

<http://www.kachouri.com>

## Un Anti-Rootkit est-il 100% efficace ?

**Tutoriel réalisé par:** Mehdi Kachouri **Ajouté le** 07 Octobre 2006

Comment tester le logiciel anti-rootkit de Sophos

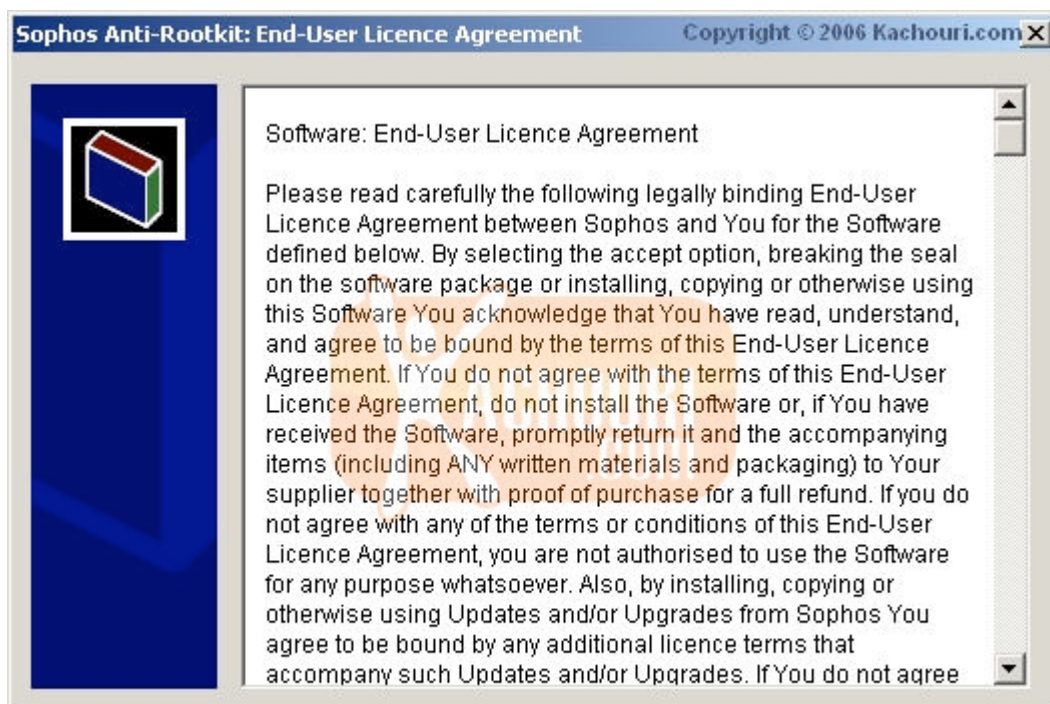
### Introduction de Sophos Anti-Rootkit

Le "rootkit" Windows, est un code malicieux vraiment complexe qui se greffe sur le noyau même du système d'exploitation et très difficile à détecter et à éradiquer. Il est ainsi capable de prendre le contrôle total d'un PC sans laisser de trace. Sa détection est difficile, parfois même impossible tant que le système fonctionne. Une fois en place, le rootkit est véritablement le maître du système. À ce titre tous les programmes, y compris les antivirus et anti-spywares, doivent passer par lui avant de faire quoi que ce soit. Ils ne peuvent donc se fier à aucune information collectée sur le système. En réalité, les rootkits sont loin d'être une nouveauté; ils existent sous Linux depuis très longtemps. L'idée de ce tutorial n'est pas de vous apprendre à créer un rootkit, ou de le mettre en place mais plus de tester votre système afin de savoir s'il existent... Bien évidemment avec des outils afin que toute personne puisse les détecter même si la tâche reste difficile et délicate.

<http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html>

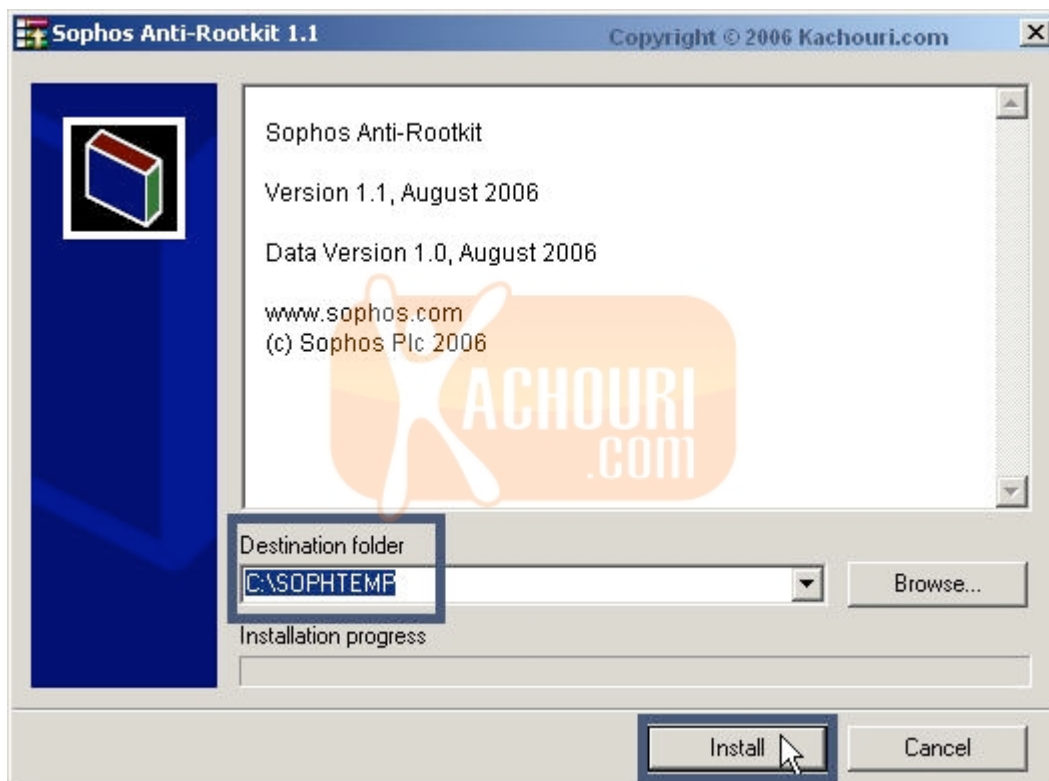
### 1. Installation de Sophos Anti-Rootkit

Une fois que vous vous êtes rendu sur le site officiel, après avoir téléchargé le logiciel et lancé l'exécutable "**sarsfx.exe**" vous aurez ceci :

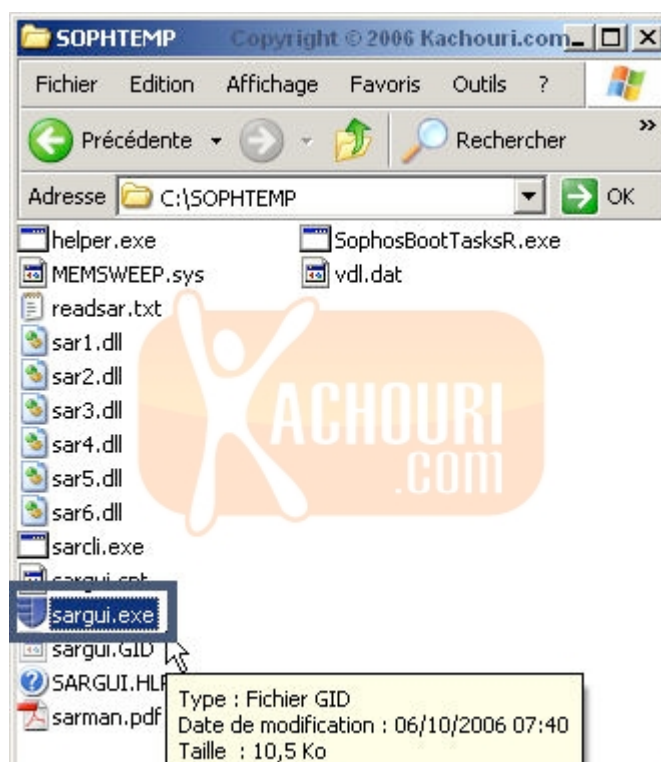




Il vous suffira alors de cliquer sur "**Accept**" pour lancer l'installation et en "**Acceptant**" vous serez ainsi d'accord avec les termes de la licence "**Sophos End-User Licence Agreement for Anti-Rootkit Tool**". Une fois ceci effectué vous obtiendrez ceci :



Vous apercevrez ainsi que "**Sophos Anti-Rootkit 1.1**" s'installera à la racine de votre disque dur dans le dossier du nom de "**SOPHTEMP**", puis cliquez sur "**Install (Installer)**". Une fois ceci effectué, vous aurez la fenêtre qui se fermera uniquement, c'est pour cette raison que nous avons bien pris note que "**Sophos Anti-Rootkit 1.1**" s'installera dans le dossier qui se trouve ici : "**C:\SOPHTEMP**", vous n'aurez plus qu'à vous rendre dans ce dossier :



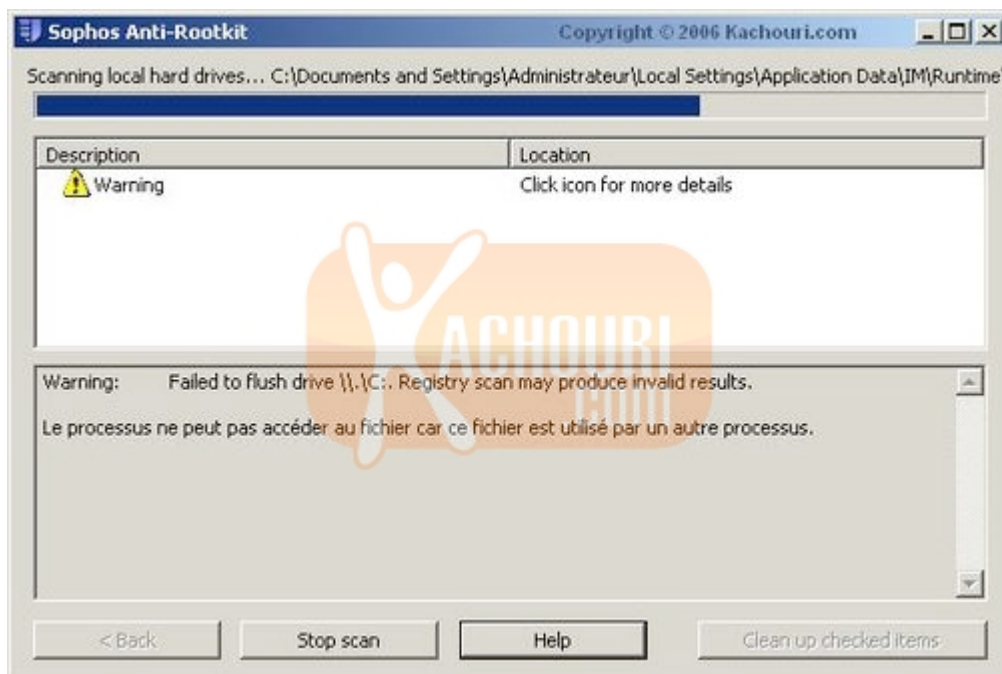


## 2. Utilisation de Sophos Anti-Rootkit

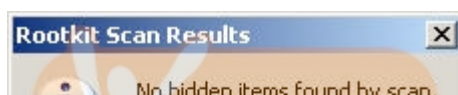
Pour lancer "**Sophos Anti-Rootkit 1.1**", vous devrez vous rendre dans le dossier "**C:SOPHTEMP**" et cliquer sur "**sargui.exe**", ou créer un raccourci bureau du fichier "**sargui.exe**", on obtiendra alors ceci :



Il vous suffira alors de cliquer sur "**Start scan (lancer le scan)**" pour vérifier si votre système contient à la base un Rootkit, vous obtiendrez alors ceci :



Vous pouvez à tout moment stopper le scan en cliquant sur "**Stop scan**", une fois que votre système sera vérifié, vous aurez ce message :

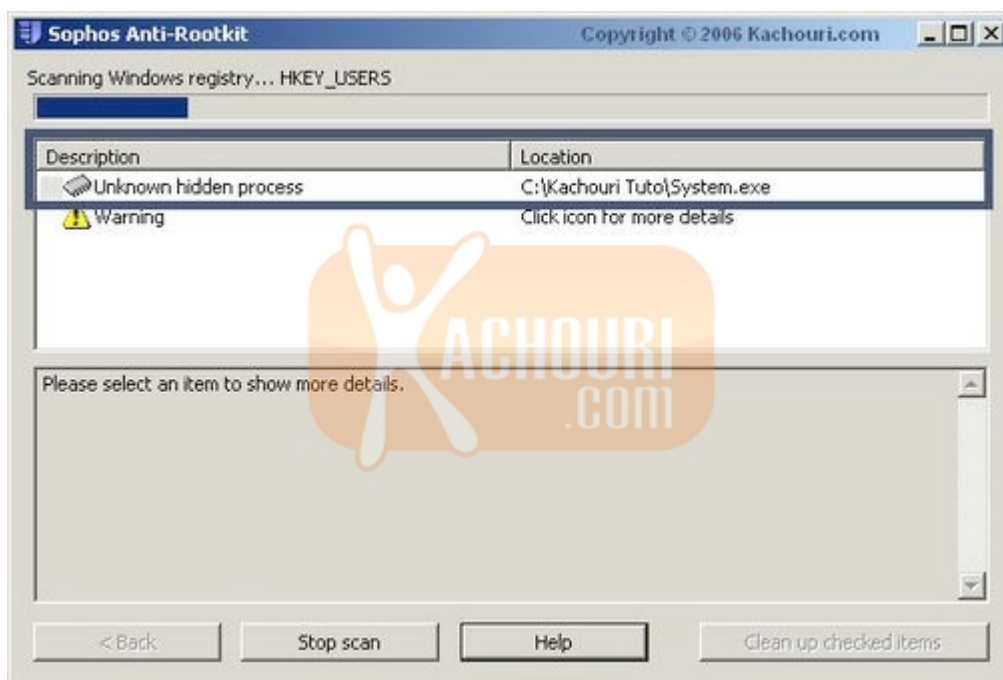




Voilà une bonne nouvelle, vous n'avez pas de Rootkit détecté par "**Sophos Anti-Rootkit 1.1**".

### 3. Test de Sophos Anti-Rootkit

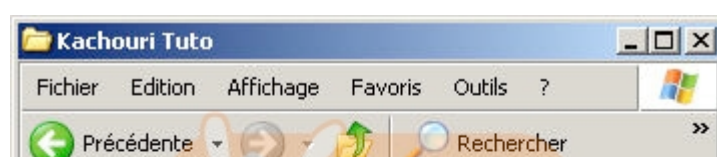
Pour notre test, il nous faut trouver un "**Rootkit**", pour cela une recherche sur un moteur de recherche et nous voilà muni d'un outil pour notre test, nous l'installons à la racine de notre disque dur ici "**C:Kachouri Tuto**" et nous le lançons (il est bien évident que ceci est juste pour tester et qu'il faut savoir ce que l'on fait, ne lancez pas n'importe quoi sur votre pc !). Pour plus d'efficacité nous vérifions qu'il est bien actif, et une fois cette manipulation effectuée, relancez le scan avec "**Sophos Anti-Rootkit 1.1**" logiquement vous devez avoir ceci :



Comme vous le remarquerez "**Sophos Anti-Rootkit 1.1**" a détecté notre "**rootkit**" de test... Et une fois le scan effectué, vous devez avoir un récapitulatif vous indiquant le nombre de "**Rootkit**" détectés, comme ceci :

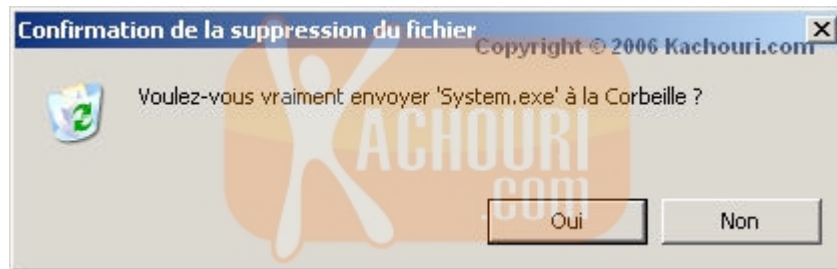


Une fois que vous avez détecté et trouvé un "**rootkit**" sur votre ordinateur, la démarche à suivre est d'essayer de le supprimer, dans la majorité des cas vous ne pourrez pas supprimer directement le fichier car celui-ci sera utilisé par votre système. Si on reprend notre exemple et que je souhaite supprimer directement le fichier du nom de "**System.exe**" qui se trouve dans le dossier "**C:Kachouri Tuto**" comme ceci :





Et que vous cliquez droit dessus puis sur **"Supprimer"** vous aurez ce message :



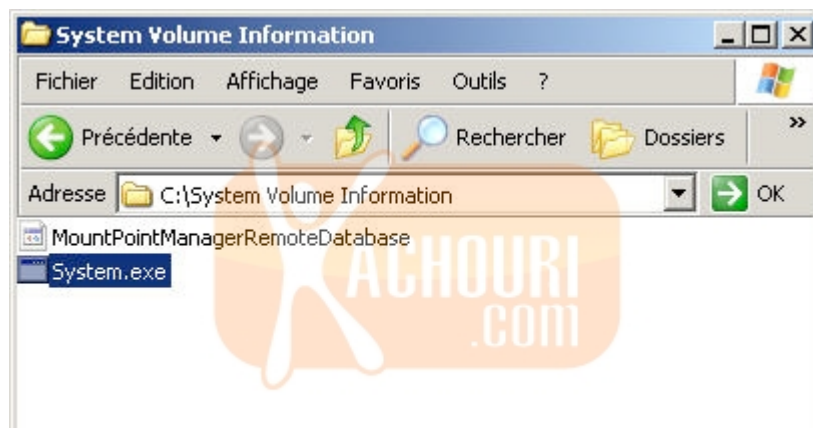
A ce message : **"Voulez-vous vraiment envoyer 'System.exe' à la Corbeille ?"**, nous allons cliquer sur **"Oui"** après quelques instants, on obtiendra alors ceci :

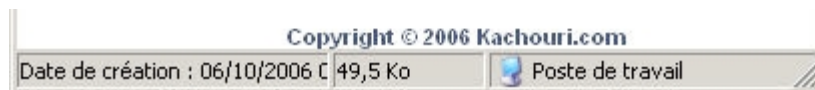


**"Impossible de supprimer System : Accès refusé. Vérifiez que le disque n'est pas plein ou protégé en écriture, et que le fichier n'est pas utilisé actuellement."** Il ne nous est pas possible de le supprimer directement. Rien ne sert non plus de redémarrer car le rootkit sera toujours actif sur votre système. Pour cela si vous ne le connaissez pas, il vous suffit soit d'installer un Anti-virus, mais très peu efficace pour la suppression des rootkit, ou essayer plus de trouver des informations au sujet de ce rootkit sur Internet en recherchant sur un moteur de recherche son nom à défaut de le savoir le nom de son fichier qui est **"System.exe"**, et de récupérer le maximum d'informations pour mieux le supprimer manuellement ou faire appel à des personnes qui maîtrisent un peu plus que vous le sujet afin qu'ils puissent supprimer tous les fichiers sans endommager ni perdre vos données. Et cela peut être très délicat avec les rootkit, qui se logent souvent au coeur du système en utilisant des hook.

#### 4. Faiblesse de Sophos Anti-Rootkit

Si le même fichier est déposé dans le dossier **"C:\System Volume Information"** et bien sûr actif, comme ceci :





Et que vous refaites un scan avec "**Sophos Anti-Rootkit 1.1**", vous vous apercevrez déjà de la faiblesse de faire confiance à un logiciel uniquement, car celui-ci ne le détectera pas et pourtant il est en activité dans la liste des processus. Comme ceci :



Cela nous prouve que "**Sophos Anti-Rootkit 1.1**" ne détecte pas le fichier malveillant lorsqu'il se trouve dans "**C:System Volume Information**".

### Conclusion

En conclusion, il faut vraiment être prudent, et ne pas croire qu'avec un simple logiciel vous allez pouvoir détecter tous les rootkit, car il existera toujours des génies de l'informatique qui seront capables de déjouer les protections et faire en sorte qu'elles soient indétectables par n'importe quel logiciel. Ce tutorial a pour but de prendre conscience de ce phénomène qui prend de plus en plus d'ampleur et infecte aussi de plus en plus de machine à l'insu de ses propriétaires.

Adresse du site internet : <http://www.kachouri.com>

**Toute reproduction partielle ou totale de la présente publication est interdite sans l'autorisation de l'auteur.**