Nouvelles menaces, les „rootkits“ :

Le monde virtuel (Internet) n'arrête pas de nous étonner, dans le bien que dans le mal. Surtout les **malware** (virus, ver, troyen, etc.) poussent comme des champignons. La créativité des programmeurs de ces codes malicieux s'emble n'avoir pas trouvé de fin.
Une nouvelle sorte de ces **malware** est apparue, les „**rootkits“** !

C'est quoi les „rootkits“ ?

Les „**rootkits“** sont bien connus depuis des années dans le monde de „**UNIX“** et de „**LINUX“** et font leur apparition officielle dans le monde de „ **Windows®“** depuis mi-février 2005, selon un communiqué officiel de **Microsoft®** et de la „**RSA SECURITY“**.

Ils s'intègrent en principe directement dans le cœur de **Windows®**, dans le „**KERNEL“** et ils se font passer comme étant des processus et services de **Windows®**. Même les scanneurs de malware (anti-virus, antitroyen, etc.), ainsi que les „**firewalls“** (**pare-feu**) n'arrivent pas à détecter ces bestioles informatiques, dû au fait qu'ils ont développé une certaine intelligence.

Ils sont capables de se faire passer pour un service légitime de **Windows®** et de cette façon ils échappent au scan des anti-virus et des pare-feu (firewall) !

Ils s'activent automatiquement dès démarrage du PC.

Leur rôle principal consiste à ne pas se faire révéler !

Ils se camouflent comme „drivers“ (pilotes), processus et services légitimes de Windows®, se cachent dans des endroits de la base des registres sans se faire remarquer !
Même étant détectés et éradiqués, ils ressuscitent et se reproduisent à nouveau !

Pour plus d'informations, veuillez télécharger nos didacticiels suivants :

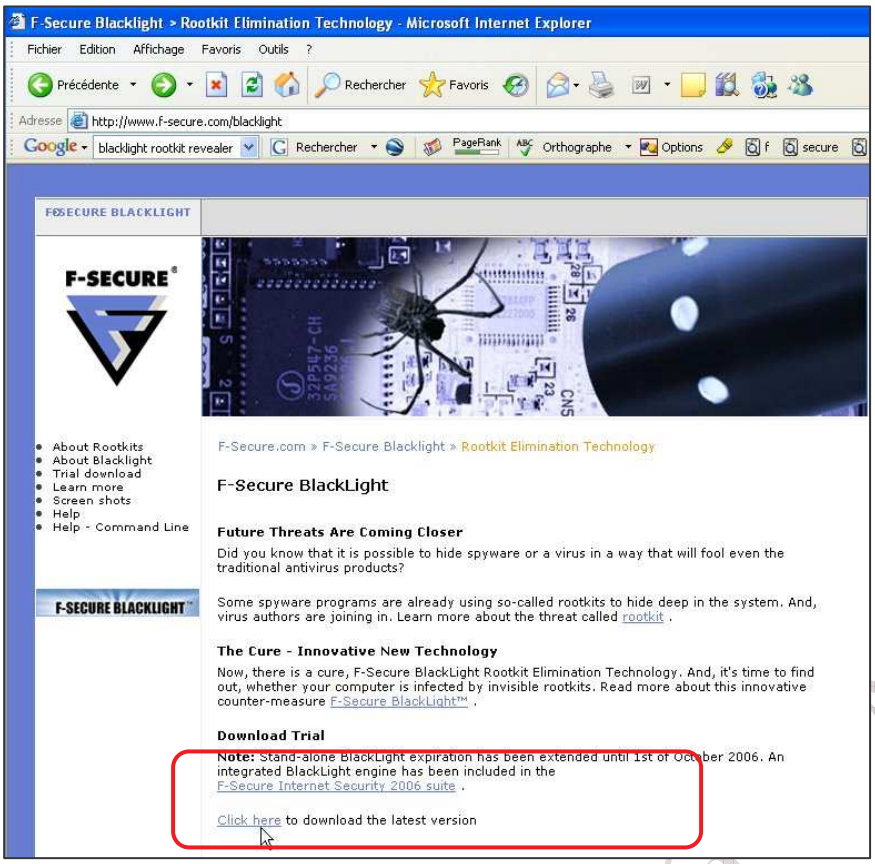
Nouvelle menaces, les rootkits :

http://www.internetmonitor.lu/download/Nouvelles_menaces_04.05.2005..doc

Rootkits 2ème partie :

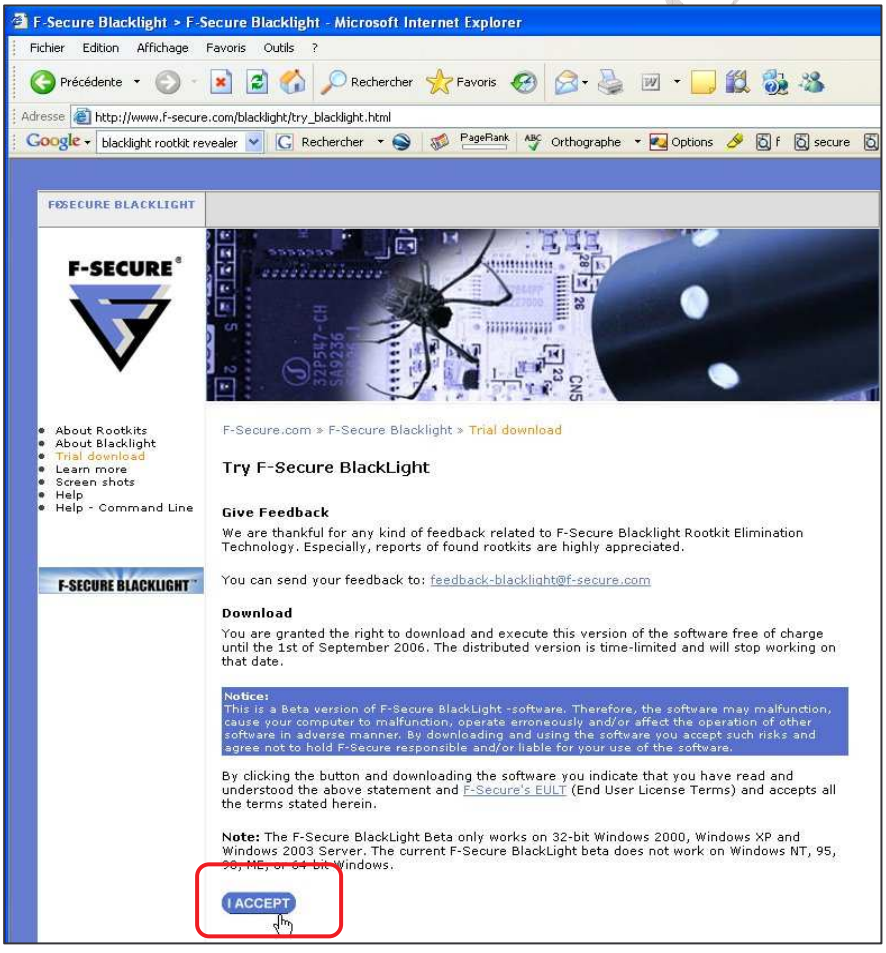
http://www.internetmonitor.lu/download/Rootkits_2eme_partie_14.06.2005..doc

Il existe néanmoins des logiciels qui détectent ces bestioles informatiques coriaces, tel que „**F Secure Blacklight**“, logiciel dont nous allons expliquer son téléchargement et son utilisation à la page suivante.

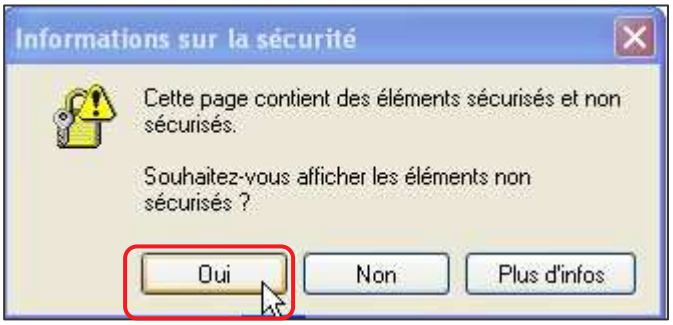


Pour télécharger le logiciel, connectez-vous à Internet et choisissez l'adresse URL suivante : www.f-secure.com/blacklight.

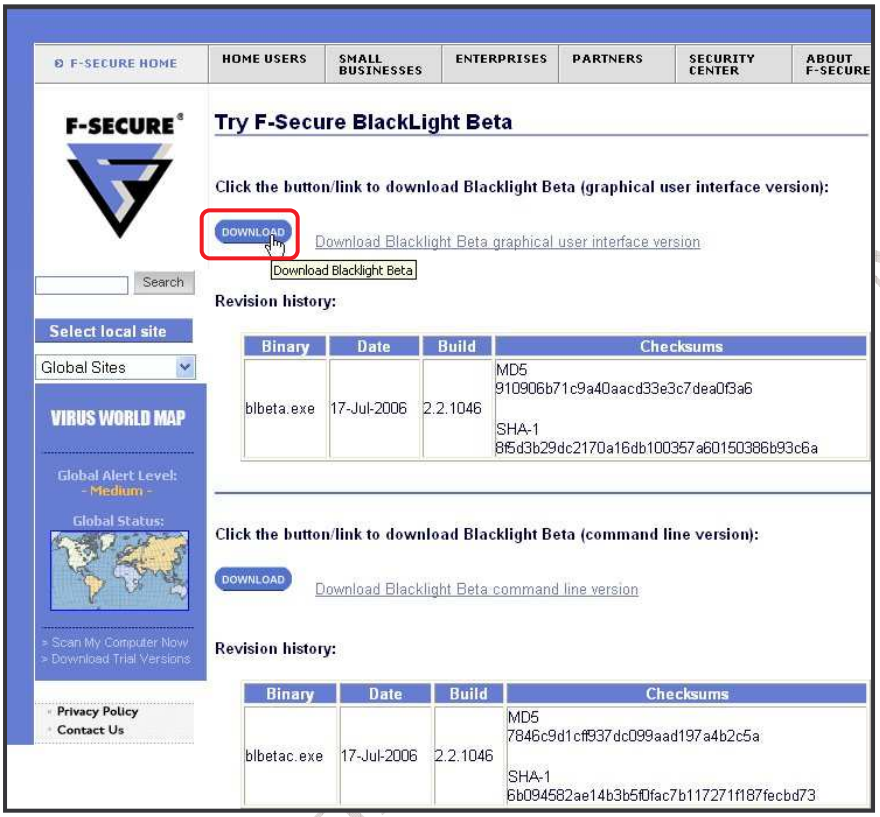
La fenêtre ci-contre s'affiche. Cliquer sur le lien „**F-Secure BlackLight**".



La fenêtre ci-contre s'affiche. Cliquer sur le bouton „**I ACCEPT**".

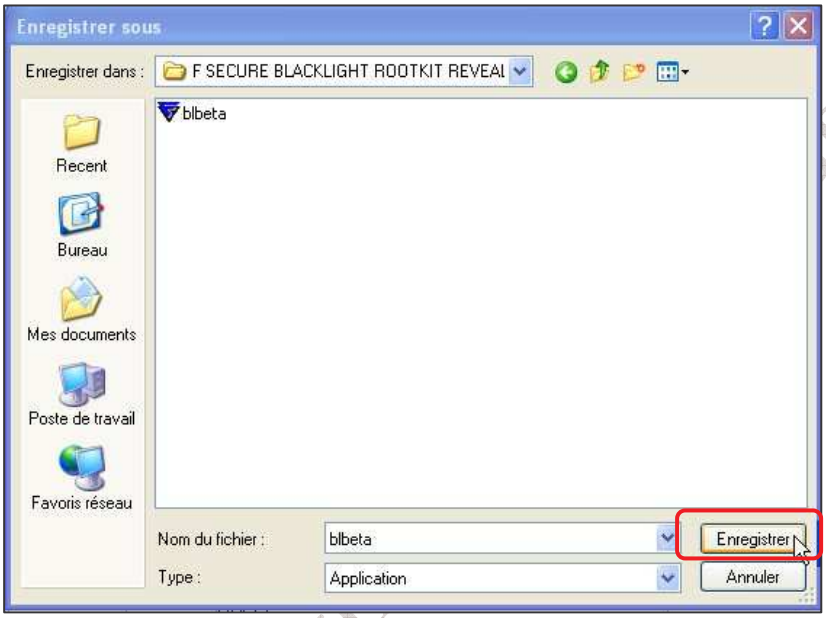


La boîte de dialogue ci-contre s'affiche. Cliquer sur le bouton „**Oui**".



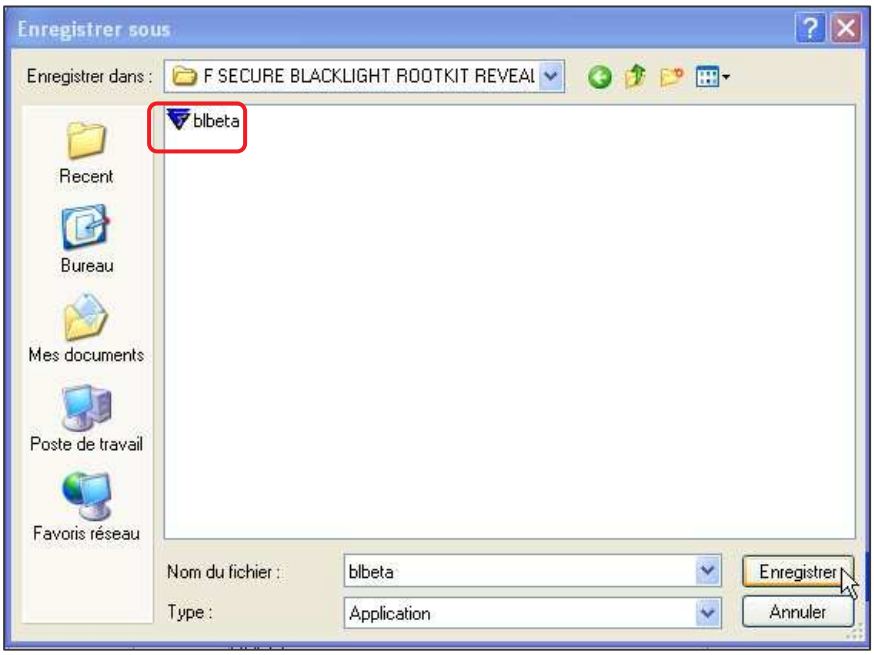
La fenêtre ci-contre s'affiche. Cliquer sur le bouton „**DOWNLOAD**".

La boîte de dialogue ci-contre s'affiche. Cliquer sur le bouton „**Enregistrer**".

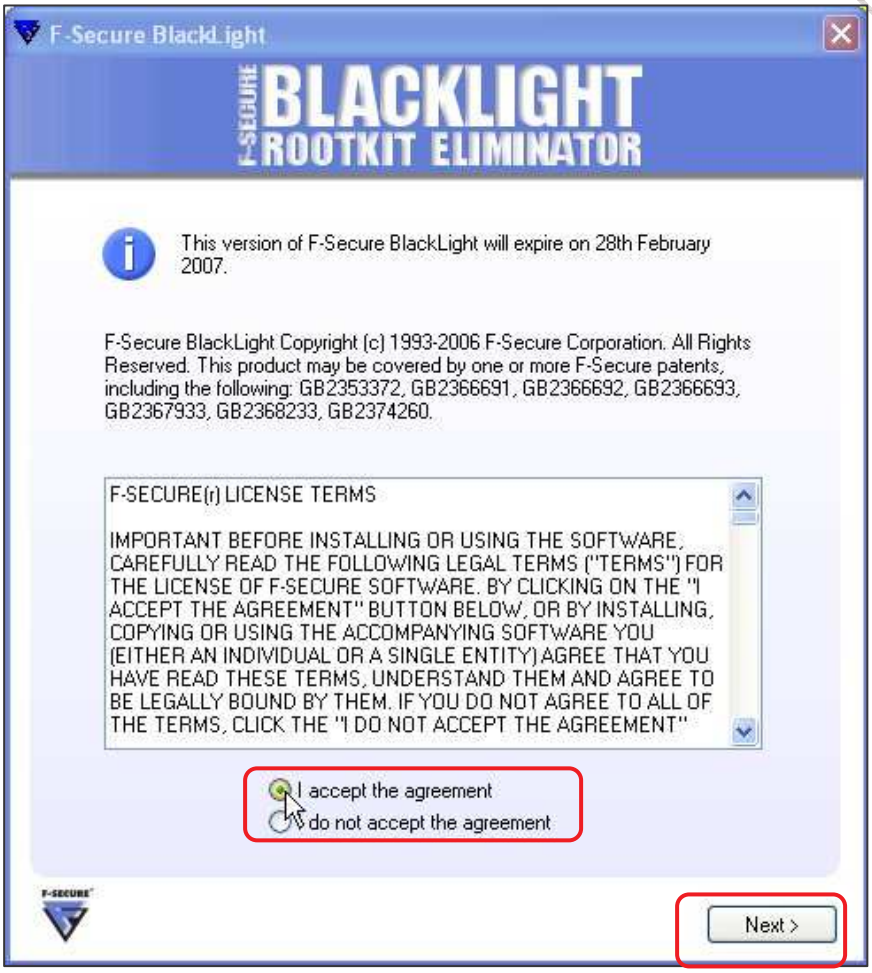


La fenêtre ci-contre s'affiche. Créez un dossier, libellé avec le nom du logiciel et enregistrez-le.

Cliquer sur le bouton „**Enregistrer**".

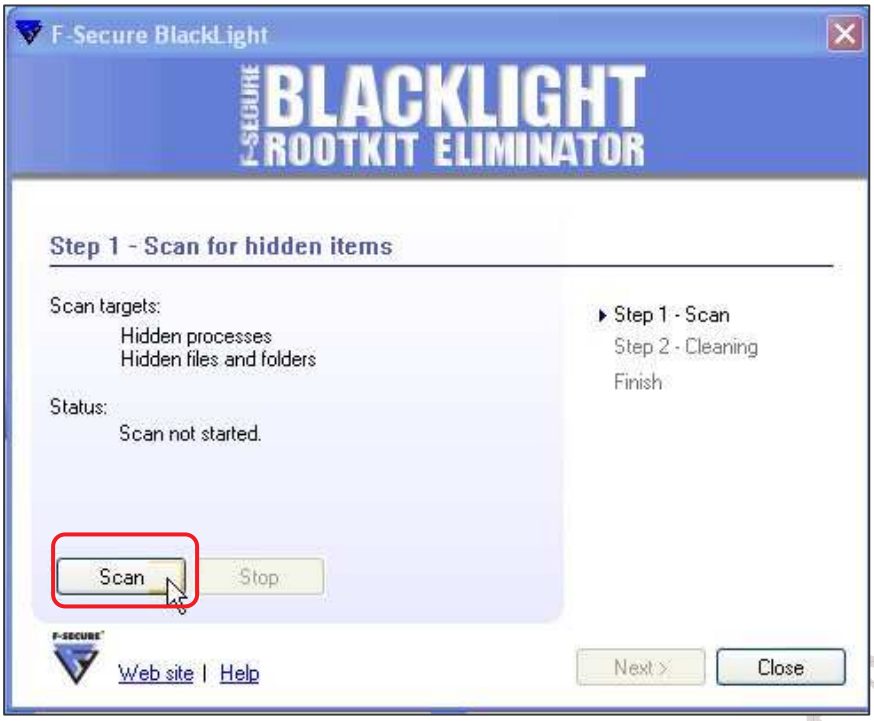


Double-cliquer ensuite le fichier téléchargé.



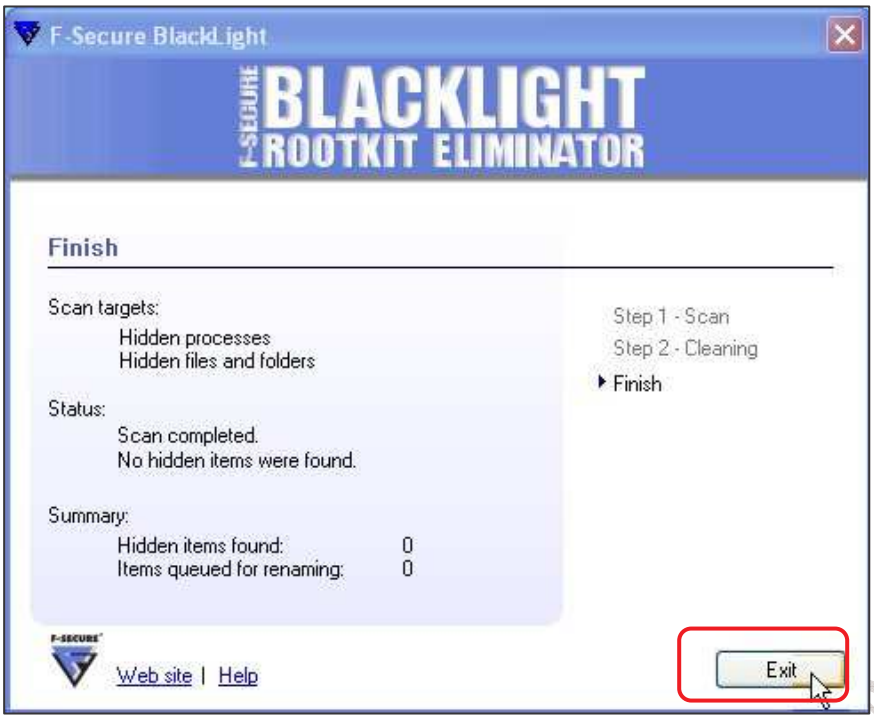
La fenêtre ci-contre s'affiche. Cocher la case „**I accept the agreement**".

Cliquer ensuite sur le bouton "**Next**".



Le logiciel est maintenant prêt à l'emploi. Cliquer sur le bouton „**Scan**".

L'écran ci-contre s'affiche pendant quelques minutes, affichant le degré de progression.



Le scan terminé, l'écran ci-contre vous affiche les résultats. Dans notre exemple aucun „**rootkit**" n'a été trouvé. Le cas contraire, suivez les instructions sur cette page pour continuer…

Cliquer ensuite sur le bouton „**Exit**" pour terminer l'action.