Antivirus ClamWin Portable

Tutorial d'une solution antivirus portable

ClamWin Portable est un antivirus complètement autonome qui ne nécessite aucune installation. L'intérêt d'une telle solution est de proposer un outil de vérification supplémentaire qui n'entre pas en conflit avec votre antivirus résident déjà installé sur votre machine. De plus, le programme peut facilement être copié sur une clé USB afin de scanner et décontaminer une autre machine. Nous verrons ici la naissance du projet de cette version dite "portable" et, en seconde partie, nous présenterons l'utilisation de l'antivirus au travers d'un tutorial complet.

A l'origine du projet

ClamWin Portable est une solution antivirus pour Windows 98/Me/2000/XP/2003 basée sur ClamWin AntiVirus. Ce dernier est un projet Open Source développé à l'origine sous Unix puis porté par la suite sous notre très cher Windows. On notera que ClamWin est lui même basé sur un autre projet libre nommé OpenAntiVirus mais qui semble aujourd'hui au point mort.
Bien que ce projet n'en soit qu'au début de son développement, il semble suivre une belle évolution qui lui permettra sans doute de rivaliser à l'avenir avec des projets commerciaux.
On ne peut donc que saluer une telle initiative car ClamWin est aujourd'hui le seul projet actif d'antivirus libre !

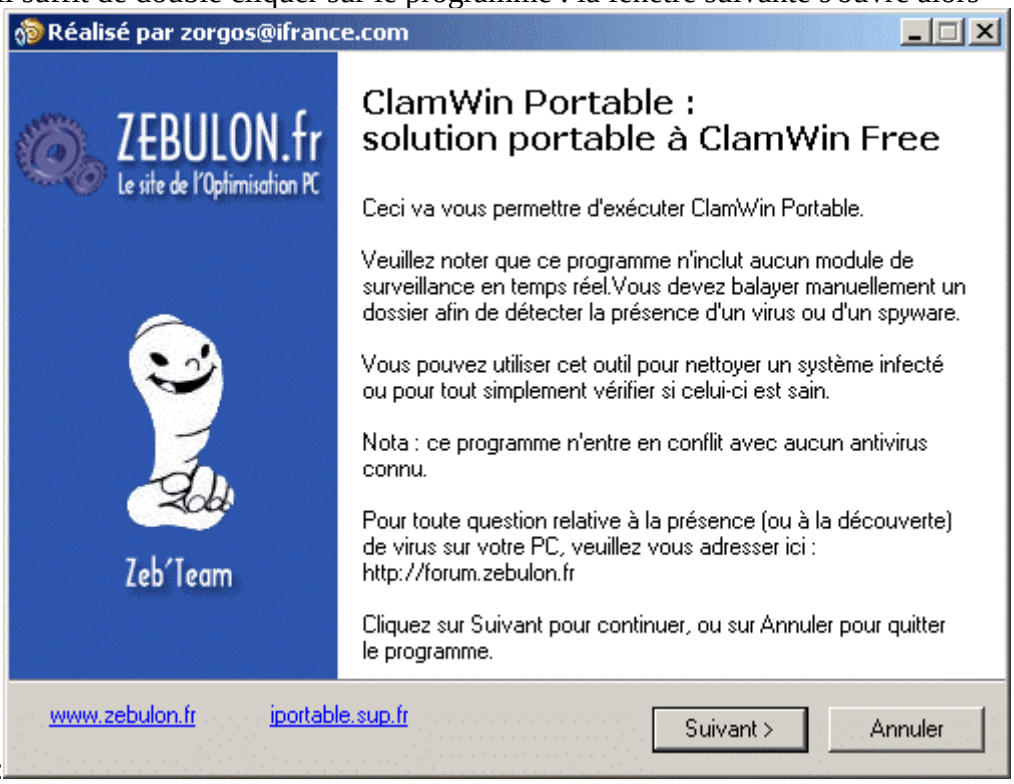
Fort de ce constat, grenouille a développé une version totalement autonome de ce logiciel : ClamWin Portable. Les intérêts d'un tel programme sont multiples :

- l'antivirus est composé d'un seul et unique fichier, aucune installation n'est nécessaire
- cette solution est un outil de vérification supplémentaire
- ClamWin Portable n'entre pas en conflit avec votre antivirus résident
- ClamWin Portable peux être facilement copié sur un support externe comme une clé USB afin de vérifier et/ou désinfecter un ordinateur
- si votre machine est déjà infectée par un virus qui empêche votre antivirus de fonctionner, ClamWin Portable peut alors vous permettre de nettoyer l'infection

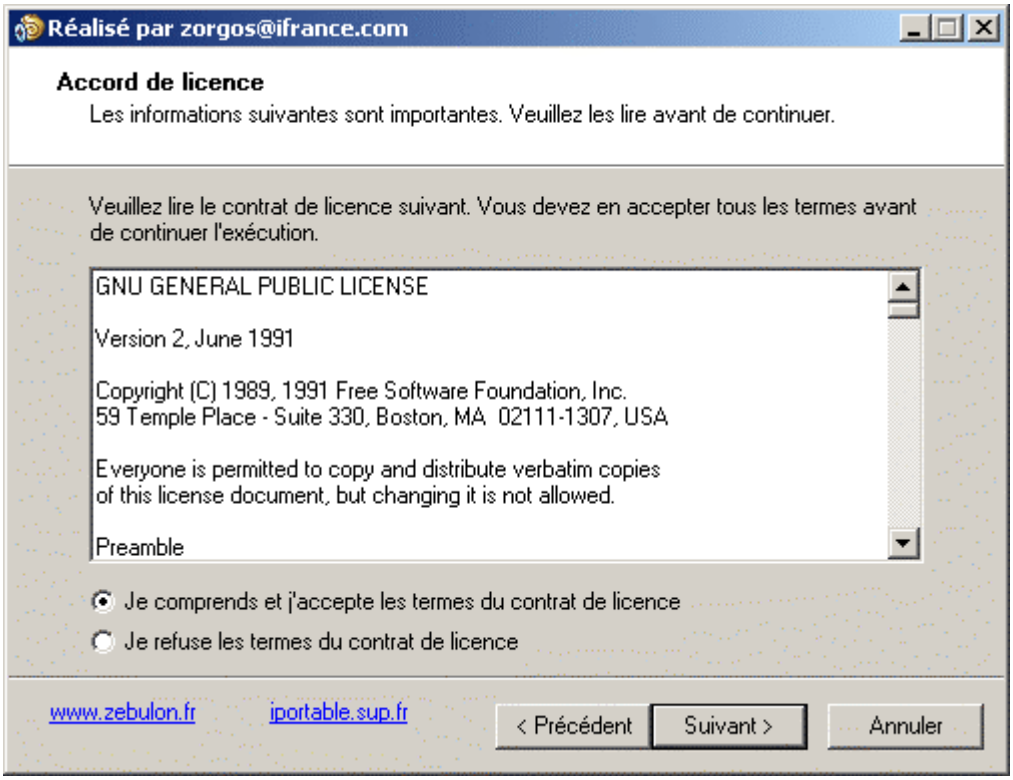
ClamWin Portable est sous licence GNU, vous pouvez télécharger ses sources ici.

Lancement de l'antivirus ClamWin Portable

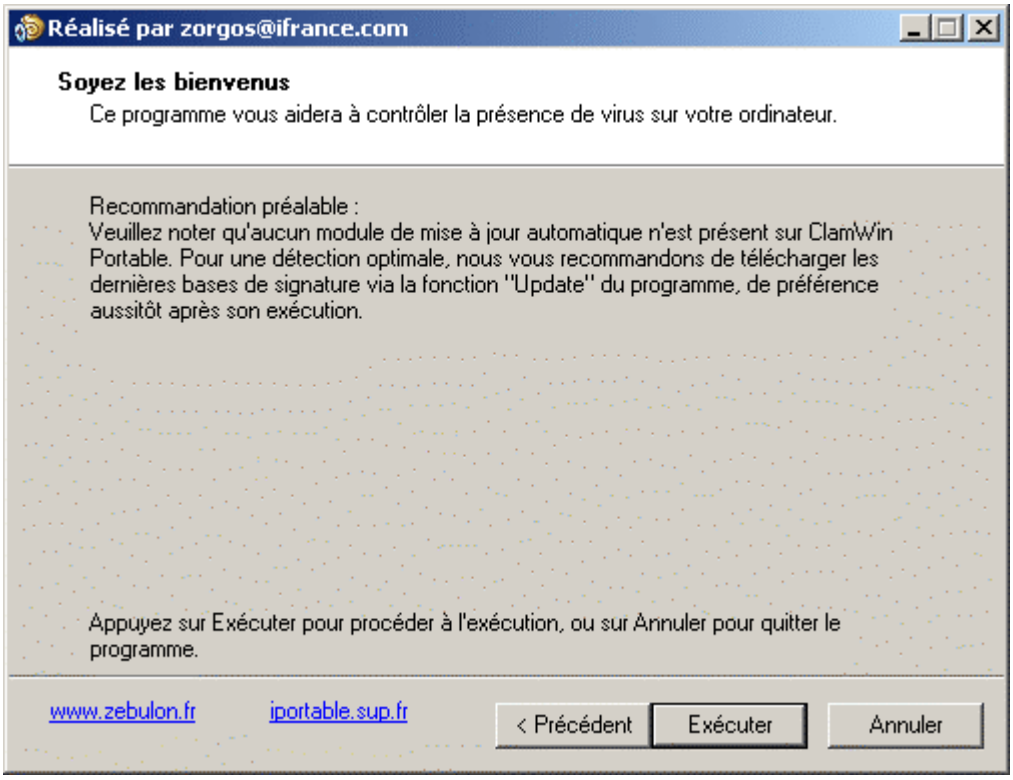
Il suffit de double cliquer sur le programme : la fenêtre suivante s'ouvre alors :



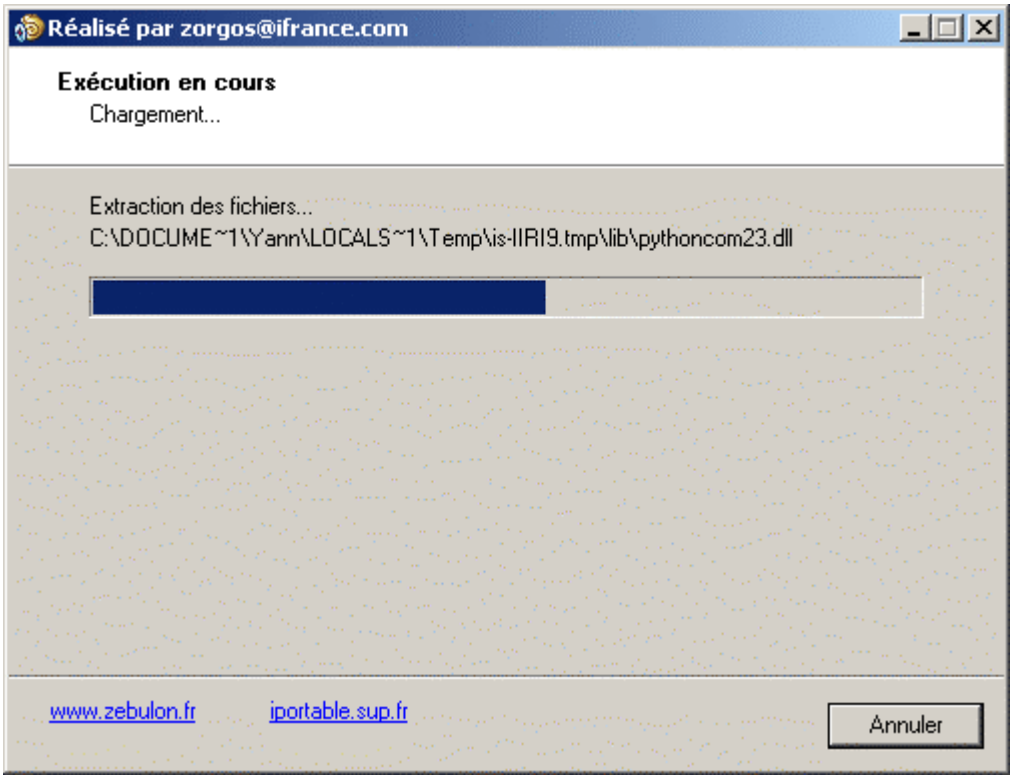
Un clic sur le bouton **Suivant** vous amènera à la fenêtre suivante :



Après avoir consulté puis accepté la licence, cliquez sur le bouton **Suivant**. Cette fenêtre apparaît alors :



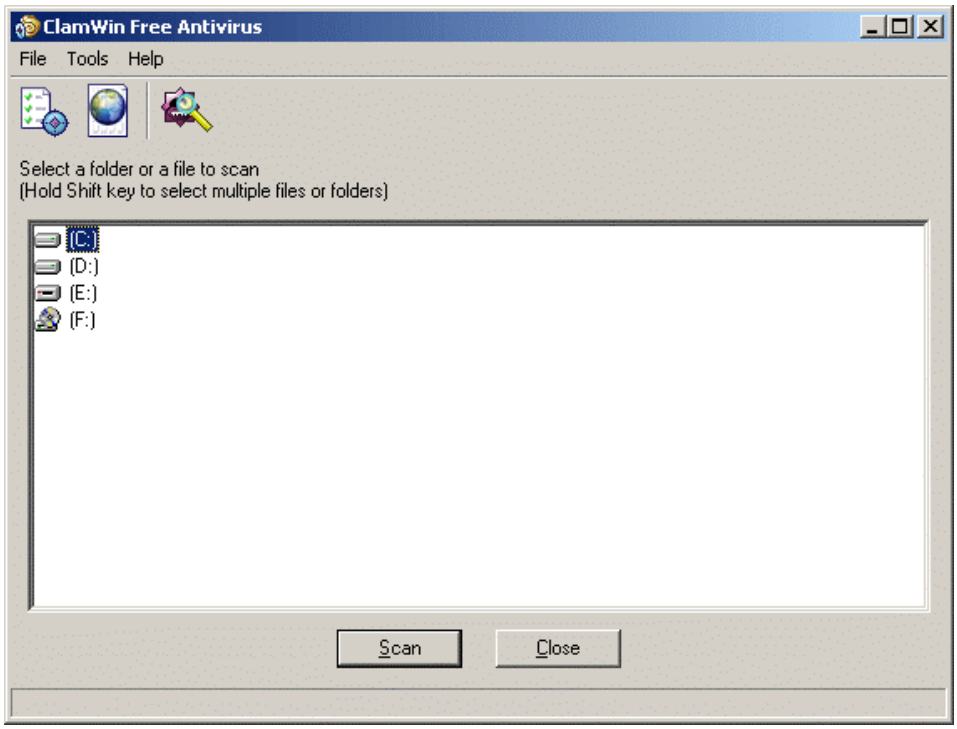
Cliquez sur le bouton **Exécuter**.



Les fichiers de ClamWin Portable sont alors décompressé dans un répertoire temporaire afin de lancer son exécution. Ces fichiers temporaires sont copiés dans le répertoire *\Documents and Settings\User\Local Settings\Temp* de votre disque. L'utilisation du programme ClamWin peut maintenant commencer.

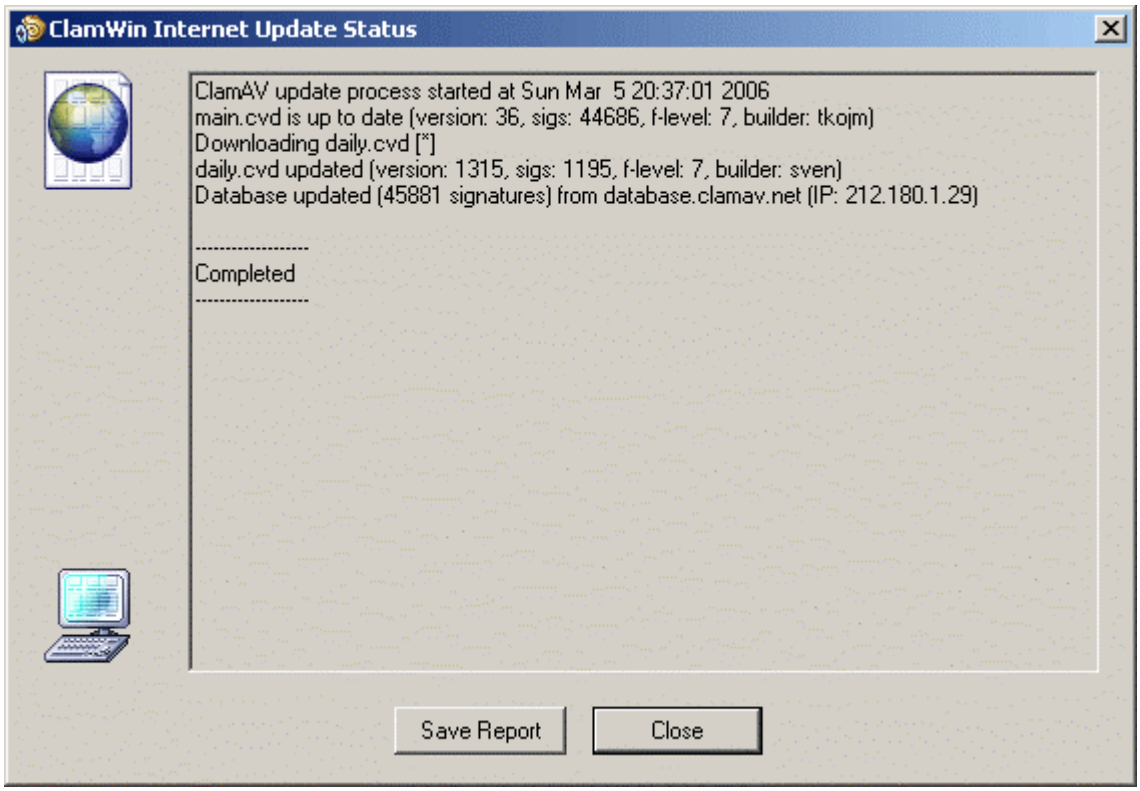
Exécution de l'antivirus ClamWin Portable

Une fois le lancement effectué, vous êtes face à la fenêtre principale de ClamWin. :



Lors de l'exécution, un nouveau dossier du nom de *ClamWin Portable* s'est créé dans votre répertoire *Windows*. Vous y trouverez le log correspondant aux mises à jour de la base des virus (*ClamUpdateLog.txt*) ainsi que le log de rapport de scan (*ClamScanLog.txt*). Ce dossier contient également deux sous-dossiers : *db* qui stocke les définitions de virus et *quarantine* qui permettra d'isoler les fichiers infectés mis en quarantaine.

Avant de commencer le scan, nous allons tout d'abord mettre à jour la base des signatures de virus. Pour cela, il suffit d'aller dans le menu **Tools** et de sélectionner l'option **Download Virus Database Update**.



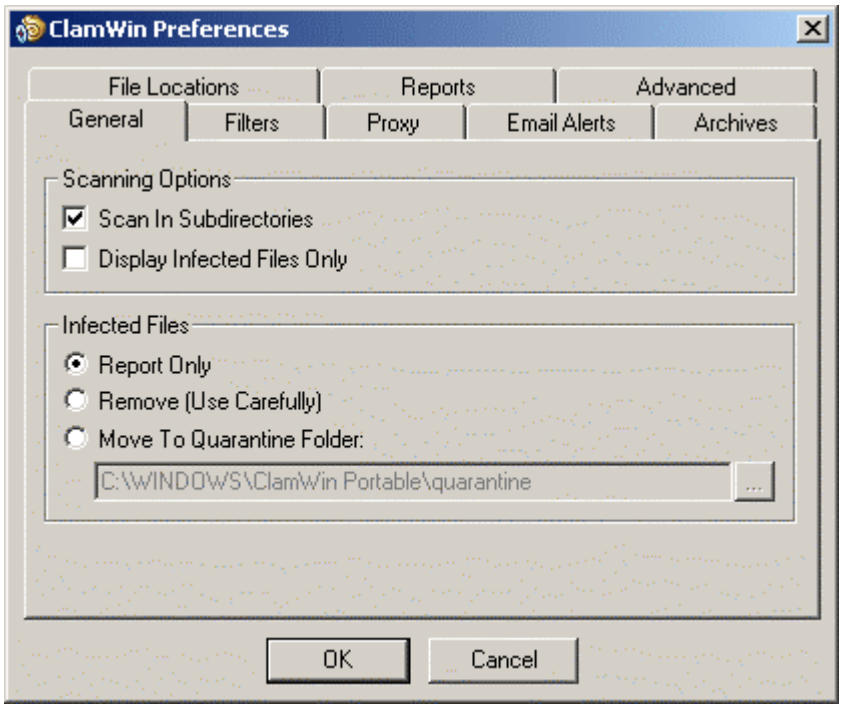
Si besoin, les nouvelles signatures de virus seront alors téléchargées. On notera que l'équipe de ClamAV met à jour quotidiennement ces bases de données de virus, ce qui est très appréciable :)

A noter que vous pouvez télécharger manuellement ces mises à jour sans pour autant utiliser ClamWin, il suffit pour cela de télécharger les fichiers de définitions suivants :
- http://database.clamav.net/main.cvd
- http://database.clamav.net/daily.cvd

Avant de commencer la vérification de vos unités de disques, commençons tout d'abord par découvrir les différentes options du programme :

Menu Files :
- **Scan** : permet de lancer le scan de(s) disque(s) ou répertoire(s) sélectionné(s)
- **Exit** : permet de quitter le programme

Menu Tools :
- **Préférences** : vous pouvez ici régler vos préférences :



La fenêtre de préférences propose pas moins de huit onglets permettant de configurer l'antivirus :

- ***General*** : cet onglet propose deux options :

  - *Scanning Options* : deux cases à cocher sont présentes

    - *Scan In Subdirectories* : cochée par défaut, cette option permet de scanner les sous répertoires des éléments sélectionnés, il est donc conseillé de laisser cette option cochée.
    - *Display Infected Files Only* : permet d'afficher uniquement les fichiers infectés lors du scan. Si cette option n'est pas coché, l'ensemble des fichiers analysés seront affichés avec l'attribut *OK* en fin de ligne signifiant que le fichier correspondant n'est pas infecté.

  - *Infected Files* : trois actions sont possibles lors de la détection d'un virus

- *Report Only* : aucune action n'est effectuée lors de la détection d'un virus, seul un avertissement sera émis. La détection sera également signalée dans le rapport de scan.

- *Remove (Use Carefully)* : le fichier infecté est effacé. **Attention !** L'activation de cette option peut s'avérer dangereuse comme par exemple dans le cas d'utilisation d'un client email qui stocke les mails dans un seul fichier (Thunderbird par exemple). En effet, si un mail contaminé est détecté, l'ensemble du "dossier" des emails du client sera effacé. Pour éviter ce problème, il est nécessaire d'exclure les fichiers stockant les mails dans l'onglet *Filters*.

- *Move To Quarantine Folder* : les fichiers infectés sont déplacés dans le dossier de quarantaine (par défaut dans *Windows**ClamWin Portable**quarantine*). Vous pouvez par la suite effacer ces fichiers, il est conseillé de choisir cette option.

- ***Filters*** : cet onglet propose de mettre en place deux types de filtres :

  - *Exclude Matching Filenames* : vous pouvez ici ajouter les extensions des fichiers qui seront ignorés lors du scan.

  - *Scan Only Matching Filenames* : vous pouvez ici ajouter les extensions des fichiers qui seront analysés lors du scan. Si aucune extension n'est spécifiée (comme cela est le cas par défaut), l'ensemble des fichiers seront scannés (sauf ceux qui sont spécifiés dans l'option précédente).

- ***Proxy*** : si vous utilisez un proxy pour vous connecter à Internet, vous pouvez le spécifier ici. Il sera alors utilisé lors de la mise à jour des fichiers de définition des virus.

- ***Email Alerts*** : vous pouvez configurer le programme pour qu'un email soit envoyé lors de la détection d'un virus, il suffit pour cela de remplir les champs correspondants à votre compte mail SMTP.

- ***Archives*** : cet onglet permet de spécifier au programme d'analyser vos archives en cochant la case *Scan In Archives*. Vous avez également la possibilité d'exclure les archives au delà d'une certaine taille, de ne pas extraire les fichiers au delà d'une certaine taille ou encore de ne pas extraire les sous-répertoires des archives au delà d'un certain niveau d'arborescence.

- ***File Locations*** : permet de modifier les chemins par défaut des fichiers de ClamWin ainsi que le répertoire des fichiers de définition. Il est inutile de modifier ces chemins lors de l'utilisation de la version portable de ClamWin.

- ***Reports*** : permet de modifier les chemins par défaut du rapport des mises à jour de la base des virus et du rapport de scan.

- ***Advanced*** : les réglages avancés permettent de spécifier au programme de scanner les boites mails et d'extraire les pièces jointes et les macros des documents MS Office.

- **Download Virus Database Update** : comme nous l'avons plus haut, cette option permet de mettre à jour la base des signatures de virus.
- **Display Reports** : permet d'afficher les rapports des mises à jour de la base des virus (*ClamUpdateLog.txt*) ainsi que le rapport de scan (*ClamScanLog.txt*) qui sont par défaut dans *Windows**ClamWin Portable*.

Menu Help :
- **Help** : permet d'afficher l'aide ; celle-ci n'est pas présente dans la solution portable de ClamWin.
- **Check Latest Version** : permet de vérifier en ligne si ClamWin Portable est basé sur la dernière version de ClamWin Free Antivirus. Actuellement, ClamWin Portable utilise la version 0.88 de ClamWin.
- **ClamWin Website** : ouvre le site de ClamWin dans votre navigateur.
- **FAQ** : ouvre la FAQ (Foire Aux Questions) de ClamWin sur sourceforge.net.
- **About** : ouvre la classique fenêtre d'informations à propos de ClamWin.

Sous la barre des menus, on remarquera également une barre d'outil avec la présence de trois icônes, il s'agit de raccourcis vers différentes fonctionnalités du programme :

 : ouvre directement la fenêtre des préférences.

 : permet de lancer la mise à jour des fichiers de définitions de virus.

 : lance le scan des unités ou répertoires sélectionnés.

Après avoir vu l'ensemble des options de ClamWin Portable, passons maintenant à l'analyse des fichiers.

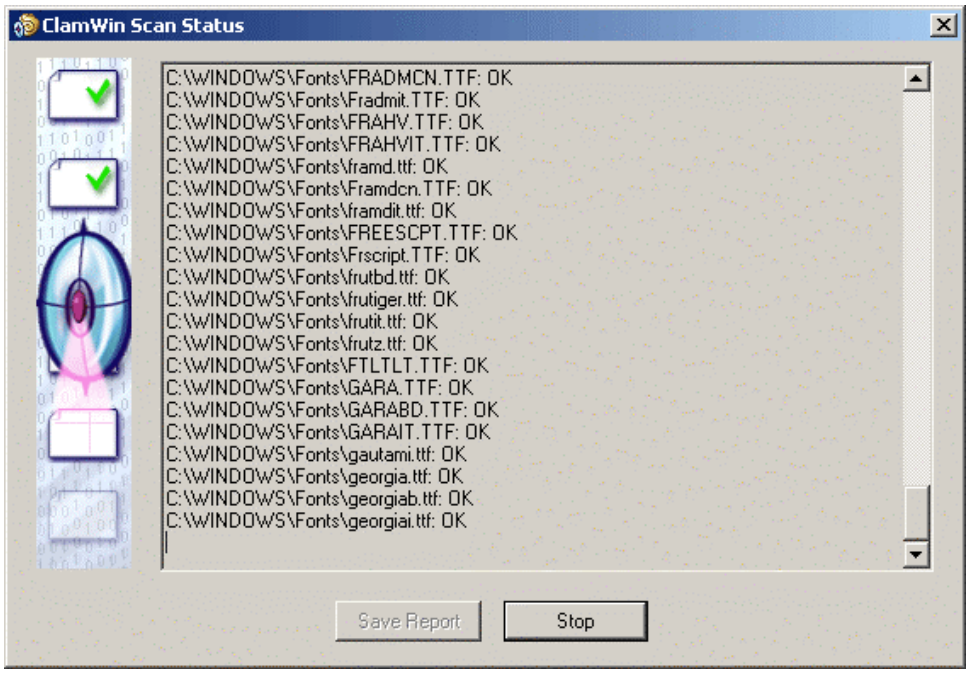
Analyse des fichiers

Afin de lancer le scan, vous devez tout d'abord sélectionner les utilités de disques de votre choix dans la fenêtre principale de ClamWin. Pour sélectionner une utilité, il suffit simplement de cliquer dessus à l'aide de la souris. Si vous souhaitez effectuer une sélection multiple, vous devez alors appuyer sur la touche **Ctrl** avant de faire votre choix.

Si vous souhaitez analyser uniquement un dossier ou un sous dossier, il suffit de double-cliquer sur l'unité de disque de votre choix puis de naviguer dans l'arborescence afin de sélectionner le dossier de votre choix.

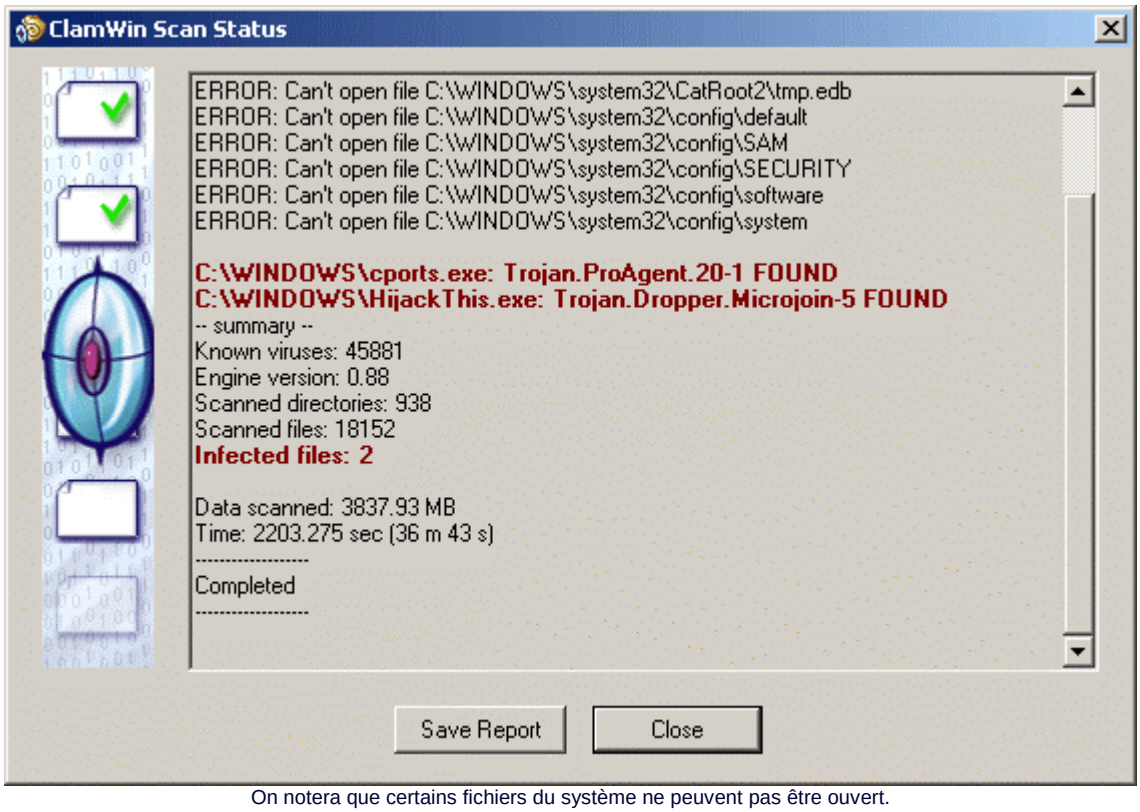
Une fois votre sélection effectuée, vous pouvez lancer l'analyse. Pour cela, il suffit de cliquer sur le bouton **Scan**. Vous pouvez également allez dans le menu **File** puis sélectionnez **Scan** ou encore cliquer sur l'icône du raccourcis vers le scan :

L'analyse des fichiers commence :



Le temps d'analyse peut bien entendu varier en fonction du nombre de fichiers à analyser. Pour le scan d'une unité complète, le temps d'analyse peut être très long, il faut donc s'armer de patience ! Un clic sur le bouton **Stop** arrêtera l'analyse.

Enfin, une fois l'analyse terminée, le programme vous affichera un rapport d'analyse :



On notera que certains fichiers du système ne peuvent pas être ouvert.

Vous pourrez trouver le log complet du scan ici : \Windows\ClamWin Portable\ClamScanLog.txt

Avertissement

ClamWin Portable, tout comme ClamWin, est un programme permettant de scanner vos fichiers afin de détecter une éventuelle infection. Il s'agit d'un outil à utiliser en plus d'un antivirus traditionnel. En effet, ClamWin Portable n'est pas un programme résident, c'est à dire qu'il n'inclut pas de scanner temps réel et ne permet pas de scanner la mémoire. Le programme ne peut donc pas empêcher les intrusions de virus. Vous devez donc scanner un fichier manuellement pour détecter un virus.

ClamWin Portable n'en reste pas moins un bon outil supplémentaire permettant d'éradiquer une infection ! Le fait de pouvoir copier aisément le programme sur un support externe comme une clé USB est également un plus non négligeable :)

Auteur : Yann
Développeur du package : grenouille
Site officiel : ClamWin