



# Faire un scan de son ordinateur à l'aide d'un live CD

Pour plus de sécurité, adoptez les réflexes CASES !

## Table des matières

- 1 Pourquoi faire une vérification de présence de virus à l'aide d'un live CD Linux ?
- 2 Téléchargement et premiers pas
- 3 Alternatives

### 1 Pourquoi faire une vérification de présence de virus à l'aide d'un live CD Linux ?

Il est très important de posséder un antivirus fonctionnel et mis à jour qui agit comme une première ligne de défense contre les programmes malveillants.

Malheureusement, l'installation d'un tel antivirus n'est pas une garantie absolue de sécurité. En effet, pour distinguer les programmes malveillants des programmes inoffensifs, les antivirus dépendent de signatures (empreintes des virus) que les créateurs d'antivirus mettent à disposition régulièrement sous forme de mises à jour. Parfois les virus peuvent être plus rapides et se nicher dans les systèmes d'exploitation avant que l'antivirus ne puisse les détecter. Comme certains possèdent des systèmes d'évasion, ils peuvent ne jamais être détectés, même après le téléchargement de la signature adéquate. Il est alors important de pouvoir analyser un système quand aucun de ses éléments n'est en fonctionnement, particulièrement les programmes malveillants éventuels.

Linux, un système d'exploitation librement téléchargeable, existe sous une forme spéciale dite « Live », qui se présente le plus souvent sous forme de disque compact permettant le démarrage d'un ordinateur sans installation préalable et n'effectuant aucun changement sur l'ordinateur utilisé.

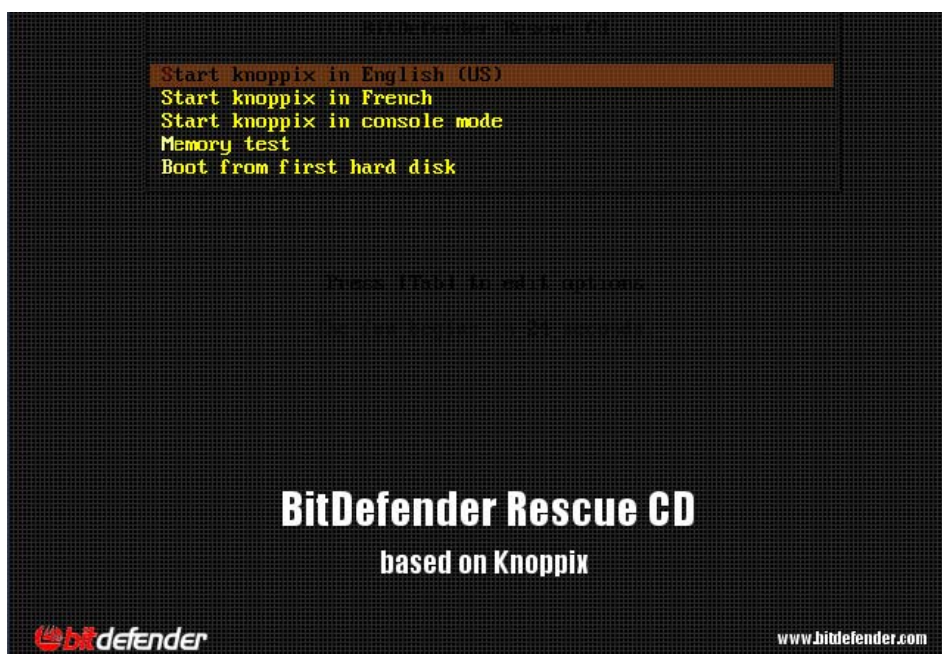
Des fabricants d'antivirus comme Bitdefender ont profité de ces systèmes d'exploitation éphémères pour créer des systèmes de détections de virus. Linux se charge sur votre ordinateur, charge l'antivirus et analyse vos disques durs tout en gardant votre système d'exploitation installé dormant, rendant ainsi la détection de virus, vers, chevaux de Troie et plus particulièrement de rootkits plus aisée.

### 2 Téléchargement et premiers pas

Le système Live de Bitdefender (Bitdefender rescue cd) est à disposition gratuitement sur le site suivant : [http://download.bitdefender.com/rescue\\_cd/](http://download.bitdefender.com/rescue_cd/).

Veillez télécharger le fichier avec l'extension « iso » (et non « md5 »). Ce fichier, relativement volumineux, est une image de disque compact prête à être gravée. Pour l'utiliser, il suffit de se servir d'un logiciel de gravure. Prenez bien garde de ne pas graver votre CD comme disque de données conventionnel avec le fichier image comme contenu, mais cherchez plutôt l'option « graver une image » ou « burn image » en anglais.

Une fois le CD gravé il faudra redémarrer votre ordinateur avec le CD dans votre lecteur. Sur la plupart des ordinateurs le disque sera lancé au démarrage au lieu du système d'exploitation habituel et vous verrez un écran de ce type :



À ce stade vous pouvez simplement appuyer sur « Entrée » pour démarrer le système d'exploitation Live.

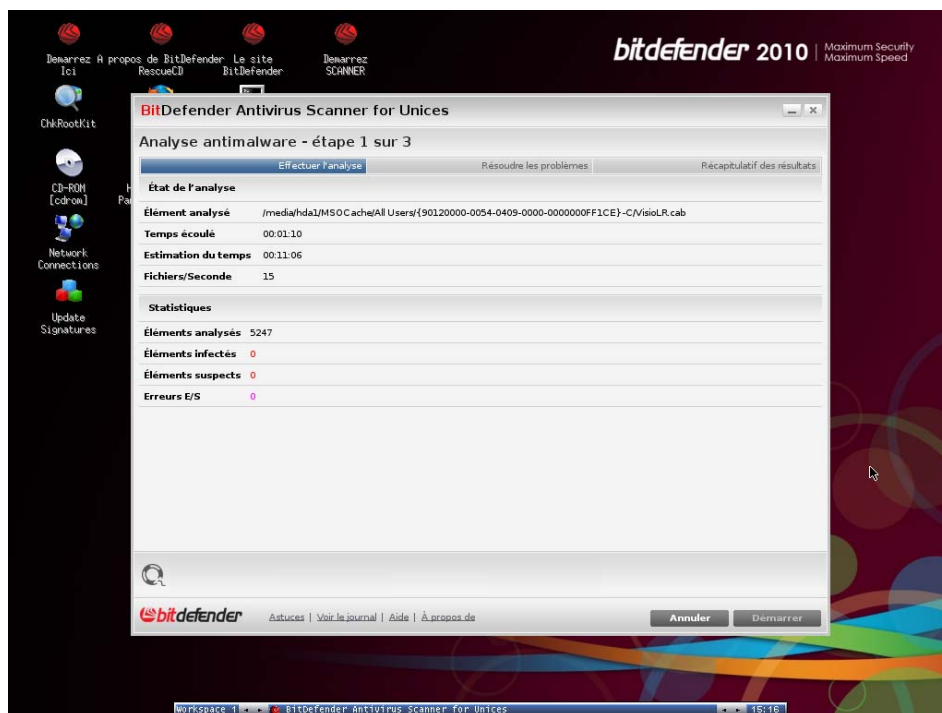
Si vous ne voyez pas cet écran, mais que votre système d'exploitation habituel démarre, votre BIOS n'est pas configuré pour démarrer sur CD. Ce réglage dépend de votre ordinateur et nous ne pouvons malheureusement que vous donner des pistes pour faire les réglages nécessaires :

- Au début du démarrage appuyez sur la touche « Del », « F12 » ou « Esc » (si cette action ne marche pas renseignez-vous auprès du fabricant de votre ordinateur). Cela ouvrira soit un menu de sélection du média de démarrage, soit le menu de configuration du BIOS de votre machine.

- Si le menu de configuration du BIOS de votre machine est ouvert par cette action, sélectionnez l'option qui définit le lecteur CD comme média de démarrage prioritaire avant le disque dur.

Pendant le démarrage, une mise à jour des signatures des virus sera tentée. Pour cela il faut que l'ordinateur ait un accès direct à Internet. Sachez que le wifi ne marchera pas la plupart du temps, pensez donc à utiliser un câble réseau pour la durée de la procédure.

Après un temps d'attente plus ou moins long (sachez être patient, en effet le lecteur CD est beaucoup plus lent qu'un disque dur), l'analyse du système sera lancée automatiquement. Vous verrez apparaître l'écran à droite de la page :



À ce stade vous devrez être patient car l'analyse peut durer des dizaines de minutes voire des heures. Une fois le scan terminé un écran de résultats apparaîtra :



Dans le cas d'une détection de logiciels malveillants, l'antivirus vous proposera certains modes d'action. Nous vous conseillons alors d'effacer les virus éventuels. Quand vous aurez fini, faites un click droit sur le fond d'écran et cliquez sur l'option « Exit », comme illustré ci-dessus.

Le système s'éteindra et éjectera le disque compact. N'oubliez pas de l'enlever pour redémarrer normalement votre système d'exploitation habituel.

### 3 Alternatives

Différentes alternatives existent, certaines payantes d'autres gratuites. Nous vous proposons une autre solution gratuite avec l'antivirus « avira » téléchargeable sur le site suivant : [http://www.free-av.com/en/tools/12/avira\\_antivir\\_rescue\\_system.html](http://www.free-av.com/en/tools/12/avira_antivir_rescue_system.html).

Sur cette page vous pourrez télécharger un exécutable Windows qu'il suffira de lancer pour graver automatiquement le compact disque Live de détection de virus.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)