impossible, l'ordinateur ramait. En plus de ceci, le moniteur à tube cathodique de 19 pouces (48,26 cm de diagonale) s'éteignait aléatoirement. **Remarque : 1 pouce = 2,54 cm, donc : 2,54x19 = 48,26 cm.**



Après que le jeune avait ramené, accompagné de son père et de sa mère, son ordinateur avec moniteur, souris, clavier et la tour („**tower**"), la première chose à faire s'était d'ouvrir le boîtier et de jeter un coup d'œil sur la carte graphique pour voir si elle était bien enfoncée dans son slot. Effectivement, il fallait pousser un peu sur la carte graphique pour bien l'enfoncer dans le slot. J'ai profité en même temps pour dépoussiérer les ventilateurs et le refroidisseur du processeur avec une bombonne d'air comprimé, chose qui était nécessaire (voir photo ci-contre).

Après branchement des câbles et mise en route de l'ordinateur, celui-ci démarrait très lentement, mais l'affichage du moniteur fonctionnait, donc un problème de résolu déjà.

Une première vérification à faire est toujours de déterminer la configuration de l'ordinateur, chose qui a été faite et qui révélait que l'ordinateur utilise le **système d'exploitation Windows® XP avec l'installation du SP2**. Les **mises à jour de Windows ont été faites** aussi, tâche que le jeune connaissait apparemment.

Mais une vérification pour s'assurer qu'un antivirus était installé révélait qu'il n'y en avait pas. **L'ordinateur fonctionnait quatre années sans protection ! La seule protection de l'ordinateur était le firewall (pare-feu) de Windows® XP qui a été activé.**

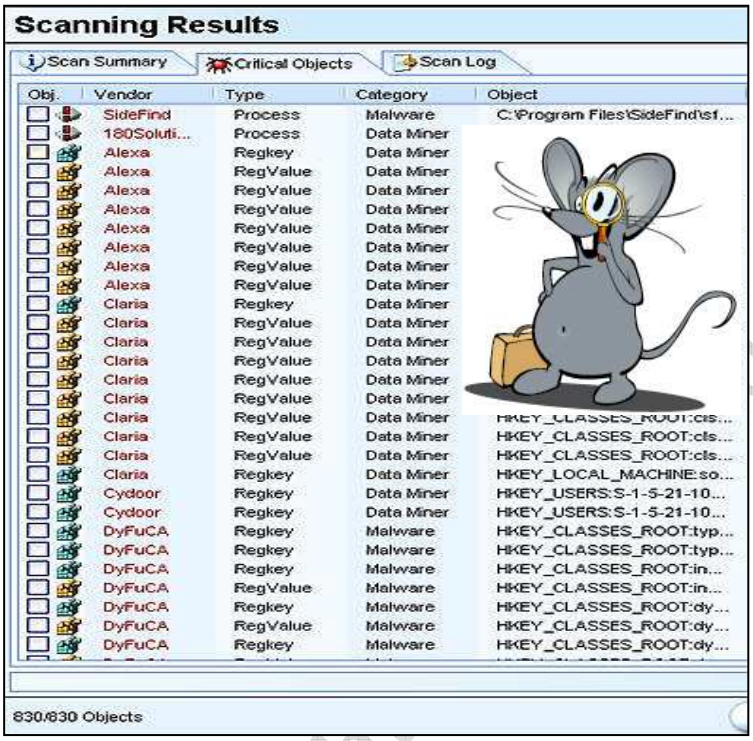
Comme le jeune ne disposait de quasiment nulle protection, il a fallu installer les logiciels suivants pour décontaminer l'ordinateur :

- Spybot Search&Destroy (antispyware): http://www.safer-networking.org.
- Ad Aware (antispyware): http://www.lavasoft.com.
- A squared (antimalware): http://www.emsisoft.net/fr.
- HijackThis: http://www.merijn.org/programs.php#hijackthis.
- Avira (antivirus): http://www.free-av.com.
- Advanced Windows One Care 2: http://www.iobit.com.
- F-Secure Blacklight (antirootkit): http://www.f-secure.com.
- CCleaner (nettoyage): http://www.ccleaner.com.
- Sweepi (nettoyage): http://www.yooapps.ch.
- Browser Hijack Retaliator: http://www.zamaansoft.com/products.
- Spyware Doctor : http://www.pctools.com/spyware-doctor/download.

Objets trouvés après plusieurs scans :

- **589 fichiers infectés et trouvés par „Spyware Doctor"**
- **477 fichiers infectés et trouvés par „a squared"**
- **708 fichiers infectés et cookies trouvés avec „Ad Aware"**

Dans le dossier „**My downloads**" se trouvaient **31.539 fichiers au format ZIP,** preuve que cet ordinateur était manifestement un „**PC zombie**" et que le disque dur de cet ordinateur servait comme point de relais pour distribuer ces fichiers, il a certainement été téléguidé et/ou servait comme place de stockage de fichiers , qui étaient détectés comme étant corrompus par l'antivirus, à l'insu de son propriétaire.



Un „**BHO**" (**Browser Helper Object/utilitaire d'aide du navigateur**) s'était avéré très coriace à enlever, le „**BHO**", „**MyWebSearch**" a été identifié comme étant un „**spyware**" (**mouchard**).
„**MyWebSearch**" a été détecté par les antispyware „**Spybot Search&Destroy**" et „**Ad Aware**", ainsi qu'avec l'antimalware „**a squared**", mais impossible de l'éradiquer avec ces utilitaires.
Une recherche sur Internet pour trouver un logiciel capable d'éradiquer ce soi-disant utilitaire à caractère d'espion a aboutit au téléchargement du logiciel payant „**Spy Emergency 2007**". La version téléchargée peut néanmoins être utilisée gratuitement pendant 15 jours et est par conséquent utilisable pour de premiers tests et enlèvement de malware en urgence.

Lors d'un scan avec cet antispyware, „**MyWebSearch**", ainsi que d'autres malware ont été détectés et éradiqués.

Ensuite comme tout a été éradiqué et que plus aucun logiciel ne détectait encore des malware, il fallait supprimer les points de restauration, pour être sûr que lors d'une restauration système les malware ne renaissent, chose qui a été faite.

Étant sûr que l'ordinateur n'était plus contaminé il fallait aussi vérifier l'état du disque dur, comprenant la suppression des fichiers temporaires et fichiers Internet temporaires, ainsi que la défragmentation du disque dur à la fin.

Pour supprimer les fichiers temporaires servaient les logiciels „**Sweepi**“ et „**CCleaner**“, dont voici les adresses URL pour télécharger les didacticiels qui vous guideront à travers l'installation et l'utilisation de ceux-ci :

http://www.internetmonitor.lu/download/ccleaner_27082006.pdf

http://www.internetmonitor.lu/download/SWEEPI.pdf

Mais lors de l'exécution de „**CCleaner**“ l'ordinateur bloquait en indiquant un message qu'un fichier Windows serait probablement endommagé et qu'il fallait lancer un „**scandisk**“ pour réparer celui-ci. Chose qui a été faite en lançant la console en tapant simultanément les touches „**Windows**“ et „**R**“ (**regedit**) et en incluant dans le champ de texte „**chkdsk“** pour lancer la vérification et la réparation du disque dur.

Après cette vérification l'ordinateur redémarra et soudainement l'antivirus se manifesta avec des fenêtres intempestives lesquelles il fallait acquitter en cochant le bouton „**supprimer virus**“, et ceci une trentaine de fois de suite et ceci se serait reproduit jusqu'à l'infini si je n'aurais interrompu l'antivirus, mais sans oublier de repérer de quel dossier venaient ces alertes.

Il s'est avéré que le dossier infecté était situé dans un autre compte utilisateur, celui de son père. Après vérification du compte utilisateur de son père il s'est avéré que celui-ci travaillait aussi sous régime d'administrateur, oh la, la, bonjour les dégâts. Deux comptes en „**administrateur“** il ne faut surtout pas le faire. Pour des raisons de sécurité il faut créer un compte „**administrateur**“ qui à lui dispose de tous les droits, et tout autre compte utilisateur il faut les créer avec accès limité.

Le dossier contaminé „**shared**“ de son père a été vérifié et quelle surprise, il contenait **22.571 objets**, la plupart des logiciels, des screensaver, vidéos, musique, etc. Évidemment il a été supprimé de suite et, rebelote, maintenant il fallait à nouveau faire des scans de sécurité avec les mêmes logiciels que pour le compte d'utilisateur du jeune.

Mais le jeune voulait absolument ramener son ordinateur à la maison (il était privé depuis cinq jours) et il téléphonait à son père pour venir chercher l'ordinateur avec la voiture, chose faite après un laps de temps de 20 minutes (ils habitent la même ville que mon lieu de travail).

Néanmoins, comme l'ordinateur n'a pu être vérifié à fond, les conseils suivants ont été donnés au père du jeune :

- Sauvegarder les images et fichiers absolument nécessaires et de les graver sur un support (CD, DVD).
- Ramener ce support de sauvegarde à l'Internetstuff pour contrôler s'il ne contient pas de virus.
- Au cas d'infection des fichiers sur ce médium de sauvegarde, les détruire, dommage, mais nécessaire.
- Repérage de liens et de logiciels utiles et création d'une liste de ceux-ci avec impression.
- Réinstallation du système d'exploitation sur l'ordinateur.
- Recherche sur Internet de la liste des liens (favoris), des logiciels, des utilitaires de sécurité et installation de ceux-ci sur l'ordinateur.
- Promesse au père, que le jeune, qui est membre dans notre Internetstuff, recevra des cours sur la sécurité PC&Internet d'une manière pertinente.
- Ce didacticiel sera aussi rendu aux parents afin qu'ils aient un rapport de suivi des actions faites sur leur ordinateur.

Récapitulatif :

Pour qu'un ordinateur soit sécurisé au maximum (**veuillez remarquer quand même qu'une sécurité à 100% n'existe pas et est illusoire**), il faut avoir installé un **antivirus**, un **firewall** (**pare-feu**), deux antispyware gratuits qui se complètent, et un **antimalware** comme „**a squared**". L'exemple ci-dessus a bien démontré en pratique ce qui puisse arriver sans ces protections.
Veuillez lire aussi notre didacticiel à l'adresse URL suivante :

http://www.internetmonitor.lu/download/L_ordinateur_bien_protege.pdf

Troubleshooting ou comment détecter, faire un diagnostique et éradiquer le cas échéant, les malware :

En ordre chronologique :

- Détecter la configuration de l'ordinateur http://www.ma-config.com.
  Voir aussi notre didacticiel comment utiliser ma-config :
  http://www.internetmonitor.lu/download/ConfigurationPC.pdf
- Vérification s'il y a un antivirus et un firewall (pare-feu) d'installé.
- Vérification si les mises à jour ont été installés http://www.secunia.com.
  Voir aussi notre didacticiel comment utiliser Secunia Software Inspector :
  http://www.internetmonitor.lu/download/Scan_gratuit_de_logiciels_installes_15122006.pdf
- Installation des utilitaires de protection suivants (Ad Aware, Spybot Search&Destroy, a squared).
- Scan de l'ordinateur avec ces utilitaires.
- Supprimer les points de restauration.
- Refaire un scan complet du système avec ces utilitaires.
- Suppression des fichiers temporaires et fichiers temporaires Internet.
- Défragmentation du disque dur :
  http://www.internetmonitor.lu/download/Defragmentation_du_disque_dur_avec_decoupe.pdf
- Créer un nouveau point de restauration du système propre et lui donner un nom bien approprié, par exemple „**système propre au 06.05.2007**".

Tableau regroupant les adresses de téléchargement des logiciels de protection et d'éradication :

Nom du logiciel	Utilisation	Adresse URL
Spybot Search&Destroy	Antispyware	http://www.safer-networking.org/fr/download/index.html
Ad Aware	Antispyware	www.lavasoft.com
a squared	Antimalware	www.emsisoft.net/fr
HijackThis	Hijacker analyse	http://www.merijn.org/programs.php#hijackthis
CCleaner	Nettoyage fichiers	www.ccleaner.com
Sweepi	Nettoyage fichiers	www.yooapps.ch
Secunia Software Inspector	Mises à jour logiciels	http://secunia.com/software_inspector/

Diagnose :

- **L'ordinateur ne comportait pas moins de 1.774 vulnérabilités, dont beaucoup de troyens.**
- **Le disque dur de cet ordinateur servait comme plate-forme de distribution des fichiers y stockés (31.539 fichiers du jeune et 22.571 fichiers du père).**
- **Cet ordinateur était un „PC zombie".**
- **L'ordinateur disposait de deux comptes administrateur, chose qu'il ne faut jamais faire. Il ne peut y avoir qu'un seul compte administrateur ! Tous les autres utilisateurs doivent être configurés avec accès limité !**
- **Les utilisateurs de l'ordinateur utilisaient du P2P (échange de fichiers), sans connaître les dangers de ce service !**

Afin que cela ne vous arrive pas, je vous conseille de lire notre didacticiel „**L'ordinateur bien protégé**" à l'adresse URL :

http://www.internetmonitor.lu/download/L_ordinateur_bien_protege.pdf.

Pour ceux qui aiment savoir plus et qui aiment aussi apprendre, je vous conseille notre école virtuelle (e-learning) sur la Sécurité PC&Internet à l'adresse URL :

http://www.ecolevirtuelle-pcsecurite.com.

Astuce pour ceux qui ne connaissent pas :

Bougez le pointeur (flèche) de la souris sur les liens présents dans ce didacticiel et enfoncez la touche „Ctrl" (Control), sur un clavier allemand c'est la touche „Strg" (Steuerungstaste), et puis cliquez sur le lien. Connexion Internet présente, vous serez de suite dirigé sur le site Internet choisi.