

# EFFECTUER UNE ANALYSE DES ROOTKITS AVEC F-SECURE BLACKLIGHT

Cette fiche pratique vous guide à effectuer une analyse des rootkits avec F-Secure Blacklight.

La fiche pratique suivante est composée de 2 parties :

- [A - Télécharger F-Secure BlackLight](#)
- [B - Lancer une analyse avec F-Secure BlackLight](#)

## A - Télécharger F-Secure Blacklight.

Etape 1 : Pour télécharger le logiciel Anti-rootkits, cliquez [ici](#).

La fenêtre suivante apparaît. Cliquez sur le bouton **Enregistrer**.

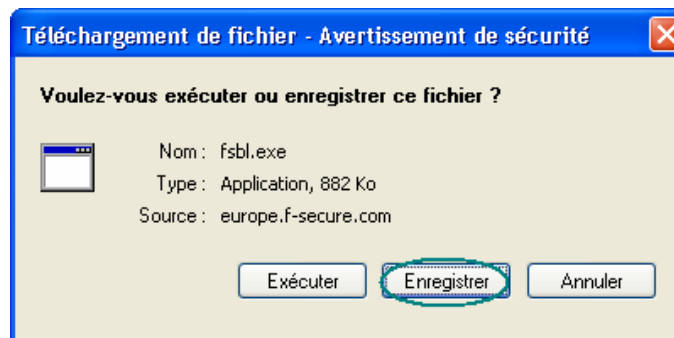


Figure 1 : Enregistrer

Etape 2 : La fenêtre suivante apparaît. Sélectionnez le "Bureau" (1) sur la partie gauche, puis cliquez sur le bouton **Enregistrer** (2).

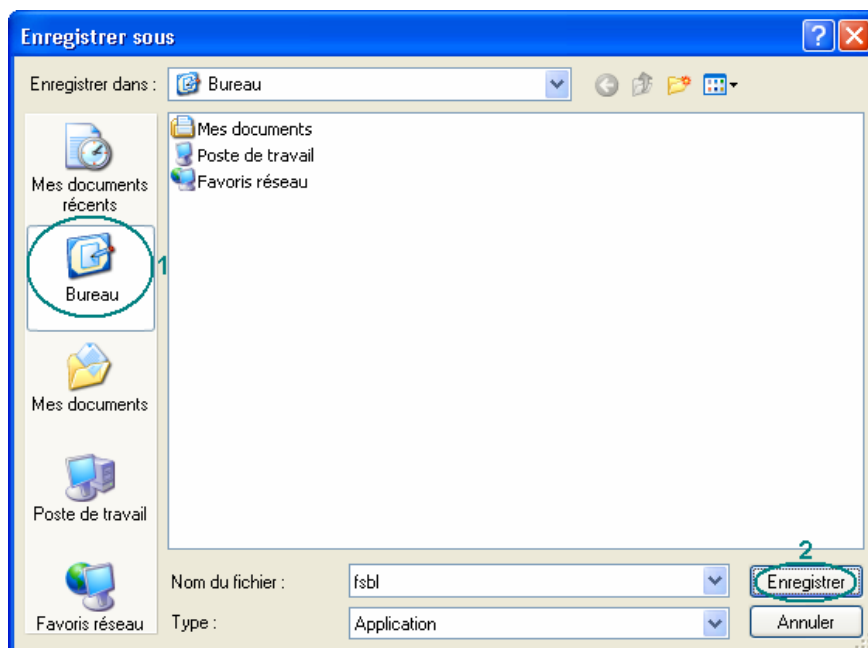


Figure 2 : Enregistrement sur le bureau

Etape 3 : Si cette fenêtre s'affiche une fois le téléchargement terminé, cliquez sur le bouton **Fermer**.



Figure 3 : Enregistrement terminé

## **B - Lancer une analyse avec F-Secure BlackLight.**

Etape 4 : Rendez-vous sur le bureau et double cliquez sur le fichier "fsbl".



Figure 4 : fsbl

Etape 5 : La fenêtre suivante apparaît. Sélectionnez "I accept the agreement", puis cliquez sur le bouton **Next (2)**.

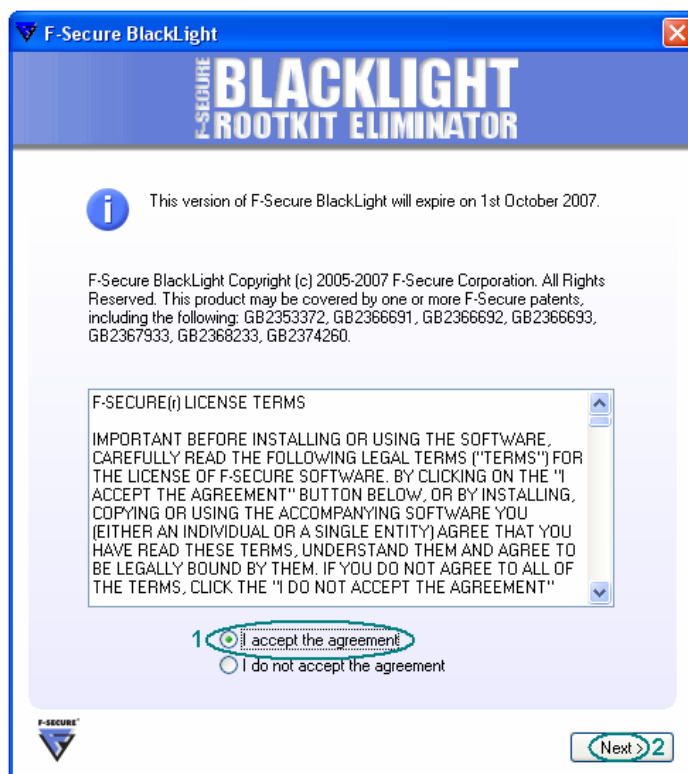
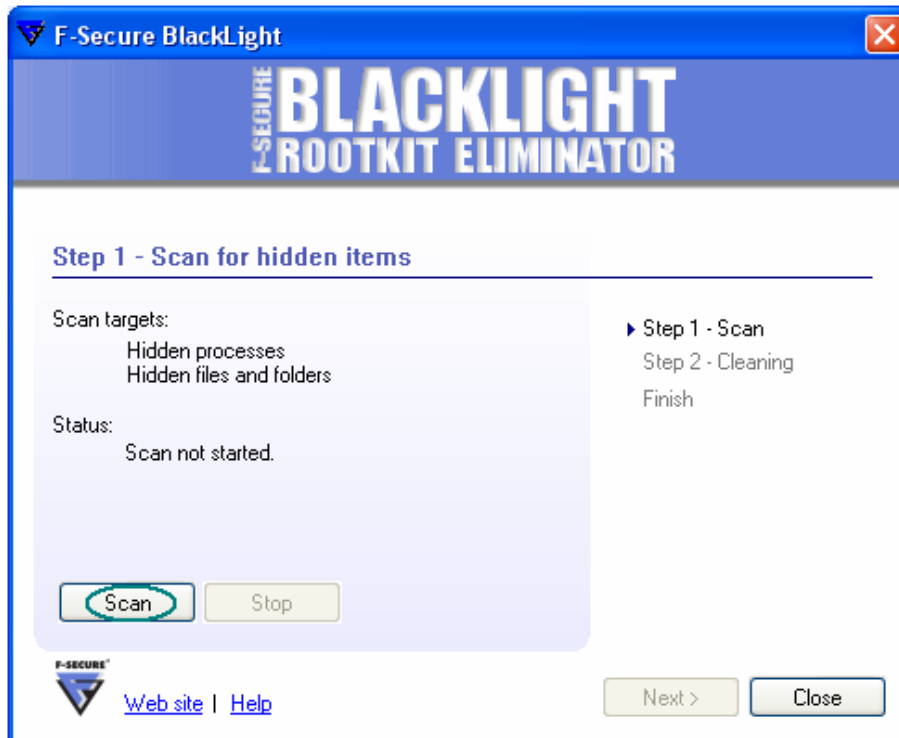


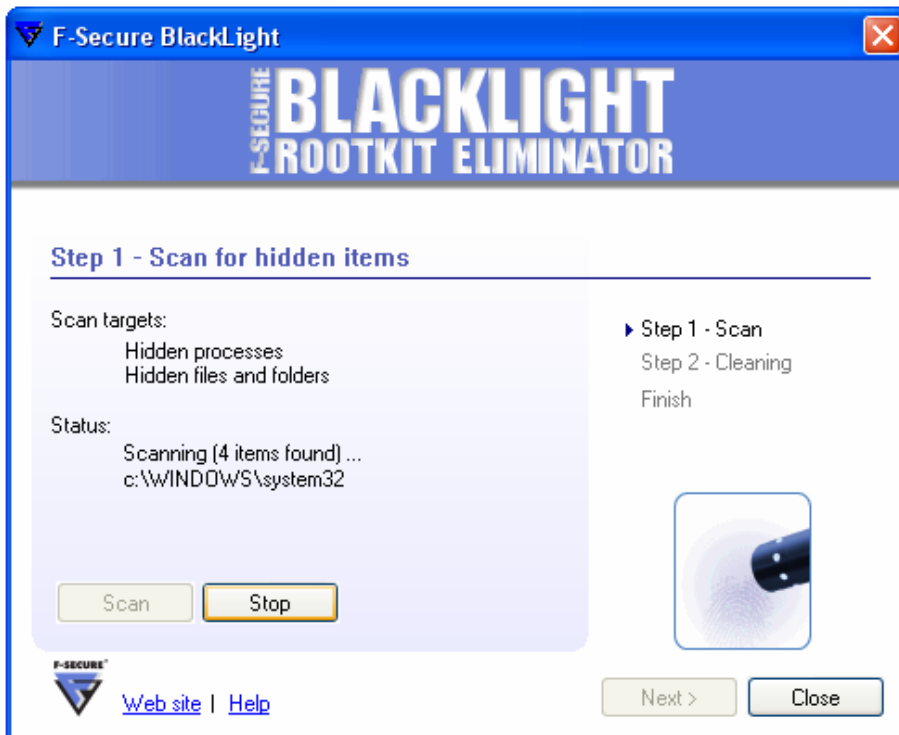
Figure 5 : Contrat

Etape 6 : Cliquez sur le bouton **Scan**.



**Figure 6 : Lancement du scan**

Etape 7 : L'analyse est en cours.



**Figure 7 : Analyse en cours**

Etape 8 : La fenêtre suivante apparaît lorsque l'analyse est terminée.  
Cliquez sur le bouton **Next** >.

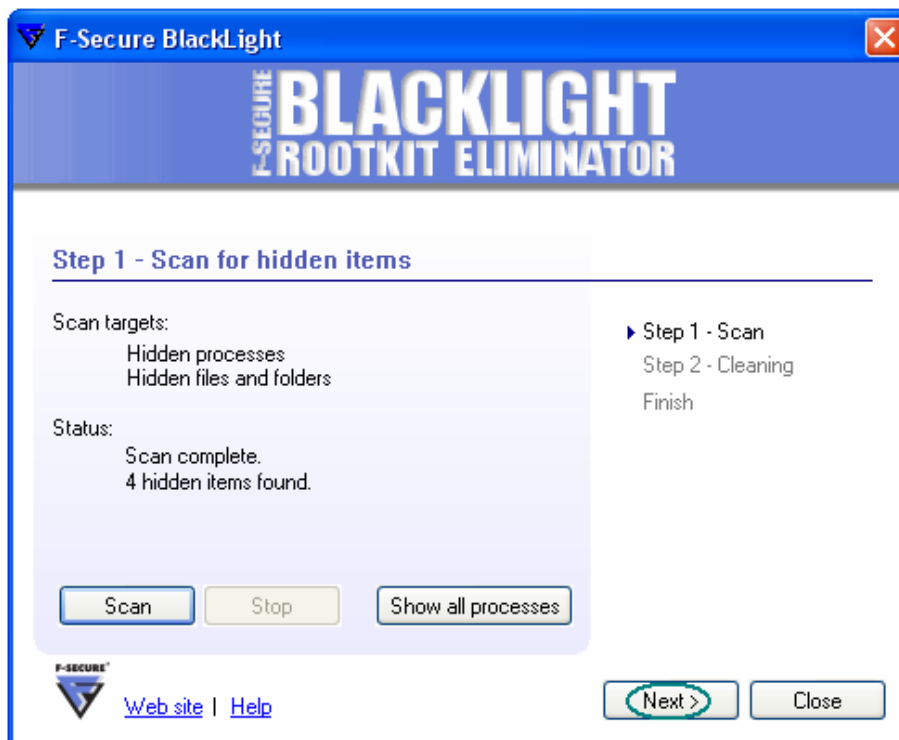


Figure 8 : Résultat de l'analyse

Etape 9 : La liste des rootkits apparaît. Sélectionnez le premier rootkit (1), et cliquez sur **Rename** (2). Recommencez cette manipulation pour tous les rootkits.

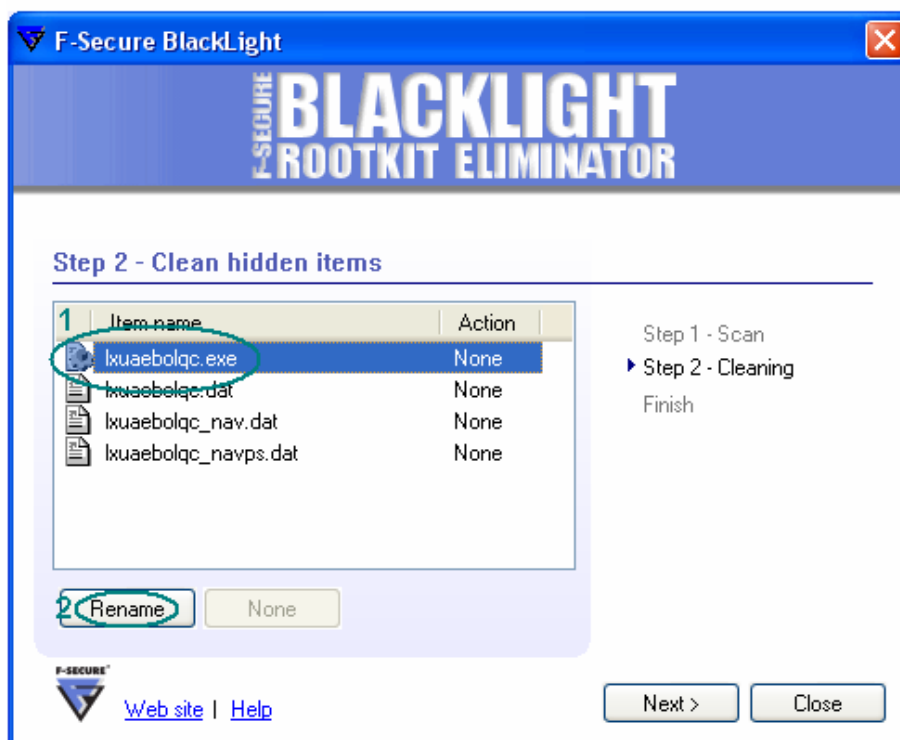


Figure 9 : Renommer

Etape 10 : Lorsque vous avez renommé tous les rootkits, cliquez sur le bouton **Next >**.

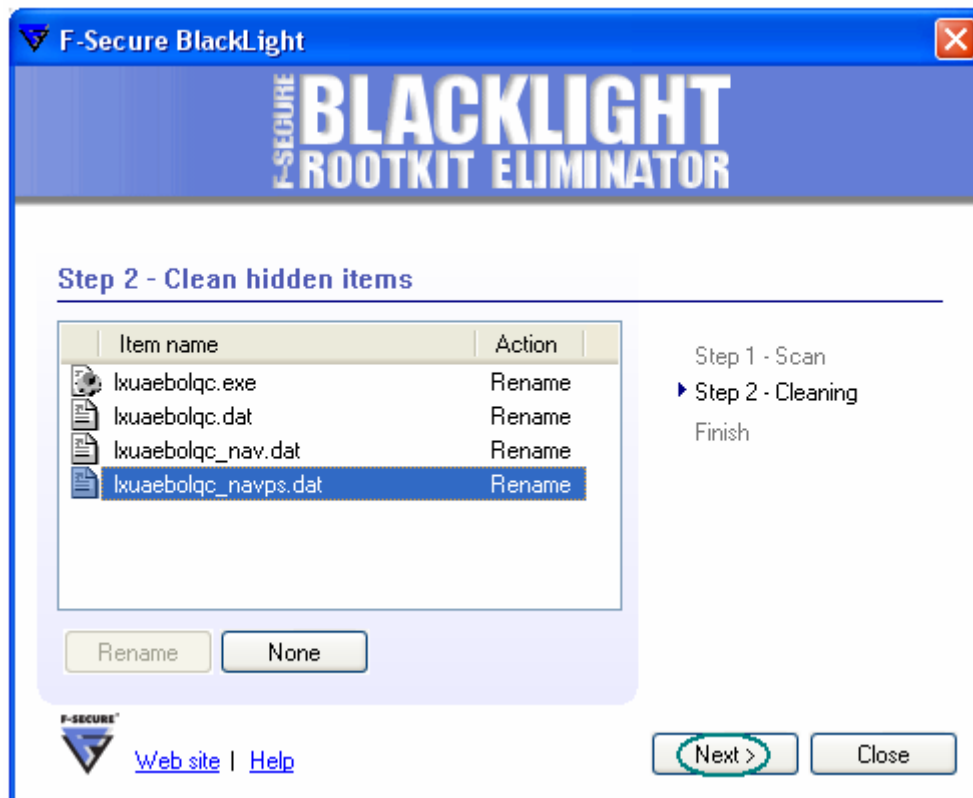


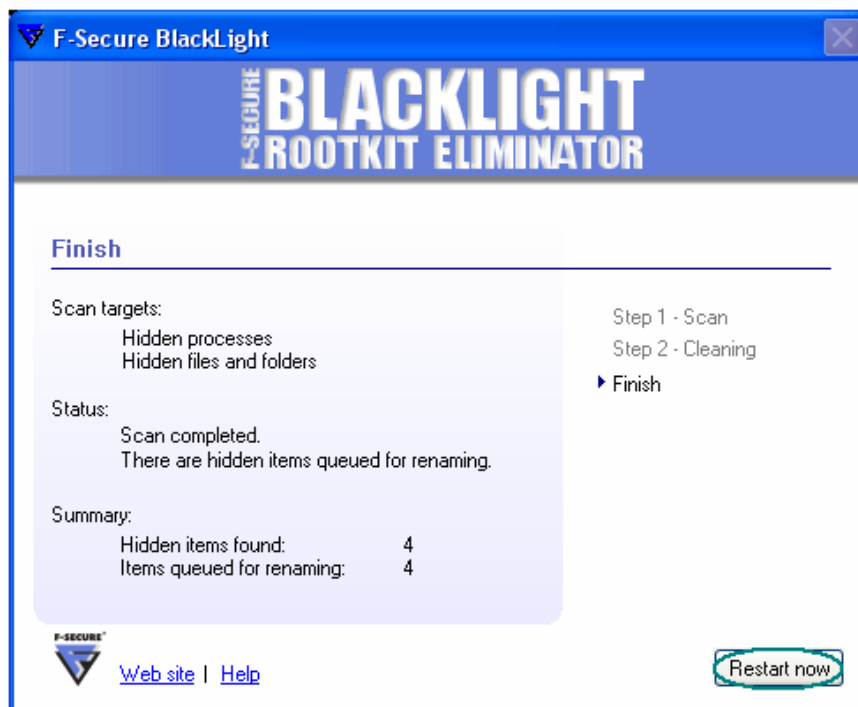
Figure 10 : Rootkits renommés

Etape 11 : La fenêtre suivante apparaît. Cochez la case devant "I understand the warning", puis cliquez sur le bouton **OK (2)**.



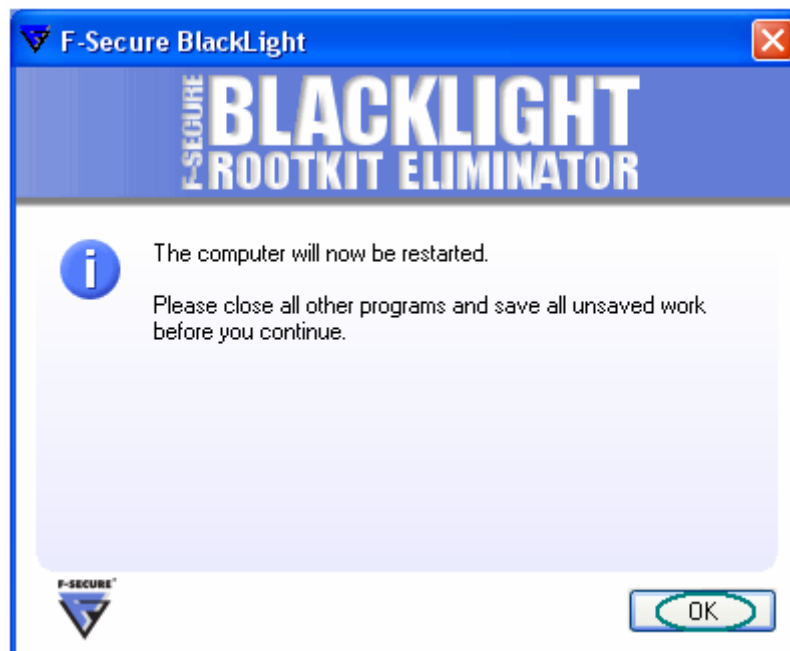
Figure 11 : Warning

Etape 12 : Le nettoyage des rootkits est maintenant terminé. Cliquez sur le bouton **Restart now**.



**Figure 12 : Nettoyage terminé**

Etape 13 : La fenêtre suivante apparaît. Cliquez sur le bouton **OK**.



**Figure 13 : Redémarrage**

Au redémarrage, les rootkits ont été supprimés de l'ordinateur.