Le registre Windows

La base de registre à la loupe

La base de registre, que l'on nomme aussi le registre ou la BDR, est très souvent sollicitée par l'utilisateur soucieux d'optimiser son système, de le personnaliser mais aussi de le réparer. Mais connaissons-nous réellement bien la base de registre de Windows ? Nous allons à travers cet article tenter d'en comprendre les principales structures et savoir ainsi la manipuler de façon optimale.
Le registre est sollicité sans arrêt par le système et les programmes qui viennent récupérer des informations de configuration afin de faire fonctionner le système et vos programmes correctement. Si une information est erronée dans le registre, Windows vous enverra peut être un message d'alerte ou éventuellement votre système plantera au démarrage ou pendant votre activité. Les virus ou malwares viennent eux aussi modifier divers paramètres de configuration dans le registre, ce qui altère alors le bon fonctionnement de votre machine.

Quelles sont les actions que l'on peut effectuer dessus ?
Il existe diverses possibilités pour intervenir sur le registre : les outils Windows, les outils dédiés spécifiques, etc. A première vue, la base de registre peut paraître compliquée à l'utilisateur lambda car les clés et les valeurs sont données en anglais et ne sont pas toujours explicites au premier abord. Pourtant, une fois que l'on a compris son fonctionnement, il devient plus facile de naviguer dans sa structure. Nous allons essayer de faire le point sur le sujet (Windows 2000/XP/2003).

Le registre est un élément essentiel au bon fonctionnement de votre système, il est important de toujours faire une sauvegarde avant de modifier quoi que ce soit.

Présentation

Le registre, c'est quoi ?

Windows conserve toutes les informations relatives à la configuration du système, ces informations peuvent être visualisées dans une base de données appelée Registre. Le Registre contient les profils de chaque utilisateur de l'ordinateur ainsi que les informations relatives au matériel du système, aux programmes installés et aux paramètres de propriétés. Windows utilise constamment ces informations dès le démarrage du système et lors de son fonctionnement.

A chaque fois que vous modifiez une propriété à l'aide d'une boîte de dialogue sur votre système, Windows inscrit immédiatement cette modification dans le registre. Ceci est valable pour toutes les actions que vous effectuez avec votre système.

Ces informations sont présentes dans divers fichiers appelés "ruches" ("hives") présents sur votre système d'exploitation, on retrouve ces fichiers dans plusieurs répertoires:

- **C:\Documents and Settings\%USERPROFILE%** *(\%USERPROFILE%\ -> correspond au nom des sessions)*
- **C:\Documents and Settings\%USERPROFILE%\Local Settings\Application Data\Microsoft\Windows**

- **C:\Windows\System32\Config**
- **C:\Windows\System32\Config\systemprofile**
- **C:\Windows\System32\GroupPolicy**

Les principaux noms de ces fichiers : **ntuser.dat, UsrClass.dat, default, SAM, SECURITY, software, system**

Vous ne pouvez pas éditer ces fichiers directement (ni les copier, les supprimer même si vous êtes l'administrateur de la machine) tout simplement parce qu'ils sont utilisés par le système. Il faut utiliser un outil connu sous le nom de "Éditeur de Base de Registre" pour visualiser leurs contenus ou y effectuer des modifications.

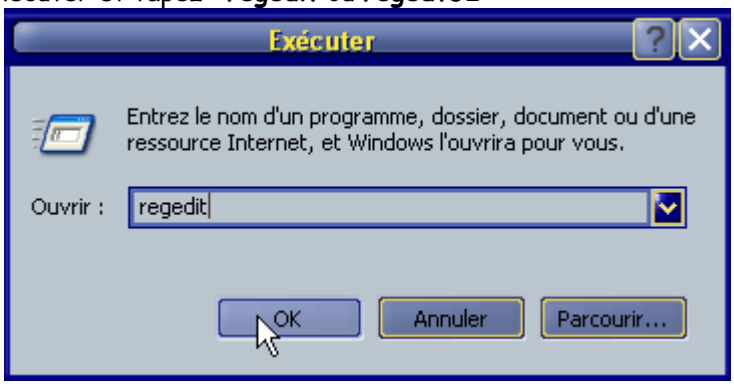
En fait, lorsque l'on accède au registre grâce aux éditeurs, on retrouve toutes ces informations rangées dans différents dossiers que nous verrons par la suite.

Accéder au registre

Les éditeurs du Registre permettent de contrôler et/ou modifier les données dans le registre. Il existe deux outils Windows présents sur le système : **Regedit.exe et Regedt32.exe**

Pour accéder au registre :

Menu Démarrer ---> Exécuter et tapez : **regedit** ou **regedt32**



Depuis Windows XP, regedit et regedt32 ont les mêmes fonctionnalités, vous pouvez également ajouter un raccourci sur votre bureau, il suffit d'aller dans votre Explorateur à :

C:\Windows\regedit.exe

ou

-C:\Windows\System32\regedit.exe

ou

-C:\Windows\System32\regedt32.exe

En cas de soucis

Dans de nombreux cas d'infections, les malwares installent des restrictions pour vous interdire d'accéder à votre registre. Voici quelques méthodes qui devraient vous tirer d'affaire et vous permettre d'accéder au registre :

Modifiez l'extension du programme :

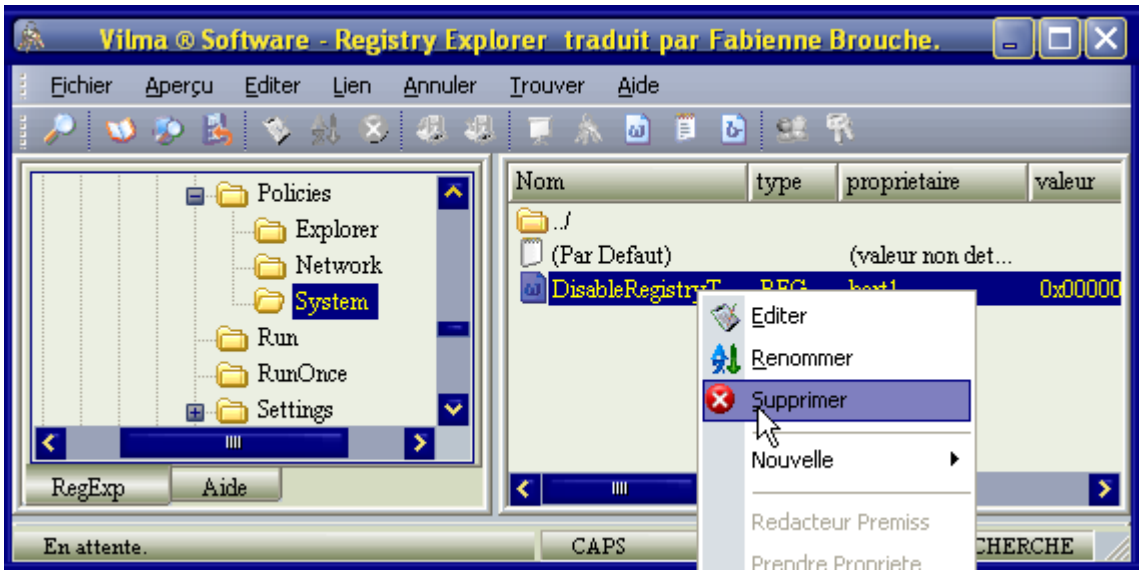
Ouvrez votre Explorateur et allez jusqu'à : C:\Windows\regedit.exe

- Clic droit sur regedit.exe ---> *Renommer* et modifiez l'extension en .com
- Ce qui donne : regedit.com --> Double-cliquez et votre éditeur de registre devrait s'ouvrir.

Si cela ne fonctionne pas, utilisez FixSwen.inf. Clic droit ---> Installer. Il est employé pour remettre en place (dans la base de registre) les associations relatives à l'exécution des fichiers exécutables (.exe, .com, .bat, .reg, etc.) altérées par le malware Swen pour paralyser le système.

Si cela ne marche toujours pas, vous avez ce joli message :

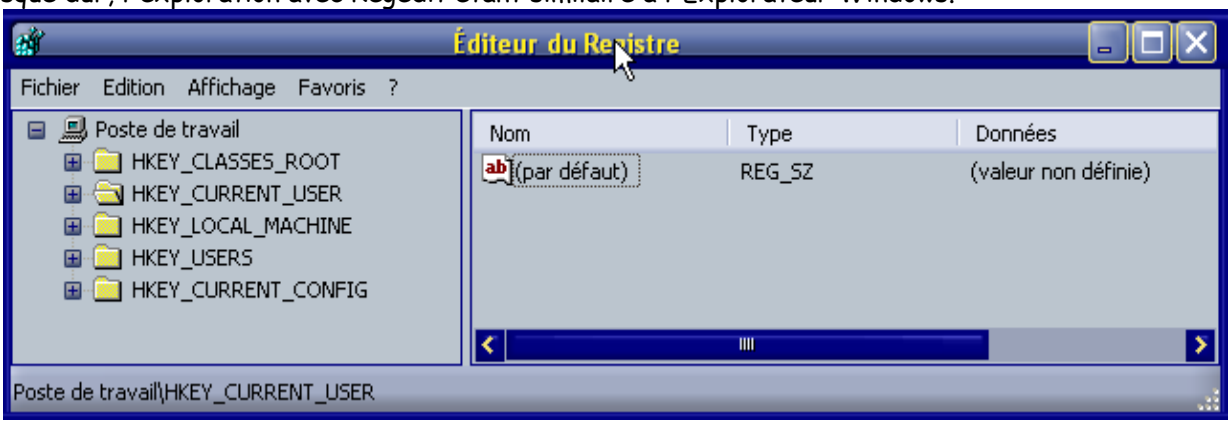
Une valeur interdit l'ouverture de votre éditeur, en principe elle se trouve ici :
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
et se nomme : DisableRegistryTools
Téléchargez ce fichier.vbs Restoreregedit.vbs et exécutez-le.
Autre solution : utilisez un autre éditeur de registre, Vilma fait ceci très bien (voir le sujet à la fin de l'article) ; eh oui, les pirates n'ont pensé qu'à bloquer Windows et ses outils ! Heureusement, ce programme fonctionne sans aucun souci même avec l'option bloquée, il suffit alors de simplement supprimer la valeur DisableRegistryTools :



En principe, avec l'une de ces options, vous devriez pouvoir accéder au registre.

L'arborescence du registre

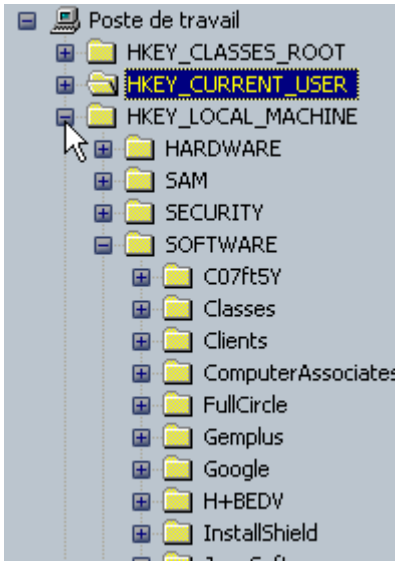
Le registre possède une structure hiérarchique ressemblant à la structure des répertoires de votre disque dur, l'exploration avec Regedit étant similaire à l'Explorateur Windows.



Quand Regedit est ouvert, vous remarquez que dans la partie gauche de la fenêtre se trouve une arborescence contenant des dossiers, et dans la partie droite le contenu (les valeurs) du dossier actuellement sélectionné.

Partie gauche

Comme pour l'Explorateur Windows, pour développer une branche, cliquez sur le signe [+] devant un dossier, ou double-cliquez simplement sur ce dossier. Pour afficher le contenu d'une clé (dossier), cliquez sur la clé désirée et examinez les valeurs énumérées dans la partie droite de la fenêtre. Vous pouvez ajouter une nouvelle clé ou valeur en sélectionnant *Nouveau* dans le menu *Édition* ou en effectuant un clic droit. Vous pouvez également renommer toute valeur et la plupart des clés par la même méthode que pour renommer un fichier ; un clic droit sur l'objet et un clic sur *Renommer*, ou deux clics de suite (lentement), ou utiliser simplement la touche *F2* du clavier. Enfin, vous pouvez supprimer une clé ou une valeur en cliquant dessus et en appuyant sur la touche *Suppr*, ou par un clic droit, en choisissant *Supprimer*.



Chaque branche principale (désignée par une icône de dossier dans le registre) est appelée une **Ruche**, et les Ruches contiennent des Clés. Chaque clé contient d'autres clés (parfois appelées sous-clés), ainsi que des Valeurs. Ces valeurs contiennent l'information actuelle stockée dans le registre.

Il existe cinq branches principales, chacune contenant une partie spécifique de l'information stockée dans le registre. Ce sont les éléments suivants:

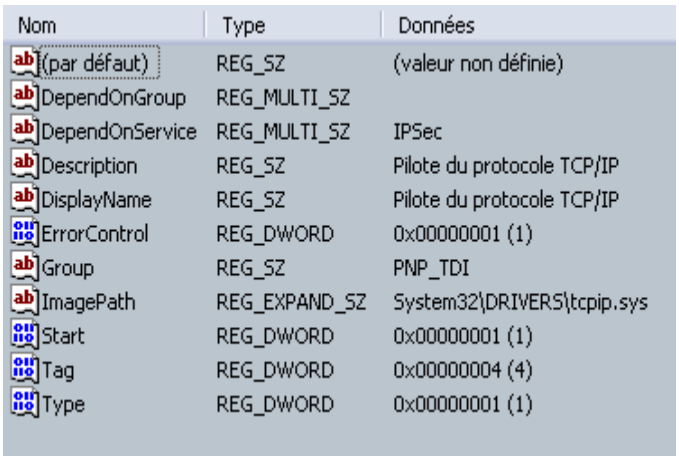
- **HKEY_CLASSES_ROOT** - Cette branche contient tous vos mappages d'associations de fichiers pour supporter la fonction de glisser-déposer, l'information OLE, les raccourcis Windows, et l'aspect coeur de l'interface utilisateur Windows.
- **HKEY_CURRENT_USER** - Cette branche est liée à la section HKEY_USERS associée à l'utilisateur actuellement en session dans le PC et contient des informations comme les noms d'ouverture de sessions, la configuration du bureau, et les options du menu Démarrer.
- **HKEY_LOCAL_MACHINE** - Cette branche contient des informations appartenant à l'ordinateur et concerne le type de matériel, de logiciels, et autres préférences pour un PC donné, ces informations étant utilisées pour tous les usagers en session dans cet ordinateur.
- **HKEY_USERS** - Cette branche contient les préférences individuelles de chaque utilisateur de l'ordinateur, chacun étant représenté par une sous-clé SID située dans la branche principale.
- **HKEY_CURRENT_CONFIG** - Cette branche est reliée à la section HKEY_LOCAL_MACHINE correspondant à la configuration matérielle courante.

Partie droite

Chaque clé ou sous-clé du Registre peut contenir des données appelées "valeurs". Certaines rubriques contiennent des informations spécifiques à chaque utilisateur, d'autres concernent tous les utilisateurs de l'ordinateur. Une rubrique comprend trois parties : le nom de la valeur, le type de données de la valeur et la valeur elle-même.

Il existe trois types de valeurs : *Chaîne*, *Binaire*, et *DWORD*

Leur utilisation dépend du contexte.



Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
DependOnGroup	REG_MULTI_SZ	
DependOnService	REG_MULTI_SZ	IPSec
Description	REG_SZ	Pilote du protocole TCP/IP
DisplayName	REG_SZ	Pilote du protocole TCP/IP
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	PNP_TDI
ImagePath	REG_EXPAND_SZ	System32\DRIVERS\tcpip.sys
Start	REG_DWORD	0x00000001 (1)
Tag	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	0x00000001 (1)

Chaque valeur de base de registre est établie sous la forme de l'un des cinq types de données principales suivantes :

REG_BINARY - Ce type contient la valeur sous forme d'une ligne de donnée binaire. La plupart des informations concernant les composants matériels sont stockées sous forme d'une donnée binaire, et peuvent être affichées à l'aide d'un éditeur de format hexadécimal.

REG_DWORD - Ce type représente les données par un nombre de quatre octets et est couramment utilisé pour les valeurs booléennes, comme "0" pour désactivé et "1" pour activé ou inversement (c'est en fonction du nom de la valeur). De plus, beaucoup de paramètres de pilotes de périphériques et de services sont de ce type et peuvent être affichés avec *REGEDT32* au format binaire, hexadécimal et décimal, ou avec *REGEDIT* au format hexadécimal et décimal.

REG_EXPAND_SZ - Ce type est une chaîne de données extensible dont la chaîne contient une variable qui sera remplacée quand elle est appelée par une application. Par exemple, pour la valeur suivante, la chaîne "%SystemRoot%" sera remplacée par l'emplacement actuel du répertoire qui contient les fichiers système de Windows.

REG_MULTI_SZ - Ce type est une chaîne multiple, il est utilisé pour représenter les valeurs qui contiennent des valeurs de liste ou multiples, chaque entrée étant séparée par un caractère NULL.

REG_SZ - Ce type est une chaîne standard, utilisé pour représenter des valeurs de texte contrôlables.

Il faut savoir que Regedit ne montre pas tout, un certain nombre de clés et valeurs sont cachées, il s'agit en principe des clés ou valeurs axées sur la sécurité, les stratégies de groupe et l'intégrité du système.

Le registre Windows

La base de registre à la loupe

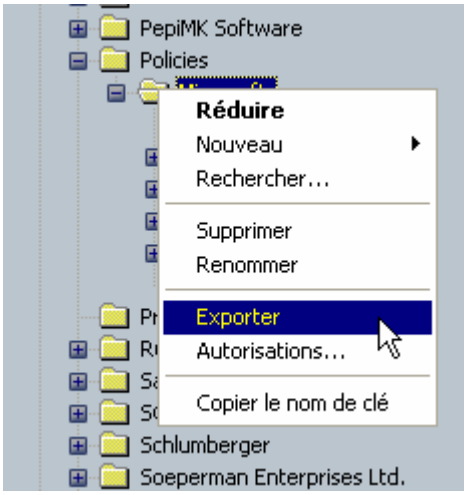
Exporter, modifier, créer, supprimer

Passons aux choses sérieuses, voici les diverses fonctions du registre.

Exporter

Avant de modifier votre registre, il est préférable de faire une sauvegarde des clés ou valeurs que vous souhaitez modifier. C'est là qu'intervient la fonction *Exporter* de regedit.

La fonction *Exporter* vous permet de créer un fichier avec une extension **.reg**. Ce fichier ainsi créé représente l'ensemble des informations de la clé ou de la sous-clé avec toutes les valeurs et les données que vous sélectionnez. Il est important de lui donner un nom "parlant" qui vous permettra par la suite de le retrouver si le besoin s'en fait sentir.

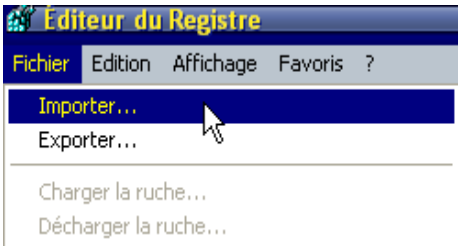


Pour exporter : dans la partie gauche du registre, faites un clic droit sur la clé en question puis choisissez *Exporter*. Une fenêtre va s'ouvrir, choisissez le dossier dans lequel vous allez garder ce fichier puis enregistrez-le.

Importer

La modification de votre registre ne vous convient pas, vous souhaitez revenir aux valeurs d'origines ou vous souhaitez simplement ajouter une nouvelle valeur à votre registre par l'intermédiaire d'un fichier .reg.

La fonction *Importer* vous permet de fusionner le contenu d'un fichier registre avec une extension **.reg**.



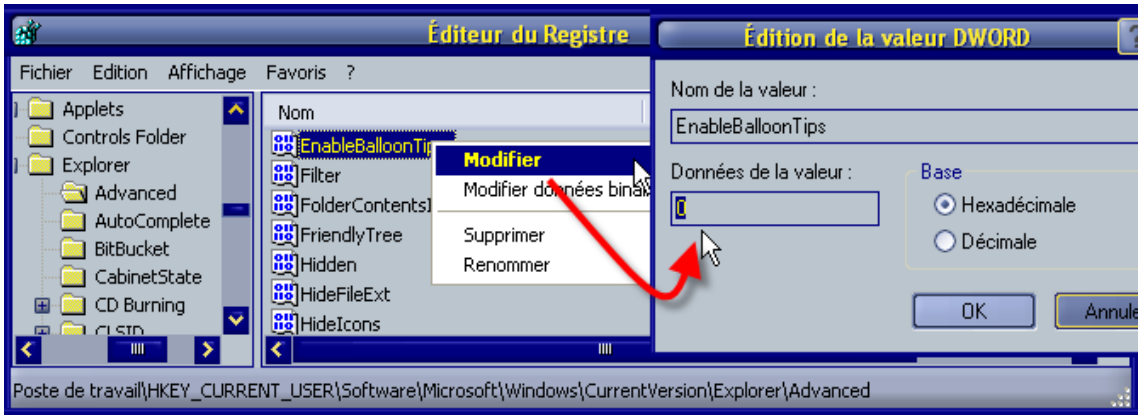
Pour importer : dans le menu du haut de l'Editeur du registre, allez dans *Fichier* puis choisissez *Importer...*. Une fenêtre va s'ouvrir, choisissez le dossier dans lequel vous allez récupérer le fichier puis cliquer sur *Ouvrir*. Votre fichier est enregistré dans votre registre.

Modifier

Prenons un exemple simple : vous souhaitez remettre les infos-bulles par défaut dans Windows. Rendez-vous à la clé :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Cherchez le nom de la valeur : *EnableBalloonTips* et modifiez la donnée de la valeur, comme sur l'image ci dessous :



1 = pour réactiver l'option (remet les infos-bulles par défaut)

0 = pour désactiver l'option (désactive les infos-bulles)

Le choix des 0 et 1 pour activer ou désactiver dépend principalement du nom de la valeur, du caractère positif ou négatif de cette valeur. Dans notre cas, si la valeur se serait nommée *DisableBalloonTips*, il aurait fallu mettre des données de valeur contraire.

Créer

De nombreuses astuces se trouvent sur Internet (et notamment sur zebulon !), il est possible d'ajouter des nouvelles valeurs à votre registre en fonction de vos besoins. **Ajouter de nouvelles valeurs dans le registre ne s'improvise pas, il est important de consulter différents sites réputés afin de constater la véracité de cette valeur, son utilité, sa fonction, etc.** Pour créer une nouvelle sous-clé ou valeur, on peut le faire de différentes manières :

- avec regedit
- en créant un fichier **.reg**, **.vbs** ou **.inf**

Avec regedit, en fonction de l'objectif :

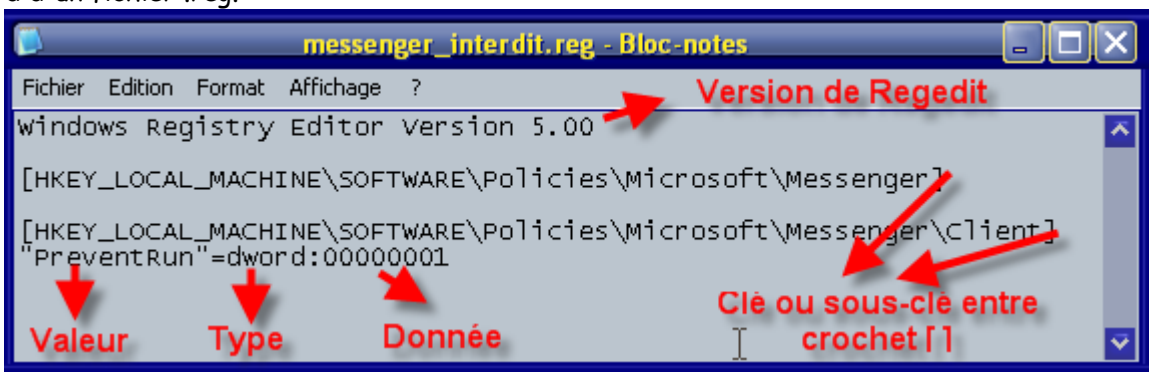
- pour créer une sous-clé --> clic droit dans la partie gauche de regedit ---> inscrivez le nom de la nouvelle clé
- - pour créer une valeur ---> clic droit dans la partie droite de regedit ---> choisissez le type de valeur

Créer un fichier (.reg, .vbs, .inf)

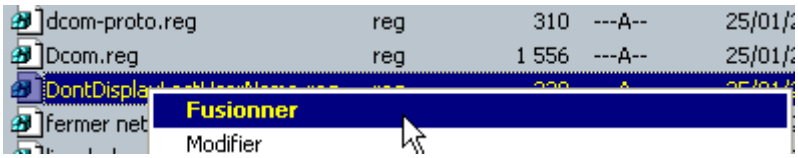
L'intérêt de créer ce type de document, c'est sa portabilité, d'une session à l'autre, d'un système à l'autre, d'un PC à l'autre. Vous l'avez compris, ces fichiers peuvent être (en fonction de l'extension) fusionnés, exécutés ou installés. Tout ceci est très pratique et fait gagner beaucoup de temps lors d'une réinstallation de système pour retrouver sa configuration personnelle. Cela permet également d'envoyer ces modifications à un ami pour le dépanner, etc.

Le gros avantage de la création d'un tel fichier est également que vous allez pouvoir le faire sur-mesure, vous pourrez placer 3 ou 50 modifications sur un seul fichier et même fichier.

L'objectif ici n'est pas de fabriquer des fichiers .reg, .vbs ou .inf, mais de vous donner la composition standard d'un fichier .reg.



Ce fichier peut être créé et enregistré avec le bloc-notes, il suffit de faire un clic droit dessus et de choisir *Fusionner* dans le menu contextuel pour qu'il inscrive les valeurs dans le registre.



On peut ajouter diverses clés les unes à la suite des autres et adjoindre un commentaire pour chaqu'une des clés. Voici un exemple d'un fichier .reg que l'on peut créer et adapter à sa configuration personnelle.
- Mettez un (point-virgule) ";" pour commenter une ligne, ce qui permet de vous retrouver facilement dans vos modifications.

```
Windows Registry Editor Version 5.00

;-------------------------------------
;Optimisation du système le 10/10/2003
;-------------------------------------

;Désactivation de la visite guidée de Windows
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Applets\
Tour]
"RunCount"=dword:00000000

;Arrêt plus rapide du système
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"WaitToKillServiceTimeout"="3000"

;Conserver la connexion active lors du changement d'utilisateur
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"KeepRasConnections"="1"

; etc.
```

Vous trouverez de nombreuses astuces concernant la modification de la base de registre dans notre section "astuces" du site. Il existe également quelques sites spécialisés dans la base de registre où vous trouverez de nombreuses astuces (vous retrouverez quelques uns de ces sites en fin d'article).
Pour les fichiers .vbs ou .inf, on entre dans le domaine de la programmation, rien de tel que de passer chez des spécialistes afin de comprendre le fonctionnement de ces fichiers :
Secret Windows - inf
Le site de JCB - VBS

Supprimer

Il peut être opportun de vouloir supprimer une valeur dans la base de registre, c'est le cas notamment pour des restrictions causées par des virus. Ici nous allons voir comment créer un fichier .reg pour la suppression. Pour supprimer une valeur, il suffit d'attribuer le signe (moins) "-" à la valeur à supprimer :

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=-
```

Pour supprimer une clé, c'est presque identique, il suffit d'attribuer le signe (moins) "-" devant le nom de la clé à supprimer et après le crochet [.

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\Software\Symantec\Nom_de_la_cle]
```

Rechercher

La fonction *Rechercher* sert beaucoup, principalement pour supprimer des valeurs ou clés de logiciels que l'on a désinstallés mais dont certaines clés subsistent encore (voir la suite du sujet dans "Nettoyer le registre").

Autorisations

De temps en temps, suite à la désinstallation d'un logiciel par exemple, il se peut que vous n'arriviez pas à supprimer une clé. Ceci peut être dû à la présence de restriction utilisateur. Le fonctionnement de cette option est identique à celle de l'explorateur (voir le sujet ici).
Nous venons de faire un tour général des diverses fonctions de regedit. La modification, la suppression ou l'ajout de clé ou valeur peut dans certain cas nécessiter un redémarrage de la machine. Il existe également d'autres fonctions tel que charger ou décharger la ruche. Ces fonctions peuvent s'avérer très utiles, vous trouverez un lien en fin d'article sur le sujet.

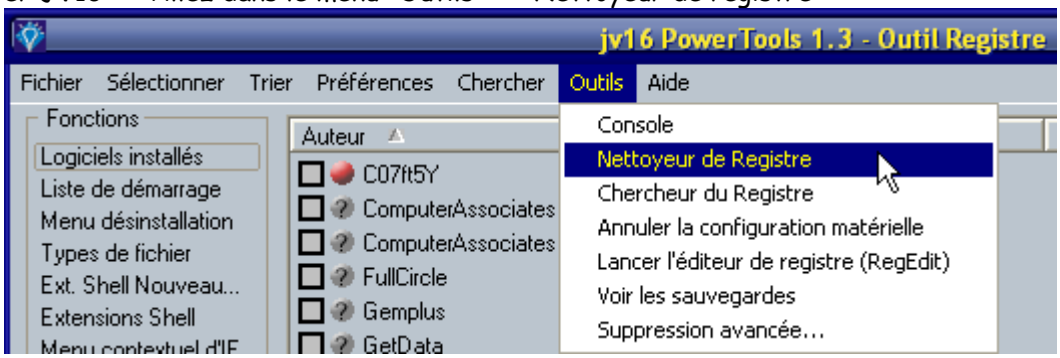
Maintenant, vous êtes capable de modifier, ajouter ou supprimer des clés ou des valeurs dans votre registre. Cela ne vous autorise pas pour autant à faire n'importe quoi, il est important de toujours rester prudent avec le registre si vous souhaitez garder votre système stable.

La base de registre à la loupe

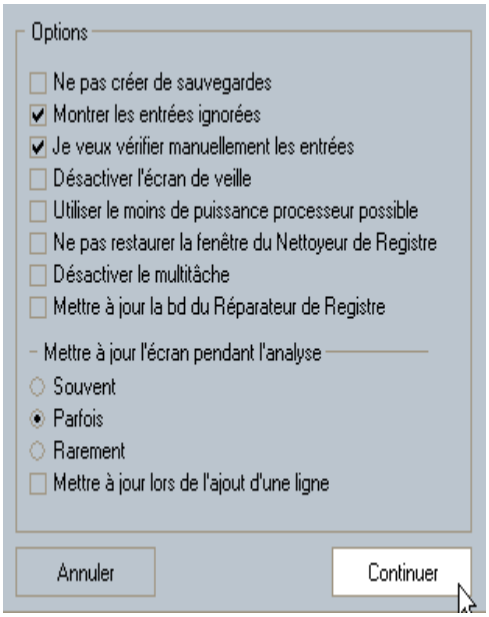
Nettoyer le registre

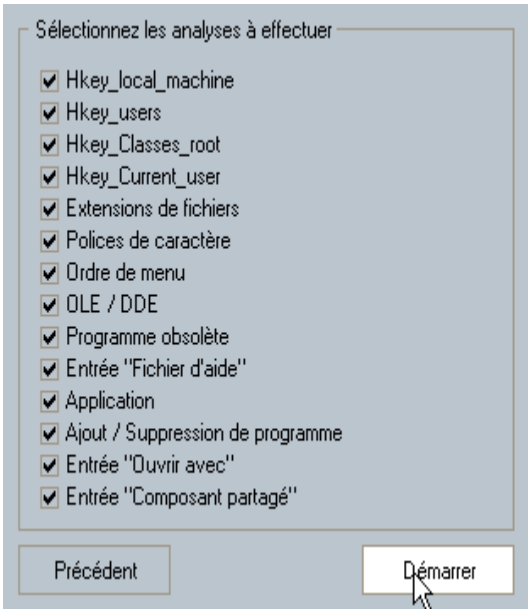
Pourquoi faire le ménage dans le registre ?
Simplement parce qu'au fur et à mesure de votre utilisation du système, vous installez ou désinstallez des logiciels, vous supprimez des documents, vous modifiez des paramètres. Il devient alors nécessaire de supprimer toutes ces entrées qui n'ont plus de références sur votre système (ces entrées sont dites "obsolètes").
Il est difficile et fastidieux de nettoyer le registre manuellement, c'est pourquoi il est intéressant d'utiliser quelques outils spécialisés dans le domaine : JV16, RegCleaner, RegSeeker, RegSupreme, etc.

JV16 PowerTools
Démarrer JV16 --> Allez dans le menu "Outils" --> Nettoyeur de registre

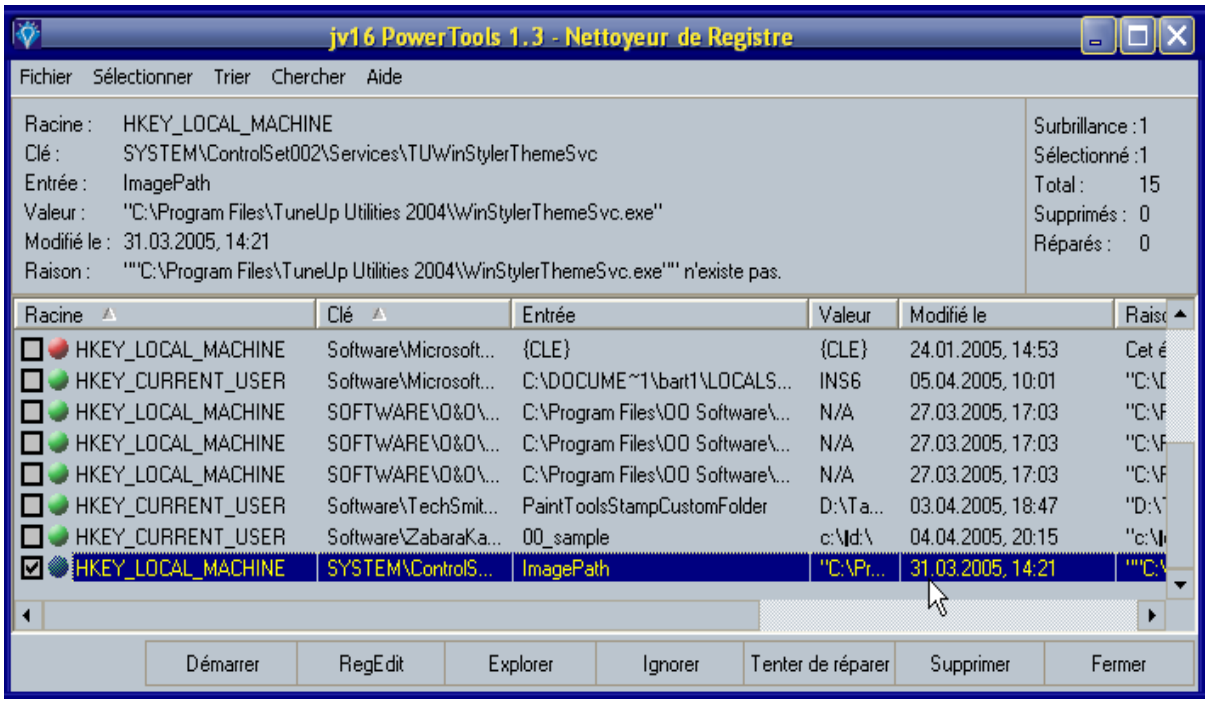


Les 2 écrans suivants permettent de paramétrer les options :





Le scan des entrées de registre commence :



Il existe deux types d'entrées à nettoyer :

Vert : représente toutes les valeurs qui peuvent être supprimées sans souci.

- Rouge : ces entrées correspondent à certains mots clés tel que *install*, etc.

Il suffit simplement de cliquer sur la ligne pour avoir les indications complètes de la ligne en haut de la fenêtre de l'écran de JV16.

Il est possible la première fois que vous utilisez ce type de logiciel que vous trouviez une grande quantité de lignes, c'est tout à fait normal. Même 1000 lignes ne représentent qu'une infime partie de votre registre qui varie entre 250 000 et 500 000 lignes environ.

Si vous souhaitez supprimer une ligne Rouge, JV16 vous renvoie un message d'alerte :

Si vous connaissez cette entrée, qu'elle correspond à un logiciel déjà désinstallé, vous pouvez la supprimer sans crainte. Si vous avez un doute sur son utilité, ne la cochez pas, vous pouvez aller la vérifier dans votre registre.

Si vous souhaitez savoir où se trouve la ligne en question dans votre registre, cliquez sur "RegEdit" :

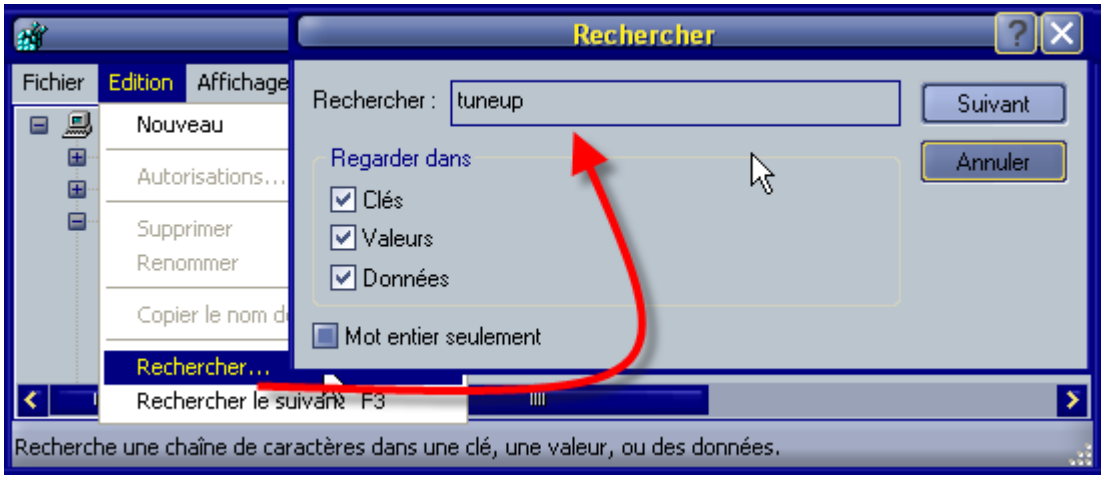
Regedit s'ouvre sur la clé, il suffit alors de vérifier la valeur dans la partie de droite pour contrôler.
La dernière version gratuite de JV16 fera très bien l'affaire pour le nettoyage de la base de registre.
Télécharger JV16 PowerTools 1.3.0.195 (dernière version gratuite)
Le site officiel de JV16

Ce type de logiciel permet de nettoyer correctement votre registre, mais il ne fait pas tout, il est possible d'aller plus loin. C'est là qu'intervient la fonction "Rechercher" de Regedit.

Rechercher

Cette fonction est la suite logique d'un nettoyage réalisé par logiciel car elle permet de vérifier la présence d'autres clés ou valeurs non supprimées par les logiciels de nettoyage automatique

.



Une fois dans regedit -> menu *Edition* --> *Rechercher*, une fenêtre s'ouvre, inscrivez un mot qui correspond à votre recherche (dans notre exemple, il y a tuneup car ce programme vient d'être désinstallé).
La recherche commence :

Pour une recherche sur l'ensemble du registre il faut se mettre sur poste de travail. Dès l'instant où regedit trouve une entrée, il s'arrête :

Si l'entrée que vous cherchez correspond au logiciel, vous pouvez supprimer la clé ou la valeur donnée. Ensuite, appuyez sur la touche F3 de votre clavier pour continuer votre recherche, et ainsi de suite jusqu'à ce que la recherche s'arrête.

RegSeeker
Outil presque identique à JV16, voici le tutoriel RegSeeker de Zebulon.
Télécharger RegSeeker sur Zebulon

RegSupreme
Tout comme JV16, RegSupreme nettoie votre registre. Voir le site officiel.

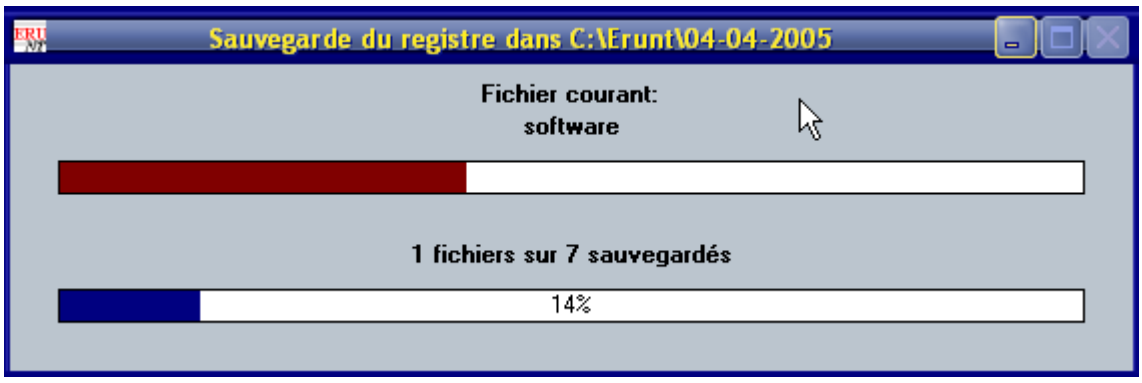
Il existe de nombreux logiciels dans cette catégorie, le choix reste une affaire personnelle, mais si le votre vous satisfait pleinement, conservez-le. Après ce nettoyage de printemps, vous pouvez sauvegarder votre registre, c'est la suite de cet article.

Sauvegarder le registre

Pourquoi sauvegarder le registre ?
Simplement pour mettre votre système à l'abri d'une défaillance et ainsi le restituer dans un parfait état de fonctionnement. Dans la famille 2000/XP, il n'est pas possible de sauvegarder l'ensemble de la base de registre, la ruche SECURITY est inaccessible et certaines clés sont carrément interdites même en lecture. Heureusement on trouve des utilitaires sur Internet : Erunt en fait partie. Erunt copie simplement les ruches au format binaire qui se trouvent dans C:\Windows\System32\Config\ et le ou les fichiers des sessions : C:\Documents and Settings\%USERPROFILE%\ntuser.dat.
Pour créer une sauvegarde, il est impératif que votre système soit en parfait état de fonctionnement, sain et exempt de tout malwares, sinon cela n'a aucun intérêt.

La sauvegarde en images
Créez un dossier spécial pour vos sauvegardes (dans notre exemple C:\Erunt\) :

S'il existe plusieurs sessions, cochez la case destinée à cet effet.
Cliquez sur "OK" ---> la sauvegarde commence :



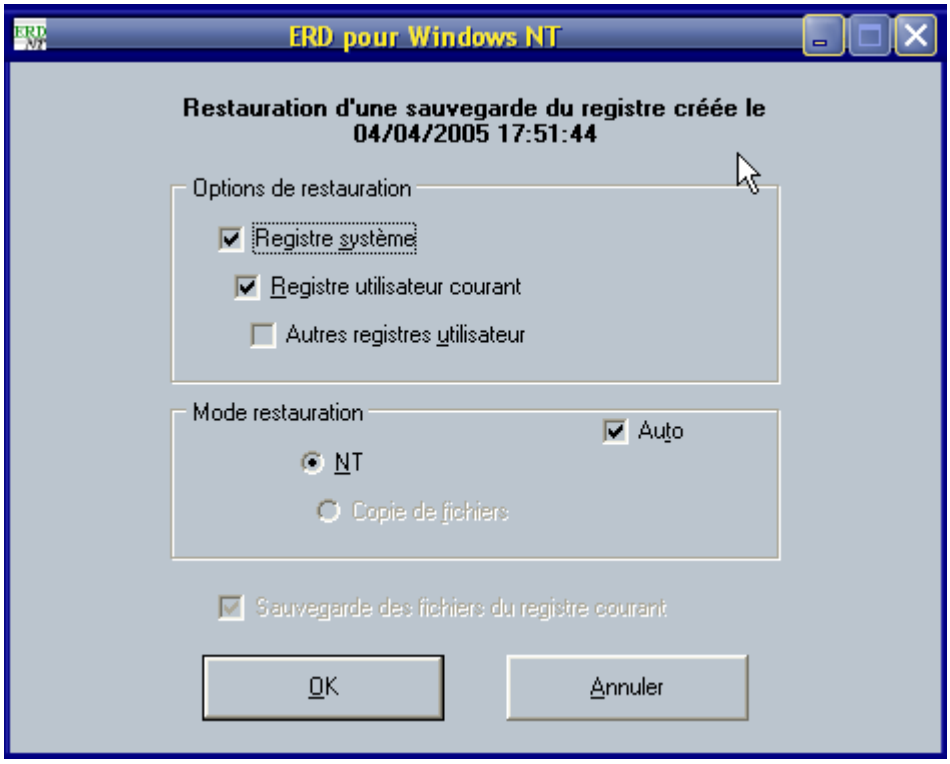
Erunt enregistre les fichiers :
ntuser.dat(ici 2), default, SAM, SECURITY, software, system dans le dossier : C:\Erunt\(date de la sauvegarde)\

Et voilà, votre sauvegarde est terminée, cela n'a duré que quelques secondes.

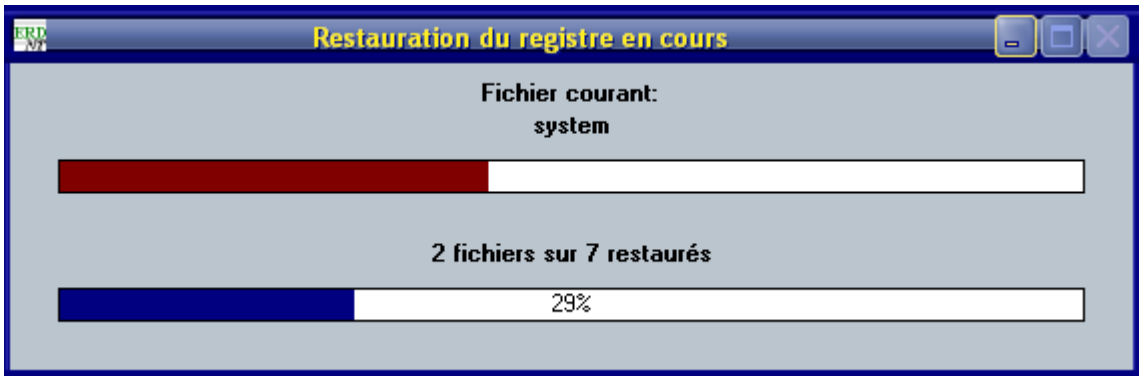
La restauration en image

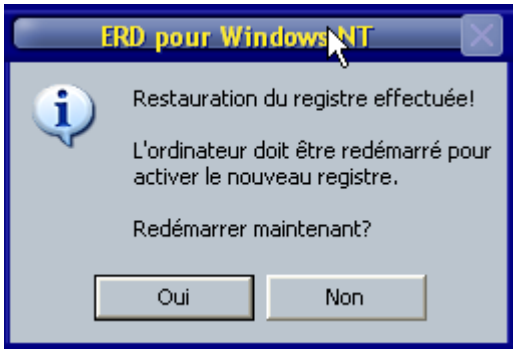
Ouvrez votre Explorateur à l'endroit où est créé votre sauvegarde, dans notre cas C:\Erunt\(date de la sauvegarde)\
Cliquez ensuite sur ERDNT.EXE.

Cliquez sur "OK".
On retrouve les mêmes options que pour la sauvegarde :



Cliquez sur "OK" ---> la restauration commence :





Et voila le travail, la restauration est terminée, redémarrez simplement votre ordinateur.
Attention, Erunt ne sauvegarde pas les stratégies de groupe si elles existent (utilisation de gpedit).

Utilisez Erunt en cas de crash système
Ne peut s'appliquer que si une sauvegarde Erunt existe. On va simplement recopier les bons fichiers en lieu et place de ceux qui sont corrompus sur le système.
Démarrer votre système en mode console de récupération (voir Installation de la console de récupération pour plus de détails) et copiez vos fichiers :
copy c:\Erunt\(date de la sauvegarde)\system c:\windows\system32\config\system
copy c:\Erunt\(date de la sauvegarde)\software c:\windows\system32\config\software
copy c:\Erunt\(date de la sauvegarde)\sam c:\windows\system32\config\sam
copy c:\Erunt\(date de la sauvegarde)\security c:\windows\system32\config\security
copy c:\Erunt\(date de la sauvegarde)\default c:\windows\system32\config\default
copy c:\Erunt\(date de la sauvegarde)\Users\0000001\ntuser.dat c:\Documents And settings\Session\ntuser.dat
- Télécharger Erunt sur Zebulon
- Le site officiel
Dans la même série, l'auteur de Erunt a créé un logiciel d'optimisation registre : NTREGOPT. Vous pouvez l'utiliser avant d'effectuer votre sauvegarde, il réduit la taille du registre et vous oblige à redémarrer le système pour que l'optimisation soit effective.
- Téléchargez NTREGOPT sur Zebulon
Pour sauvegarder le registre, il existe d'autres logiciels : WinRescue XP en fait partie, l'inconvénient est qu'il s'agit d'un shareware (payant).
Vous pourrez néanmoins le trouver ici.
On peut également sauvegarder le registre en utilisant les points de restauration système (uniquement sur XP), mais c'est un autre sujet qui ne sera pas abordé ici.

Le registre Windows

La base de registre à la loupe

Les clés à surveiller

La lutte contre les malwares fait rage, il est important de connaître les clés névralgiques de son système et de faire une vérification de temps en temps. Malheureusement la liste s'agrandit de jour en jour ! Voici la liste des clés les plus connues où l'on peut trouver des entrées néfastes.

Démarrage automatique

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_USER\S-1223-etc\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\S-1234-etc\Software\Microsoft\Windows\CurrentVersion\RunOnce

Menu démarrer -> Programmes --> Démarrage

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Application d'ouverture UserInit

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Appinit_Dlls

Addons Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\shell Extension\Approved
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskSheduler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore\Browser Helper Object
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore\ShellExecuteHooks

Démarrage de l'environnement
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\Shell

Autres endroits susceptibles de contenir des entrées néfastes
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\Load
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Scripts\Logon
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Scripts\Logon

Heureusement, il existe des outils spécifiques qui aident bien dans cette démarche et permettent de vérifier ces clés d'un seul coup d'oeil, c'est le cas par exemple de HijackThis ou d'Autoruns que nous allons découvrir dans le chapitre suivant.

Les autres outils dédiés au registre

De nombreux logiciels existent pour modifier, nettoyer, dégraisser le registre, certains étant plus spécialisés que d'autres. L'intérêt de ces outils réside dans le fait que vous n'ouvrez pas le registre, les logiciels se chargent de tout (en principe). Mais attention tout de même à ne pas cocher n'importe quoi, à trop vouloir optimiser, on peut facilement arriver à obtenir l'inverse du résultat escompté. Voici une liste non exhaustive des plus connus.

Optimisation complète

De nombreux logiciels existent dans cette catégorie, ils permettent d'optimiser le système, de gagner en rendement ou encore de modifier l'apparence de Windows. Chacun des ces logiciels mériterait un article tellement leurs options sont nombreuses.

TuneUP

TuneUp Utilities® 2004 optimise les performances de votre ordinateur, élimine les problèmes et permet une adaptation simple du système à vos besoins personnels.
Ce logiciel est shareware (payant).
Site officiel

TweakXP

Ce logiciel est la réunion de plusieurs utilitaires qui vous permettront de personnaliser, configurer et optimiser à souhaits Windows XP. Il va vous aider à modeler comme vous l'entendez votre système d'exploitation mais aussi à accroître ses performances en terme de rapidité. Ne nécessitant aucune connaissance particulière, il s'adresse aussi bien aux débutant qu'aux initiés.
Ce logiciel est shareware (payant).
Téléchargez TweakXP sur Zebulon

X-Setup

X-Setup a de nombreux avantages qui font de lui "*L'outil ultime pour modifier les paramètres cachés du système*". Il fonctionne sur toutes les versions de Windows (y compris Windows XP), est léger, facile à utiliser, évolutif et puissant. Il couvre de nombreux aspects de votre ordinateur et a plus d'option que n'importe quel autre tweaker. Ce logiciel est Freeware (gratuit).
Télécharger X-Setup sur Zebulon
Site officiel
Le site français

Microsoft PowerToys Windows XP

Quelques outils Microsoft bien pratiques.
Télécharger PowerToy XP sur Zebulon
Site officiel

Désinfection

HijackThis

S'il fallait choisir un seul logiciel qui permet de désinfecter un système, c'est bien celui-ci tellement ses qualités sont importantes. Bien sûr, il faut avoir quelques compétences pour être capable d'interpréter les diverses informations données, mais quel temps gagné pour faire la chasse aux intrus ! Vous pouvez poser toutes vos questions ou demander une étude de vos logs HijackThis sur le forum sécurité de zebulon. Voici un lien très détaillé sur le sujet : Apprendre à utiliser HijackThis par ipl_001.
Ce logiciel est Freeware (gratuit).Télécharger HijackThis sur Zebulon
Télécharger le patch français pour HijackThis sur Zebulon
Site officiel

Spybot Search & Destroy

L'anti-spyware par excellence, ce logiciel recherche directement les valeurs des spywares et autres malwares dans la base de registre et les supprime. Il a d'autres arguments tout aussi convaincants. Ce logiciel est Freeware (gratuit).
Tutorial sur Spybot-S&D
Télécharger Spybot Search & Destroy sur Zebulon
Site officiel

Surveillance

Autoruns

Pour obtenir une vue complète de tout ce qui se lance automatiquement dans le système, par catégorie. Cet outil est un excellent complément à Hijackthis. Ce logiciel est Freeware (gratuit).
Site officiel

Regmon

Surveille en temps réel l'activité du registre. Avec les outils statiques, vous pourrez voir quelles valeurs et clefs d'enregistrement ont changé.
Ce logiciel est Freeware (gratuit).
Site officiel

Regshot

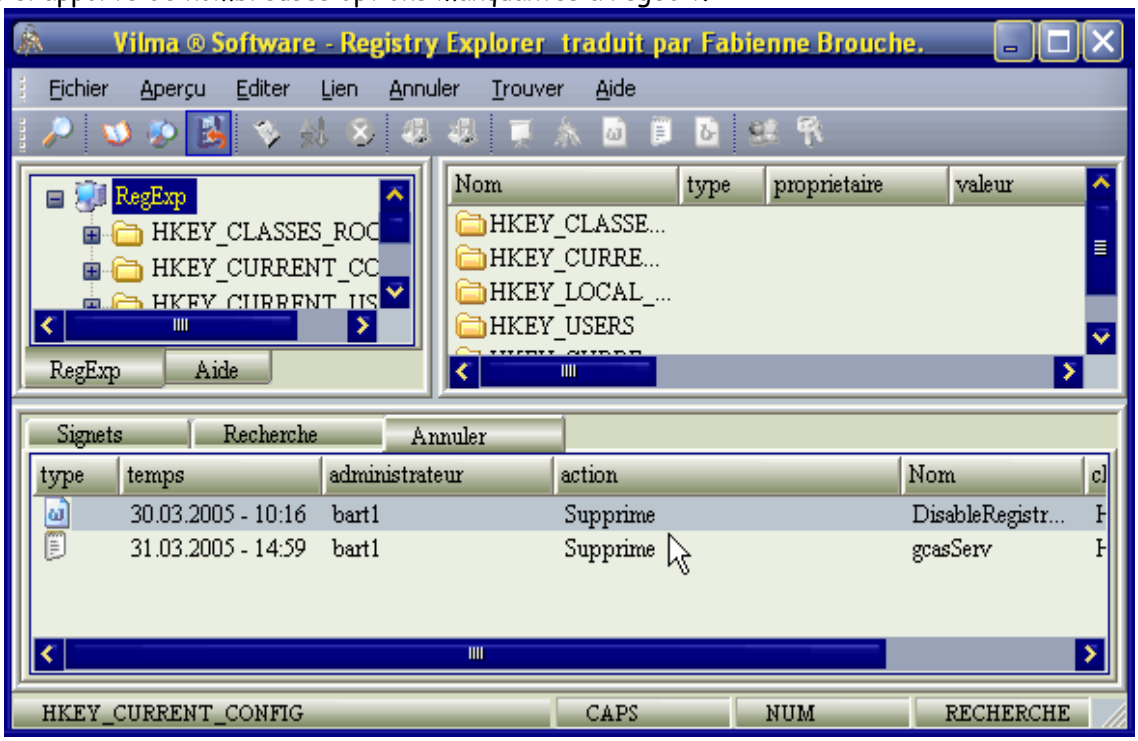
C'est un programme qui compare votre base de registre en prenant des clichés de votre registre à des moments différents. Le rapport des changements peut être produit au format HTML et contient une liste de toutes les modifications qui ont eu lieu entre les deux clichés.
Ce logiciel est Freeware (gratuit).
Site officiel
Il existe de nombreux autres logiciels tout aussi performants, il est difficile de faire un point complet tellement ils sont nombreux. Il s'agit souvent d'utilitaires faits par des internautes avides de programmation et d'optimisation pour améliorer les qualités intrinsèques de nos systèmes d'exploitation. En voici la dernière preuve, celui créé par un membre de Zebulon (Sebdraluorg) qui reprend un grand nombre de nos astuces : Zeb-Utility.

Editeurs de registre alternatifs

Regedit permet de faire pas mal de choses, mais un autre éditeur peut s'avérer utile dans certaines circonstances (voir le début du sujet). C'est pourquoi nous pouvons avoir recours à des outils comme Vilma Registry Explorer, RegAlyzer ou encore Registrar Lite. Mais intéressons nous au premier.

Vilma Registry Explorer 1.6.0

Son interface ressemble à celle de l'éditeur de registre de Windows. Ce logiciel vous permet d'effectuer vous même vos propres manipulations en sauvegardant chacune d'elles. A noter qu'il ne s'agit pas d'un nettoyeur de registre. Il comporte un moteur de recherche, un gestionnaire de signets, l'import / export de la base de registre au format propriétaire .Rpx ou plus commun .Reg. La barre d'outils permet de créer d'un simple clic des clés supplémentaires, en fonction de leur format : Dword, binaire, texte. Un historique est présent afin de faciliter le retour en arrière en cas d'erreur. Ce logiciel apporte de nombreuses options manquantes à regedit.



Comme vous pouvez le remarquer sur cette image, il existe une partie supplémentaire, avec des options avantageuses, telles que la visualisation des modifications déjà effectuées sur le registre. Vous pouvez à tout moment revenir en arrière, mais également mettre des clés dans la partie "Signets" que vous avez l'habitude de surveiller, etc. Un excellent produit pour les aficionados du registre.
Télécharger Vilma Registry Explorer sur Zebulon
Le site officiel : Vilma Software
Télécharger le pack français pour Vilma Registry Explorer
Le registre est un sujet important, en faire le tour pour apprendre les commandes reste facile. Pour aller plus loin sur le sujet, voici quelques liens qu'il est toujours utile de connaître :

- Site jurixt
- Site Comment ça marche
- Site de Laurent Gébeau (MVPS)
- Site Secretswindows.com
- Site leregistre-fr.net