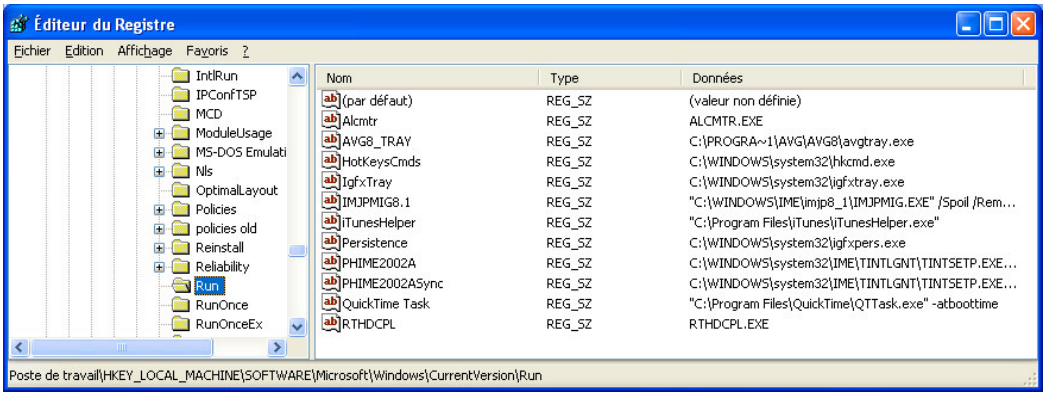
ANNEXE IV : anomalies de la Base de Registre

Avant tout, vous faîtes une remarque intéressante : comment se fait-il que nous n'ayons pas accès à la Base de Registre (avec REGEDIT) et que les virus, eux, ont accès

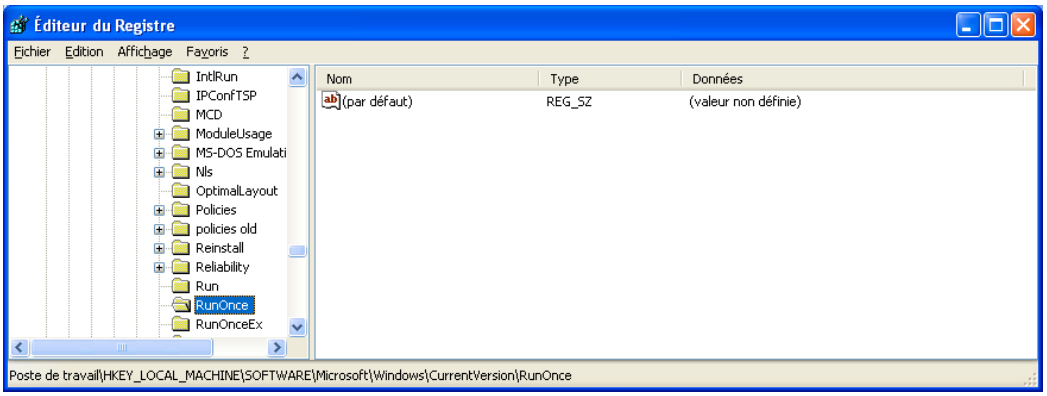
Tout le système Windows repose sur la bonne entente entre application. La sécurité n'existe pas. Elle est maintenue par le fait que chaque organe « regarde » s'il a le droit avant de faire une action. Or, le Virus, lui, ne demande pas s'il a le droit …
D'ailleurs, au besoin, il existe un REGEDIT qui ne demande pas les autorisations pour se lancer…

Les lieux de démarrage :

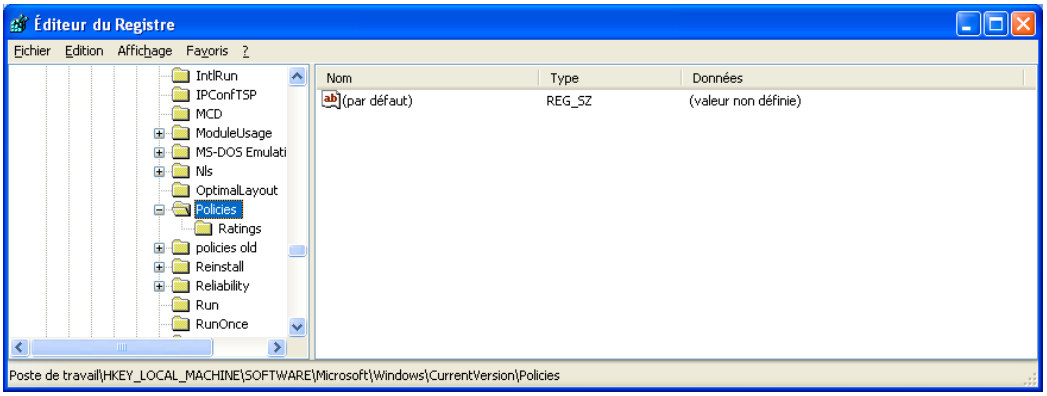


Logiciels qui se lancent quelque soir le User (après ouverture de session).

Un virus lance, dans 99% des cas, un programme qui se trouve dans les fichiers temporaires d'internet explorer.



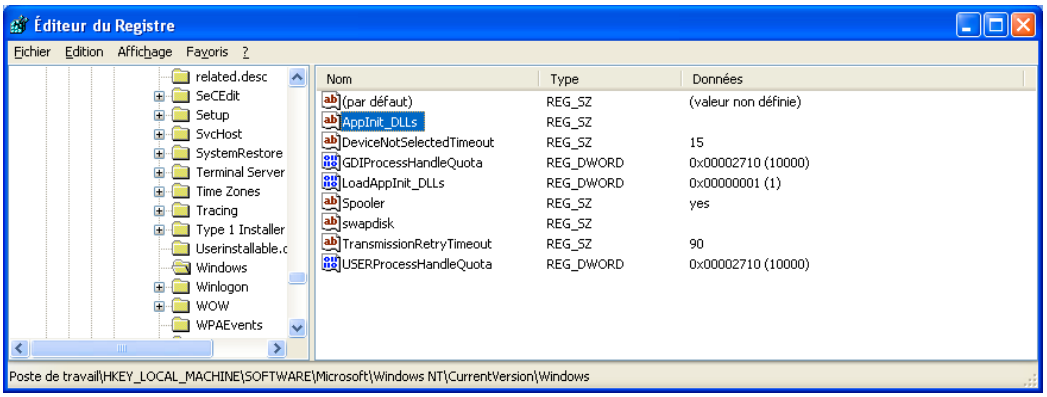
Lancement d'application lors du démarrage puis l'entrée est automatiquement supprimée afin que le dit logiciel ne se relance pas encore une fois. A l'origine, ca permet à des logiciels de se post-configurer au redémarrage.
Beaucoup de virus s'inscrivent ici au cas où ils auraient été trouvés dans la section « RUN ».



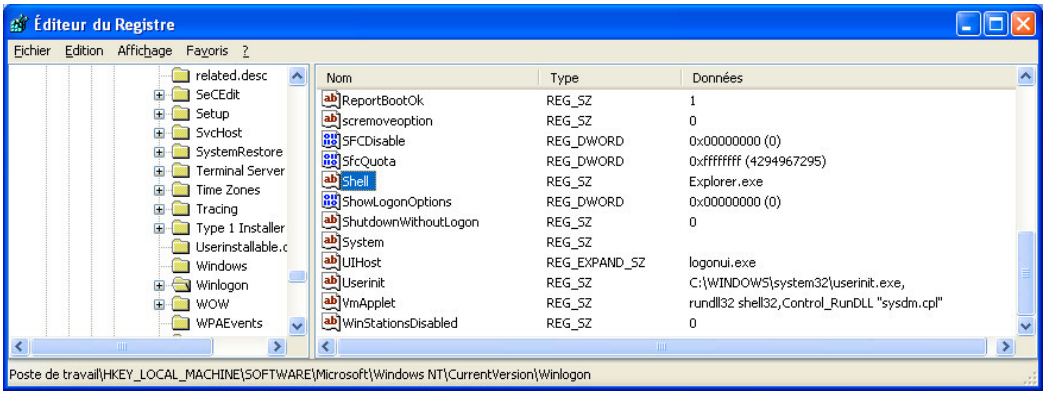
Ici se trouvent tous les blocages : accès à la base de registre, fond d'écran, écran de veille troublant non-supprimable ! ! !

Il suffit de renommer la clef – et Hop !

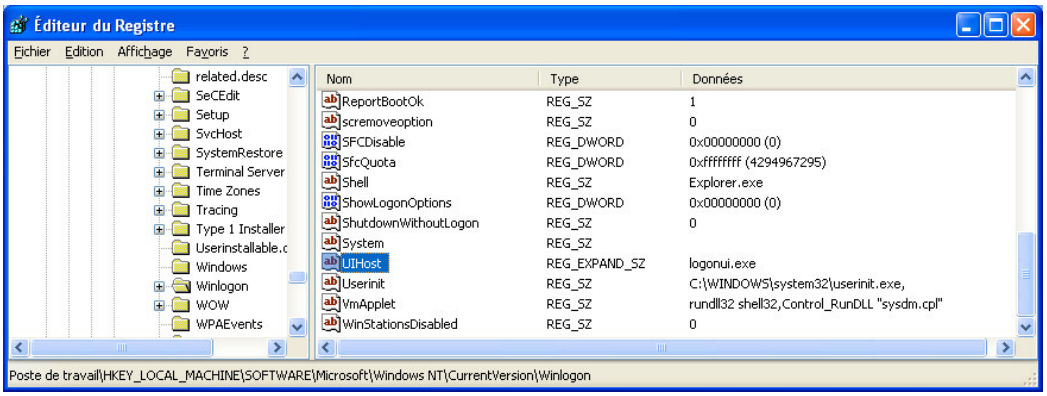
Un Hacker cache ses actions ici pour ne pas être repéré.

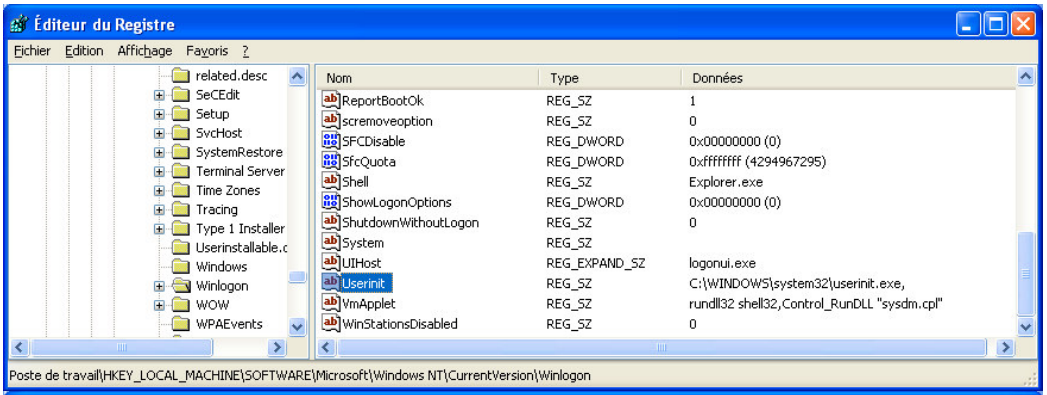


Ici se lancent toutes les DLL de virus.
Un EXE est vu dans la liste des tâches – mais une DLL non ! !

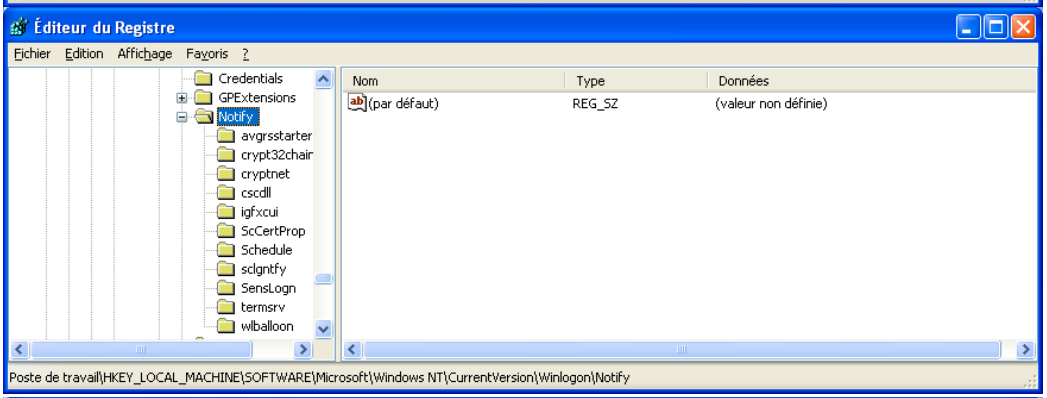


La ligne dans le fichier « win.ini » Shell fait la même chose : choisir le programme principal de Windows – ici c'est Explorer (celui qui met les icônes + menu démarrer).
En ajouter le nom d'un programme après explorer.exe, ce programme se lancera à l'ouverture de session (avant tous les autres).
Ici, le logiciel qui valide le User.
En l'enlevant, il n'est plus possible de se connecter – fermeture de session immédiate à l'ouverture !



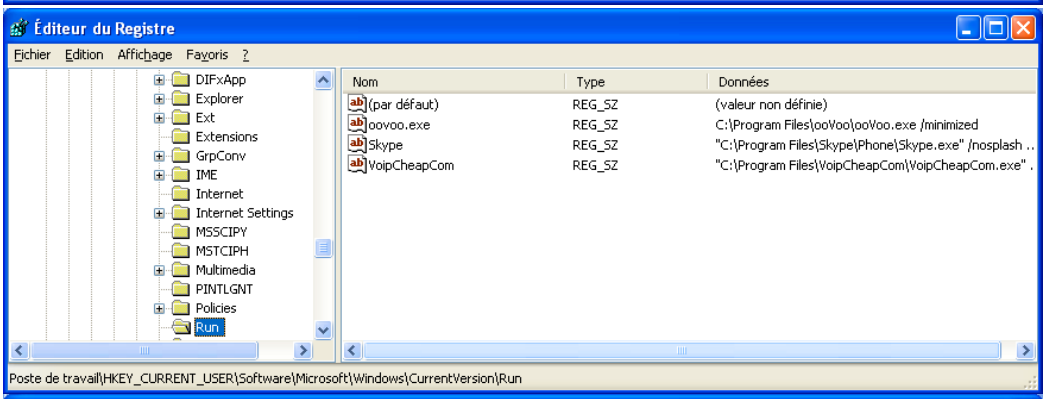


Userinit.exe est le programme qui lance les droits du User.
En ajouter des programmes derrière la virgule, les programmes se lanceront à l'ouverture de session (avant même les icônes de windows)



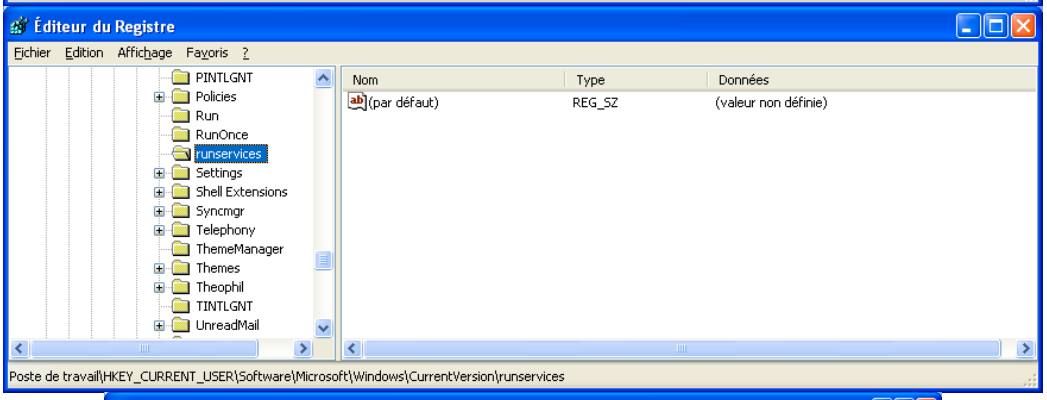
Dans la zone « Notify » sont placés les virus qui se redéclancheront sur un événement (à la fermeture de windows pas exemple).

Facilement reconnaissable – lorsque l'ordi met trop de temps à s'arrêter.



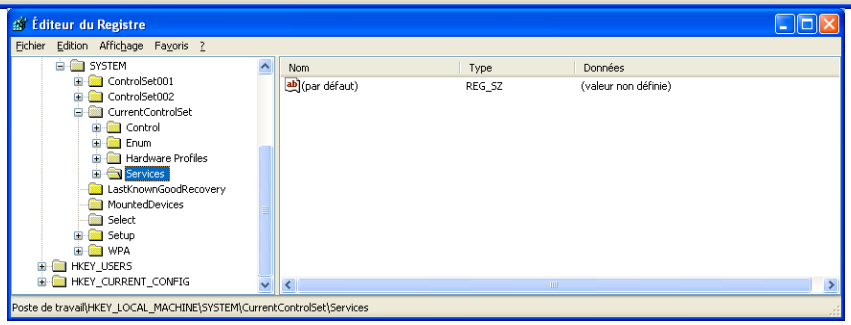
Pour chaque USER, les clefs sont presque identiques

Run, Runonce et policies



Une veille section qui permettait sous windows 95 et 98 de lancer des services.

Cette section marche très bien sous windows XP – non documentée, cette section est utilisées très rarement.

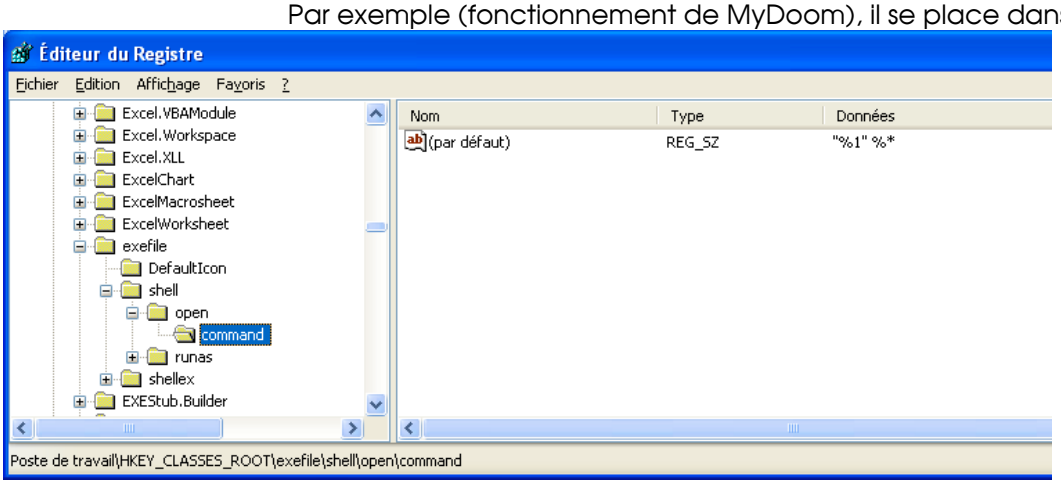


Lancement d'un service.

Attention, il n'y a aucun contrôle de la part de Windows.

Bien sûr cette liste n'est pas exhaustive.

Par exemple (fonctionnement de MyDoom), il se place dans



et oui, aussi absurde que cela puisse paraître, lorsque vous demandez de lancer un programme par Windows

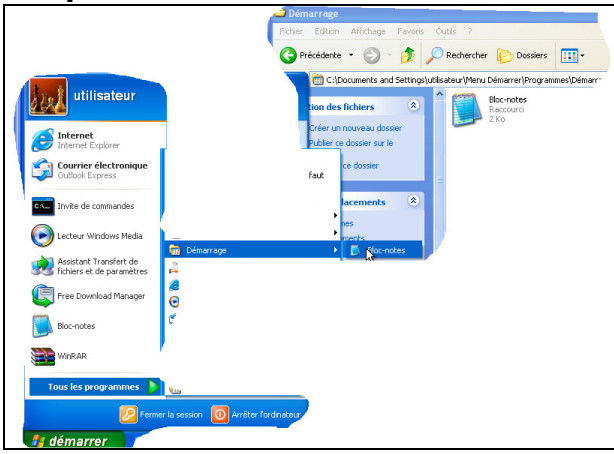
il exécute la commande « %1 » %* ce qui veut dire « le programme demandé » suivi des paramètres passés. En clair, Mydoom remplace cette ligne par : progPirate %* ce qui veut dire qu'à chaque lancement de programme, Windows lance ProgPirate afin que LUI (le virus) lance le programme demandé !

Fort non ?

le démarrage par un fichier

Si le pirate souhaite lancer une programme ou une DLL, il peut aussi le placer dans le dossier de démarrage. S'il cache le fichier, ce lancement devient invisible !

Exemple de lancement :



Ici, que le fichier raccourci soit placé dans le dossier « Démarrage » ou dans le menu, c'est pareil. Tous les menus sont des fichiers (pas forcément des liens – ils peuvent être des exécutables ou virus !)

En suite, il est possible de lancer un programme d'installation de virus sur la session de dépannage (mode sans échec).