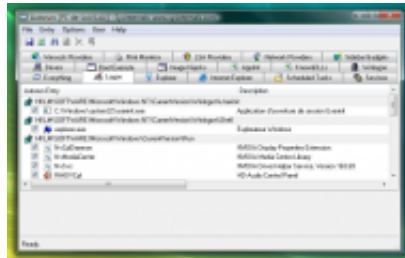


Réparez 90% des problèmes informatiques avec un seul outil



agrandir la photo

Au lancement, le programme analyse automatiquement toutes les zones clés du système, toutes celles qui - d'une manière ou d'une autre - conduisent à une exécution de programme à l'insu de l'utilisateur.

Les différents éléments trouvés sont alors classés par thèmes, chaque thème ayant son onglet:

- **Drivers** : Liste des pilotes installés dans le système et donc lancés à chaque démarrage du PC
- **Boot Execute** : Programmes lancés au démarrage du Noyau (au tout début du démarrage du PC, donc)
- **Image Hijack** : Options d'exécution liées à certains formats d'image (vecteur d'attaque de spywares)
- **Applnit** : Zone d'initialisation, en avance de boot, de bibliothèques DLL
- **KnownDLLs** : Liste des bibliothèques DLL connues du système (enregistrées dans le système)
- **WinLogon** : Liste des applications lancées sur l'écran d'ouverture des sessions
- **Logon** : Liste des applications lancées automatiquement une

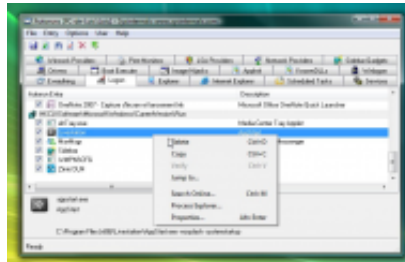
fois l'utilisateur authentifié

- **Explorer** : Liste des applications/extensions qui viennent se greffer sur l'explorateur Windows
 - **Internet Explorer** : Liste des add-ons, barres d'outils et spywares greffés sur Internet Explorer
 - **Scheduled Tasks** : Liste des programmes lancés par le planificateur de tâches de Windows
 - **Services** : Liste des "*Services NT*", autrement dit des programmes greffés au coeur du système
 - **Winsock Providers** : Liste des programmes infiltrés dans les couches Internet de Windows
 - **Print Monitors** : Liste des programmes greffés sur le système d'impression de Windows
 - **LSA Providers** : Liste des programmes insérés dans les couches de communication de Windows
 - **Network Providers** : Liste des programmes présents dans les couches réseau
 - **Sidebar Gadgets** : Liste des applications présentes dans le Volet Windows sous Vista
- L'onglet **Everything** regroupe toutes les entrées trouvées en un seul écran.

Note: Rappelons qu'une DLL est un ensemble de routines conçues pour être partagées entre plusieurs applications.

Voyons maintenant comment désactiver un programme pour empêcher son chargement automatique.

Réparez 90% des problèmes informatiques avec un seul outil



agrandir la photo

D'une manière générale, un "*malware*" peut s'infiltrer dans n'importe laquelle des catégories vues précédemment pour réaliser ses actes malveillants.

Toutefois, en cas de fenêtre intempestive, on étudiera en priorité les onglets Internet Explorer, Logon, Winsock et LSA Providers.

En cas de conflit entre applications, on s'attardera davantage sur les onglets KnownDlls, Explorer, Logon, Services, Drivers et Network Providers.

Les plantages de l'explorateur Windows, eux, trouvent souvent leur origine dans les onglets Logon et Explorer.

Les problèmes de plantages d'Internet Explorer se résolvent généralement en désactivant les entrées dans l'onglet Internet Explorer.

Les lenteurs de démarrage et d'extinction trouvent leur solution dans les onglets WinLogon, Logon, Services et Drivers.

Pour repérer une application louche, vous pouvez vous appuyer sur la colonne **Publisher** (ce qui n'est pas signé "*Microsoft Corporation*" n'appartient sûrement pas au système) et sur la colonne **Description**.

Pour désactiver une entrée auto-exécutée au démarrage, il suffit de décocher la case qui précède sa ligne dans la fenêtre principale d'Autoruns.

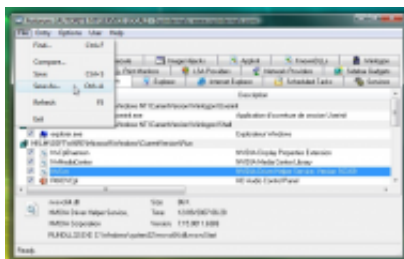
En fait, n'hésitez pas à décocher tout ce qui vous semble suspect. Car si vous vous trompez, vous pourrez toujours venir les re-cocher plus tard... Toutefois, ne désactivez que ce qui vous semble louche; ne désactivez pas tout et n'importe quoi sans réfléchir car alors le système pourrait ne pas redémarrer ou présenter de nombreuses anomalies au redémarrage!

Pour valider les manipulations, redémarrez le PC.

Note: pour désactiver certains spywares, il peut être nécessaire de lancer Autoruns en démarrant le PC en mode sans échec (touche **[F8]** à l'allumage du PC) .

Utilisateurs Avancés: En décochant la case liée à chaque entrée, on ne fait que désactiver le lancement automatique. En cliquant du bouton droit sur une entrée, un menu contextuel donne accès à différentes options comme "*Verify*" (pour vérifier que l'action est bien prise en compte) ou "*Delete*" pour supprimer l'entrée définitivement.

Réparez 90% des problèmes informatiques avec un seul outil



agrandir la photo

Avant de désactiver une entrée auto-exécutable, vous pouvez tenter d'obtenir des informations sur celle-ci en appuyant sur la combinaison de touches **[Ctrl]+[M]** (ou en allant sur "Search Online" dans le menu "Entry"). Cela lance automatiquement une recherche sur cet élément via le moteur Live Search.

Mais il existe une autre solution pour se faire aider efficacement! Le logiciel permet de sauvegarder une vue de votre système, sous la forme d'un fichier que vous pourrez ensuite envoyer par email à un ami expert afin qu'il vous aide et vous guide dans le nettoyage du système.

Pour générer un tel fichier:

- Ouvrez le menu **File**
- Cliquez sur **Save AS**
- Sauvegardez le fichier sur le bureau par exemple.