Introduction

Panda Antivirus

Panda Antivirus est une solution complète et efficace qui protège votre ordinateur contre tout type de virus. Il inclut les versions Windows 95, Windows NT Workstation, Windows 3.1x, DOS et OS/2 pour que vous soyez protégé quel que soit votre système d'exploitation. Cette aide correspond à **Panda Antivirus** pour Windows NT Workstation.

Stratégies de protection

Panda Antivirus emploie plusieurs stratégies de protection contre les virus :

- **Protection permanente :** la protection permanente se charge de protéger l'ordinateur de façon continue contre les virus, sans l'intervention de l'utilisateur. Le principal avantage de cette stratégie de protection est qu'elle permet de protéger l'ordinateur de façon entièrement automatique.
- **Analyse sur demande :** l'analyse sur demande permet d'analyser n'importe quelle partie de l'ordinateur à la demande de l'utilisateur. Une fois que l'on aura choisi la zone à analyser, le programme commencera à rechercher des virus dans la zone indiquée.
- **Désinfection :** lorsqu'un virus a été détecté, plusieurs solutions sont possibles. L'une d'elles est la désinfection, qui consiste à éliminer le virus du fichier de façon à restituer celui-ci exactement comme il était avant l'infection.
- **Analyse heuristique :** l'analyse heuristique est une technique d'analyse différente des techniques précédentes. L'analyse heuristique fonctionne sur demande. C'est-à-dire que l'utilisateur doit indiquer la zone de l'ordinateur qu'il souhaite analyser à l'aide de cette méthode à un moment déterminé. Cette technique d'analyse est conçue pour détecter des virus inconnus.
- **Recherche de chaînes :** de même que l'analyse heuristique, il s'agit d'une technique d'analyse différente qui fonctionne également à la demande de l'utilisateur. Elle permet de rechercher de nouveaux virus à partir d'informations fournies par le service d'assistance technique de Panda Software.
- **Autres options :** cette section regroupe certaines fonctions destinées à offrir des informations ou à faciliter la gestion de l'antivirus. Par exemple, il est possible d'obtenir un rapport de résultats présentant les différents incidents et les opérations réalisées par l'antivirus.

Solutions antivirus Panda Software

Panda Software vous offre les solutions anti-virus suivantes :

- **24h-365d® Assurance Antivirus® pour PC individuels.** *Licences.*
- **24h-365d® Assurance Antivirus® pour PC en réseau.** (distribution automatique depuis des serveurs).
- **24h-365d® Assurance Antivirus® pour serveurs de réseau.** (Novell NetWare et Windows NT Server).
- **24h-365d® Assurance Antivirus® pour réseaux locaux.**
- **24h-365d® Assurance Antivirus® pour clients de e-mail et logiciel de groupe.**
- **24h-365d® Assurance Antivirus® pour serveurs de e-mail et logiciel de groupe.**
- **24h-365d® Assurance Antivirus® pour serveurs de courrier SMTP.**
- **24h-365d® Assurance Antivirus® pour PC connectés à Internet.**

- **24h-365d® Assurance Antivirus® pour serveurs d'Internet (SMTP, FTP et HTTP)**.
- **24h-365d® Assurance Antivirus® pour Proxys.**

Qu'est-ce que 24h-365d Assurance Antivirus Panda Software?

24h-365d® Assurance Antivirus® Panda Software est un nouveau concept révolutionnaire de protection anti-virus offrant une sécurité optimale. **24h-365d® Assurance Antivirus® Panda Software** est une combinaison parfaite de produits et services qui garantit les niveaux de protection les plus élevés contre les virus. **24h-365d® Assurance Antivirus® Panda Software** peut être souscrit pour une durée et une périodicité de mise à jour variables.

Ce produit est fourni par **Panda Antivirus**, un anti-virus qui a obtenu les certificats les plus exigeants en matière de détection de virus :

- Le **Certificat ICSA :** décerné par le prestigieux organisme américain ICSA aux produits anti-virus qui détectent périodiquement 100% des virus *In the Wild* (les virus les plus répandus à tout moment) et plus de 90% de la *Zoo Collection* (collection de milliers de virus moins courants).
- Le **Certificat CheckMark :** décerné par la revue anglaise spécialisée en sécurité informatique *Secure Computing*.

Si vous ne possédez pas **24h-365® Assurance Antivirus® Panda Software**, vous pouvez le souscrire en utilisant le bon de commande inclus dans la carte d'enregistrement. Voici un résumé des services offerts par **24h-365® Assurance Antivirus® Panda Software** :

- **Hot-Line :** pendant UN an, nous résoudrons vos problèmes techniques par téléphone, fax, Internet ou courrier électronique. A n'importe quelle heure du jour ou de la nuit, vous trouverez des techniciens hautement qualifiés qui seront à votre disposition 24 heures sur 24 et 365 jours par an. C'est un service exclusif de **Panda Software.**
- **S.O.S. Virus :** si vous trouvez un virus que **Panda Antivirus** ne peut détecter ou éliminer, nous enverrons un coursier à votre domicile (ou nous irons chercher l'échantillon suspect par tout autre moyen) et nous développerons en moins de 24 heures une nouvelle version capable de détecter et d'éliminer le nouveau virus. Nous vous enverrons cette nouvelle version totalement gratuitement.
- **Service de mises à jour avec livraison à domicile :** votre anti-virus sera actualisé en permanence. Vous recevrez à votre domicile des mises à jour mensuelles ou trimestrielles sur CD ou disquette si vous avez souscrit à notre solution **24h-365d® Assurance Antivirus® Panda Software.** Vous pourrez également mettre à jour le produit à travers notre WEB autant de fois que vous le souhaiterez, pendant un an, sachant que nous vous garantissons au moins une nouvelle actualisation chaque jour.
- **Service WEB** : résolution des problèmes les plus fréquents et informations sur les virus.

Installation

Configuration requise

Pour pouvoir installer **Panda Antivirus** pour Windows NT Workstation, les éléments suivants sont nécessaires :

- Ordinateur compatible IBM avec processeur 486 ou supérieur.
- 16 Mo de RAM.
- 4 Mo d'espace libre sur le disque dur.
- Système d'exploitation Windows NT 3.51 ou supérieur.
- Lecteur de CD-Rom.
- Souris.

Procédure d'installation

Il existe deux versions de **Panda Antivirus** pour Windows NT Workstation. L'une d'elles correspond à la version 3.51 de ce système d'exploitation et l'autre à la version 4.0. On veillera à installer la version correspondant au système d'exploitation utilisé.

Les deux versions ne peuvent être installées qu'à partir du CD-Rom livré avec le produit. Pour installer l'une comme l'autre, il faut exécuter le programme CDMENU.COM. Ce programme offre un menu d'options très simple. On choisira d'abord la langue souhaitée, puis la version à installer. Dans ce cas, on choisira l'une des deux versions de **Panda Antivirus** pour Windows NT, la 3.51 ou la 4.0, en fonction du système d'exploitation installé.

Pour pouvoir installer la version de **Panda Antivirus** pour Windows NT Workstation, vous devez posséder des droits d'administrateur sur votre ordinateur. En effet, ces droits sont nécessaires pour l'installation du gestionnaire chargé d'assurer la protection permanente.

La procédure d'installation se déroule de la manière suivante :

1. Vous verrez tout d'abord s'afficher un écran de bienvenue.
2. On vous demandera de fournir un certain nombre de renseignements sur l'utilisateur.
3. On vous demandera d'indiquer le répertoire dans lequel vous voulez installer l'application.
4. On vous demandera d'indiquer le groupe de programmes dans lequel seront créées les icônes d'accès à l'antivirus.
5. On vous demandera de choisir d'installer la protection permanente (pilote **Sentinel**) ou non.
6. Les fichiers seront copiés sur le disque dur.
7. Une fois la copie de fichiers terminée, il est recommandé de relancer l'ordinateur pour que la protection permanente se mette en marche.

Mise à jour de l'antivirus

Pour mettre à jour une version, il suffit d'installer la nouvelle version reçue sur l'ancienne.

Désinstallation

La désinstallation de **Panda Antivirus** pour Windows NT 3.51 s'effectue au moyen du programme DÉSINSTALLER qui se trouve dans le groupe de fichiers de l'application.

La désinstallation de **Panda Antivirus** pour Windows NT 4.0 s'effectue au moyen de l'option *Ajouter ou Enlever applications* du *Panneau de Configuration*. Il suffit de choisir **Panda Antivirus** dans la liste affichée dans cette option et d'appuyer sur le bouton *Ajouter ou Enlever*. Pour terminer la désinstallation, il est nécessaire de relancer l'ordinateur.

N'essayez pas de désinstaller cette version en supprimant le dossier dans lequel vous l'avez installée. Veillez à toujours suivre la procédure de désinstallation indiquée.

Qu’est-ce que la protection permanente?

La protection permanente est un programme qui, dès le démarrage de l’ordinateur, intercepte toutes les opérations impliquant un risque de contagion pour vérifier qu’aucun virus n’entre dans le système.

La protection permanente fonctionne de manière totalement automatique, sans aucune intervention de l’utilisateur. Malgré la surveillance constante, le rendement du système n’est pas affecté. Il est donc fortement conseillé d’installer la protection permanente puisqu’elle augmente considérablement le niveau de protection de l’ordinateur.

Comment utiliser la protection permanente

La protection permanente est une des options d'installation. Si vous choisissez d'installer cette option, la protection permanente (**Sentinel**) se mettra en marche dès que vous démarrerez l'ordinateur.

Si le système d'exploitation est Windows NT Workstation 3.51, **Sentinel** apparaîtra sous forme d'icône réduite sur le bureau de Windows. Si le système d'exploitation est Windows NT Workstation 4.0, **Sentinel** apparaîtra sous forme d'icône à côté de l'horloge sur la barre de tâches.

La protection permanente fonctionne de manière entièrement automatique. Lorsque **Sentinel** détecte la présence d'un virus au cours d'une opération quelconque, il émet un message d'avertissement et prend les mesures appropriées.

Comment configurer la protection permanente

La protection permanente peut être configurée en fonction des besoins de chaque utilisateur. En cliquant deux fois sur l'icône de **Sentinel**, on ouvre une fenêtre dotée de plusieurs onglets. Chaque onglet se rapporte à la configuration d'un des différents aspects de **Sentinel**. Les options de configuration sont les suivantes :

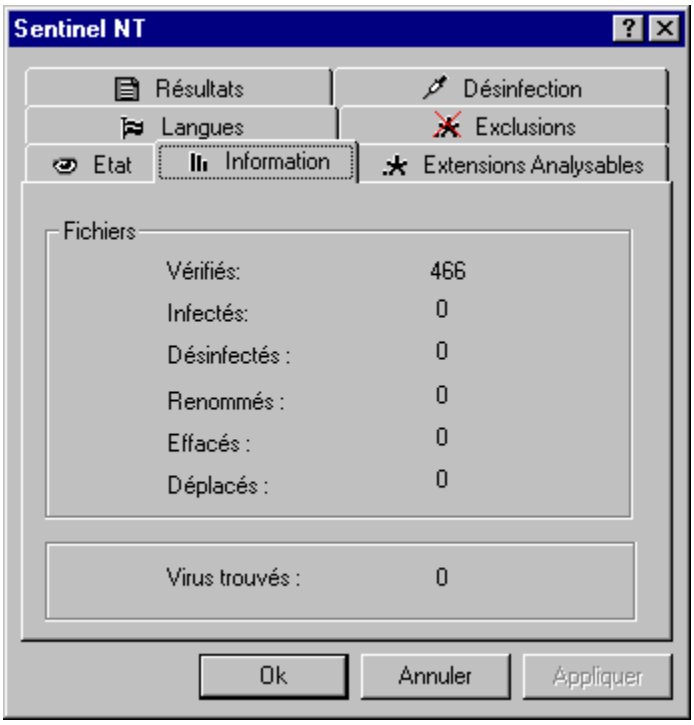
Etat

L'état de la protection permanente est indiqué dans chaque onglet.

- **Activé :** cette option permet d'activer ou de désactiver la protection permanente. Il faut savoir que si l'on désactive la protection permanente, l'ordinateur ne sera plus protégé contre les virus.
- **Entrées :** lorsque la protection permanente est activée, cette option indique qu'il faut analyser toutes les entrées de fichier dans l'ordinateur. Les créations et les modifications de fichiers seront également analysées.
- **Sorties :** lorsque la protection permanente est activée, cette option indique qu'il faut analyser toutes les sorties de fichier de l'ordinateur. Les ouvertures et les exécutions de de fichiers seront également analysées.
- **Renommé :** lorsque la protection permanente est activée, cette option indique qu'il faut analyser toutes les opérations de changement de nom de fichiers.
- **Réseau Microsoft :** lorsque la protection permanente est activée, cette option indique qu'il faut analyser à distance toutes les opérations effectuées sur une unité de réseau Microsoft.
- **Réseau Novell :** lorsque la protection permanente est activée, cette option indique qu'il faut analyser à distance toutes les opérations effectuées sur une unité de réseau Novell.

Information

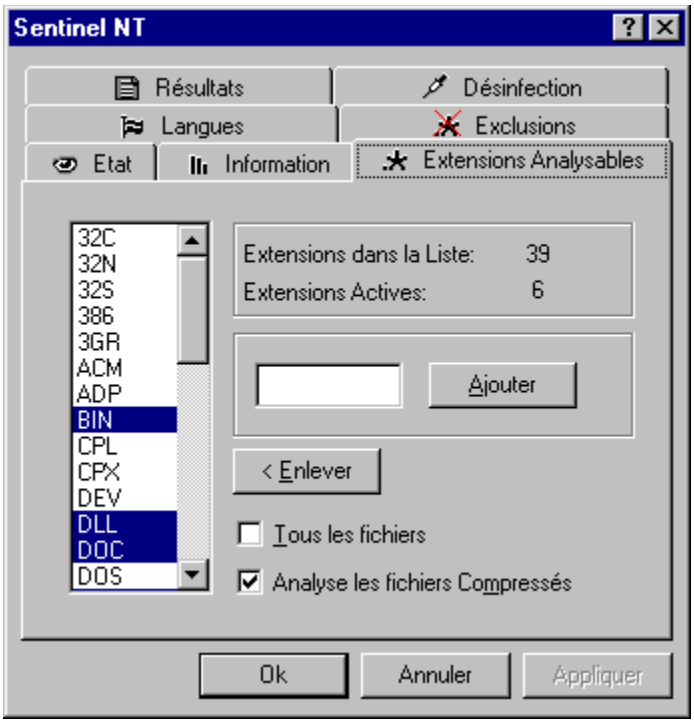
Cet onglet contient diverses informations sur l'activité de la protection permanente.



- **Révisés :** indique le nombre de fichiers que la protection permanente a contrôlés depuis le démarrage du système.
- **Infectés :** indique le nombre de fichiers infectés que le programme a localisés.
- **Désinfectés :** indique le nombre de fichiers désinfectés par la protection permanente.
- **Renommés :** indique le nombre de fichiers renommés par la protection permanente.
- **Supprimés :** affiche le nombre de fichier que la protection permanente a supprimés parce qu'ils étaient infectés par un virus.
- **Déplacés :** informe du nombre de fichier que la protection permanente a déplacés parce qu'ils étaient infectés par un virus.
- **Virus localisés :** enfin, on trouvera ici le nombre de virus détectés.

Extensions à analyser

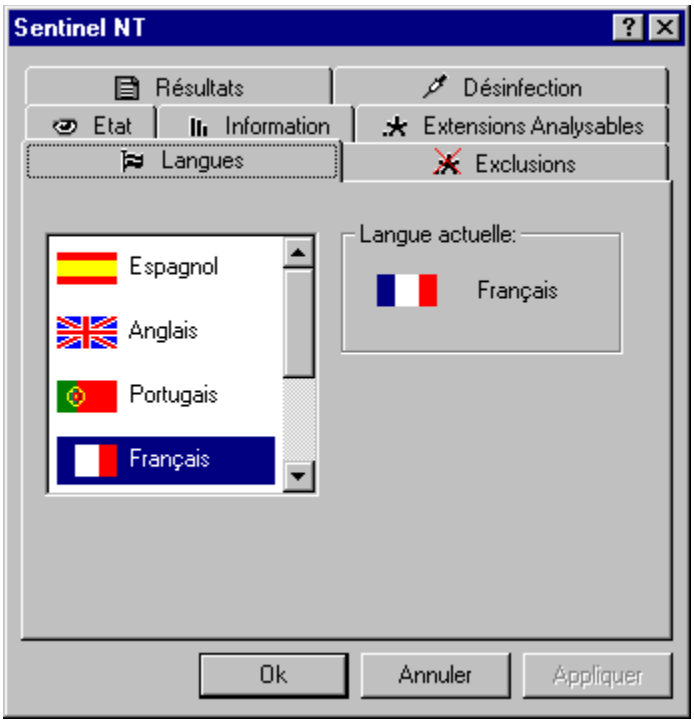
Cet onglet indique les extensions à analyser par la protection permanente.



- **Liste des extensions:** toutes les extensions que l'on souhaite analyser peuvent être cochées sur la liste des extensions. La protection permanente continuera d'intercepter tous les fichiers auxquels on accèdera, mais elle analysera uniquement les fichiers possédant l'une des extensions sélectionnées. Quelles que soient les extensions sélectionnées, les fichiers EXE et COM seront systématiquement analysés.
- **Extensions dans la liste :** indique le nombre d'extensions figurant dans la liste.
- **Extensions actives :** informe du nombre d'extensions cochées pour analyse sur la liste.
- **Ajouter extension :** pour ajouter une extension à la liste, on écrira l'extension dans la case prévue à cet effet, puis on appuiera sur le bouton *Ajouter*.
- **Eliminer extension :** pour ajouter une extension à la liste, on la sélectionnera dans la liste, puis on appuiera sur le bouton *Eliminer*.
- **Tous les fichiers :** si cette option est cochée, tous les fichiers seront analysés, quelles que soient les extensions sélectionnées.
- **Analyser les fichiers comprimés :** si cette option est cochée, tous les fichiers comprimés auxquels on accèdera seront analysés.

Langues

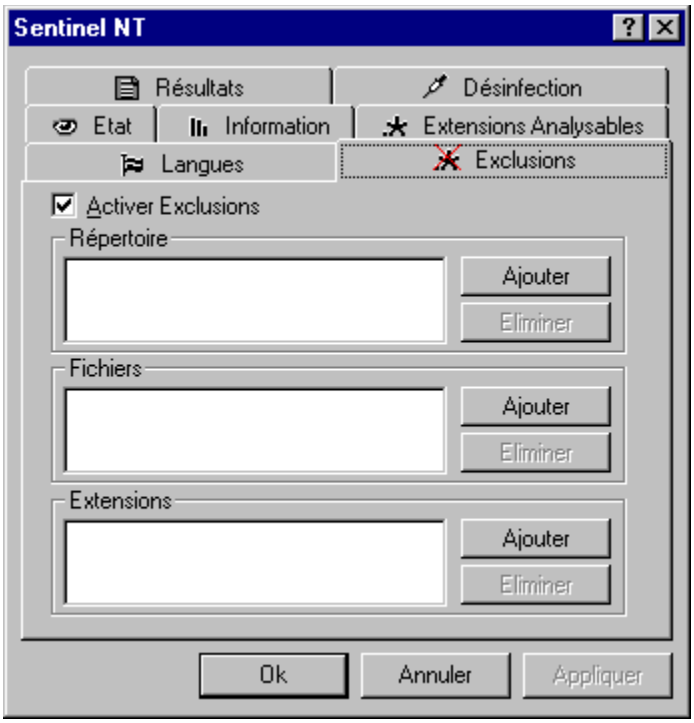
Cet onglet permet de vérifier dans quelle langue la protection permanente a été configurée et de choisir une autre langue sur la liste des langues disponibles.



- **Langues disponibles :** une liste indique les différentes langues disponibles pour la protection permanente. Pour changer de langue, il suffit de sélectionner la langue souhaitée et d'appuyer sur le bouton *Accepter* ou sur le bouton *Appliquer*.
- **Langue actuelle :** indique la langue dans laquelle la protection permanente est actuellement configurée.

Exclusions

Cet onglet permet d'indiquer les zones, fichiers ou extensions que l'on ne souhaite pas analyser. Indépendamment des indications fournies dans l'onglet *Extensions*, toutes les zones, tous les fichiers et toutes les extensions indiqués ici **ne seront pas analysés**.



- **Activer exclusions :** si cette option est cochée, la fonction d'exclusion sera activée en fonction des données indiquées.
- **Répertoire :** cette zone affiche la liste de tous les répertoires qui ne doivent pas être analysés.
- **Ajouter répertoire :** cette option permet d'ajouter des répertoires à la liste des répertoires qui ne doivent pas être analysés.
- **Eliminer répertoire :** cette option permet d'éliminer des répertoires de la liste des répertoires qui ne doivent pas être analysés.
- **Fichier :** cette zone affiche la liste des fichiers qui ne doivent pas être analysés.
- **Ajouter fichier :** cette option permet d'ajouter des fichiers à la liste des fichiers qui ne doivent pas être analysés.
- **Eliminer fichier :** cette option permet d'éliminer des fichiers de la liste des fichiers qui ne doivent pas être analysés.
- **Extensions :** cette zone affiche la liste des extensions qui ne doivent pas être analysées. Même si l'une de ces extensions se trouve sur la liste des extensions à analyser, elle ne sera pas analysée.
- **Ajouter extension :** cette option permet d'ajouter des extensions à la liste des extensions qui ne doivent pas être analysées.
- **Eliminer extension :** cette option permet d'éliminer des extensions de la liste des extensions qui ne doivent pas être analysées.

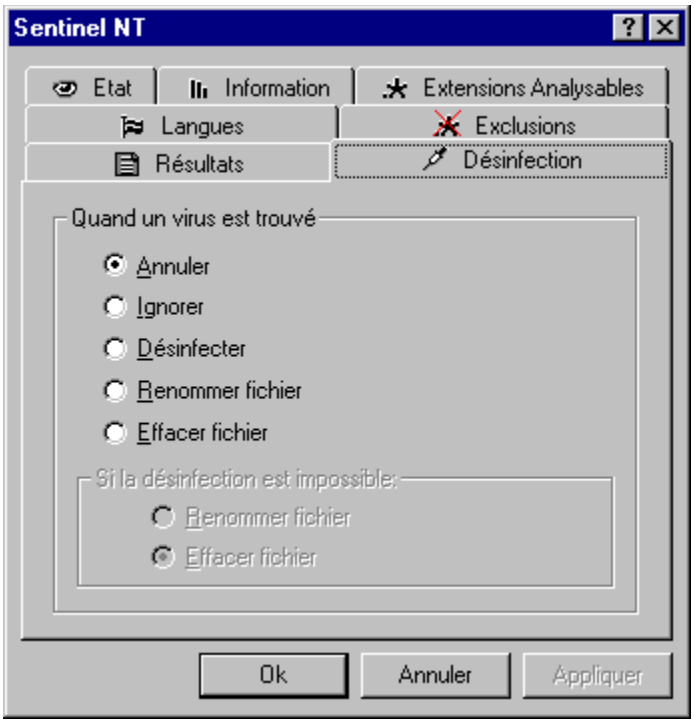
Résultats

Cet onglet permet de configurer le fonctionnement du système fournissant les rapports sur les incidents détectés par la protection permanente.

- **Créer rapport local :** si cette option est activée, le programme établira un rapport sur les différents incidents détectés par la protection permanente.
- **Utilisateur :** indique le nom de l'utilisateur de l'ordinateur.
- **Voir rapport :** ce bouton permet d'afficher le rapport sur les incidents détectés jusqu'à présent.
- **Imprimer rapport :** ce bouton permet d'imprimer le rapport d'incidents.
- **Effacer rapport :** ce bouton permet d'effacer le rapport d'incidents.

Désinfection

Cet onglet permet de configurer le mode de désinfection des fichiers contaminés par un virus et détectés par la protection permanente.

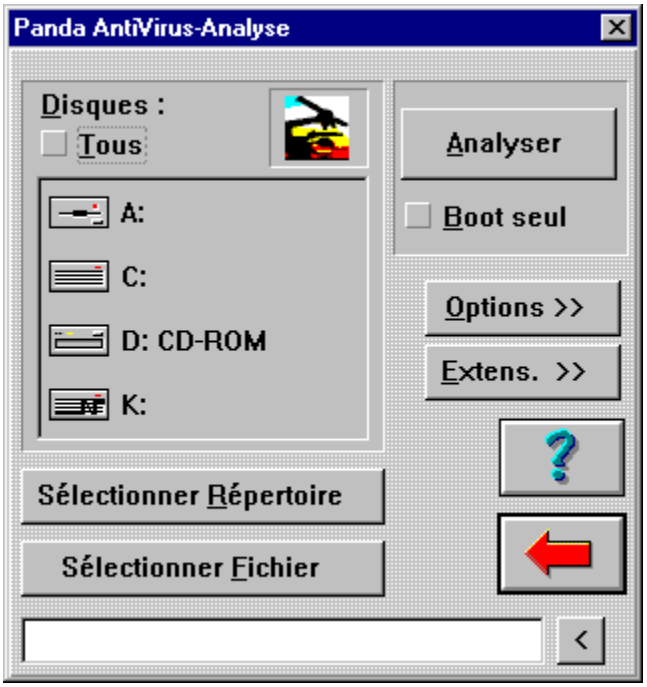


- **Annuler :** si vous cochez cette option, l'opération au cours de laquelle le virus a été détecté sera annulée. Par exemple, si le virus a été localisé dans un fichier que l'on essayait d'exécuter, l'exécution de ce fichier sera annulée.
- **Ignorer :** lorsque cette option est cochée, les détections de virus sont ignorées.
- **Désinfecter :** si vous cochez cette option et si la protection permanente détecte un virus, elle procèdera à la désinfection du fichier, le restituant dans les conditions préalables à l'infection.
- **Renommer fichier :** lorsque cette option est cochée, si un virus est détecté, **Sentinel** renommera le fichier en lui attribuant l'extension VIR.
- **Supprimer fichier :** si vous cochez cette option et si **Sentinel** détecte un virus dans un fichier, celui-ci sera supprimé.
- **Si la désinfection est impossible, renommer fichier :** si cette option est activée, lorsque **Sentinel** détectera un virus et essaiera de le désinfecter, si cette opération ne peut être réalisée de façon satisfaisante, le fichier sera renommé.
- **Si la désinfection est impossible, supprimer fichier :** si cette option est activée, lorsque **Sentinel** détectera un virus et essaiera de le désinfecter, si cette opération ne peut être réalisée de façon satisfaisante, le fichier sera supprimé.

Qu’est-ce que l’analyse sur demande?

L’analyse sur demande vous permet d’analyser n’importe quelle zone de votre ordinateur au moment où vous le souhaitez. Chaque analyse effectuée peut être configurée à l’aide d’une série d’options simples.

Comment utiliser l’analyse sur demande



Pour réaliser une analyse sur demande, on procèdera de la manière suivante :

1. **Exécuter l’anti-virus :** pour exécuter l'anti-virus, placez-vous dans le groupe de programmes où les icônes permettant de le lancer ont été créées. Cliquez deux fois sur *l'icône Panda Antivirus*.
2. **Aller dans la section d’analyse :** pour vous placer dans cette section, appuyez sur le bouton *Analyser* sur la barre de boutons de l'application. Vous verrez apparaître une fenêtre dans laquelle vous pourrez préciser la zone à analyser et le mode d'analyse.
3. **Choisir la zone à analyser :** vous devrez ensuite choisir la zone que vous souhaitez analyser. Une liste indique les différentes unités reconnues par le système. Vous pouvez également indiquer un répertoire ou un fichier spécifique à l'aide des boutons prévus à cet effet.
4. **Configurer les extensions :** cette opération est facultative. Le programme enregistre la configuration des extensions que vous souhaitez analyser. Une fois que les extensions sont configurées, il n'est donc pas nécessaire de les reconfigurer lors de chaque analyse.
5. **Configurer les options d'analyse :** cette opération est également facultative. Le programme enregistre la configuration des options d'analyse. Une fois que l'analyse est configurée, il n'est donc pas nécessaire de la reconfigurer lors de chaque analyse. On ne modifiera cette configuration que lorsque l'on souhaitera choisir un ensemble d'options différent. Vous trouverez des explications plus détaillées sur les options d'analyse dans le chapitre de configuration de ce même document.
6. **Indiquer si l'on souhaite analyser uniquement le secteur d’amorce :** cette option est facultative. Si vous cochez cette option, seul le secteur d’amorce des unités sélectionnées sera analysé, pas les fichiers. Si l'on n'active pas cette option, le secteur d’amorce et les fichiers de toutes les unités sélectionnées seront analysés.
7. **Commencer l'analyse :** le bouton *Analyser* lance la recherche de virus dans les zones sélectionnées en fonction des options choisies.

Comment configurer l'analyse sur demande

Comme nous l'avons dit plus haut, pour effectuer une analyse, il faut indiquer :

- La zone à analyser.
- Les extensions à prendre en compte lors de l'analyse.
- La façon dont l'analyse va être réalisée.

Pour configurer l'analyse, vous devrez spécifier les extensions concernées et les options d'analyse.

Extensions

En appuyant sur le bouton *Extensions*, vous ouvrirez une fenêtre dans laquelle vous pourrez indiquer les extensions à analyser.

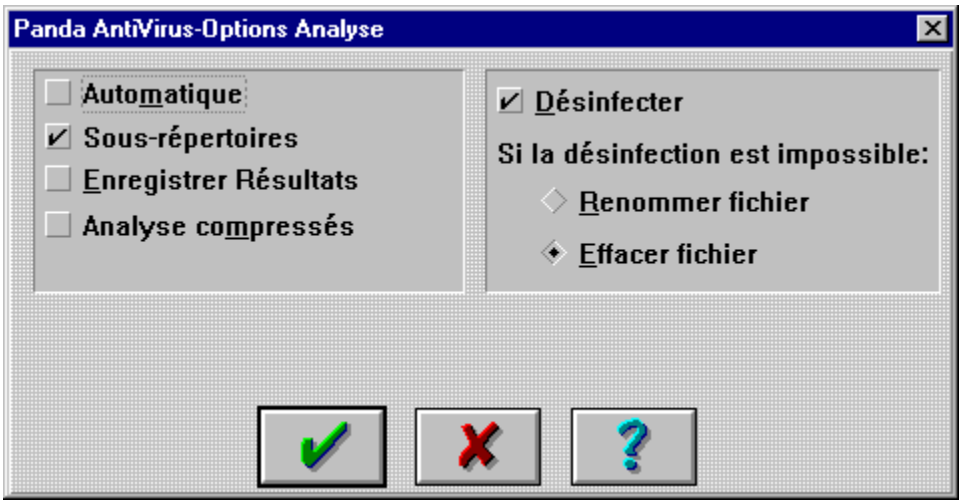
L'option *Toutes* figurant sur la liste des extensions indique que tous les fichiers devront être analysés, quelle que soit leur extension. Si cette option n'est pas activée, le programme analysera seulement les fichiers dont l'extension coïncide avec celles comprises dans la liste.

Deux boutons permettent d'ajouter et d'éliminer des extensions dans la liste. Le programme indique par défaut une liste des extensions les plus courantes et une sélection de celles susceptibles de contenir un virus.

Quelles que soient les extensions sélectionnées, les fichiers EXE et COM seront toujours analysés.

Options d'analyse

Après avoir appuyé sur le bouton *Options*, vous verrez apparaître une fenêtre dans laquelle vous pourrez choisir parmi les options d'analyse suivantes :



- **Automatique :** si vous cochez cette option, le processus d'analyse s'effectuera de façon

entièrement automatique. Lorsqu'un virus sera détecté, un message d'information apparaîtra mais le processus continuera. Cela est particulièrement utile lorsque l'ordinateur possède de nombreux fichiers infectés que l'on souhaite désinfecter.

- **Entrer dans les sous-répertoires :** si vous cochez cette option, le programme analysera les sous-répertoires trouvés dans les zones analysées. Si vous ne cochez pas cette option, les sous-répertoires trouvés ne seront pas analysés. Par conséquent, si vous choisissez d'analyser une unité sans activer cette option, le programme analysera seulement le répertoire racine de l'unité.
- **Enregistrer les résultats :** si vous cochez cette option, les données relatives à l'analyse en question seront enregistrées dans le fichier de résultats.
- **Analyser les fichiers comprimés :** si vous cochez cette option, tous les fichiers comprimés trouvés seront analysés.
- **Désinfecter :** si vous cochez cette option, l'anti-virus essaiera de désinfecter automatiquement les virus détectés.
- **Si la désinfection est impossible, renommer fichier :** si vous cochez cette option, lorsque le programme détectera un virus impossible à désinfecter, le fichier en question sera renommé.
- **Si la désinfection est impossible, supprimer fichier :** si vous cochez cette option, lorsque le programme détectera un virus impossible à désinfecter, le fichier en question sera supprimé.

Qu’est-ce que l’analyse heuristique?

L’analyse heuristique est une technique d’analyse supplémentaire spécialement conçue pour détecter les virus inconnus.

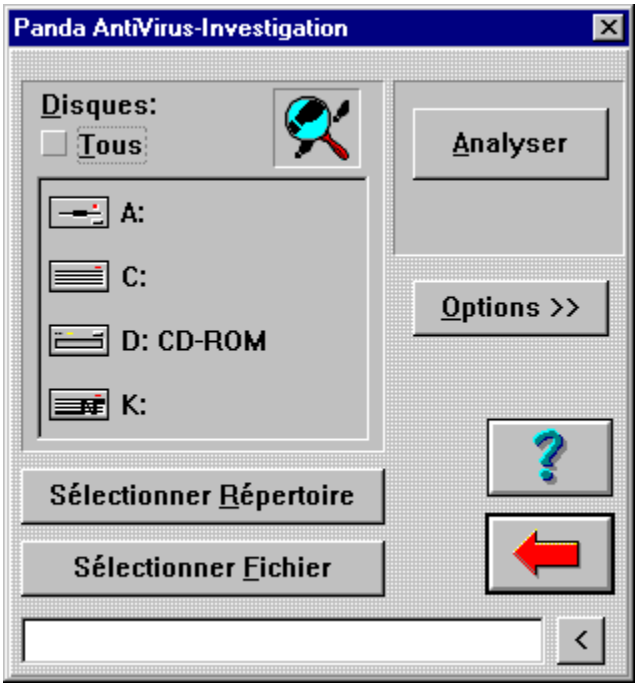
De même que l’analyse sur demande, l’analyse heuristique s’effectue de manière immédiate à la demande de l’utilisateur. La méthode d’analyse sur laquelle est fondée l’analyse heuristique est complètement différente de la méthode d’analyse sur demande. Cette dernière essaie de détecter un des virus connus par l’antivirus, tandis que l’analyse heuristique essaie de déterminer s’il existe un virus en se basant sur des caractérsitiques générales communes à la plupart des virus.

Etant donné que l’analyse heuristique se limite à détecter un fichier susceptible d’être infecté par un virus sur lequel on ne dispose pas d’informations suffisantes, les virus potentiels détectés par l’analyse heuristique ne peuvent être désinfectés.

Il est important de savoir que l’analyse heuristique est un complément de l’analyse sur demande.

Le fonctionnement de l’analyse heuristique est similaire à celui de l’analyse sur demande.

Comment utiliser l’analyse heuristique



Pour réaliser une analyse sur demande, on procèdera de la manière suivante :

1. **Exécuter l’anti-virus :** pour exécuter l'anti-virus, placez-vous dans le groupe de programmes où les icônes permettant de le lancer ont été créées. Cliquez deux fois sur *l'icône Panda Antivirus*.
2. **Aller dans la section d’analyse heuristique :** pour vous placer dans cette section, appuyez sur le bouton *Enquêter* sur la barre de boutons de l'application. Vous verrez apparaître une fenêtre dans laquelle vous pourrez préciser la zone à analyser à l’aide de la méthode heuristique et le mode d'analyse.
3. **Choisir la zone à analyser :** vous devrez ensuite choisir la zone que vous souhaitez analyser. Une liste indique les différentes unités reconnues par le système. Vous pouvez également indiquer un répertoire ou un fichier spécifique à l'aide des boutons prévus à cet effet.
4. **Configurer les options de l'analyse heuristique :** cette opération est facultative. Le programme enregistre la configuration des options de l'analyse heuristique. Une fois que l'analyse est configurée, il n'est donc pas nécessaire de la reconfigurer lors de chaque analyse. On ne modifiera cette configuration que lorsque l'on souhaitera choisir un ensemble d'options différent. Vous trouverez des explications plus détaillées sur les options d'analyse heuristique dans le chapitre de configuration de ce même document.
5. **Commencer l'analyse :** le bouton *Analyser* lance la recherche heuristique de virus dans les zones sélectionnées en fonction des options choisies.

Comment configurer l'analyse heuristique

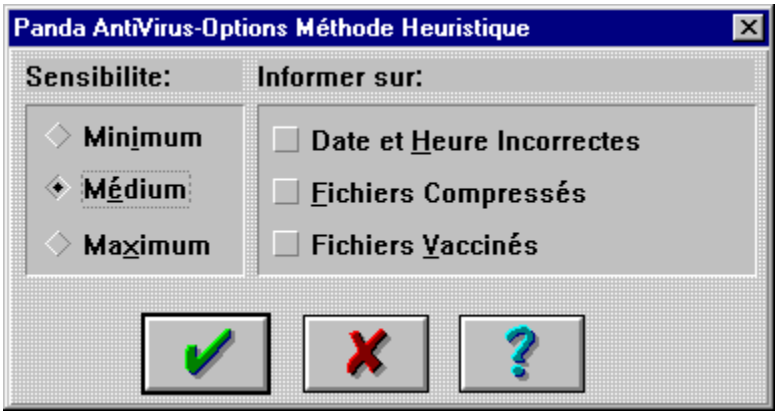
Comme nous l'avons dit plus haut, pour effectuer une analyse heuristique, il faut indiquer :

- La zone à analyser à l'aide de cette méthode.
- La façon dont l'analyse va être réalisée.

Pour configurer l'analyse heuristique, vous devrez préciser les options spécifiques à ce type d'analyse.

Options d'analyse

En appuyant sur le bouton *Options*, vous ouvrirez une fenêtre dans laquelle vous pourrez choisir parmi les options d'analyse heuristique suivantes :



- **Sensibilité minimum :** si vous cochez cette option, la sensibilité de l'analyse heuristique sera faible, de façon que seuls les fichiers hautement susceptibles de contenir un virus seront indiqués comme potentiellement infectés.
- **Sensibilité moyenne :** si vous cochez cette option, l'analyse heuristique sera réalisée avec une sensibilité moyenne. De cette façon, les fichiers ne seront déclarés suspects que lorsque la probabilité d'infection sera assez élevée.
- **Sensibilité maximum :** si vous cochez cette option, la sensibilité de l'analyse heuristique sera maximale, c'est-à-dire que tous les fichiers présentant la moindre possibilité d'être infectés seront déclarés suspects. Toutefois, la probabilité qu'un fichier non infecté soit déclaré suspect, même à ce niveau de sensibilité, est très faible.
- **Signaler les erreurs de date et d'heure :** si vous cochez cette option, le programme vous avertira lorsqu'il trouvera un fichier dont la date ou l'heure sont erronées.
- **Signaler les fichiers comprimés :** si vous cochez cette option, le programme vous avertira lorsqu'il trouvera un fichier comprimé.
- **Signaler les fichiers vaccinés :** si vous cochez cette option, le programme vous avertira lorsqu'il trouvera un fichier vacciné.

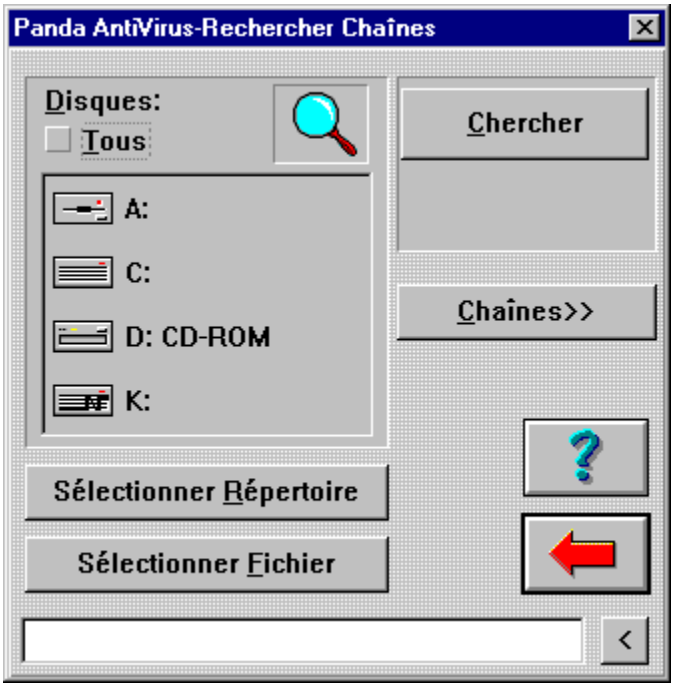
Qu’est-ce que la recherche de chaînes?

L’analyse sur demande consiste à chercher dans les fichiers des parties de virus connues par l’antivirus. Etant donné que de nouveaux virus apparaissent chaque jour, l’analyse sur demande devient vite dépassée.

La recherche de chaînes fait appel à la même méthode que l’analyse sur demande, à la différence près que l’on peut indiquer une chaîne (partie d’un virus) à rechercher. De cette façon, le service clientèle de **Panda Software** peut vous indiquer une chaîne correspondant à un nouveau virus pour que l’antivirus puisse la détecter même s’il ne possède pas d’informations sur ce virus.

De même que l’analyse sur demande, la recherche de chaînes s’effectue de manière immédiate, à la demande de l’utilisateur.

Comment utiliser la recherche de chaînes



Pour réaliser une recherche de chaînes, on procèdera de la manière suivante :

1. **Exécuter l'anti-virus :** pour exécuter l'anti-virus, placez-vous dans le groupe de programmes où les icônes permettant de le lancer ont été créées. Cliquez deux fois sur *l'icône Panda Antivirus*.
2. **Aller dans la section de recherche de chaînes :** pour vous placer dans cette section, appuyez sur le bouton *Rechercher* sur la barre de boutons de l'application. Vous verrez apparaître une fenêtre dans laquelle vous pourrez préciser la zone à analyser à l'aide de la recherche de chaînes et le mode d'analyse.
3. **Choisir la zone où réaliser la recherche :** vous devrez ensuite choisir la zone où vous souhaitez effectuer la recherche. Une liste indique les différentes unités reconnues par le système. Vous pouvez également indiquer un répertoire ou un fichier spécifique à l'aide des boutons prévus à cet effet.
4. **Indiquer les chaînes à rechercher :** vous devez écrire les chaînes que l'anti-virus doit rechercher ou choisir des chaînes déjà introduites dans une liste. Etant donné que le programme conserve les chaînes introduites précédemment, cette étape n'est pas nécessaire si vous ne souhaitez pas introduire de nouvelle chaîne.
5. **Commencer la recherche :** le bouton *Rechercher* lance la recherche des chaînes indiquées dans les zones sélectionnées.

Comment configurer la recherche de chaînes

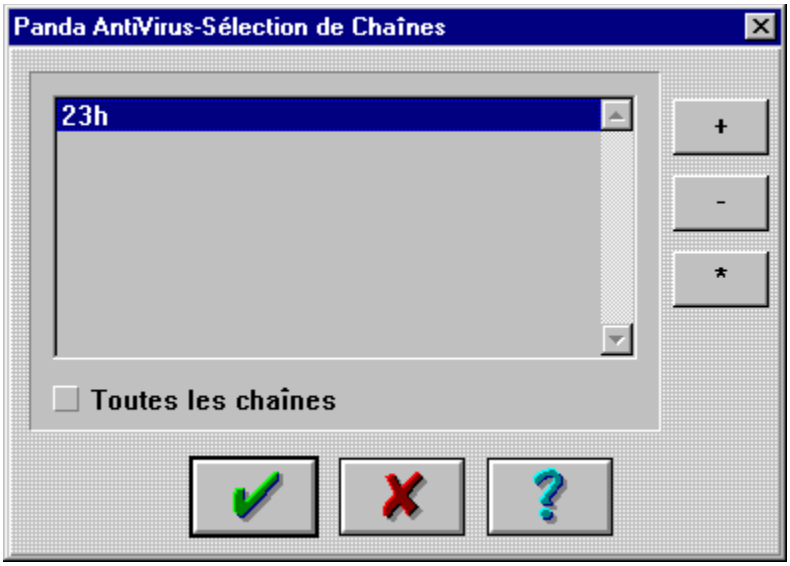
Comme nous l'avons dit plus haut, pour effectuer une analyse, il faut indiquer :

- La zone à analyser à l'aide de cette méthode.
- Les chaînes à rechercher.

La configuration d'une recherche de chaînes consiste à spécifier les chaînes à rechercher.

Chaînes

En appuyant sur le bouton *Chaînes*, vous ouvrirez une fenêtre dans laquelle vous pourrez choisir les chaînes à rechercher.



Cette fenêtre comporte une liste des chaînes introduites. A l'aide de boutons prévus à cet effet, il est possible d'ajouter une chaîne à cette liste, de modifier une des chaînes déjà introduites ou d'éliminer une chaîne de la liste.

Le programme ne recherchera pas toutes les chaînes indiquées dans la liste, sauf si l'on coche l'option *Toutes les chaînes*. Si cette option n'est pas cochée, seules les chaînes sélectionnées dans la liste seront recherchées.

Comment désinfecter à l'aide de Panda Antivirus?

Il n'existe pas de section consacrée spécifiquement à la désinfection dans **Panda Antivirus**. La désinfection est associée à l'analyse sur demande ou à la protection permanente. Lorsque le programme détecte un virus au moyen de l'analyse sur demande ou de la protection permanente, il essaie de l'éliminer (si cette option a été activée dans les sections correspondantes).

La configuration de la désinfection permet de spécifier que tous les fichiers contaminés qui ne peuvent être désinfectés doivent être supprimés ou renommés.

Les virus peuvent être détectés dans le secteur d'amorce du disque ou dans des fichiers. Selon le cas, on procédera de manière légèrement différente. On consultera les chapitres correspondants pour obtenir une description détaillée des procédures de désinfection.

Désinfection d'un virus de secteur d'amorce

Partition FAT

Pour désinfecter un virus de secteur d'amorce de l'unité C, procédez de la manière suivante :

1. Eteignez votre ordinateur. Introduisez une disquette de démarrage non infectée (si vous allez procéder à la désinfection depuis le CD-Rom, la disquette devra charger les pilotes du CD) et relancez l'ordinateur.
2. Une fois l'ordinateur relancé, exécutez l'anti-virus en ligne de commande (PAVCL) en respectant les indications suivantes :

   - Si vous souhaitez exécuter **Pavcl** à partir d'une disquette, introduisez la disquette 1 de **Panda Antivirus** pour DOS/Windows 3.1x et tapez la commande suivante :

     ```
     PAVCL C: /CLV
     ```

   - Si vous souhaitez exécuter **Pavcl** à partir du CD-Rom, introduisez celui-ci dans le lecteur, placez-vous dans le répertoire DOSWIN3X et dans la langue souhaitée et tapez la commande suivante :

     ```
     PAVCL C: /CLV
     ```

     Dans les deux cas, si vous voyez apparaître un message indiquant que l'unité choisie n'est pas valide, tapez la commande suivante :

     ```
     PAVCL /HD0 /CLV
     ```

Partition NTFS

Pour désinfecter un virus de secteur d'amorce avec une partition NTFS, il est important de déterminer si le virus affecte le secteur d'amorce principal, le secteur d'amorce ou les deux à la fois. Au cas où le virus affecte seulement le secteur d'amorce principal, la procédure indiquée pour les partitions FAT est également valable dans ce cas.

Si le virus affecte le secteur d'amorce, on pourra éliminer le virus en remplaçant le secteur d'amorce par un autre de type générique à l'aide des outils fournis par Windows NT à cet effet.

Désinfection d’un virus présent dans des fichiers

Si un virus a été détecté dans des fichiers, nettoyez votre système en configurant l’anti-virus de la manière suivante :

- Dans *Optiones d’analyse*, activez *Toutes les extensions*, *Désinfecter* et *Analyse automatique*.
- Placez-vous dans la section d’analyse et sélectionnez l’option permettant d’analyser l’ensemble du système (toutes les unités). Au fur et à mesure de l’analyse, les fichiers infectés seront nettoyés.

Désinfection à l’aide de la protection permanente

Sentinel est capable de désinfecter les virus qu’il détecte. Si **Sentinel** détecte un virus et a été configuré pour le désinfecter, il le désinfectera avant que l’opération en cours ne soit réalisée. Une fois le virus éliminé, il poursuivra l’opération en cours au moment de la détection du virus. **Sentinel** affiche toujours une fenêtre indiquant la détection du virus.

Analyse en ligne de commandes

Panda Antivirus comporte un programme appelé **Pavcl** que l'on exécute à partir de la ligne de commandes de MS-DOS. Notre analyseur depuis la ligne de commandes détecte et désinfecte les mêmes virus que toute autre version de **Panda Antivirus**.

Pavcl est un analyseur rapide qui occupe peu de mémoire. Cependant, son utilisation exige une certaine connaissance des paramètres qu'il admet. **Pavcl** est disponible sur la disquette numéro 1 de la version DOS/Windows 3.1x ou dans le répertoire de la langue correspondante à l'intérieur du répertoire DOSWIN3X sur le CD-Rom.

Paramètres de Pavcl

Tâches

`/NOM` Ne pas analyser la mémoire.

`/NOB` Ne pas analyser le secteur d'amorce.

`/NOF` Ne pas analyser les fichiers.

`/AUL` Analyser toutes les unités du système.

`/INVx` Rechercher les virus inconnus dans l'unité "x".
Exemple : `/INVA` recherche dans l'unité A:.

`/CLV` Eliminer les virus détectés.

`/LIS` Lister les virus connus par cette version.

`/HEU` Activer la méthode de détection heuristique.

`/CMP` Analyser les fichiers comprimés.

`/CDR` Affiche les codes de retour de **Pavcl**.

`/SAV` Enregistrer les paramètres dans un fichier. Lors des prochaines exécutions, ces paramètres seront ajoutés à ceux introduits lors de chaque séance.

`/IB+` Ajouter vaccin Interne au secteur d'amorce.
`/IB-` Enlever vaccin Interne au secteur d'amorce.
`/IB*` Vérifier vaccin Interne du secteur d'amorce.

`/EB+` Ajouter vaccin Externe au secteur d'amorce.

`/EB-` Enlever vaccin Externe au secteur d'amorce.
`/EB*` Vérifier vaccin Externe du secteur d'amorce.

`/IF+` Ajouter vaccin Interne à un Fichier.
`/IF-` Enlever vaccin Interne à un Fichier.
`/IF*` Vérifier vaccin Interne d'un Fichier.

`/EF+` Ajouter vaccin Externe à un Fichier.
`/EF-` Enlever vaccin Externe à un Fichier.
`/EF*` Vérifier vaccin Externe d'un Fichier.

`/B+` Ajouter vaccin Interne et Externe au secteur d'amorce.
`/B-` Enlever vaccin Interne et Externe au secteur d'amorce.
`/B*` Vérifier vaccin Interne et Externe du secteur d'amorce.

`/F+` Ajouter vaccin Interne et Externe à un Fichier.
`/F-` Enlever vaccin Interne et Externe d'un Fichier.
`/F*` Vérifier vaccin Interne et Externe d'un Fichier.

Modificateurs

`/NSB` Ne pas analyser les sous-répertoires de niveau inférieur.

`/PTH` Analyser les répertoires contenus dans la variable PATH du DOS.

`/ISO` Activer la méthode d'isolement.

`/NOS` Désactiver le son.

`/AEX` Analyser tous les fichiers, quelle que soit leur extension.

`/AUT` Exploration sans l'intervention de l'utilisateur.

`/OVR` Remplacer avant de supprimer.

`/NOR` Ne pas créer de fichier de résultats.

`/DEL` Supprime les fichiers infectés même si on peut les désinfecter.

`/LOC` Analyse toutes les unités locales.

`/NBR` Ne permet pas d'annuler le processus d'analyse.

`/ITW` **Pavcl** recherchera uniquement les virus *In The Wild*. Ce paramètre ne doit être employé que

dans des conditions particulières.

En outre, on dispose de l'aiguillage "/?" standard sous DOS, permettant d'accéder à une liste des aiguillages disponibles. Elle comprend également ceux qui correspondent aux langues admises par la version de **Pavcl**.

Les tâches par défaut sont :

- Analyser Mémoire.
- Analyser Secteur d'amorce.
- Analyser Fichiers.

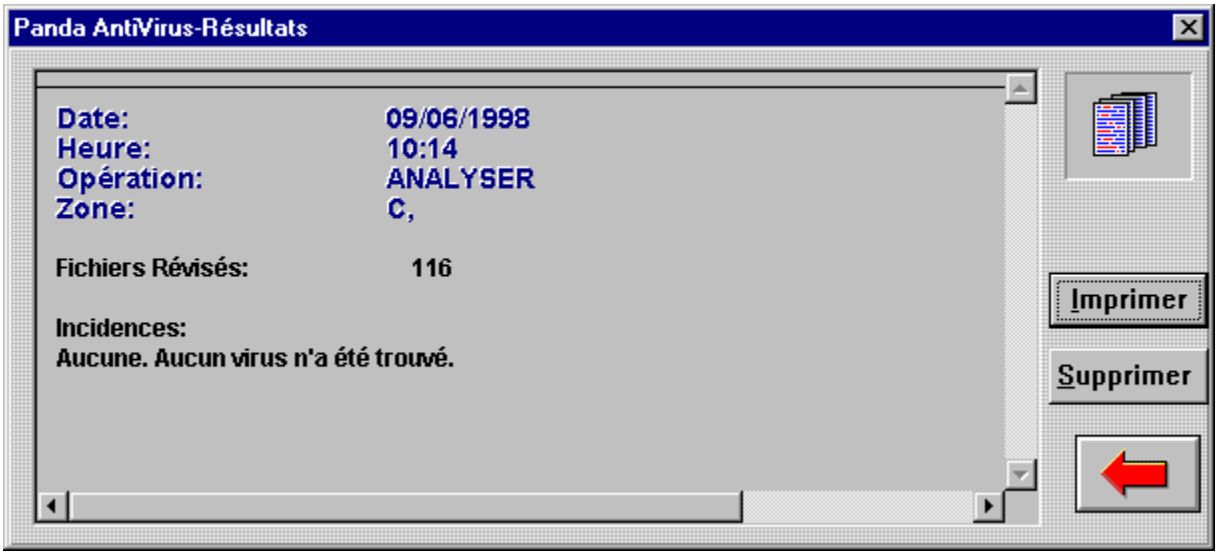
Et les modificateurs par défaut sont :

- Analyser sous-répertoires.
- Ne pas désinfecter.
- Effets de son activés.
- Analyser seulement les extensions exécutables.
- Créer un fichier de résultats.

Les tâches /?, /LIS, /INVx sont exclusives, c'est-à-dire que lorsqu'elles sont sélectionnées, aucune autre tâche ne peut être réalisée. Une fois que ces tâches sont terminées, le programme retourne au DOS. Le chemin ou les chemins à analyser seront indiqués comme d'habitude sous DOS :

[Unité:][Chemin][NomFichier]

Rapport de résultats



Le rapport de résultats enregistre au fur et à mesure les différentes opérations réalisées avec l'anti-virus ainsi que les différents incidents qui se produisent.

Les informations contenues dans le rapport de résultats sont conservées d'une séance à l'autre. Vous pouvez donc consulter en permanence toutes les activités réalisées avec l'anti-virus.

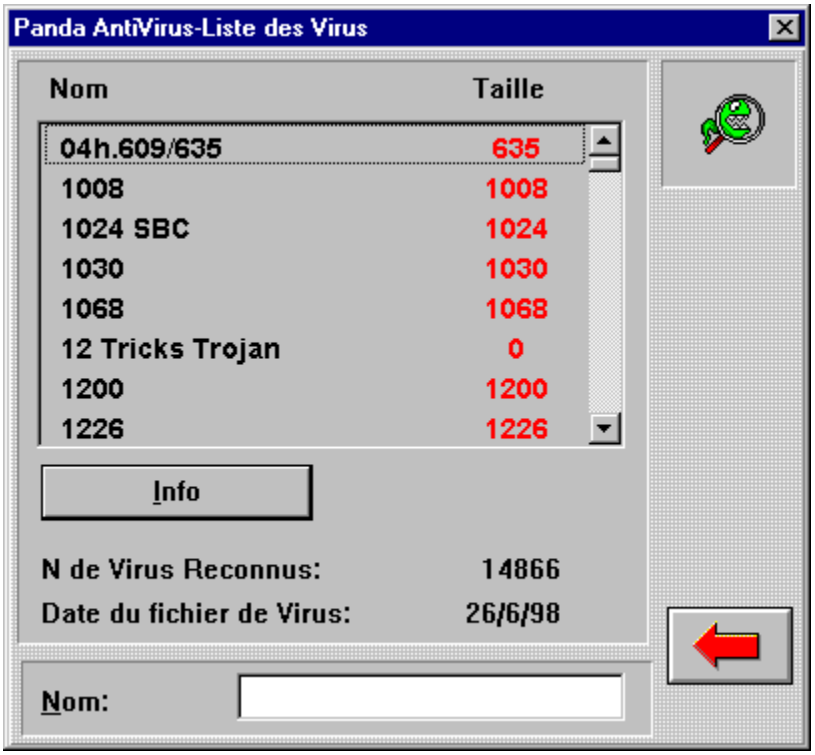
Pour chaque opération réalisée, les informations suivantes sont enregistrées :

- Date et heure.
- Type d'opération.
- Zone dans laquelle l'opération a été effectuée.
- Nombre de fichiers contrôlés.
- Tous les incidents ayant eu lieu en rapport avec un virus.

Pour que les informations soient stockées dans le rapport de résultats, il est nécessaire d'activer l'option *Enregistrer résultats* dans la fenêtre des *Options d'Analyse*.

Il est possible d'imprimer le contenu du rapport de résultats pour faciliter sa consultation. On peut également effacer le contenu du rapport de résultats à tout moment pour éviter qu'il ne prenne un volume trop important.

Liste des virus



La liste des virus indique tous les virus que **Panda Antivirus** est capable de détecter, en précisant le nom et la taille de chacun d'eux.

A côté de la liste, on trouvera également le nombre de virus reconnus dans cette version de **Panda Antivirus**. La date du fichier de virus apparaît également, ce qui permet de connaître le degré d'actualisation de l'anti-virus.

Il est possible d'indiquer le nom d'un virus déterminé dans la case prévue à cet effet afin de le localiser plus facilement dans la liste. De même, la liste des virus est classée par ordre alphabétique.

Une fois le virus choisi, si vous appuyez sur le bouton *Info*, vous verrez s'afficher une fenêtre fournissant une série d'informations sur ce virus :

- Nom.
- Origine.
- Taille.
- Surnom.
- Date à laquelle il a été détecté pour la première fois.
- Possibilité de désinfection.
- Zones de l'ordinateur pouvant être affectées par le virus.
- Caractéristiques du comportement du virus.

En fonction de leurs caractéristiques, les virus sont regroupés dans les catégories suivantes :

- **Résident :** lors de son exécution, le virus se réserve une petite partie de la mémoire dans laquelle il s'installera avant de se propager dans l'ordinateur.
- **Furtif :** technique utilisée par certains virus résidents. Cette technique consiste à camoufler les changements introduits par le virus dans les fichiers infectés. Lorsque quelqu'un essaie de voir une des caractéristiques du fichier que le virus a modifié, le virus qui réside dans la mémoire intercepte la consultation et offre les informations antérieures à la modification.
- **Crypté :** les virus de ce type sont capables d'adopter un cryptage différent chaque fois qu'ils infectent un fichier. Cela rend impossible la recherche de virus à l'aide de chaînes.
- **Superposition :** les virus de superposition, qui peuvent être résidents ou non, remplacent le fichier qu'ils infectent. Le fichier en question devient donc inutilisable. La taille du fichier ne change pas, sauf si la taille du virus est supérieure à celle du fichier. La seule façon d'éliminer ces virus consiste à supprimer le fichier infecté et à le remplacer par une copie non infectée.
- **Polymorphe :** les virus polymorphes sont des versions élaborées des virus cryptés. Ils sont capables de modifier la méthode de cryptage d'une génération à l'autre, de façon qu'aucune partie du virus ne reste inchangée.

Fonctionnement général

Panda Antivirus pour Windows NT offre une interface pratique et facile à utiliser. Dans la fenêtre principale du programme, les options les plus courantes peuvent être activées à l'aide de boutons de grande dimension.

En appuyant sur ces boutons, on accède aux différentes parties du programme. Vous trouverez des explications détaillées dans le chapitre correspondant à chaque fonction.