



Exécuter son navigateur Internet dans un espace protégé

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

- 1 Pourquoi faire tourner son navigateur Internet dans un espace protégé ?
- 2 Premiers pas avec Sandboxie
- 3 Remarques finales

1 Pourquoi faire tourner son navigateur Internet dans un espace protégé ?

Une maxime importante dans le domaine de la sécurité :

« Il existe un nombre infini de vulnérabilités dans un système ou programme donné. La plupart ne seront jamais découvertes. » Roger J. Johnston

En effet, plus une application est analysée, plus les experts semblent y trouver de vulnérabilités. De ce fait, il est utile de considérer son browser, programme principal utilisé pour accéder au contenu d'Internet, comme une porte ouverte à tous types d'attaques ou un point d'accès pour de nombreux programmes malveillants. D'où l'idée de faire tourner les applications critiques dans un « bac à sable » ou « sandbox ». Ceci afin de ne causer aucun tort au reste du système.

Une manière assez simple de le faire est d'utiliser un programme gratuit appelé « Sandboxie ». Cet utilitaire est téléchargeable sur le site www.sandboxie.com.

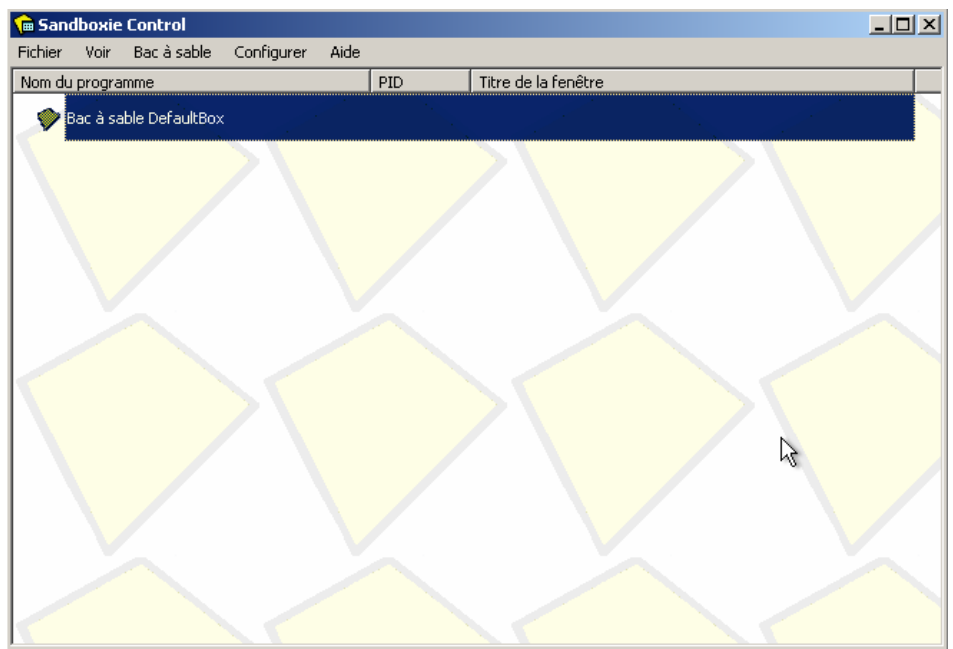


La version gratuite affiche, après trente jours, une fenêtre qui fait la promotion de la version payante. L'utilitaire n'est pas un programme de type shareware, mais bien une version gratuite, qui peut être utilisée dans un cadre privé après cette période.

2 Premiers pas avec Sandboxie

Sandboxie va exécuter les programmes de votre choix dans un espace protégé appelé « bac à sable », « sandbox ». On dira que le logiciel est sandboxé. Physiquement ce bac à sable se présente sous la forme d'un répertoire tampon sur le disque dur, dans lequel seront enregistrées toutes les écritures faites par le logiciel « sandboxé ». À la fin de l'utilisation du logiciel il sera alors aisé de passer un gros coup de râteau virtuel dans le bac à sable et d'effacer tous les changements produits dans le répertoire tampon. Aucune modification n'aura été effectuée sur le disque en dehors du répertoire tampon.

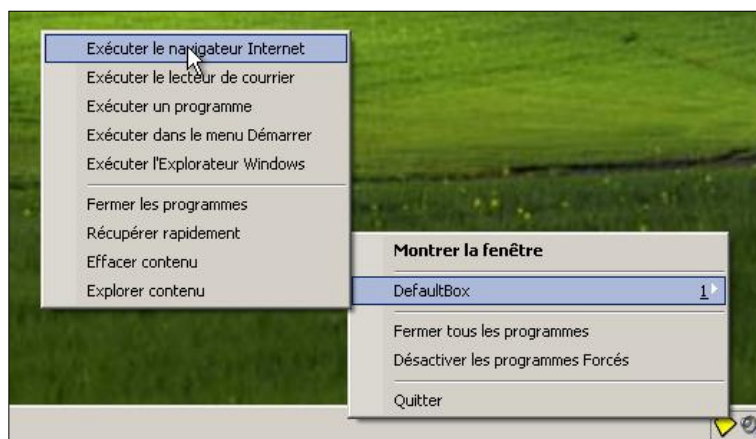
Par défaut Sandboxie crée un bac à sable appelé « DefaultBox ». D'autres bacs à sable sont configurables, mais nous n'entrerons pas dans le détail ici.



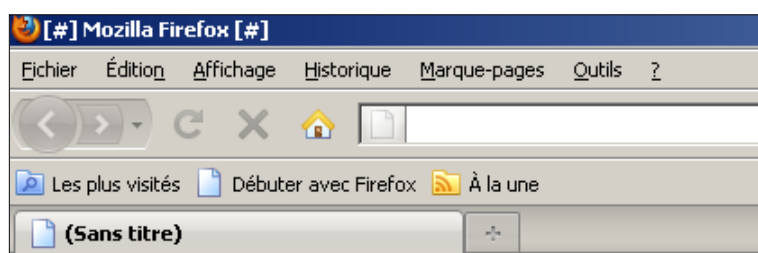
Après installation il se chargera en mémoire automatiquement au démarrage de votre machine.



Pour l'utiliser, il suffit alors de faire un click droit sur l'icône dans le Systray, de choisir son bac à sable (« DefaultBox ») et de cliquer « Exécuter le navigateur Internet ».



Le navigateur par défaut du système s'ouvrira (ici firefox) et les symboles « [#] » entoureront le titre de l'application pour montrer qu'elle est bien « sandboxée ».



Visitez alors tranquillement les pages que vous voulez, tous les changements au système faits par le logiciel « sandboxé » seront appliqués au bac à sable uniquement, donc dans le répertoire tampon.

L'icône de Sandboxie constellée de petits points rouges montre qu'un logiciel est en cours d'utilisation dans un bac à sable.



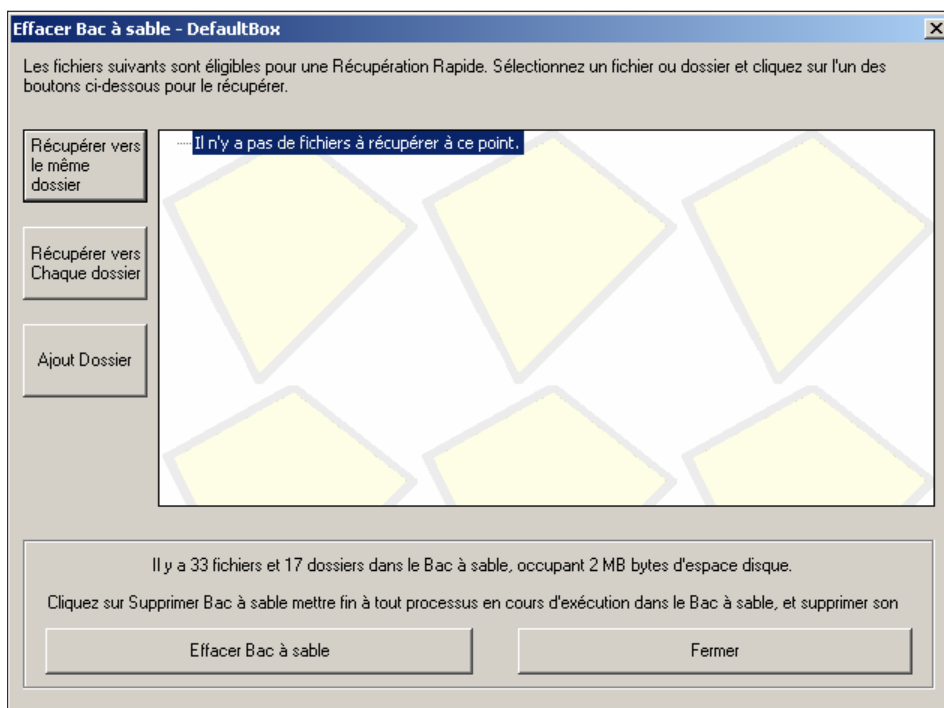
Une fois l'utilisation du browser terminée choisissez l'option « Effacer contenu » pour effacer tous les changements opérés par le browser, même ceux qui auraient été opérés par des codes malicieux voulant exploiter des vulnérabilités. Il faut savoir que l'historique de navigation ainsi que toutes autres traces laissées par le navigateur seront aussi effacés.



Une fenêtre vous proposera alors de sauver des fichiers éventuellement téléchargés avant l'effacement complet des données.

Après le click sur « Effacer Bac à sable » votre système sera de nouveau à l'état initial, c'est-à-dire comme avant le lancement du navigateur.

L'opération pourra être renouvelée autant de fois que nécessaire.



3 Remarques finales

- Sandboxie permet aussi de mettre d'autres logiciels dans le bac à sable et est ainsi très pratique pour tester des applications, les installer dans un bac à sable, tout en gardant son système à l'abri de changements indésirables.
- Parfois il est difficile de savoir si l'on peut ouvrir un document ou pas. Par exemple, un ami vous envoie un fichier pdf ou powerpoint issu d'une source inconnue. Vous pouvez faire confiance à votre ami, mais pouvez vous faire confiance au créateur du document en question ?

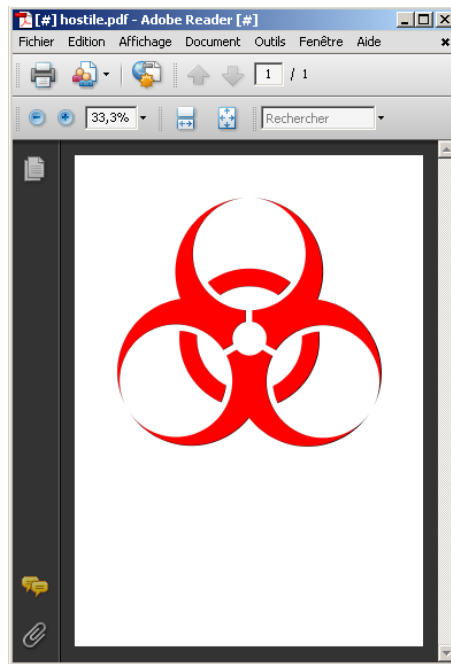
Pour éviter un éventuel souci :



Faites un click droit sur le fichier et choisissez l'option « Exécuter sandboxé » dans le menu contextuel.



Cela ouvrira le document dans un bac à sable, protégeant ainsi votre système en cas de problème.



Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu