Il y'a encore trois ans, les **spywares** ou logiciels espions étaient considérés comme une menace relativement mineure par rapport aux virus et autres vers qui étaient la priorité des éditeurs de logiciels de sécurité. En trois ans, la situation a considérablement changé et l'espionnage de l'utilisateur à des fins de vol d'identité, ou l'installation à son insu de logiciels malveillants sont devenus des rouages essentiels d'une véritable économie de la **cyber criminalité**. En conséquence, les éditeurs comme **Symantec**, **McAfee**, **BitDefender** ou **Kaspersky** ont progressivement ajouté à leurs antivirus des fonctionnalités de lutte contre les **spywares**. Il est même impossible, aujourd'hui, de trouver un antivirus dénué de cette fonctionnalité, même en version de base.

Mais qu'en est-il alors des **antispywares** dédiés ? Apparus en même temps que ces menaces, des logiciels tels que **Spybot Search & Destroy** ou **Ad Aware** étaient rapidement devenus indispensables. A l'heure où les suites de sécurité tout en un se répandent, ces outils sont loins d'avoir disparus : ils continuent à évoluer et pour certains utilisateurs avertis, recherchant une protection personnalisée plutôt qu'une suite monolithique, ils peuvent encore s'avérer utiles.

Ce test réuni 5 logiciels **antispyware** pour ce comparatif : **Spyware Doctor** de **PC Tools**, **Spy sweeper** de **Webroot** et **Ad-Aware 2007 Plus** de **Lavasoft** représentent les logiciels commerciaux. Face à eux, deux gratuits : **Windows Defender** de **Microsoft** et **Spybot Search & Destroy**.

Quelques notions sur les spywares

Avant de rentrer dans le vif du sujet, rappelons quelques notions et définitions sur le monde pas toujours très facile d'accès des spywares. Evidemment, ces notions ne seront pas indispensables aux utilisateurs confirmés.

Qu'est-ce qu'un spyware ?

De manière générale, le spyware est un logiciel qui s'installe à l'insu de l'utilisateur pour y effectuer des opérations malveillantes telles que l'envoi de publicité, l'installation de chevaux de Troie ou encore la collecte d'informations personnelles. Parler de spyware est cependant assez vague, il existe en fait de nombreux types de menaces rentrant dans cette catégorie. De plus, quelques termes utilisés fréquemment par ces logiciels nous semblent assez peu connus du grand public pour les expliciter :

- **Les adwares :** tirant leur préfixe du mot « advertising », les adwares diffusent de la publicité à l'insu de l'utilisateur, souvent sous forme de fenêtres pop-up. Les adwares sont souvent proposés à l'installation d'un autre logiciel, profitant de l'empressement des utilisateurs à cliquer sur le bouton « Suivant » de l'installation sans détecter les éventuelles cases à cocher ou décocher. Le lecteur vidéo BSPlayer est un exemple de logiciel incluant un adware (WhenU Save).

- **Les keyloggers :** ces logiciels particulièrement nuisibles enregistrent vos frappes claviers. Les keyloggers sont particulièrement utilisés pour les fraudes impliquant des vols d'informations sensibles telles que des coordonnées bancaires.

- **Les Browser Helper Objects (BHO)** : à la base, un Browser Helper Object n'est pas un spyware mais un module complémentaire pour Internet Explorer. Spybot Search & Destroy, que nous testerons lors de notre comparatif, inclut par exemple un BHO pour bloquer certains téléchargements. Néanmoins, les BHO à caractère malveillants sont légion.

- **Fichier Hosts** : ce fichier, qui contient notamment l'adresse IP locale d'une machine, est notamment utilisé pour le filtrage des sites. On peut par exemple passer par ce fichier pour attribuer une adresse IP locale à un nom de domaine. En pratique, ce fichier peut être utilisé à bon escient, par exemple pour rediriger des noms de domaines associés à des logiciels

malveillants. Néanmoins, le fichier peut également être utilisé dans le sens inverse, c'est-à-dire pour détourner des noms de domaine connus vers des sites peu fréquentables.

- **Browser hijack :** cette expression anglophone est utilisée par certains logiciels à la traduction incomplète. En français dans le texte, il s'agit d'un détournement de navigateur, concernant notamment la page de démarrage et le moteur ou le moteur de recherche par défaut.