Les antivirus utilisent différentes techniques pour détecter et prévenir les infections par des logiciels malveillants. Trois approches courantes sont l'analyse heuristique, l'analyse par signature et l'utilisation de sandbox.

Analyse Heuristique :

Principe : L'analyse heuristique repose sur des règles et des modèles de comportement plutôt que sur des signatures spécifiques de logiciels malveillants connus. L'antivirus analyse le comportement des programmes en examinant des caractéristiques potentiellement suspectes ou des modèles d'activité malveillante.

Avantages : Utile pour détecter de nouveaux types de logiciels malveillants pour lesquels aucune signature n'existe encore.

Inconvénients : Peut parfois générer des faux positifs en classant à tort des programmes légitimes comme malveillants.

Analyse par Signature :

Principe : L'analyse par signature repose sur des signatures spécifiques, c'est-à-dire des empreintes digitales uniques de logiciels malveillants connus. L'antivirus compare ces signatures avec les fichiers présents sur le système pour trouver des correspondances.

Avantages : Efficace pour détecter des menaces connues avec des signatures établies.

Inconvénients : Ne peut pas détecter les nouvelles menaces pour lesquelles aucune signature n'a été développée.

Utilisation de Sandbox :

Principe : Une sandbox est un environnement isolé dans lequel un programme peut s'exécuter sans affecter le système hôte. Les antivirus utilisent des sandboxes pour exécuter de manière sécurisée des fichiers suspects et observer leur comportement.

Avantages : Permet la détection des menaces inconnues en observant les actions qu'elles entreprennent dans un environnement isolé.

Inconvénients : Peut entraîner une charge de travail plus importante et des performances réduites, et certaines menaces peuvent être conçues pour échapper à la détection dans un environnement de sandbox.

En pratique, de nombreux antivirus combinent ces approches pour offrir une protection plus complète. L'analyse heuristique et l'utilisation de sandbox sont particulièrement utiles pour identifier de nouvelles menaces, tandis que l'analyse par signature offre une protection solide contre les logiciels malveillants connus