

SOIGNEZ VOS MACHINES ! Jacques DELATTRE – delattre.jck@wanadoo.fr

Nous recevons fréquemment, au cercle, des machines malades de virus ou d'indigestion, voire des deux. Les remettre en forme peut être long, fastidieux et entraîner des opérations chirurgicales à risques encore appelées formatage du disque C. Plutôt que de vous aider à remettre vos machines en état, nous préfererions vous aider à les protéger contre les risques des promenades sur Internet et contre les malaises qui les guettent : mieux vaut prévenir que guérir.

Vous trouverez ci-après de brèves descriptions des remèdes que nous utilisons au cercle et que nous sommes prêts à vous montrer et à vous aider à installer et à paramétrer : anti-virus, pare-feu, nettoyage de fichiers Internet, nettoyage de Windows. Il en existe d'autres que vous trouvez par exemple dans le Petit Péciste, mais on ne peut pas tout connaître ... Précision : nous n'avons aucun intérêt chez les éditeurs des produits mentionnés.

Anti-virus

Les auteurs de virus ont, dans leur ensemble, le niveau mental des casseurs de voitures : casser pour le plaisir, anonymement, sans risques, « ... ah dis dons, le pied quoi, keum ! ». Tous les moyens de contamination sont bons avec une prédilection pour les documents Internet et notamment les annexes attachées au courrier. L'arrosage est général pour causer un maximum de dégâts. On ne peut plus se contenter de filtrer son courrier, la seule défense est un logiciel anti-virus **COMPLET** et **A JOUR**. Il en existe plusieurs, fonctionnant généralement par recherche des signatures des virus répertoriés (leur ADN en quelque sorte, quelque 65000 aujourd'hui) et/ou des formes syntactiques propres au genre virus, elles sont en nombre limité comme dans la nature.

Nous utilisons Norton AntiVirus de Symantec : connu depuis longtemps il a intégré les produits anti-virus d'IBM. Symantec est une société importante (4000 personnes) spécialisée dans la protection des réseaux, des serveurs, des stations de travail et des ordinateurs personnels. Elle dispose d'un réseau de traque étendu, des forces nécessaires pour réagir vite et propose un système de mise à jour du fichier des signatures et du moteur de recherche lui-même, par Internet. Les mises à jour peuvent être manuelles ou rendues automatiques (LiveUpdate), la fréquence recommandée hebdomadaire, au moins. Revers de la médaille: le services est gratuit pendant un an, puis payant, environ 15€ par an sans limite d'utilisation. Notez aussi que NAV se connecte à son site pendant la recherche dans les pièces jointes pour détecter les nouveaux virus et disposer des dernières définitions ; cette fonction peut être désactivée si vous avez des craintes quant à la confidentialité.

Le cercle met à votre disposition un système de mise à jour des signatures (mais pas du moteur) par disquettes, particulièrement utile si vous n'êtes pas connecté à Internet. Merci à Jean Bayon.

Pare-feu (firewall)

Les pare-feux contrôlent les appels du réseau vers votre machine pour éviter des prises de contrôle indésirables, et les appels de votre machine vers le réseau pour éviter la transmission indue d'informations vers le contrôleur indélicat.

Ces intrusions sont généralement le fait de pirates (hackers) souvent très compétents et parfois géniaux. Elles visent essentiellement les entreprises et les organismes gouvernementaux dans leurs activités et nécessitent de connaître l'adresse IP (Internet Protocol) de l'installation visée. Nous sommes des particuliers, nous utilisons généralement une connexion par le réseau téléphonique commuté (RTC) dont l'adresse IP change à chaque connexion et nous sommes relativement à l'abri de ces inconvénients.

Cependant, les connexions à haut débit par ADSL ou par le câble utilisent en général un lien permanent, donc un numéro IP fixe. Les auteurs de virus plus astucieux que la masse voient là un nouveau champ d'activité tout aussi aléatoire mais plus varié « ... j'y ai piqué ses jpeg et ses MP3 et puis j'y ai péché sa bécane, le pied ! mec ».

ZoneAlarm, un des pare-feux les plus efficaces et les plus faciles à utiliser est gratuit pour nous, individuels, dans sa version de base. Il serait dommage de s'en priver et vous serez prêts pour passer en haut débit. ZoneAlarm a ainsi contrôlé deux tentatives en un an sur ma machine en RTC ... et j'ai découvert les appels de NAV vers son site qui ne sont pas explicitement indiqués dans l'aide en ligne !

Nettoyage des fichiers Internet

Une virée sur le réseau laisse des scories dans votre machine, indépendamment des virus : les « cookies » bien connus, mais aussi tous les éléments constitutifs des pages affichées (ce qui permet de les reconstituer), les adresses des sites visitées, les programmes amenés plus ou moins clandestinement dans des documents (ActiveX et Plugs-in) dont des programmes espions renseignant directement leurs commanditaires sur vos activités etc... L'ensemble prend de la place, peut vous valoir une inflation de publicités diverses ou des désagréments plus pernecieux, permet de retrouver vos activités et leurs résultats.

Vous pouvez nettoyer ou supprimer ces fichiers ou programmes individuellement par l'explorateur de Windows ou par Cleansweep de Symantec mais nous préférons utiliser Internet Cleanup de Ontrack qui permet de tout nettoyer d'un seul clic. Ad-aware de Lavasoft (programme gratuit) affine la destruction des fichiers espions.

Nettoyage de Windows

Windows (y compris XP) efface mal ses traces et s'encrasse au fur et à mesure de l'utilisation: fichiers orphelins, duplications, programmes mal terminés, fichiers sur disques émiettés, registres périmés. Dans le meilleur des cas la machine ralentit, dans le pire des cas elle s'arrête par indigestion.

Norton Utilities propose des programmes de vérification et de rectification de Windows (Windoctor) et des disques (Windisk). Norton CleanSweep suit la trace de l'installation de nouveaux programmes et permet des désinstallations propres. Attention: les anciennes versions de ce programme peuvent être délicates à manier.

En résumé

L'installation de Norton System Works de Symantec (regroupant Norton AntiVirus, Norton Utilities et CleanSweep), de Internet Cleanup de Ontrack et de Ad-Aware de Lavasoft (ces deux derniers gratuits) vous assurent une bonne sécurité de fonctionnement, à condition de les maintenir à jour. Les animateurs du cercle sont prêts à vous les montrer et à vous aider.