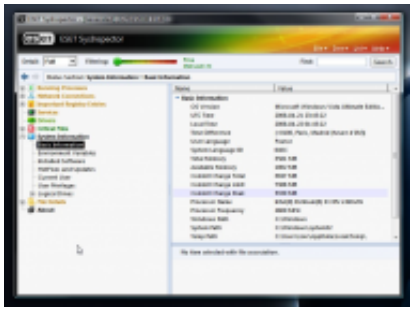
Controlez la présence de menaces cachées

Rootkits et Trojans ont ceci de particulier qu'ils se dissimulent au coeur du système, masquant leurs actions néfastes aux yeux de l'utilisateur et parfois même à ceux des antivirus. L'éditeur ESET, connu pour son antivirus NOD32, propose un outil gratuit qui analyse votre PC, explore ses caractéristiques techniques, note ses performances mais surtout met en évidence les anomalies système engendrées par la présence des menaces de ce type.

Prise en main



agrandir la photo
SysInspector peut être téléchargé en suivant ce lien .
Il s'agit là de la version 32 bits, mais il en existe aussi une version 64 bits sur le site de l'éditeur.

Le logiciel se lance directement sans installation. Au premier lancement, il faut accepter la licence en amenant l'ascenceur de la fenêtre tout en bas puis en cliquant sur *"I Agree"*.

Après un temps d'analyse assez long (quelques minutes), la fenêtre principale du logiciel apparaît.

Elle comporte une barre de menu en haut à droite (eh oui, à

droite), une barre de filtrage et recherche, un panneau de navigation sur la gauche, une fenêtre de description (panneau supérieur droit) et une fenêtre de détails (panneau inférieur droit).

La liste de navigation est l'élément central de ce logiciel:

* **Running Processes** liste tous les processus en cours d'exécution lors de l'analyse.
* **Network Connections** liste toutes les applications qui communiquent en TCP/IP
* **Important Registry Entries** affiche le contenu des clés de registres dans lesquelles se cachent les malwares
* **Services** liste les services Windows
* **Drivers** liste les pilotes installés dans le système
* **Critical files** surveille quelques fichiers fondamentaux de Windows
* **System Information** détaille votre matériel et votre configuration
* **File details** liste les fichiers importants pour la sécurité comme les exécutables, screensavers, etc.

Ce qu'il vous faut

Niveau : Intermédiaire / **Temps :** 5 minute(s)

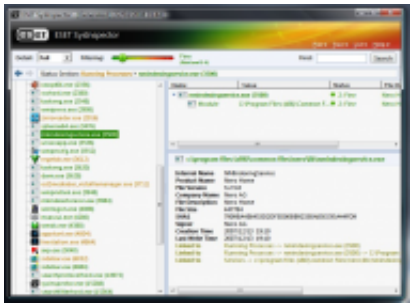
Logiciels :

ESET SysInspector (Windows)

Matériel :

- Rien

Controlez la présence de menaces cachées



agrandir la photo

Le logiciel affiche ainsi par défaut une pléthore de données techniques concernant votre machine. Mais un ascenceur *("Filtering")* dans la barre de filtrage permet de restreindre l'affichage aux seules informations significatives d'un risque. Il sufffit pour cela de le pousser vers la zone jaune.

Sur SysInspector, les informations s'affichent en couleur en fonction des risques potentiels:

* **en noir** les informations sans importance (en termes de sécurité).

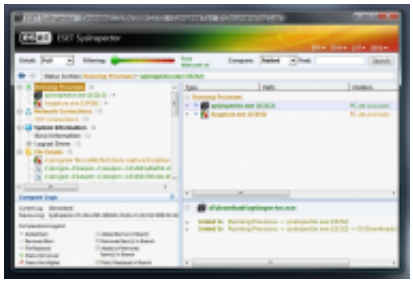
* **en vert** les informations jugées normales ou sans risques.

* **en jaune** les anomalies inconnues (ce que le système trouve anormal par manque de connaissances).

* **en rouge** les informations potentiellement dangereuses, trahissant un risque reconnu.

Cliquez par exemple sur *"Running Processes"* et faites varier l'ascenceur *"Filtering"*. Remarquez que les processus habituels du système ou d'Office apparaissent en vert. Les processus inconnus sont en jaune. Les processus qui trahissent la présence d'un virus/trojan/malware apparaissent en rouge.

Controlez la présence de menaces cachées



agrandir la photo

L'une des fonctions les plus utiles de SysInspector est sa fonction de comparaison de LOG...

Une fois la première analyse faite, cliquez sur le menu **File** et choisissez *"Save Log"*. Attribuez ensuite un nom spécifique à cette sauvegarde.

Par la suite, régulièrement ou à chaque fois que vous avez un doute ou que la machine semble ramer, relancez le logiciel.

Après analyse, allez dans le menu **File** et choisissez *"Compare Log"* puis sélectionnez votre fichier Log de référence. Le logiciel va comparer ce Log à celui actuellement en mémoire. Un rapport affiche alors les valeurs nouvelles, celles qui ont disparu et signale si, entre ces deux logs, le niveau de risque s'est accru ou s'il a diminué.