

Comment fonctionne un antivirus ?

Date de dernière mise à jour : 29/04/2014 à 12:40

Source : <http://www.vulgarisation-informatique.com/fonctionnement-antivirus.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)

Pourquoi un antivirus ?

Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les virus présents dans votre micro, et de prendre des mesures pour les empêcher de nuire.

Les antivirus sont des programmes devenus de plus en plus indispensables au fil des années. En effet, ceux qui se souviennent des débuts d'internet peuvent en témoigner : on pouvait auparavant surfer tranquillement sur la toile à l'aide d'un simple pare-feu, sans être trop inquiet, dès lors que l'on **faisait attention à ce que l'on téléchargeait**.

Aujourd'hui, cette époque est révolue. **Le moindre site internet un peu trop malicieux peut vous infecter**, la plupart du temps via des **plugins** (Flash, Java pour ne pas les citer).

Son fonctionnement ne consiste pas qu'à analyser les fichiers du système, puisque si un fichier est infecté, le mal est souvent fait. Le rôle de l'antivirus consiste aussi à prévenir l'attaque virale, en **analysant le comportement**.

Pour détecter un virus, il se sert de plusieurs techniques :

Détection de la signature

On l'appelle aussi **scan** ou **scanning**. C'est la méthode la plus ancienne et la plus utilisée. Cette méthode consiste à analyser le disque dur à la recherche de la **signature** du virus, qui est présente dans la base de données du logiciel, si celui-ci est à jour et si il connaît ce virus.

La signature est un **morceau de code** ou une **chaîne de caractères** du virus qui permet de l'identifier. Chaque virus a sa propre signature, qui doit être connue de l'antivirus. Cette méthode n'est pas efficace contre les nouveaux virus ou les virus dits **polymorphes**, dont la signature change à chaque réplique.

L'avantage de la technique du scan est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée.

Pour rester efficace, l'antivirus doit procéder à la mise à jour régulière de sa base de données antivirale. Une fréquence de mise à jour mensuelle est un minimum acceptable.

La signature EICAR

La signature mise au point par [EICAR](#) est un faux virus. Suivez mon [tutoriel pour savoir comment créer un virus](#) de test. Votre antivirus devrait vous alerter, soit après analyse du fichier (changez d'antivirus) ou alors dès l'enregistrement de celui-ci sur le disque dur (analyse permanente, gage d'une meilleure sécurité).

Le contrôle d'intégrité

Vérifier l'**intégrité** d'un fichier consiste à contrôler qu'il n'a **pas été modifié ou altéré au cours du temps**.

L'antivirus, pour contrôler l'intégrité des fichiers, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations qui peuvent changer lorsque le fichier est modifié :

- La taille
- La date et heure de dernière modification
- La somme de contrôle (CRC : code de redondance cyclique) éventuelle.

Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus **réside en mémoire**), l'antivirus recalcule la somme de contrôle et vérifie que

les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé.

Pour contrer en partie cette parade, les virus ne modifient pas forcément la date de modification du fichier, ou la rétablissent.

L'analyse heuristique

C'est la méthode la plus puissante car elle permet de détecter d'éventuels virus inconnus par votre antivirus. Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes.

Le comportement du virus

L'antivirus surveille en permanence le comportement des logiciels actifs (si il est en fonctionnement et que la protection automatique est activée). Il analyse tous les fichiers modifiés et créés. En cas d'anomalie, il avertit l'utilisateur par un message explicite. Cette méthode n'est jamais utilisée seule et vient en complément de l'une des deux premières. Cette protection est indispensable lorsque vous surfez sur internet.

Lorsque l'antivirus a détecté un virus, il offre trois possibilités à l'utilisateur.

Réparer le fichier - : L'antivirus doit être capable de réparer un fichier atteint. Mais ce n'est pas toujours possible.

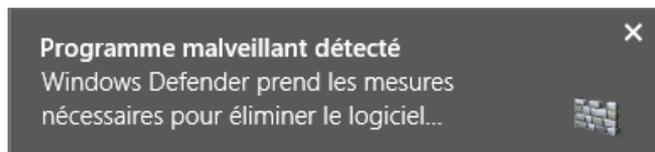
Supprimer le fichier - : Si l'antivirus n'est pas capable de supprimer le fichier, vous pouvez le supprimer. Je vous conseille cette option si le fichier n'est pas important, sinon, mettez le en quarantaine.

Mise en quarantaine du fichier infecté- : C'est une solution d'attente. L'antivirus place le fichier dans un dossier sûr du disque dur. Lorsque l'antivirus sera capable de réparer le fichier, vous pourrez extraire le fichier du dossier et le réparer (ne comptez pas dessus si des données sensibles sont en quarantaine).

Quel antivirus choisir ?

Si vous ne souhaitez pas acheter un antivirus, sachez qu'il existe des solutions gratuites sur internet. Vous pouvez diagnostiquer votre micro à l'aide d'un [antivirus en ligne gratuit](#). Il permet de détecter et d'éliminer la plupart des virus connus.

Un antivirus excellent existe depuis quelques années : MSE (Microsoft Security Essentials), inclus de base dans **Windows 8**. C'est un antivirus entièrement gratuit que vous pouvez [télécharger ici](http://www.microsoft.com/fr-fr/download/details.aspx?id=5201). Il est très léger mais aussi très efficace, vous pouvez donc vous passer de votre antivirus actuel si vous en avez un.



Source : <http://www.vulgarisation-informatique.com/fonctionnement-antivirus.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)