Pour plus de souplesse Windows est architecturé en services (ou processus) fonctionnant en arrière-plan du système. Un grand nombre de ces processus sont des processus liés directement au système, par contre d'autre appartiennent à des applications tierces. On peut afficher la liste des processus en faisant : contrôle+alt+suppression et en sélectionnant processus. Si le système semble ralentir anormalement il est intéressant de vérifier dans cette liste quels processus consomment le plus de ressources. De plus la présence de virus, vers, chevaux de Troie, spywares, adwares est trahie souvent par la présence de processus suspects prenant un nom proche du nom d'un processus utilisé par le système.

Ci-dessous une liste des principaux processus présents.

srvany - srvany.exe

Le processus **srvany.exe** (*srvany* signifiant *Run any program as a service*) est un processus générique de Windows NT/2000/XP permettant de démarrer n'importe quel programme en tant que service.

Le processus srvany n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système pouvant être arrêté.

taskmgr - taskmgr.exe

Le processus **taskmgr.exe** (*taskmgr* signifiant *task Manager*) est le gestionnaire des tâches de Windows lui-même. Il est donc systématiquement lancé à chaque fois que vous souhaitez voir les processus d'arrière-plan !

Le processus taskmgr n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus pouvant être arrêté.

svchost - svchost.exe

Le processus **svchost.exe** (*svchost* signifiant *Service Host Process*) est un processus générique de Windows 2000/XP servant d'hôtes pour les autres processus dont le fonctionnement repose sur des librairies dynamiques (DLLs). Il existe ainsi autant d'entrées svchost qu'il y a de processus qui l'utilisent.

L'utilitaire *tlist.exe* fourni sur le CD-ROM de Windows 2000/XP permet de lister les applications utilisant ce service grâce à la commande suivante :

```
tlist -s
```

Le service svchost original possède une faille de sécurité qu'il est impératif de corriger en mettant à jour le système avec le service WindowsUpdate.

Il ne s'agit en aucun cas d'un Virus résident, d'un ver, d'un cheval de Troie, d'un spyware, ni d'un AdWare

tapisrv - tapisrv.exe

Le processus **tapisrv.exe** (*tapisrv* signifiant *Telephony API Service*) est un processus générique de Windows NT/2000/XP servant à gérer les services téléphonique tels que la composition de numéros, etc.

Le processus tapisrv n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

systray - systray.exe

Le processus **systray.exe** (*systray* signifiant *System Tray Service*) est un processus générique de Windows NT/2000/XP correspondant à la barre des tâches.

Le processus systray n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus pouvant être arrêté, ce qui provoque la fermeture de la barre des tâches

spoolsv - spoolsv.exe

Le processus **spoolsv.exe** (*spoolsv* signifiant *Printer Spooler Service*, en français *spouleur d'impression*) est un processus générique de Windows NT/2000/XP servant à mettre en mémoire (file d'attente) les travaux d'impression.

Il ne s'agit en aucun cas d'un Virus résident, d'un ver, d'un cheval de Troie, d'un spyware, ni d'un AdWare.

Il s'agit d'un processus pouvant être arrêté.

spool32 - spool32.exe

Le processus **spool32.exe** (*spool32* signifiant *Windows Spooler 32-bit*) est un processus générique de Windows NT/2000/XP servant à gérer de façon transparente les files d'attente d'impression.

Le processus spool32 n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système pouvant être arrêté.

services - services.exe

Le processus **services.exe** (*Windows Service Controller*) est un processus générique de Windows NT/2000/XP permettant de reconnaître et d'adapter les modifications matérielles du système sans intervention de l'utilisateur.

Le processus services n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système critique ne pouvant pas être arrêté.

rpcss - rpcss.exe

Le processus **rpcss.exe** (*rpcss* signifiant *Remote Procedure Call Subsystem*) est un processus générique de Windows NT/2000/XP permettant à des applications d'utiliser les procédures RPC déclarées sur le système.

Le processus rpcss n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système critique ne pouvant pas être arrêté.

rundll32 - rundll32.exe

Le processus **rundll32.exe** (*rundll32* signifiant *Run a DLL as a 32-bit application*) est un processus générique de Windows NT/2000/XP servant à charger les librairies dynamiques (DLLs) en mémoire afin de les rendre utilisables par d'autres programmes.

Le fichier correspondant à ce processus est normalement située dans le répertoire "*%SystemRoot%\System32\rundll32.exe*" (*%SystemRoot%* étant généralement *C:\WINDOWS* par défaut).

Le processus rundll32 n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système critique ne pouvant pas être arrêté.

scm - scm.exe

Le processus **scm.exe** (*scm* signifiant *Service Control Manager*) est un processus générique de Windows NT/2000/XP servant à la gestion de l'ensemble des services de Windows.

Le processus scm n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système critique ne pouvant pas être arrêté.

rnaapp - rnaapp.exe

Le processus **rnaapp.exe** (*Windows Modem Connection*) est un processus générique de Windows NT/2000/XP servant à initier la numérotation et la gestion du modem lors d'une connexion à Internet en RTC.

Le processus rnaapp n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus pouvant être arrêté. L'arrêt de ce service provoque évidemment la perte de la connexion via le modem.

rapimgr - rapimgr.exe

Le processus **rapimgr.exe** est un processus correspondant à un module du logiciel ActiveSync permettant de synchroniser un PDA et un ordinateur personnel. Le fichier correspondant à ce processus est normalement située dans le répertoire "*C:\Program Files\Microsoft ActiveSync*".

Il s'agit d'un processus applicatif pouvant être arrêté.

ntfrs - ntfrs.exe

Le processus **ntfrs.exe** (*ntfrs* signifiant *NT File Replication Service*) est un processus générique de Windows NT/2000/XP servant à gérer la réplication et la synchronisation de fichiers entre plusieurs machines et serveurs.

Le processus ntfrs n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système pouvant être arrêté.

mstask - mstask.exe

Le processus **mstask.exe** (*mstask* signifiant *Microsoft Task Scheduler*) est un processus générique de Windows NT/2000/XP servant à planifier l'exécution automatique de tâches (sauvegardes, lancement d'une application, mises à jour, etc.) à des horaires particuliers.

Le processus mstask n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Le processus mstask est un processus pouvant être arrêté.

mssearch - mssearch.exe

Le processus **mssearch.exe** (*mssearch* signifiant *Microsoft Search*) est un processus générique de Windows NT/2000/XP servant à créer des index "full text" pour le service d'indexation de Windows (cidaemon.exe).

Le processus mssearch n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système pouvant être arrêté.

msiexec - msiexec.exe

Le processus **msiexec.exe** (*msiexec* signifiant *Windows Installer Component*) est un processus générique de Windows NT/2000/XP servant à installer, réparer et supprimer des programmes fournis en packages Windows Installer (dont l'extension est *.msi*).

Le processus msiexec n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Le processus msiexec est un processus pouvant être arrêté.

msdtc - msdtc.exe

Le processus **msdtc.exe** (*msdtc* signifiant *Microsoft Distributed Coordinator*) est un processus générique de Windows NT/2000/XP servant à gérer la coordination des bases de données, des file d'attente de messages et des sytèmes de fichiers.

Le processus msdtc n'est en aucun cas un Virus résident, un ver, un cheval de Troie, un spyware, ni un AdWare.

Il s'agit d'un processus système pouvant être arrêté.

Information fichier taskeng.exe

Le processus **Task Scheduler Engine** ou **Aufgabenplanungsmodul** ou **Moteur du Planificateur de tâches** ou **taskeng.exe** appartient au logiciel **taskeng.exe** ou **Microsoft Windows Operating System** ou **Betriebssystem Microsoft Windows** ou **Système d'exploitation Microsoft Windows** de la compagnie **Microsoft Corporation** (www.microsoft.com).

Description : Fichier taskeng.exe est dans le répertoire C:\Windows\System32. Les tailles de fichiers connues sous Windows XP sont 166,400 octets (occurrence de 48%), 169,472 octets, 169,984 octets. Fichier système de Windows. Le processus a une fenêtre invisible. C'est un fichier de confiance Microsoft. La note de sécurité technique attribuée équivaut à *3% de dangerosité*, pensez à lire les commentaires des utilisateurs.

Si taskeng.exe se trouve sur un sous-répertoire de "C:\Documents and Settings" alors la note de sécurité attribuée est *71% de dangerosité*. La taille du fichier est de 55,296 octets. Aucune description du programme. Ce n'est pas un fichier de base de Windows. Le programme est caché. Le processus est chargé au démarrage de Windows (voir la clé de Registre : HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, -, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\scrfile\shell\open\command,). Ce programme utilise les ports pour se connecter au LAN ou Internet.

Si taskeng.exe se trouve sur un sous-répertoire de "C:\Program Files" alors la note de sécurité attribuée est *74% de dangerosité*. La taille du fichier est de 55,296 octets. Aucune information de fichier. Le programme a une fenêtre invisible. L'application se lance au cours du démarrage de Windows (voir la clé de Registre : HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, -, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\scrfile\shell\open\command,). Ce n'est pas un composant système de Windows.

Important: Certains malwares se dissimulent en tant que taskeng.exe, notamment ceux qui se trouvent dans le répertoire c:\windows ou c:\windows\system32. Pensez à vérifier le processus taskeng.exe sur votre PC s'il cause des problèmes. Nous vous conseillons d'utiliser **Security Task Manager** pour vérifier combien votre système est sécurisé.