Les processus systèmes de Windows

Sur les forums, il arrive parfois que des internautes posent des questions sur des processus Windows en demandant si ce dernier est légitime ou un virus.
Les réponses données sont parfois erronées en indiquant qu'un fichier système est un virus alors qu'il s'agit d'un fichier système de Windows.

Voici une liste des principaux fichiers systèmes de Windows.

Les processus systèmes de Windows

Introduction

Un processus est une application en cours d'exécution, quand on parle d'application, vous pensez probablement aux programmes installés.

Windows étant un logiciel complexe, modulé, le système d'exploitation embarque ses propres applications.
Il peut s'agit de fichiers systèmes qui sont là pour effectuer les opérations courantes de Windows, comme gérer l'ouverture de session, gérer les fenêtres, le bureau etc.
Mais aussi parfois de tâche plus spécifique, comme les mises à jour Windows Update.

Dans ce vaste monde qu'est Windows, il est parfois complexe pour les internautes de savoir si un fichier est légitime ou malicieux.
Parfois, sur les forums, les indications données sont incorrectes.

Voici quelques explications, conseils et liste des principaux fichiers systèmes de Windows.

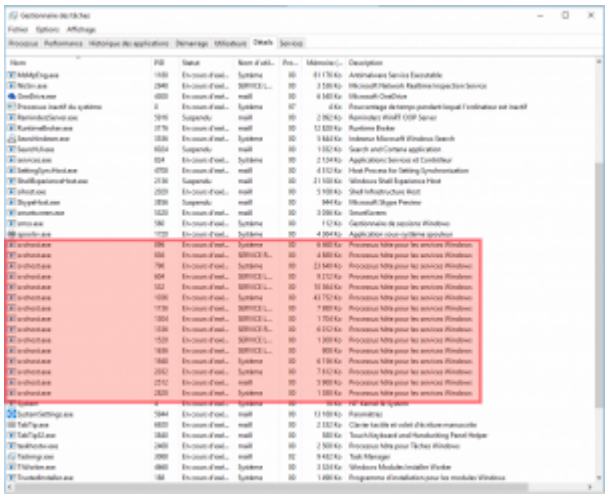
Pour rappel, il existe un long dossier sur la compréhension des processus Windows : Processus et Services Windows

Les bons emplacements

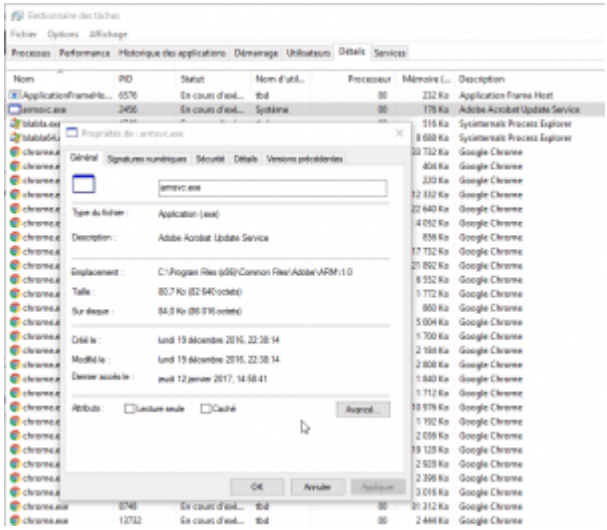
Afin de semer le trouble, les noms de fichiers utilisés par les logiciels malveillants peuvent reprendre celles d'applications connues ou de fichiers systèmes Windows.
Il s'agit d'une méthode de camouflage.
Si un trojan utilise un nom de fichier svchost.exe, un fichier système de Windows, dans le gestionnaire de tâches, vous aurez un svchost.exe de plus dans la liste. L'internaute risque de ne pas se rendre compte et faire la différence entre les svchost.exe légitimes, de celui malicieux.

L'emplacement joue beaucoup, ainsi :

- C:\Windows\system32\svchost.exe est légitime
- C:\Windows\system\svchost.exe est malicieux
- C:\Users\<users\>AppData\svchost.exe est aussi malicieux



Depuis Windows 8, le [le gestionnaire de tâches] permet facilement de connaître l'emplacement d'un processus, par un clic droit / Propriétés ou un clic droit / Ouvrir l'emplacement du fichier.
Sinon vous pouvez utiliser un gestionnaire de tâche avancé comme [Process Explorer], en double-cliquant dessus, le chemin se trouve dans PATH.

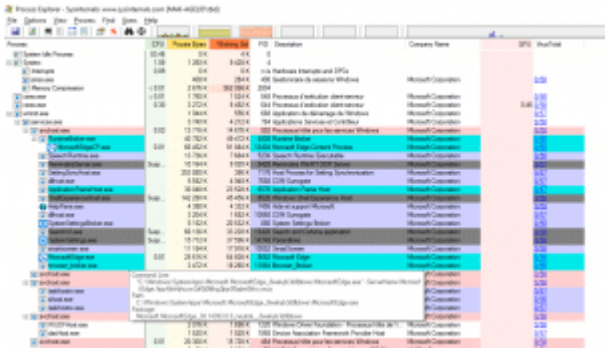


Connaître les emplacements des fichiers systèmes Windows aide donc à ne pas faire d'erreurs et dissocier les vrais processus légitimes Windows, des processus malveillants.
L'emplacement générique étant C:\Windows\system32

Pensez aussi que depuis Windows 8.1 et encore plus sur Windows 8, Windows embarque des applications Windows Store.
Les applications Windows Store en natinf ([Edge], [Cortana], etc)

se trouvent dans *C:\Windows\SystemApps*

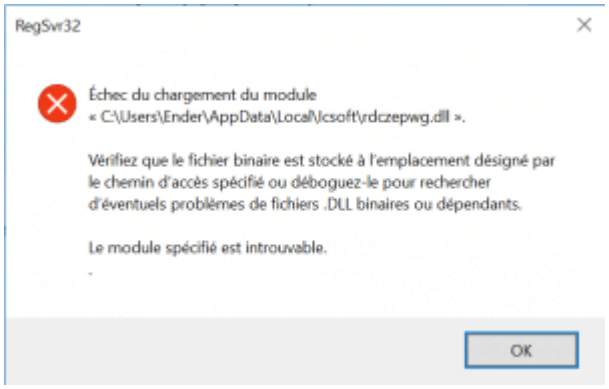
Exemple avec l'emplacement de Microsoft Edge :



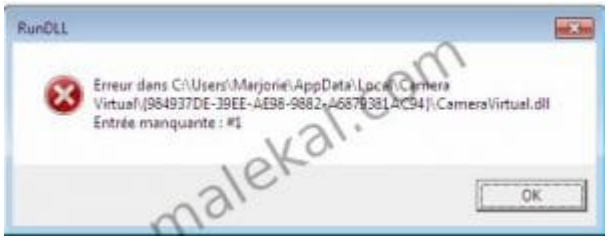
Les messages d'erreur

Les messages d'erreur au démarrage de Windows liés à des logiciels malveillants peuvent aussi semer la confusion si mal interprété.
Ces erreurs « Le module spécifié est introuvable » peuvent faire penser que certains processus systèmes sont malicieux.

Ainsi dans **le message d'erreur RegSvr32** suivant qui indique que C:\Users\Ender\AppData\Local\lcsoft\rdczepwg.dll est manquant.
Si mal compris, on peut penser que RegSvr32 en titre de fenêtre est malicieux alors qu'il s'agit d'un processus système.



Même chose, si dessous avec **une erreur RunDLL** et une erreur d'entrée manquante.



Mauvais outil

Une mauvaise compréhension des rapports ou une utilisation d'outil non à jour peuvent aussi mal auguiller.
Ainsi, le programme HijackThis et l'utilisation de hijackthis.de va marquer tous les svchost.exe malicieux alors qu'ils sont en réalité sain.

Côté détection, je vous conseille de lire cette page sur l'abus de scan AdwCleaner, RogueKiller et ZHPDiag : AdwCleaner, RogueKiller, ZHPCleaner : mauvaises habitudes …

Liste des processus Windows

Suivez la liste de la page suivante : Liste des processus système Windows ou encore Liste des processus Windows
Dans cette page, vous trouverez la liste des processus système accompagné d'une description brève de ces derniers.

Les principaux processus systèmes de Windows 10.
La plupart des fichiers systèmes se trouvent dans C:\Windows\system32 :

- browser_broker.exe
- conhost.exe

- explorer.exe
- csrss.exe
- dasHost.exe
- dllhost.exe
- dwm.exe
- fontdrvhost.exe
- HelpPane.exe (dans C:\Windows)
- lsass.exe
- msiexec.exe
- NisSrv.exe
- services.exe
- smartscreen.exe
- RuntimeBroker.exe
- SearchIndexer.exe
- searchUI.exe
- SettingSyncHost.exe
- ShellExperienceHost.exe
- SystemSettingsBroker.exe
- SystemSettings.exe
  (dans C:\Windows\ImmersiveControlPanel)
- sihost.exe
- smss.exe
- SpeechRuntime.exe
  (dans C:\Windows\System32\Speech_OneCore\Common)
- spoolsv.exe
- svchost.exe
- taskhost.exe (Windows 7)
- taskhostw.exe
- userinit.exe
- wininit.exe
- winlogon.exe
- WmiPrvSE.exe
- WUDFHost.exe

Non listé dans le gestionnaire de tâches mais que vous pouvez rencontrer :

- RegSvr32.exe : permet d'enregistrer une bibliothèque DLL
- RunDLL : permet de lancer un fichier DLL

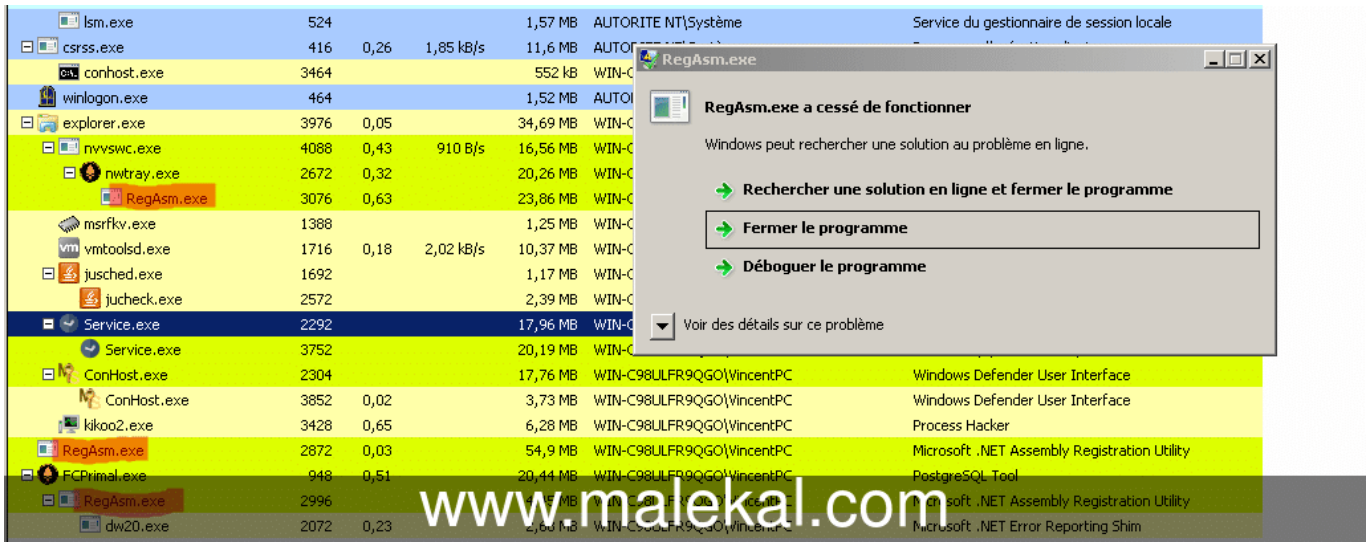
Les processus systèmes liés à Windows Defender, l'emplacement est C:\Program Files\Windows Defender :

- MpCmdRun.exe
- MSASCuiL.exe
- MsMpEng.exe

Lié au .NET Framework (si installé) :

- PresentationFontCache.exe
  (dans C:\Windows\Microsoft.NET\Framework64\v3.0\WPF)

Note le fichier RegASM.exe qui est lié au .NET Framework peut se lancer si un Trojan écrit en .NET Framework est actif dans le système, notamment les Trojans RAT :



Lié à Cortana (C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy) :

- RemindersServer.exe
- ShellExperienceHost.exe

Microsoft Edge (C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe) :

- microsoftedgecp.exe
- MicrosoftEdge.exe

Détecter les virus ou piratage

Lisez la page : Comment vérifier si ordinateur a été hacké ou piraté ?
Cette page vous explique comment surveiller son système et détecter des logiciels malveillants (trojan, keylogger, virus, backdoor)