

bitdefender **ANTIVIRUS v10**



10th anniversary

Manuel d'utilisation



Antivirus
Antispyware

BitDefender Antivirus v10

Manuel d'utilisation

BitDefender

Publié le 2007.01.17

Version 10.2

Copyright© 2007 SOFTWIN

Notice Légale

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduit ou transmis, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de SOFTWIN. L'inclusion de courtes citations dans des tests n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et sa documentation sont protégées par copyright. Les informations de ce document sont données à titre indicatif, sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs ne pourront être tenu responsables envers quiconque de toute perte ou dommage occasionné, ou supposé occasionné, directement ou indirectement par les informations contenues dans ce document.

Ce manuel contient des liens vers des sites web de tiers qui ne sont pas sous le contrôle de SOFTWIN, et SOFTWIN n'est pas responsable du contenu de ces sites. Si vous accédez à un l'un des sites web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. SOFTWIN indique ces liens uniquement à titre informative, et l'inclusion de ce lien n'implique pas que SOFTWIN assume ou accepte la responsabilité du contenu de ce site web d'un tiers.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques enregistrées ou non dans ce document sont la propriété unique de leur propriétaire respectif.





Table des matières

Accord de licence	ix
Préface	xiii
1. Conventions utilisées dans ce manuel	xiii
1.1. Normes Typographiques	xiii
1.2. Avertissements	xiv
2. Structure du manuel	xiv
3. Commentaires	xv
A propos de BitDefender	1
1. A propos de BitDefender	3
1.1. Pourquoi choisir BitDefender?	3
1.2. A propos de SOFTWIN	5
Installation du produit	7
2. Installation de BitDefender Antivirus v10	9
2.1. Configuration requise	9
2.2. Etapes d'installation	9
2.3. Assistant de première installation	12
2.3.1. Etape 1 sur 8 - Début de l'assistant d'installation	13
2.3.2. Etape 2 sur 8 - Enregistrement de BitDefender Antivirus v10	13
2.3.3. Etape 3 sur 8 - Création d'un compte BitDefender	14
2.3.4. Etape 4 sur 8 - Entrer les renseignements du compte	15
2.3.5. Etape 5 sur 8 - En savoir plus sur le RTVR	16
2.3.6. Etape 6 sur 8 - Sélectionner les tâches à lancer	17
2.3.7. Etape 7 sur 8 - Merci d'attendre la fin de la tâche	18
2.3.8. Etape 8 sur 8 - Voir le récapitulatif	19
2.4. Mise à jour majeure	19
2.5. Supprimer, réparer ou modifier BitDefender	20
Description et caractéristiques	21
3. BitDefender Antivirus v10	23
3.1. Antivirus	23
3.2. Antispyware	24
3.3. Autres Fonctions	24
4. Modules BitDefender	27
4.1. Module Général	27
4.2. Module Antivirus	27
4.3. Module Antispyware	27

4.4. Module de Mise à jour	28
Console de gestion	29
5. Vue d'ensemble	31
5.1. Barre d'état système	32
5.2. Barre d'analyse de l'activité	33
6. Module Général	35
6.1. Administration centrale	35
6.1.1. Tâches prédéfinies	36
6.1.2. Niveau de sécurité	36
6.1.3. Etat de l'enregistrement	37
6.2. Paramètres de la console de gestion	37
6.2.1. Paramètres Généraux	38
6.2.2. Paramètres du rapport des virus	39
6.2.3. Paramètres d'Interface	40
6.2.4. Gérer les paramètres	40
6.3. Événements	40
6.4. Enregistrement du produit	42
6.4.1. Assistant d'enregistrement	42
6.5. A propos	46
7. Module Antivirus	49
7.1. Analyse à l'accès	49
7.1.1. Niveau de protection	50
7.2. Analyse à la demande	54
7.2.1. Tâches d'analyse	55
7.2.2. Propriétés des tâches d'analyse	56
7.2.3. Menu de raccourci	67
7.2.4. Types d'analyse à la demande	68
7.2.5. Recherche de Rootkits	73
7.3. Quarantaine	74
8. Module Antispyware	79
8.1. Etat de l'Antispyware	79
8.1.1. Niveau de protection	81
8.2. Protection de la vie privée - Paramètres avancés	81
8.2.1. Assistant de configuration	82
8.3. Contrôle de la base de registre -Paramètres avancés	86
8.4. Contrôle des numéroteurs -Paramètres avancés	88
8.4.1. Assistant de configuration	90
8.5. Contrôle des cookies - Paramètres avancés	92
8.5.1. Assistant de configuration	94
8.6. Contrôle des scripts - Paramètres avancés	95
8.6.1. Assistant de configuration	96
8.7. Informations Système	97



9. Module de Mise à jour	99
9.1. Mise à jour automatique	99
9.2. Mise à jour manuelle	100
9.2.1. Mise à jour manuelle avec <code>weekly.exe</code>	101
9.2.2. Mise à jour manuelle avec des archives <code>zip</code>	101
9.3. Configuration des Mises à jour	103
9.3.1. Paramètres du choix de l'emplacement des mises à jour	104
9.3.2. Options de mise à jour automatique	104
9.3.3. Paramètres de la mise à jour manuelle	105
9.3.4. Paramètres avancés	105
Utilisation optimale	107
10. Utilisation optimale	109
10.1. Comment protéger votre ordinateur contre les malwares	109
10.2. Comment configurer une tâche d'analyse	110
CD de secours BitDefender	111
11. Vue d'ensemble	113
11.1. Qu'est que Knoppix ?	113
11.2. Configuration requise	113
11.3. Logiciels inclus	114
11.4. Les solutions de sécurité BitDefender pour Linux	114
11.4.1. BitDefender SMTP Proxy	114
11.4.2. Console de gestion distante de BitDefender	115
11.4.3. BitDefender pour Linux	115
12. Fonctionnement de LinuxDefender	117
12.1. Démarrer et arrêter	117
12.1.1. Lancer LinuxDefender	117
12.1.2. Arrêter LinuxDefender	118
12.2. Configurer la connexion Internet	119
12.3. Mise à jour de BitDefender	120
12.4. Analyse antivirus	120
12.4.1. Comment accéder à mes données Windows ?	120
12.4.2. Comment lancer une analyse antivirus ?	121
12.5. Création d'un moteur de filtrage de messagerie	122
12.5.1. Configuration nécessaire	122
12.5.2. Le filtre email	122
12.6. Réaliser un audit de la sécurité du réseau	123
12.6.1. Vérifier la présence de Rootkits	123
12.6.2. Le moteur d'analyse réseau - Nessus	124
12.7. Vérifier le bon fonctionnement de votre mémoire RAM	124
Demander de l'aide	127

13. Support technique	129
13.1. Service de support technique	129
13.2. Aide en ligne	129
13.2.1. Base de connaissances BitDefender	129
13.3. Contacts	130
13.3.1. Adresses Web	130
13.3.2. Bureaux BitDefender	130
Glossaire	131



Accord de licence

Si vous n'acceptez pas les termes et conditions n'installez pas ce logiciel. En choisissant "J'accepte", "Ok", "Continuer", "Oui" ou en installant ou utilisant le logiciel de quelque manière que ce soit, vous confirmez que vous comprenez parfaitement et acceptez les termes et conditions de cette licence.

Les termes de cette licence incluent les Solutions et Service BitDefender pour votre usage personnel, y compris les documentations relatives aux produits, les mises à jour et mises à niveau des applications ou les services qui vous sont proposés dans le cadre de la licence, ainsi que toute reproduction de ces éléments.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et SOFTWIN pour l'usage du produit de SOFTWIN identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation "en ligne" ou électronique (" BitDefender "), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord.

Si vous n'acceptez pas les termes de cette licence, n'installez pas ou n'utilisez pas BitDefender.

Accord de licence BitDefender. BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

DROITS DE LICENCE. Ce logiciel restant la propriété de SOFTWIN, vous et vous seul disposez néanmoins de certains droits d'utilisation non exclusifs et non transférables, une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants:

LOGICIEL: Vous pouvez installer et utiliser BitDefender, sur autant d'ordinateurs que nécessaire dans le cadre de la limitation imposée par le nombre d'utilisateurs ayant une licence. Vous pouvez réaliser une copie à des fins de sauvegarde.

ACCORD DE LICENCE POUR ORDINATEUR. Cette licence s'applique au logiciel BitDefender qui peut être installé sur un ordinateur unique ne proposant pas de service en réseau. Chaque utilisateur principal peut utiliser ce logiciel sur un ordinateur unique et peut réaliser une copie de sauvegarde sur un support différent. Le nombre d'utilisateurs principal correspond au nombre d'utilisateurs définit dans l'accord de licence.

DUREE DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et expirera à la fin de la période pour laquelle la licence a été acquise.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par SOFTWIN comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur. Les termes et conditions de cette licence annule et remplace tout accord préalable ayant pu exister entre vous et SOFTWIN concernant un produit complet ou un produit mis à jour.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de SOFTWIN. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. SOFTWIN garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par SOFTWIN du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. SOFTWIN ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur. SOFTWIN REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QU'ELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES



GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

A l'exception des termes définis dans cet accord de licence, SOFTWIN refuse toute autre forme de garantie, explicite ou implicite en rapport avec le produit, ses améliorations, sa maintenance, ou son support ainsi que tout autre matériel relatif (tangible ou intangible) ou service fourni par celui ci. SOFTWIN refuse explicitement toutes garanties et conditions incluant, sans limitation, les garanties liées à la commercialisation, l'adaptation à un emploi particulier, la non interférence, la précision des données, la précision de contenus d'informations, l'intégration système, et la non violation des droits d'une tierce partie en filtrant, désactivant ou supprimant un logiciel, spyware, adware, des cookies, des emails, des documents, une publicité ou un autre produit du même type, d'un telle tierce partie, quel que soit leur mode d'utilisation.

REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender accepte les risques qu'il peut encourir concernant la qualité et la performance de BitDefender. En aucun cas SOFTWIN ne sera tenu responsable à votre égard de tout dommage particulier direct ou indirect, de réclamations liées à une perte quelconque découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si SOFTWIN a été avisé de l'éventualité de tels dommages. CERTAINS ETATS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE RESPONSABILITE EN CAS DE DOMMAGE. LA REGLE EDICTEE CI-DESSUS CONCERNANT LES LIMITATIONS OU EXCLUSIONS CITEES PEUT NE PAS S'APPLIQUER A VOTRE CAS - QU'ELLES QUE SOIENT LES CONDITIONS LA REponsabilite de SOFTWIN NE POURRA EXCEDER LE MONTANT QUE VOUS AVEZ PAYE POUR BITDEFENDER. Les limitations édictées ci dessus s'appliqueront que vous acceptiez ou non d'utiliser, d'évaluer ou de tester BitDefender.

INFORMATION IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS PREVU POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. La seule juridiction compétente en cas de désaccord concernant cet accord de licence sera la Cour de justice de Roumanie.

Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu.

Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

BitDefender et le logo de BitDefender sont des marques déposées de SOFTWIN. Toutes les autres marques et produits associés appartiennent à leurs propriétaires respectifs.

La licence prendra fin immédiatement sans qu'il soit besoin de vous avertir si vous ne respectez pas une ou plusieurs des conditions édictées dans cet accord. Il ne vous sera pas possible de demander un remboursement de la part de SOFTWIN ou d'un de ses représentants en cas de cloture de cette licence. Les termes et conditions de respect de confidentialité et leurs restrictions doivent rester de mise même après la fin du contrat.

SOFTWIN s'autorise à revoir quand il le souhaite les termes de cette licence, ceux-ci s'appliqueront automatiquement aux produits distribués qui incluent les termes modifiés. Dans l'éventualité d'une invalidité d'une partie de cet accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise éditée par Softwin sera déclarée valide. En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise éditée par Softwin sera déclarée valide.

Contact SOFTWIN: Rue Fabrica de Glucoza, No. 5, Code postal 020331 - Sector 2, Bucarest, Roumanie, ou au Tel No: +40-21-2330780 ou Fax: +40-21-2330763, adresse e-mail: <office@bitdefender.com>.



Préface

Ce Manuel d'utilisation est destiné à tous les utilisateurs qui ont choisi **BitDefender Antivirus v10** comme solution de sécurité pour leur ordinateur personnel. Les informations présentées dans ce livret sont destinées aussi bien aux utilisateurs expérimentés en informatique qu'à n'importe quelle personne sachant utiliser Windows.

Ce Manuel d'utilisation vous guidera pas à pas dans le processus d'installation de **BitDefender Antivirus v10**, il vous apprendra comment le configurer. Vous y apprendrez les méthodes d'utilisation de **BitDefender Antivirus v10**, la méthode de mise à jour, de test et de personnalisation. Vous saurez tirer le meilleur de BitDefender.

Nous vous souhaitons un apprentissage agréable et utile.

1. Conventions utilisées dans ce manuel

1.1. Normes Typographiques

Plusieurs styles de texte sont utilisés dans ce livret pour une lisibilité améliorée. Leur aspect et signification sont présentés dans la liste ci dessous.

Apparence	Description
<code>sample syntax</code>	Les exemples et quelques données numériques sont imprimés avec des caractères séparés d'un espace.
http://www.bitdefender.com	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
<code><support@bitdefender.com></code>	Les adresses Email sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. xiii)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
<code>filename</code>	Les fichiers et répertoires sont imprimés en utilisant des caractères séparés d'un espace.
option	Toutes les informations sur le produit sont imprimées en utilisant des caractères Gras .

Apparence	Description
<code>sample code listing</code>	Les textes cités sont fournis en guise de référence.

1.2. Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.



Note

La note est une courte observation. Bien que vous puissiez l'omettre, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien à un thème proche.



Important

Cette icône requiert votre attention et il n'est pas recommandé de le passer. Habituellement, il apporte des informations non critiques mais significatives.



Avertissement

Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. A lire très attentivement car décrit une opération potentiellement très risquée.

2. Structure du manuel

Le manuel est composé de 7 parties reprenant les principaux thèmes: A propos de BitDefender, Installation du produit, Description et caractéristiques, Console de gestion, Utilisation optimale, CD de secours BitDefender et Demander de l'aide. De plus un glossaire est disponible pour clarifier certains termes techniques.

A propos de BitDefender. Présentation rapide de BitDefender. Elle explique qui sont BitDefender et Softwin.

Installation du produit. Des instructions pas à pas pour installer BitDefender sur un poste. Un tutorial clair sur l'installation et la configuration de **BitDefender Antivirus v10**. Commencant par les prérequis pour une installation réussie, vous serez guidé à travers le processus d'installation entier et lors de la première session. A la fin, la procédure de désinstallation est décrite au cas où vous auriez besoin de désinstaller BitDefender.

Description et caractéristiques. **BitDefender Antivirus v10**, ses caractéristiques et les modules du produit vous sont présentés.



Console de gestion. Description de la gestion standard et de la maintenance de BitDefender. Les chapitres expliquent en détail toutes les options de **BitDefender Antivirus v10**, comment enregistrer le produit, comment analyser l'ordinateur, comment lancer les mises à jour. La manière de configurer et d'utiliser tous les modules BitDefender vous sera également montrée.

Utilisation optimale. Suivez ces instructions pour utiliser au mieux votre produit BitDefender

CD de secours BitDefender. Description du CD de secours BitDefender. Mode d'emploi pour comprendre l'utilisation du CD bootable de secours.

Demander de l'aide. Où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

Glossaire. Le glossaire tente de vulgariser des termes techniques et peu communs que vous trouverez dans ce document.

3. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutes les informations mais vous pouvez trouver que certaines fonctions ont changé. N'hésitez pas à nous écrire pour nous dire si vous avez trouvé des erreurs dans ce livret ou concernant toute amélioration que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Faites-le nous savoir en nous écrivant à cette adresse [<documentation@bitdefender.com>](mailto:documentation@bitdefender.com).



Important

Merci d'envoyer vos demandes par email afin que nous puissions les traiter avec la plus grande efficacité.



A propos de BitDefender



1. A propos de BitDefender

BitDefender fournit des solutions de sécurité qui répondent aux besoins de protection de l'environnement informatique actuel. BitDefender dispose d'une gamme de logiciels de sécurité des plus efficace, fixant de nouvelles normes en matière de prévention des menaces, de détection en temps réel et de réduction des risques. BitDefender fournit des produits et des services à plus de 41 millions de foyers et d'entreprises dans plus de 180 pays. BitDefender dispose de bureaux aux **Etats-Unis**, au **Royaume-Uni**, en **Allemagne**, en **Espagne** et en **Roumanie**.

- Inclut les fonctions: antivirus, firewall, antispyware, antispam et contrôle parental pour les entreprises et les particuliers.
- La gamme de produits BitDefender est prévue pour être installée sur des architectures informatiques complexes (stations de travail, serveurs de fichiers, serveurs de mails et passerelle), sur les plateformes Windows, Linux et FreeBSD.
- Distribution mondiale, des produits disponibles en 18 langues.
- Facile d'emploi, avec un assistant d'installation qui guide les utilisateurs pendant l'installation et ne pose que quelques questions.
- Des produits certifiés au niveau international: Virus Bulletin, ICSA Labs, CheckMark, IST Prize, etc.
- Assistance client toujours disponible: le support client est disponible 24h/24, 7J/7.
- Un temps de réponse ultrarapide en cas de nouvelles attaques.
- Le meilleur taux de détection.
- Mises à jour automatiques toutes les heures - ou actions programmées pour assurer une protection contre les nouveaux virus.

1.1. Pourquoi choisir BitDefender?

Reconnu. Editeur antivirus le plus réactif. La réactivité de BitDefender en cas d'épidémie virale a été confirmée lors des dernières attaques de virus comme: CodeRed, Nimda, Sircam et Badtrans.B ou d'autres codes malicieux à propagation rapide et dangereuse. BitDefender a été le premier à fournir des antidotes contre ces codes malveillants et à les rendre disponible gratuitement sur Internet pour toutes les personnes infectées. Aujourd'hui, avec l'expansion rapide de virus du type Klez – dans de nombreuses versions – une protection antivirus immédiate est devenue d'autant plus vitale pour n'importe quel ordinateur.

Innovant. Primé pour son innovation par la Communauté Européenne et EuroCase. BitDefender a été proclamé vainqueur du prix IST Européen, remis par la commission Européenne et les représentants de 18 académies en Europe. Dans sa huitième année, le prix Européen IST est une décoration pour les nouveaux produits qui représentent le meilleur des innovations Européenne en matière de technologie d'information.

Simple. Couvre chaque point d'entrée potentiel, vous apportant une sécurité totale. La solution sécurité BitDefender pour les environnements professionnels remplit les conditions de protection des environnements de travail récents, permettant la gestion des menaces sérieuses qui mettent en danger les réseaux, d'un réseau local de petite taille aux WAN multi plateformes en passant par les multiseveurs.

Votre Protection Ultime. La frontière finale à toute menace possible pour votre ordinateur. La détection de virus basée sur l'analyse de code n'ayant pas toujours assuré de bons résultats, BitDefender a implémenté une protection basée sur le comportement, apportant une sécurité contre les nouveaux malwares encore inconnus.

Voici **les coûts** que les entreprises souhaitent éviter et ce que nos produits de sécurité sont destinés à empêcher:

- Attaques de Ver
- Perte de communication à cause d'e-mails infectés
- Dysfonctionnement de l'E-mail
- Nettoyage et restauration de systèmes
- Perte de productivité rencontrées par les utilisateurs finaux à cause d'indisponibilité du système
- Piratage et accès non autorisé causant des dommages

Certains **développements et avantages** simultanés peuvent être accomplis en utilisant la suite de sécurité BitDefender:

- Amélioration de la disponibilité du réseau en stoppant la propagation des attaques de codes malicieux (type Nimda, Chevaux de Troie, DDoS).
- Protection utilisateurs distants contre les attaques.
- Réduction des coûts administratifs avec les capacités de gestion et de déploiement rapide de BitDefender Enterprise.
- Arrêt de la propagation de malware par e-mail, en utilisant la protection e-mail BitDefender sur le portail de la compagnie. Bloquez temporairement ou de manière permanente les codes non autorisés, et les connexions d'application coûteuses.

Pour plus d'informations sur BitDefender, visitez notre site: <http://www.bitdefender.com>.



1.2. A propos de SOFTWIN

Créée en 1990, primée par l'IST Prize en 2002, SOFTWIN est désormais considéré comme le leader technologique des éditeurs de logiciels de l'Europe de l'Est avec un taux de croissance annuel de plus de 50% sur les cinq dernières années et un chiffre d'affaire réalisé à plus de 70% à l'export.

SOFTWIN se concentre sur le développement de solutions logicielles et de services qui permettent aux entreprises grandissantes de résoudre leur challenge critique d'activité et de capitaliser sur de nouvelles opportunités de commerce.

Actif sur les marchés informatiques les plus développés de l'union européenne et des Etas-Unis, SOFTWIN se développe sur 4 marchés interconnectés.

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management



Installation du produit



2. Installation de BitDefender Antivirus v10

La section **Installation de BitDefender Antivirus v10** de ce Manuel d'utilisation concerne les sujets suivants:

- Configuration système
- Etapes d'installation
- Assistant initial de démarrage
- Mise à jour majeure
- Supprimer, réparer ou modifier BitDefender

2.1. Configuration requise

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que l'un des systèmes d'exploitation suivants fonctionne sur votre ordinateur et que vous disposez de la bonne configuration :

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Processeur Pentium II 350 MHz ou supérieur
- Mémoire minimum 128Mo de RAM (256Mo recommandés)
- Au moins 60Mo d'espace disque disponible.
- Internet Explorer 5.5 (ou version supérieure)

Microsoft Windows Vista 32-bit

- Processeur 800 MHz ou supérieur
- Mémoire minimum : 512Mo de RAM (1 GB recommandés)
- Au moins 60Mo d'espace disque disponible.

BitDefender Antivirus v10 peut être téléchargé en version d'évaluation depuis le site <http://www.bitdefender.com>.

2.2. Etapes d'installation

Localisez le fichier d'installation et double-cliquez dessus. Cela lancera l'assistant d'installation, qui vous guidera à travers le processus d'installation:

The screenshots illustrate the following steps:

- 1. Bienvenue dans l'assistant d'installation:** Welcome screen with a red sphere logo and a 'Suivant' button.
- 2. Conseil:** Screen advising to uninstall other security products. It lists BitDefender's features like real-time analysis, protection, and scanning.
- 3. Conseil:** Warning screen stating that other antivirus products have been detected and offering to uninstall them.
- 4. Accord de licence:** License agreement screen with 'Accepter les termes de la licence d'installation' selected.
- 5. Choisir le type d'installation:** Selection screen with 'Personnalisée' (Custom) selected.
- 6. Installation personnalisée:** Component selection screen where 'Analyseur' (Scanner) is checked.
- 7. Prêt pour installer:** Ready to install screen with a 'Suivant' button.
- 8. Terminer l'Assistant d'installation:** Completion screen with a 'Terminer' button.

Étapes d'installation

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.
2. Cliquez sur **Suivant** pour continuer ou sur **Retour** pour revenir à la première étape.
3. BitDefender Antivirus v10 vous prévient si il y a déjà un autre antivirus installé sur votre ordinateur.

Attention



Il est fortement recommandé de désinstaller les autres antivirus avant d'installer BitDefender. Faire fonctionner plusieurs antivirus sur le même ordinateur le rend généralement inutilisable.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

**Note**

Si BitDefender Antivirus v10 ne détecte pas d'autre produit antivirus sur votre ordinateur vous passerez cette étape.

4. Merci de lire l'Accord de Licence, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.
5. Vous pouvez choisir quel type d'installation vous souhaitez: typique, personnalisée ou complète.

Typique

Le programme sera installé avec les options les plus communes. Cela est recommandé pour la plupart des utilisateurs.

Personnalisé

Cela vous donne la possibilité de choisir les composants que vous souhaitez installer. Recommandé pour les utilisateurs « avancés » uniquement.

Complète

Pour l'installation complète du produit. L'ensemble des modules BitDefender seront installés.

Si vous choisissez **Typique** ou **Complète** vous ne passerez pas par l'étape 6.

6. Si vous avez sélectionné **Personnalisé**, une nouvelle fenêtre apparaîtra, contenant la liste de tous les composants de BitDefender afin de pouvoir choisir ceux que vous souhaitez installer.

Si vous cliquez sur l'un des composants, une courte description (incluant l'espace disque nécessaire) s'affichera sur le côté droit. Si vous cliquez sur l'un des icônes une fenêtre apparaîtra où vous pouvez choisir d'installer ou non le module sélectionné.

Vous pouvez sélectionner le répertoire dans lequel installer le produit. Le répertoire par défaut est `C:\Program Files\Softwin\BitDefender 10`.

Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et, dans la fenêtre qui s'ouvre, choisissez le répertoire. Cliquez sur **Suivant**.

7. Vous avez quatre options sélectionnées par défaut:
 - **Ouvrir le fichier lisezmoi** - pour ouvrir le fichier lisez moi à la fin de l'installation.
 - **Créer un raccourci sur le bureau** - pour mettre un raccourci sur le bureau à la fin de l'installation.

Cliquez sur **Installer** afin de commencer l'installation du produit.



Important

Pendant la procédure d'installation un **assistant** apparaîtra. Il vous aide à enregistrer votre **BitDefender Antivirus v10**, créer un compte et configurer BitDefender pour exécuter les tâches de sécurité importantes.

Complétez l'assistant d'installation pour passer à l'étape suivante.

8. Cliquez sur **Terminer** pour compléter l'installation du produit. Si vous avez accepté les paramètres par défaut pour le répertoire d'installation, un nouveau répertoire du nom de `Softwin` est créé dans `Program Files` contenant le sous-répertoire `BitDefender 10`.



Note

Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation.

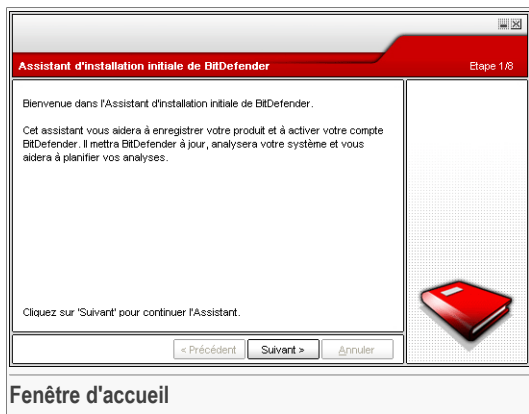
2.3. Assistant de première installation

Pendant la procédure d'installation un **assistant** apparaîtra. Il vous aide à enregistrer votre **BitDefender Antivirus v10**, créer un compte et configurer BitDefender pour exécuter les tâches de sécurité importantes.

Compléter cet assistant n'est pas obligatoire. Cependant, nous vous recommandons de le faire pour gagner du temps et vous assurer que votre système est sain même avant l'installation de BitDefender.

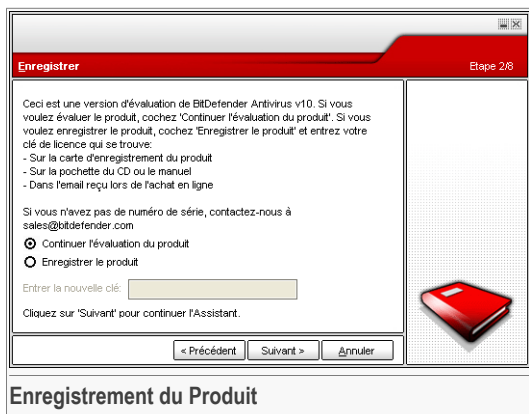


2.3.1. Etape 1 sur 8 - Début de l'assistant d'installation



Cliquez sur **Suivant**.

2.3.2. Etape 2 sur 8 - Enregistrement de BitDefender Antivirus v10



Choisissez **Enregistrer le produit** pour enregistrer **BitDefender Antivirus v10**. Entrez la clé de licence dans le champ **Entrer une nouvelle clé**.

Pour continuer à évaluer le produit, sélectionnez **Continuer l'évaluation du produit**. Cliquez sur **Suivant**.

2.3.3. Etape 3 sur 8 - Création d'un compte BitDefender

Enregistrer le produit Etape 3/8

Vous devez créer un compte pour accéder au support technique de BitDefender et aux autres services personnalisés de BitDefender. Si vous avez déjà un compte BitDefender, veuillez entrer les informations requises. Si vous n'avez pas de compte BitDefender, veuillez entrer votre adresse électronique et un mot de passe.

Adresse électronique:

Mot de passe:

Retapez le mot de passe:

[Vous avez oublié votre mot de passe?](#)

Passer cette étape

Cliquez sur 'Suivant' pour continuer ou sur 'Annuler' pour quitter l'Assistant.

< Précédent Suivant > Annuler

Veuillez entrer une adresse électronique valide. Un courrier de confirmation vous sera envoyé à cette adresse.

Création de compte

Je n'ai pas de compte BitDefender

Pour bénéficier du support technique gratuit et d'autres services, il faut créer un compte BitDefender.

Entrez une adresse email valide dans le champ **E-mail**. Entrez votre mot de passe dans le champ **Mot de passe**. Confirmez le mot de passe dans le champ **Retapez Mot de passe**. Utilisez l'adresse mail et le mot de passe pour vous connecter à votre compte sur <http://myaccount.bitdefender.com>



Note

Votre mot de passe doit comporter au moins quatre caractères.

Pour créer votre compte vous devez d'abord activer votre adresse e-mail. Vérifiez votre messagerie et suivez les instructions reçues dans l'email qui vous a été envoyé par le service d'enregistrement BitDefender.



Important

Merci d'activer votre compte avant de passer à l'étape suivante.



Si vous ne souhaitez pas créer un compte BitDefender, sélectionnez **Passer cette étape**.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

J'ai déjà un compte BitDefender

Si vous avez déjà un compte BitDefender, entrez votre adresse email et le mot de passe de votre compte. Si vous tapez un mot de passe incorrect, il vous sera demandé de le ressaisir quand vous cliquerez sur **Suivant**. Cliquez sur **Ok** pour ressaisir votre mot de passe ou sur **Annuler** pour sortir de l'assistant.

Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

2.3.4. Etape 4 sur 8 - Entrer les renseignements du compte

Configurer mon compte Etape 4/8

Veuillez entrer les informations concernant votre compte. Les données que vous fournissez ici resteront confidentielles. Si avez déjà un compte, l'assistant affichera les informations que vous avez fournies au moment de sa création.

Prénom:

Nom:

Pays:

Cliquez sur 'Suivant' pour continuer ou sur 'Annuler' pour quitter l'Assistant.

Renseignements du compte



Note

Vous passerez cette étape si vous avez choisi **Passer cette étape** dans la **troisième étape**.

Entrez vos noms et prénoms et choisissez votre pays.

Si vous avez déjà un compte, l'assistant affichera les informations que vous avez renseignées précédemment. Vous pouvez les modifier si besoin.



Important

Les informations communiquées ici resteront confidentielles.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

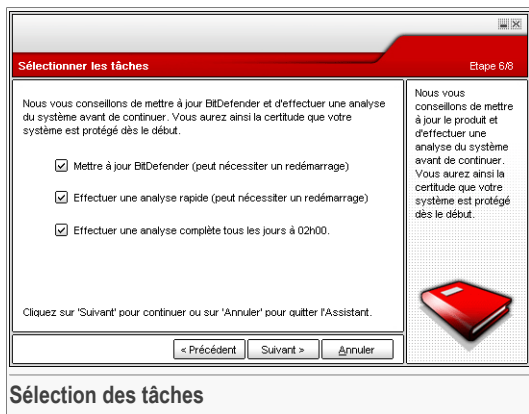
2.3.5. Etape 5 sur 8 - En savoir plus sur le RTVR



Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.



2.3.6. Etape 6 sur 8 - Sélectionner les tâches à lancer



Paramétrez BitDefender Antivirus v10 pour lancer les tâches de sécurité importantes pour votre ordinateur.

Les options suivantes sont disponibles:

- **Mettre à jour les moteurs BitDefender Antivirus v10 (peut nécessiter un redémarrage)** - une mise à jour des moteurs de BitDefender Antivirus v10 aura lieu pendant la prochaine étape pour protéger votre ordinateur contre les dernières menaces.
- **Lancer une analyse rapide (peut nécessiter un redémarrage)** - Une analyse rapide sera lancée pendant la prochaine étape afin que BitDefender Antivirus v10 s'assure que les fichiers contenus dans le dossier `Windows and Program Files` ne sont pas infectés.
- **Lancer une analyse complète de l'ordinateur tous les jours à 02h00** - Lance une analyse complète du système tous les jours à 02h00.



Important

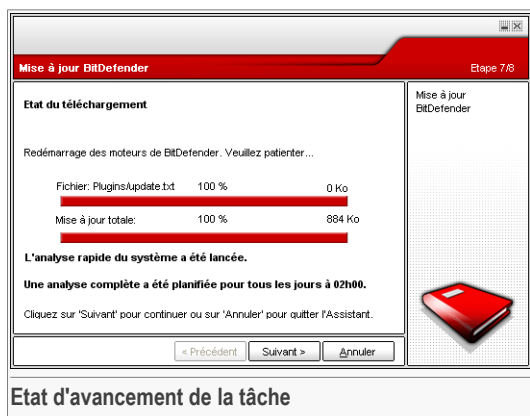
Il est fortement recommandé d'activer ces options avant de passer à l'étape suivante pour assurer la sécurité de votre système.

Si vous sélectionnez uniquement la dernière option ou aucune option, vous passerez l'étape suivante.

Vous pouvez faire n'importe quelle modification en retournant dans les étapes précédentes (cliquez sur **Précédent**). A partir d'ici, le processus est irréversible: si vous choisissez à continuer, vous ne pourriez plus revenir au pas précédent.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

2.3.7. Etape 7 sur 8 - Merci d'attendre la fin de la tâche



Merci d'attendre la fin de la tâche. Vous pouvez vérifier ici l'avancement de la tâche que vous avez sélectionnée lors de l'étape précédente.

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.



2.3.8. Etape 8 sur 8 - Voir le récapitulatif



Il s'agit de l'étape finale de l'assistant de configuration.

Sélectionnez **Ouvrir mon compte BitDefender** pour entrer votre compte BitDefender. Une connexion Internet est nécessaire.

Cliquez sur **Terminer** pour terminer l'assistant et continuer avec l'installation du produit.

2.4. Mise à jour majeure

La procédure de mise à jour majeure peut se faire ainsi:

- **Installer sans désinstaller les versions précédentes - pour BitDefender v8 ou plus récent, sauf Internet Security**

Double-cliquez sur le fichier d'installation et suivez l'assistant décrit dans la section « *Etapes d'installation* » (p. 9).



Important

Durant le processus d'installation, un message d'erreur causé par le *Filespy service*, apparaîtra. Cliquez sur **OK** pour continuer l'installation.

- **Désinstallez votre ancienne version et installez la nouvelle - pour toutes les versions BitDefender**

En premier lieu, vous devez désinstaller la version précédente, redémarrer l'ordinateur et installer la nouvelle comme décrit dans la rubrique « *Etales d'installation* » (p. 9).

**Important**

Si vous passez à une version supérieure du produit BitDefender, nous vous recommandons de sauvegarder les **paramètres BitDefender**. Une fois que vous serez passé à la version supérieure, vous pouvez les recharger.

2.5. Supprimer, réparer ou modifier BitDefender

Si vous voulez modifier, réparer ou supprimer **BitDefender Antivirus v10**, suivez le chemin depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 10** → **Modifier, Réparer ou Désinstaller**.

Il vous sera demandé une confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Modifier** - pour sélectionner de nouveaux composants du programme à ajouter ou pour sélectionner des composants déjà installés et à retirer;
- **Réparer** - pour réinstaller tous les composants choisis lors de l'installation précédente;

**Important**

Avant de réparer le produit, nous vous recommandons de sauvegarder les **paramètres BitDefender**. Dès que le processus de réparation est fini, vous pouvez les charger.

- **Supprimer** - pour supprimer tous les composants installés.

Pour continuer le processus, sélectionnez l'une des trois options listées ci-dessus. Nous recommandons **Supprimer** pour refaire une installation. Après la désinstallation, supprimez le sous-répertoire `Softwin` dans le répertoire `Program Files`.



Description et caractéristiques



3. BitDefender Antivirus v10

La solution antivirus et antispyware pour votre ordinateur !

BitDefender Antivirus v10 est un puissant outil antivirus et antispyware qui répond au mieux à vos besoins en matière de sécurité. Facilité d'utilisation et mises à jour automatique font de **BitDefender Antivirus** un produit de type "installez et oubliez".

3.1. Antivirus

L'objectif du module Antivirus est d'assurer la détection et la suppression de tous les virus en circulation. L'Antivirus BitDefender utilise des moteurs d'analyse robustes, certifié par ICSA Labs, Virus Bulletin, Checkmark, CheckVir et TÜV.

Détection proactive. B-HAVE émule un ordinateur virtuel dans un ordinateur où des morceaux de logiciel sont lancés de manière à vérifier leur comportement potentiellement malveillant. Cette technologie propriétaire de BitDefender représente un nouveau modèle de sécurité qui permet de conserver son système d'exploitation à l'abri de virus inconnus en détectant les morceaux de codes malicieux pour lesquels des signatures n'ont pas encore été créées.

Protection Antivirus Permanente. Les nouveaux moteurs d'analyse améliorés de BitDefender analyseront et désinfecteront les fichiers à l'accès, réduisant les pertes de données. Les documents infectés peuvent maintenant être récupérés au lieu d'être supprimés.

Détection et Suppression des Rootkits. A nouveau module BitDefender recherche les rootkits (programmes malicieux destinés au contrôle d'un PC, en restant camouflé) et les supprime.

Analyse du Web. Le trafic Internet est maintenant filtré en temps réel avant même d'atteindre votre navigateur Internet ce qui vous permet de profiter en toute sécurité de votre navigation.

Protection des Applications Peer-2-Peer et des messageries instantanées. Filtres contre les virus se propageant via les messageries instantanées et les logiciels de partage de fichiers.

Protection totale des emails. BitDefender se charge au niveau des protocoles POP3/SMTP, filtrant les messages entrants et sortants, quel que soit le client mail utilisé (MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.), et sans aucune configuration additionnelle.

3.2. Antispyware

BitDefender contrôle et prévient en temps réel les différentes menaces de spywares, avant qu'ils puissent endommager votre système. Par l'utilisation d'une base de données étendues de signatures de spywares, votre ordinateur restera à l'abri des spywares.

Antispyware en Temps Réel. BitDefender surveille des dizaines de points sensibles potentiels sur votre système, sur lesquels un spyware pourrait agir, et contrôle également les changements effectués sur votre système et vos applications. Les menaces spywares connues sont bloquées en temps réel.

Analyse et nettoyage des Spywares. BitDefender peut analyser complètement ou partiellement votre système contre les menaces de spywares connus. L'analyse utilise une base de données de signatures de spywares constamment mise à jour.

Protection de la vie privée. Le module de protection de vie privée surveille les flux HTTP (Web) et SMTP (Email) qui sortent de votre ordinateur en bloquant vos informations personnelles - telle que vos numéros de carte bancaire, de sécurité sociale ou autres séquences de caractères comme les mots de passe par exemple.

Anti-Dialer. Un anti-dialer configurable empêche des applications malicieuses de vous connecter sur des n° surtaxés.

Contrôle des Cookies. L'antispyware filtre les fichiers de type cookies entrants et sortants, conservant ainsi votre identité et vos préférences confidentielles quand vous surfez sur Internet.

Contrôle des Contenu Actifs. Bloque tous les scripts potentiellement malicieux tels que: ActiveX, Applettes Java ou code de type Java Scripts.

3.3. Autres Fonctions

Déploiement et utilisation. Un assistant se lance directement après l'installation permettant aux utilisateurs de choisir les paramètres de mises à jour les plus appropriés, la planification d'analyse du système, l'enregistrement et l'activation du produit.

Expérience utilisateur. BitDefender a revu le concept d'expérience de l'utilisateur en mettant en avant la simplicité et la facilité d'utilisation. Il en résulte que de nombreux modules de BitDefender v10 ont une utilisation beaucoup plus transparente pour l'utilisateur grâce à l'automatisation des tâches et à l'auto apprentissage.

Mise à jour chaque heure. Votre version de BitDefender sera mise à jour 24 fois par jour par Internet, directement ou via un serveur Proxy. Le logiciel est capable de



se réparer lui-même si nécessaire, en téléchargeant les fichiers endommagés ou manquants depuis les serveurs de BitDefender.

Support technique 24H/24 et 7J/7. Assuré en ligne par des représentants support qualifiés mais également par une base de données en ligne répondant aux questions les plus fréquemment posées.

Disque de Secours. BitDefender Antivirus v10 est fourni sur un CD bootable. Ce CD peut être utilisé pour analyser/réparer/désinfecter un système corrompu qui ne démarre plus.



4. Modules BitDefender

BitDefender Antivirus v10 est composé de modules différents: **Général**, **Antivirus**, **Antispyware** et **Mise à jour**.

4.1. Module Général

BitDefender est par défaut paramétré pour une sécurité optimale.

Vous pouvez configurer le niveau de sécurité et exécuter d'importantes tâches dans le module **Général**. Vous pouvez également enregistrer votre produit et paramétrer le comportement global de BitDefender.

4.2. Module Antivirus

BitDefender vous protège des virus, spyware et autre malware entrants dans votre système en analysant les fichiers, e-mails, téléchargement et tous les autres contenus qui arrivent sur votre ordinateur.

La protection offerte par BitDefender est divisée en deux catégories:

- **Analyse à l'accès** - empêche les nouveaux virus, spyware et autre malware de pénétrer votre système. C'est ce qu'on appelle la protection en temps réel – les fichiers sont analysés lorsque l'utilisateur y accède. BitDefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception. BitDefender analyse les fichiers dès que vous les utilisez.
- **Analyse à la demande** - détecte les virus, spyware et autre malware qui résident déjà dans votre ordinateur. C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que BitDefender doit analyser et BitDefender le fait – A la demande.

4.3. Module Antispyware

BitDefender contrôle des dizaines de "points à risque" dans votre système où les spywares pourraient agir, et analyse également les modifications apportées à votre système et à vos logiciels. C'est efficace contre les chevaux de Troie et autres outils installés par des hackers, qui essaient de compromettre votre vie privée et d'envoyer vos informations personnelles, comme vos numéros de carte bancaire, de votre ordinateur vers le pirate.

4.4. Module de Mise à jour

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures virales. Par défaut, BitDefender recherche automatiquement des mises à jour toutes les heures.

La rubrique Mise à jour de ce Manuel d'utilisation contient les thèmes suivants:

- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.
- **Mise à jour des moteurs antispyware** - de nouvelles signatures seront ajoutées à la base de données. Elles s'affichent sous le nom de **Spyware Definitions Update**.
- **Mise à jour produit** - lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**.

De plus, du point de vue de l'intervention de l'utilisateur, nous proposons:

- **Mise à jour automatique** - BitDefender contacte automatiquement le serveur de mise à jour afin de vérifier si une nouvelle mise à jour est disponible. Si tel est le cas, BitDefender est mis à jour automatiquement. Cette mise à jour automatique peut également être faite n'importe quand en cliquant sur **Mise à jour** depuis le **module de** mise à jour.
- **Mise à jour manuelle** - vous devez télécharger et installer les dernières signatures virales manuellement.




Console de gestion



5. Vue d'ensemble

BitDefender Antivirus v10 a été conçu avec une console de gestion centralisée, qui permet la configuration des options de protection de chaque module de BitDefender. Autrement dit, il suffit d'ouvrir la console pour accéder aux différents modules: **Antivirus** et **Antispyware**.

L'accès à cette console se fait par le menu Démarrer de Windows, en suivant le chemin suivant: **Démarrer** → **Programmes** → **BitDefender 10** → **BitDefender Antivirus v10** ou en double-cliquant simplement sur  l'icône **BitDefender** à partir de la barre d'état système.



Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants:

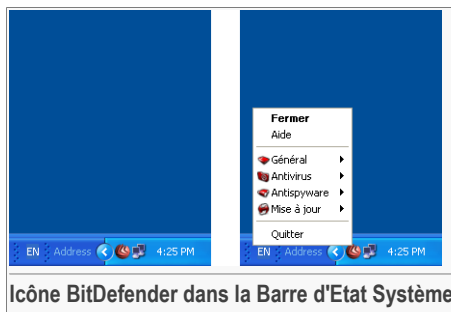
- **Général** - Dans cette rubrique, vous pouvez définir le niveau général de sécurité et exécuter des tâches de sécurité importantes. Vous pouvez également à partir de ce point enregistrer le produit et obtenir une vue d'ensemble des paramètres généraux, des contacts et des informations produit BitDefender.
- **Antivirus** - pour accéder à la fenêtre de configuration de l'**Antivirus**.

- **Antispyware** - pour accéder à la fenêtre de configuration de l' **Antispyware**.
- **Mise à jour** - pour accéder à la fenêtre de configuration des **Mises à jour**.

Dans la partie droite de la console de gestion vous pouvez voir l'info concernant la rubrique dans laquelle vous vous trouvez. L'option **Plus d'infos**, placée en bas à droite ouvre la rubrique d'**Aide**.

5.1. Barre d'état système

Lorsque la console est réduite, une icône apparaît dans la barre d'état système:



Icône BitDefender dans la Barre d'Etat Système

De plus, en faisant un clic-droit, un menu contextuel apparaîtra. Ce menu vous fournit un moyen de gestion rapide de BitDefender.

- **Afficher / Fermer** - ouvre la console de gestion ou la réduit dans la barre d'état système.
- **Aide** - ouvre la documentation d'aide électronique.
- **Général** - administration du module **général**.
 - **Entrer la nouvelle clé** - démarre l'assistant d'enregistrement qui vous guidera tout au long du processus d'enregistrement.
 - **Editer un compte** - démarre un assistant qui vous aidera à créer un compte BitDefender.
- **Antivirus** - administration du module **Antivirus**.
 - **La protection en temps réel est activée/désactivée** - montre l'état de la protection en temps réel (activée/désactivée). Cliquez sur cette option pour activer ou désactiver la protection en temps réel.
 - **Analyser** - ouvre un sous-menu à partir duquel vous pouvez choisir de lancer une des tâches d'analyse depuis l'onglet **Analyse**.
- **Antispyware** - administration du module **Antispyware**.



- **L'antispyware comportemental est activé/désactivé** montre l'état de la protection antispyware comportementale (activée/désactivée)- Cliquez sur cette option pour activer ou désactiver la protection antispyware comportementale.
- **Paramètres avancés** - vous permet de configurer les contrôles antispyware.
- **Mise à jour** - administration du module de **mise à jour**.
- **Mettre à jour** - effectue une **mise à jour immédiate**.
- **La protection en temps réel est activée/désactivée** - montre l'état de la **mise à jour automatique** (activée/désactivée). Cliquez sur cette option pour activer ou désactiver les mises à jour automatiques.
- **Quitter** - ferme l'application. En choisissant cette option, l'icône dans la barre d'état système disparaîtra et pour la faire apparaître de nouveau, vous devrez la lancer depuis le menu Démarrer.

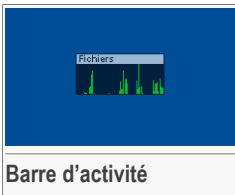
Note



Si vous désactivez un ou plusieurs des modules BitDefender, l'icône sera grisée. Ainsi vous saurez si quelques modules sont désactivés sans ouvrir la console de gestion. L'icône clignotera si une mise à jour est disponible.

5.2. Barre d'analyse de l'activité

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.



Les barres vertes (la **Zone de fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.

Note



La **Barre de l'activité d'analyse** vous annonce si le Résident est désactivé avec une croix rouge sur l'aire correspondante (**Zone Fichier**). Ainsi vous saurez si vous êtes protégé sans ouvrir la console de gestion.

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**.

Note



Pour cacher complètement cette fenêtre, décochez l'option **Activer la barre d'analyse de l'activité (graphique de l'activité du produit)** (depuis le module **Général**, rubrique **Paramètres**).



6. Module Général

La section **Général** de ce Manuel d'utilisation contient les thèmes suivants:

- Administration centrale
- Paramètres de la console de gestion
- Evénements
- Enregistrement du produit
- A propos

Note



Pour plus de détails concernant le module **Général** consultez la description de « *Module Général* » (p. 27).

6.1. Administration centrale


Pour accéder à cette section, cliquez sur l'onglet **Etat** dans le module **Général**.

Administration centrale

Cette rubrique contient des informations sur le statut de vos licences BitDefender. Vous pouvez enregistrer votre produit et voir sa date d'expiration.

6.1.1. Tâches prédéfinies


BitDefender propose un accès rapide aux tâches de sécurité essentielles. En utilisant ces tâches prédéfinies vous pouvez maintenir BitDefender à jour, lancer une analyse de système ou bloquer le trafic Internet.

Pour faire une analyse complète du système, cliquez sur  **Analyser**. La **fenêtre d'analyse** apparaîtra et une analyse complète du système démarrera.



Important

Nous vous recommandons fortement de lancer une analyse complète de votre système au moins une fois par semaine. Pour plus d'informations sur les tâches d'analyse et le processus d'analyse, allez dans la partie [Analyse à la demande](#) de ce manuel.

Avant d'analyser votre système, nous vous recommandons de mettre à jour votre produit pour qu'il puisse détecter les dernières menaces. Pour le mettre à jour, cliquez sur  **Mettre à jour**. Patientez quelques secondes ou regardez la rubrique [Mise à jour](#) pour regarder l'avancement du processus.



Note

Pour plus d'informations sur les mises à jour consulter le chapitre [Mise à jour automatique](#) du manuel.

6.1.2. Niveau de sécurité

Vous pouvez choisir le niveau de sécurité qui répond le mieux à vos besoins de sécurité. Déplacer le curseur sur l'échelle pour sélectionner le niveau de sécurité adapté.

Il y a 3 niveaux de sécurité:

Niveau de sécurité	Description
Maintenance	N'offre pas de protection. Seule la mise à jour automatique est active. Fait uniquement les mises à jour BitDefender. Même s'il n'offre pas de protection, ce niveau de sécurité peut s'avérer utile pour les administrateurs système.



Niveau de sécurité	Description
Système local	Assure la protection antivirus. Spécialement recommandé pour les ordinateurs non connectés à un réseau ou à Internet. Le niveau de consommation de ressources système est très faible. Les fichiers accédés sont analysés pour détecter la présence de virus.
Système local Plus	Offre une protection antivirus&antispyware. Recommandé particulièrement pour les ordinateurs qui ne sont pas connectés à un réseau ou à Internet. Le niveau de consommation des ressources est faible. Tous les fichiers seront analysés à l'accès pour détecter les virus et les spywares.


BitDefender Antivirus v10 est recommandé pour les ordinateurs sans réseau ou sans accès à Internet.

Vous pouvez paramétrer le niveau de sécurité en cliquant sur **Personnalisé**. Sélectionnez dans la fenêtre apparue les options de protection BitDefender que vous désirez activer et cliquez sur **OK**.

Si vous cliquez sur **Défaut** vous chargerez les paramètres par défaut.

6.1.3. Etat de l'enregistrement

Cette rubrique contient des informations sur l'état de vos licences BitDefender. Vous pouvez voir comment enregistrer votre produit et voir sa date d'expiration.

Pour entrer une nouvelle clé d'activation, cliquez sur  **Entrer une nouvelle clé**. Compléter l'**assistant d'enregistrement** pour finaliser l'enregistrement de BitDefender.

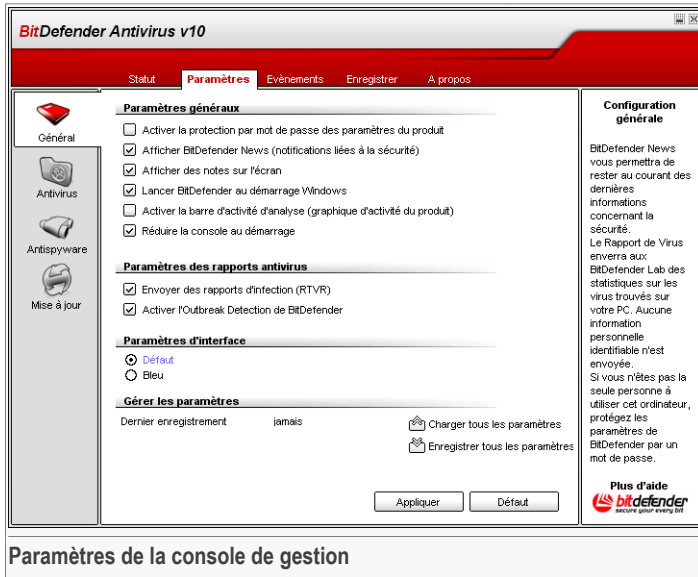


Note

Pour plus d'informations sur l'enregistrement, reportez vous à la rubrique **Enregistrement du produit** du manuel utilisateur.

6.2. Paramètres de la console de gestion

Pour accéder à cette section, cliquez sur l'onglet **Configuration** dans le module **Général**.



Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se réduit automatiquement.

Il existe 4 catégories d'options: **Paramètres généraux**, **Paramètres des rapports antivirus**, **Paramètres d'interface** et **Gérer les paramètres**.

6.2.1. Paramètres Généraux

- **Activer la protection par mot de passe pour les paramètres du produit** - permet de choisir un mot de passe afin de protéger la configuration de la console de gestion BitDefender ;



Note

Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres BitDefender par un mot de passe.

La fenêtre suivante apparaîtra:



Confirmation mot de passe

Mot de passe

Reintroduire le mot

Le mot de passe devrait avoir au moins 9 caractères.

Mot de passe

Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Reintroduire le mot de passe** et cliquez sur **OK**.

A présent, si vous souhaitez changer les options de configuration de BitDefender, le mot de passe vous sera demandé.



Important

Si vous avez oublié votre mot de passe vous devrez réinstaller partiellement le produit pour modifier la configuration de BitDefender.

- **Recevoir alertes de sécurité** - affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par les serveurs de BitDefender.
- **Afficher des notes sur l'écran** - affiche des fenêtres de notifications sur l'état de votre produit.
- **Lancer BitDefender au démarrage Windows** - lance automatiquement BitDefender au démarrage du système.



Note

Nous vous recommandons de garder cette option active.

- **Activer la barre d'analyse de l'activité (sur le graphique de l'activité du produit)** - active/désactive la [barre d'analyse de l'activité](#).
- **Minimiser la console au lancement** - réduit la console de gestion BitDefender après son chargement au démarrage. Seul l'icône BitDefender apparaîtra dans la barre d'état système.

6.2.2. Paramètres du rapport des virus

- **Envoyer des rapports de virus** - envoie aux BitDefender Labs des rapports concernant les virus identifiés sur votre ordinateur. Les informations envoyées nous servent à garder une trace des apparitions de virus.

Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations

envoyées contiendront uniquement le nom des virus et seront utilisées dans le seul but de créer des rapports statistiques.



- **Activer l'Outbreak Detection de BitDefender** - envoi des rapports aux BitDefender Labs à propos d'apparitions éventuelles de virus.

Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront uniquement les virus potentiels et seront utilisées dans le seul but de créer des rapports statistiques.

6.2.3. Paramètres d'Interface

Vous permet de sélectionner la couleur de la console de gestion. Le skin représente l'image de fond de l'interface. Pour sélectionner un skin différent, cliquez sur la couleur correspondante.

6.2.4. Gérer les paramètres

Utilisez les boutons  **Enregistrer tous les paramètres** /  **Charger tous les paramètres** pour sauvegarder / charger les paramètres établis pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.



Important

Seuls les utilisateurs ayant des droits administrateurs peuvent sauvegarder et charger les paramètres.

Cliquez sur **Appliquer** pour sauvegarder les modifications. Si vous cliquez sur **Défaut** vous chargerez les paramètres par défaut.

6.3. Événements

Pour accéder à cette section, cliquez sur l'onglet **Evénements** dans le module **Général**.



BitDefender Antivirus v10

Statut Paramètres **Événements** Enregistrer A propos

Liste des événements

Général Sélectionner la source Toutes

Type	Date	Temps	Description	Source
Informations	10/2/2006	4:15:34 ...	Mise à jour réussie	Mise à jour
Informations	10/2/2006	4:17:12 ...	Analyse terminée	Antivirus

Journal des événements

Les cas d'objets infectés ou suspects, les alertes du pare-feu et les mises à jour sont conservés afin de fournir les informations nécessaires à la prise de décisions sur la sécurité de votre système.

Les événements peuvent être filtrés par module ou par importance.

Cliquer sur "Nettoyer les logs" supprimera définitivement toutes les entrées.

Plus d'aide
 bitdefender
 antivirus pour windows XP

Événements

Tous les événements générés par BitDefender sont affichés dans cette partie.

Il existe 3 types d'événements: **Information**, **Alerte** et **Critique**.

Exemples d'événements:

- **Information** - quand un email est analysé;
- **Alerte** - quand un fichier suspect est détecté;
- **Critique** - quand un fichier infecté est détecté.

Pour chaque événement sont fournies les informations suivantes: la date et l'heure de la production de l'événement, une brève description et sa source (**Antivirus** ou **Mise à Jour**). Double-cliquez sur un événement pour voir ses propriétés.

Vous pouvez filtrer ces événements de 2 manières (par type ou par source):

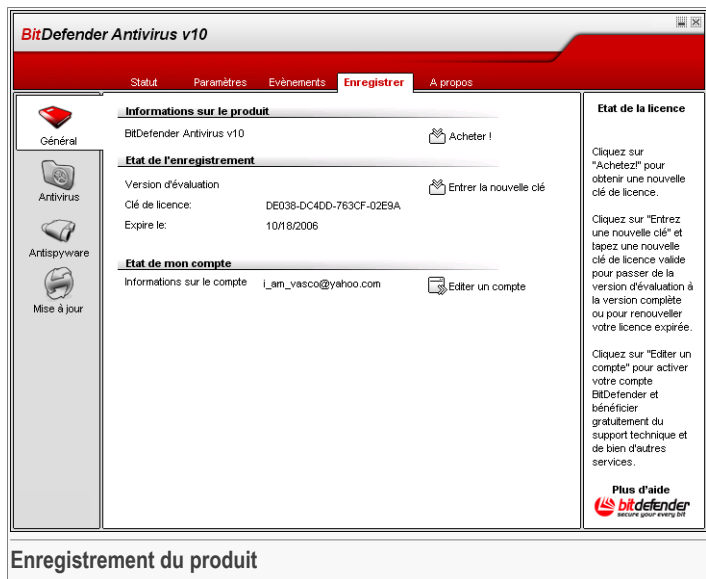
- Cliquez sur **Filtrez** pour sélectionner les types d'événements à afficher;
- Sélectionnez la source de l'événement depuis le menu déroulant.

Si la [console de gestion](#) est ouverte à la rubrique **Événements** et qu'un même temps un événement apparaît, vous devez cliquer sur **Actualiser** pour voir l'événement.

Pour effacer tous les événements de la liste cliquez **Nettoyer les logs**.

6.4. Enregistrement du produit

Pour accéder à cette section, cliquez sur l'onglet **Enregistrer** dans le module **Général**.



Cette rubrique contient des informations sur le produit BitDefender (état de l'enregistrement, identité du produit, date d'expiration) et sur le compte BitDefender. Vous pouvez enregistrer votre produit et configurer votre compte BitDefender ici.

Cliquez sur le bouton **Acheter** pour obtenir une nouvelle clé de licence de la boutique en ligne BitDefender.

En cliquant sur **Entrer une nouvelle clé** vous pouvez enregistrer le produit, modifier la clé d'enregistrement ou les détails du compte. Pour configurer votre compte BitDefender, cliquez sur **Editer un compte**. Dans les deux cas, l'assistant d'enregistrement apparaîtra.

6.4.1. Assistant d'enregistrement

L'assistant d'enregistrement est une procédure en 5 étapes.



Etape 1 sur 5 - Bienvenue dans l'assistant d'enregistrement BitDefender

Assistant d'installation initiale de BitDefender Etape 1/5

Bienvenue dans l'Assistant d'installation initiale de BitDefender.
Cet assistant vous aidera à enregistrer votre produit et à activer votre compte BitDefender.

Cliquez sur 'Suivant' pour continuer l'Assistant.

< Précédent **Suivant >** Annuler

Fenêtre d'accueil

Cliquez sur **Suivant**.

Etape 2 sur 5 - Enregistrement de BitDefender

Enregistrer Etape 2/5

Ceci est une version d'évaluation de BitDefender Antivirus v10. Si vous voulez évaluer le produit, cochez 'Continuer l'évaluation du produit'. Si vous voulez enregistrer le produit, cochez 'Enregistrer le produit' et entrez votre clé de licence qui se trouve:

- Sur la carte d'enregistrement du produit
- Sur la pochette du CD ou le manuel
- Dans l'email reçu lors de l'achat en ligne

Si vous n'avez pas de numéro de série, contactez-nous à sales@bitdefender.com

Continuer l'évaluation du produit
 Enregistrer le produit

Entrer la nouvelle clé:

Cliquez sur 'Suivant' pour continuer l'Assistant.

< Précédent **Suivant >** Annuler

Enregistrement du Produit

Choisissez **Enregistrer le produit** pour enregistrer **BitDefender Antivirus v10**. Entrez la clé de licence dans le champ **Entrer une nouvelle clé**.

Pour continuer à évaluer le produit, sélectionnez **Continuer l'évaluation du produit**.

Cliquez sur **Suivant**.

Etape 3 sur 5 - Création d'un compte BitDefender

Enregistrer le produit Etape 3/5

Vous devez créer un compte pour accéder au support technique de BitDefender et aux autres services personnalisés de BitDefender. Si vous avez déjà un compte BitDefender, veuillez entrer les informations requises. Si vous n'avez pas de compte BitDefender, veuillez entrer votre adresse électronique et un mot de passe.


Adresse électronique:

Mot de passe:

Vous avez oublié votre mot de passe ?

Passer cette étape

Cliquez sur "Suivant" pour continuer ou sur "Annuler" pour quitter l'Assistant.



< Précédent Suivant > Annuler

Création de compte

Je n'ai pas de compte BitDefender

Pour bénéficier du support technique gratuit et d'autres services, il faut créer un compte BitDefender.

Entrez une adresse email valide dans le champ **E-mail**. Entrez votre mot de passe dans le champ **Mot de passe**. Confirmez le mot de passe dans le champ **Retapez Mot de passe**. Utilisez l'adresse mail et le mot de passe pour vous connecter à votre compte sur <http://myaccount.bitdefender.com>



Note

Votre mot de passe doit comporter au moins quatre caractères.

Pour créer votre compte vous devez d'abord activer votre adresse e-mail. Vérifiez votre messagerie et suivez les instructions reçues dans l'email qui vous a été envoyé par le service d'enregistrement BitDefender.



Important

Merci d'activer votre compte avant de passer à l'étape suivante.

Si vous ne souhaitez pas créer un compte BitDefender, sélectionnez **Passer cette étape**.

Cliquez sur **Suivant**.



J'ai déjà un compte BitDefender

Si vous avez déjà un compte BitDefender, entrez votre adresse email et le mot de passe de votre compte. Si vous tapez un mot de passe incorrect, il vous sera demandé de le ressaisir quand vous cliquerez sur **Suivant**. Cliquez sur **Ok** pour ressaisir votre mot de passe ou sur **Annuler** pour sortir de l'assistant.

Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

Cliquez sur **Suivant**.

Etape 4 sur 5 - Entrez les renseignements du compte

Configurer mon compte Etape 4/5

Veuillez entrer les informations concernant votre compte. Les données que vous fournissez ici resteront confidentielles. Si avez déjà un compte, l'assistant affichera les informations que vous avez fournies au moment de sa création.

Prénom:

Nom:

Pays:

Cliquez sur 'Suivant' pour continuer ou sur 'Annuler' pour quitter l'Assistant.

< Précédent Suivant > Annuler



Note

Vous ne remplirez pas cette étape si vous avez sélectionné **Passer cette étape à la troisième étape**.

Entrez vos noms et prénoms et choisissez votre pays.

Si vous avez déjà un compte, l'assistant affichera les informations que vous avez renseignées précédemment. Vous pouvez également modifier ces informations.



Important

Les informations communiquées ici resteront confidentielles.

Cliquez sur **Suivant**.

Etape 5 sur 5 - Récapitulatif



Il s'agit de l'étape finale de l'assistant de configuration. Vous pouvez faire n'importe quelle modification en retournant dans les étapes précédentes (cliquez sur **Précédent**).

Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour terminer l'assistant.

Sélectionnez **Ouvrir mon compte BitDefender** pour entrer votre compte BitDefender. Une connexion Internet est nécessaire.

6.5. A propos

Pour accéder à cette rubrique, cliquez sur l'onglet **A propos** dans le module **Général**.



BitDefender Antivirus v10

Statut Paramètres Événements Enregistrer **A propos**

<p> Général</p> <p> Antivirus</p> <p> Antispyware</p> <p> Mise à jour</p>	<p>Informations sur le produit</p> <p>BitDefender Antivirus v10 - Build 108 (c) 2001-2006 SOFTWIN. Tous droits réservés.</p> <hr/> <p>Contacts</p> <p>Web: www.bitdefender.com Email: sales@bitdefender.com Phone: 954.776.6262 Fax: 954.776.6462 Web:</p> <hr/> <p>Support technique</p> <p>Support technique: support@bitdefender.com FAQ: http://www.bitdefender.com/support/faq.htm Base de connaissance: http://kb.bitdefender.com/</p>	<p>A propos de BitDefender</p> <p>BitDefender fournit des solutions de sécurité répondant aux impératifs de protection des environnements informatiques actuels, assurant la protection efficace de plus de 120 millions d'utilisateurs dans plus de 200 pays. BitDefender est certifié par ICSA Labs, CheckMark, CheckVir, AV-Comparatives, TÜV et Virus Bulletin, et est le 1er produit de sécurité à avoir reçu le prix de l'innovation technologique: IST Prize.</p> <p>Plus d'aide bitdefender <small>SECURE. YOUR. WAY. TO. IT.</small></p>
---	--	--

Informations générales

Dans cette partie vous pouvez trouver des informations sur votre produit et les contacts dont vous pourriez avoir besoin.

BitDefender™ fournit des solutions de sécurité qui répondent aux besoins de protection de l'environnement informatique actuel. BitDefender™ offre une gamme de logiciels de sécurité des plus efficace, fixant de nouvelles normes en matière de prévention des menaces, de détection en temps réel et de réduction des risques. BitDefender fournit des produits et services à plus de 41 millions de foyers et d'entreprises dans plus de 180 pays.

BitDefender est certifié par tous les principaux organismes de tests indépendants - **ICSA Labs**, **CheckMark** et **Virus Bulletin**, et est la seule solution de sécurité à avoir reçu le prix européen de l'innovation technologique **IST Prize**.

Pour plus d'informations sur BitDefender, visitez notre site: <http://www.bitdefender.com>.



7. Module Antivirus

La rubrique **Antivirus** de ce Manuel d'utilisation contient les thèmes suivants:

- Analyse à l'accès
- Analyse à la demande
- Quarantaine



Note

Pour plus de détails concernant le module **Antivirus** consulter la description de « *Module Antivirus* » (p. 27).

7.1. Analyse à l'accès

Pour accéder à cette section cliquez sur l'onglet **Résident** dans le module **Antivirus**.


The screenshot shows the BitDefender Antivirus v10 interface. The 'Résident' tab is active, showing 'Protection en temps réel activée'. The 'Niveau de protection' is set to 'Défaut'. A traffic graph is visible at the bottom, showing activity over a 120-second period. The interface includes a sidebar with navigation options like 'Général', 'Antivirus', 'Antispyware', and 'Mise à jour'. A 'Statistiques' section shows the last analyzed file and a 'Plus de statistiques' link.

Protection en temps réel.

Dans cette rubrique vous pouvez configurer la **protection en temps réel** et voir les informations concernant son activité. La **protection en temps réel** protège votre ordinateur en analysant les emails, téléchargements et tous les fichiers à l'accès.

**Important**

Pour prévenir l'infection de votre ordinateur par des virus, laissez la **protection en temps réel** activée.

Dans la partie inférieure de cette rubrique, vous pouvez voir les statistiques de **protection en temps réel** sur les fichiers et emails analysés. Cliquez sur  **Plus de statistiques** si vous voulez ouvrir une fenêtre plus détaillée.

7.1.1. Niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

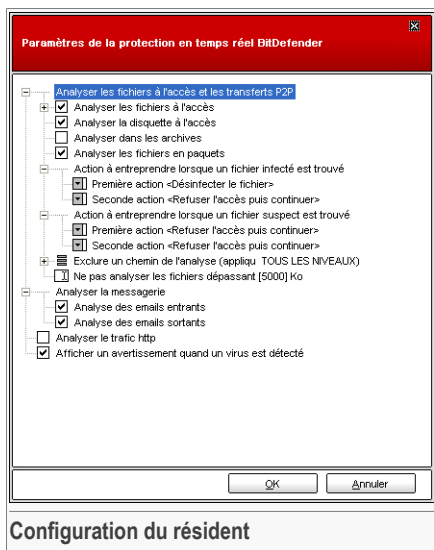
Il existe trois niveaux de protection:

Niveau de protection	Description
Tolérant	<p>Couvre les besoins de sécurité de base. La consommation de ressources système est très faible.</p> <p>Les programmes et emails entrants ne sont analysés que pour rechercher les virus. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.</p>
Défaut	<p>Offre un niveau de sécurité standard. La consommation de ressources système est faible.</p> <p>Tous les fichiers et les emails entrants ou sortants sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.</p>
Agressif	<p>Offre un niveau de sécurité élevé. La consommation de ressources système est modérée.</p> <p>Tous les fichiers, les emails entrants ou sortants et le trafic Web, sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises envers les fichiers infectés sont les suivantes: nettoyer le fichier / refuser l'accès.</p>



Les utilisateurs avancés peuvent vouloir profiter des possibilités de paramétrage d'analyse de BitDefender. Le module d'analyse peut être paramétré pour ne pas analyser les extensions de fichiers, répertoires ou archives que vous savez être sans danger. Cela peut considérablement réduire le temps d'analyse et améliorer le temps de réaction de votre ordinateur durant une analyse.

Vous pouvez personnaliser la **protection en temps réel** en cliquant sur **Niveau personnalisé**. La fenêtre suivante apparaîtra:



Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows.

Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Vous pourrez observer que certaines options d'analyse ne peuvent pas s'ouvrir, même si un signe "+" apparaît à leur côté. La raison est que ces options n'ont pas encore été sélectionnées. Si vous les cochez, elles pourront être ouvertes.

Configuration du résident

- Sélectionnez **Analyser à l'accès les fichiers et les transferts P2P** pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

Option	Description
Analyser les fichiers accédés	Analyse de tous les fichiers Tous les fichiers à l'accès seront analysés, quel que soit leur type.
	Analyse des extensions à risques seulement Seuls les fichiers avec les extensions suivantes seront analysés: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd;

Option	Description
	.sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml et .nws.
Analyse des extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ",".
Exclusion des extensions de l'analyse	Tous les fichiers à l'accès seront analysés à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ",".
Rechercher riskware	<p>Rechercher des riskware. Ces fichiers seront traités comme des fichiers infectés. Il est possible que les logiciels contenant des composants de type adware ne fonctionnent pas si cette option est activée.</p> <p>Sélectionnez Exclure les dialers et les applications de l'analyse si vous souhaitez exclure ce genre de fichiers de l'analyse.</p>
Analyser la disquette à l'accès	Analyser le lecteur de disquette quand il est utilisé.
Analyser dans les archives	Les archives seront également analysées. Avec cette option activée, l'ordinateur sera ralenti.
Analyser dans les fichiers compressés	Tous les fichiers compressés seront analysés.
Première action	Sélectionnez à partir du menu déroulant la première action à entreprendre sur les fichiers suspects et infectés.
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Désinfecter fichier	Pour désinfecter un fichier infecté.



Option	Description
Effacer le fichier	Pour supprimer un fichier infecté, sans alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine.
Deuxième action	Sélectionnez à partir du menu déroulant la deuxième action à entreprendre sur les fichiers infectés, au cas où la première action échoue.
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Effacer le fichier	Pour supprimer un fichier infecté, sans alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine.
Ne pas analyser les fichiers d'une taille supérieure à [x] Ko	Tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.
Exclure le chemin de l'analyse (appliqué à TOUS LES NIVEAUX)	<p>Cliquez sur le "+" correspondant à cette action pour spécifier un dossier qui sera exclu de l'analyse. En conséquence, l'option sera élargie et une nouvelle option <i>Nouvel objet</i>, apparaîtra. Cochez la case correspondante au nouvel objet, et sélectionnez le dossier que vous voulez voir exclu de l'analyse à partir de la fenêtre d'exploration.</p> <p>Les éléments sélectionnés ici seront exclus de l'analyse, quel que soit le niveau de protection choisi (pas uniquement pour le Niveau personnalisé).</p>

- **Analyser le trafic de messagerie** - analyse le trafic de la messagerie.

Les options suivantes sont disponibles:

Option	Description
Analyser les emails entrants	Analyser tous les emails entrants.
Analyser les emails sortants	Analyser tous les emails sortants.

- **Analyser le trafic http** - analyse le trafic http.
- **Afficher une alerte si un virus est trouvé** - une fenêtre d'alerte sera affichée lorsqu'un virus sera détecté dans un fichier ou message e-mail.

Pour un fichier infecté, la fenêtre d'alerte contiendra le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où l'on peut trouver plus d'informations sur ce virus. Pour un message e-mail infecté, la fenêtre d'alerte contiendra également des informations sur l'expéditeur et le destinataire.

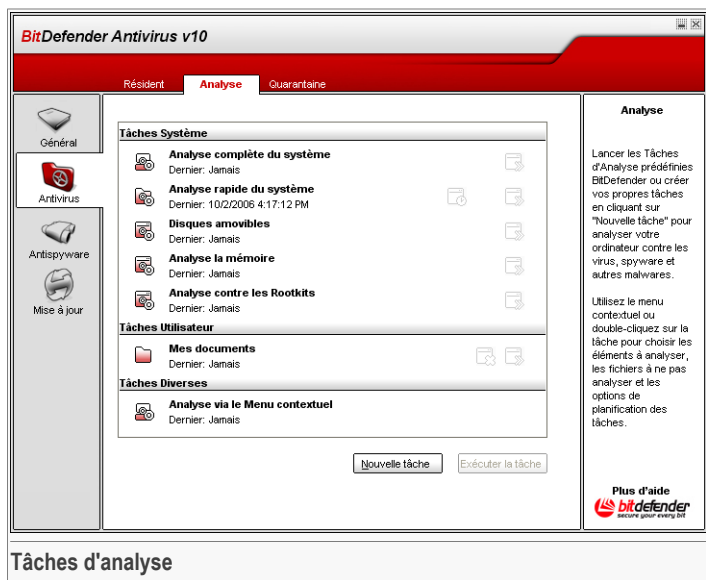
Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera à envoyer ce fichier aux BitDefender Labs pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

Si vous voulez retourner au niveau par défaut, cliquez sur **Niveau par défaut**.

7.2. Analyse à la demande

Pour accéder à cette section cliquez sur l'onglet **Analyse** dans le module **Antivirus**.



Tâches d'analyse



Dans cette rubrique vous pouvez configurer BitDefender pour analyser votre ordinateur. L'objectif principal de BitDefender est de conserver votre ordinateur sans virus. Cela se fait avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender. Et il est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

7.2.1. Tâches d'analyse

L'analyse à la demande est basée sur les tâches d'analyses. L'utilisateur peut choisir d'utiliser les tâches d'analyse par défaut ou ses propres tâches prédéfinies.

Il y a trois catégories de tâches d'analyse:

- **Tâches système** - contiennent une liste des tâches système par défaut. Les tâches suivantes sont disponibles:

Tâche d'analyse par défaut	Description
Analyse approfondie du système	Analyse l'ensemble du système, y compris les archives, pour rechercher les virus et les spywares.
Analyse complète du système	Analyse l'ensemble du système, mis à part les archives, pour rechercher les virus et les spywares.
Analyse rapide du système	Analyse tous les programmes pour rechercher les virus et les spywares.
Analyse des disques amovibles	Analyse les disques amovibles pour rechercher les virus et les spywares.
Analyse de la mémoire	Analyse la mémoire pour trouver les menaces connues de type spyware.
Analyse contre les Rootkits	Analyse la mémoire pour trouver les menaces camouflées.



- **Tâches prédéfinies** - contiennent les tâches prédéfinies par l'utilisateur.

Une tâche appelée `Mes documents` est disponible. Utilisez cette tâche pour analyser les documents contenus dans le dossier `Mes documents`.

- **Tâches diverses** - contiennent une liste de tâches diverses. Ces tâches font référence à des modes d'analyse différents qui ne peuvent pas être lancés depuis

cette fenêtre. Vous pouvez uniquement modifier leurs paramètres et voir le rapport d'analyse.

Trois boutons sont disponibles à la droite de chaque tâche :

-  **Planifier la tâche** - indique que la tâche sélectionnée est planifiée pour plus tard. Cliquez sur ce bouton pour aller à la [rubrique Planification](#) à partir de la fenêtre **Propriétés** où vous pouvez modifier ce paramètre.
-  **Supprimer** - supprime la tâche sélectionnée.

**Note**

Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

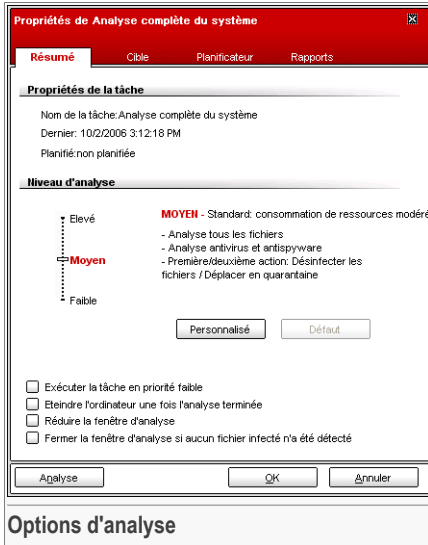
-  **Analyser** - lance la tâche sélectionnée, démarrant ainsi une [analyse immédiate](#).

7.2.2. Propriétés des tâches d'analyse.

Chaque tâche d'analyse dispose de sa propre fenêtre de **Propriétés**, dans laquelle vous pouvez configurer les options d'analyse, définir les éléments à analyser, programmer une tâche ou voir le rapport. Pour entrer dans cette fenêtre, double-cliquez sur la tâche. La fenêtre suivante apparaîtra :



Options d'analyse



Vous trouverez dans cette rubrique les informations concernant les tâches (nom, dernière analyse, planification) et aurez la possibilité de définir les paramètres d'analyse.

Niveau d'analyse

Premièrement, il faut choisir le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau approprié.

Il y a 3 niveaux d'analyse:

Niveau de protection	Description
Basse	Offre un niveau de détection correct. La consommation de ressources est faible. Seuls les programmes sont scannés pour détecter les virus. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer / mettre en quarantaine.

**Niveau de Description
protection**

Moyenne Offre un niveau de détection efficace. La consommation de ressources système est modérée.

Tous les fichiers sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer / mettre en quarantaine.

Agressif Offre un niveau de détection élevé. La consommation de ressources système est élevée.

Tous les fichiers et les fichiers archives sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes: nettoyer / mettre en quarantaine.

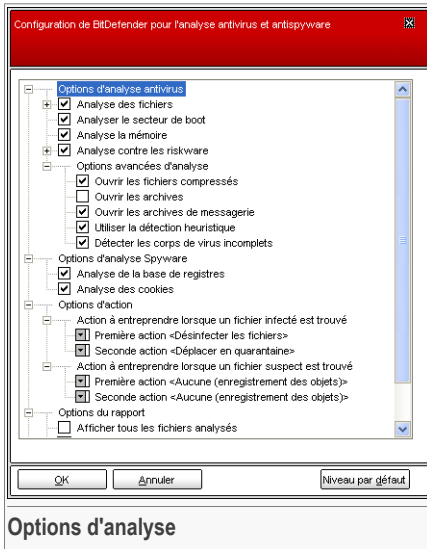
**Important**

Analyse contre les Rootkits - La tâche a le même niveau d'analyse. Cependant, les options sont différentes:

- **Basse** - Seuls les processus sont analysés. Aucune action n'est prise sur les objets détectés.
- **Moyenne** - Fichiers et processus sont analysés pour rechercher des objets cachés. Aucune action ne sera appliquée sur les objets détectés.
- **Analyse** - Fichiers et processus sont analysés pour rechercher des objets cachés. Les objets détectés sont renommés.

Les utilisateurs avancés peuvent vouloir profiter des possibilités de paramétrage d'analyse de BitDefender. Le moteur d'analyse peut être paramétré pour éviter certaines extensions de fichiers, répertoires ou archives que vous savez être sans danger. Cela peut considérablement réduire le temps d'analyse et améliorer le temps de réaction de votre ordinateur durant une analyse.

Cliquez sur **Personnaliser** pour définir vos propres options d'analyse. La fenêtre suivante apparaîtra:



Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows.

Les options d'analyse sont groupées en cinq catégories:

- **Options d'analyse des virus**
- **Options de l'analyse antispyware**
- **Options d'action**
- **Options du rapport**
- **Autres options**

Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.



Important

Pour la tâche **Recherche de Rootkits** seulement trois catégories sont disponibles: **Option d'analyse des Rootkits**, **Options de Rapport** et **Autres options**. Depuis la première catégorie, vous pouvez choisir ce que vous voulez analyser (fichiers et/ou mémoire) et vous pouvez définir l'action à prendre sur les objets détectés (**Aucune (log des objets)/Renommer les fichiers**). Les deux dernières catégories sont identiques à celles décrites ci-dessous.

- Spécifiez le type d'objets à analyser (archives, emails et autres) ainsi que d'autres options. Cela se fait par la sélection de certaines options dans la catégorie **Options d'analyse des virus**.

Option	Description
Analyser les fichiers	Analyse de tous les fichiers Tous les fichiers à l'accès seront analysés, quel que soit leur type.
	Analyse des extensions à risques seulement Seuls les fichiers avec les extensions suivantes seront analysés: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml et nws.
	Analyse des extensions définies par l'utilisateur Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ",".
	Exclusion des extensions définies par l'utilisateur Tous les fichiers à l'accès seront analysés à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ",".
Analyser les secteurs de boot	Analyser les secteurs de boot du système.
Analyse de la mémoire	Analyser la mémoire pour détecter les virus et les autres malwares.
Analyse contre les riskware	Analyser les menaces autres que virales, tels que les dialers et adwares. Ces fichiers seront traités comme des fichiers infectés. Il est possible que les logiciels contenant des composants de type adware ne fonctionnent pas si cette option est activée. Choisir Ne pas inclure les applications et les dialers si vous voulez exclure de l'analyse ce type de fichiers.
Options d'analyse avancées	Ouvrir les fichiers compressés Analyser les fichiers compressés.
	Ouvrir les fichiers archives Analyser l'intérieur des fichiers archives.
	Ouvrir les archives de messagerie Analyser dans les archives de messagerie.



Option	Description
Utiliser la détection heuristique	Active l'analyse heuristique des fichiers. Le but de l'analyse heuristique est d'identifier de nouveaux virus, se basant sur des algorithmes spécifiques, avant que ces virus ne soient connus. De fausses alertes peuvent apparaître. Quand un tel fichier est détecté, il est classé comme étant suspect. Dans ce cas, nous vous recommandons d'envoyer le fichier aux BitDefender Labs afin qu'il soit analysé.
Détecter les morceaux de virus incomplets	Détecte les morceaux de virus incomplets.

- Spécifiez la cible d'analyse antispyware (base de registres, cookies). Cela se fait par la sélection de certaines options dans la catégorie **Options de l'analyse antispyware**.

Option	Description
Analyse de la base de registre	Analyse les entrées du Régistre.
Analyse des cookies	Analyse les cookies.

- Spécifiez l'action à appliquer aux fichiers suspects et infectés. Ouvrez **Options d'action** pour voir toutes les actions possibles sur les fichiers infectés.

Choisissez l'action à entreprendre quand un fichier suspect ou infecté est détecté. Vous pouvez déterminer différentes options ainsi que des solutions alternatives en cas d'échec de la première méthode.

Action	Description
Aucune	Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Demander l'utilisateur l'action	à Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du

Action	Description
	fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Désinfecter	Pour désinfecter un fichier infecté.
Effacer	Pour supprimer un fichier infecté, sans alerte.
Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.
Renommer	Pour renommer les fichiers infectés. La nouvelle extension des fichiers infectés sera <code>.vir</code> . En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et une analyse ultérieure.



Important

Renommer les fichiers a un effet similaire sur les fichiers camouflés (rootkits). La nouvelle extension des fichiers détectés sera `.bd.ren`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et une analyse ultérieure.

- Spécifiez les options du fichier de rapport. Ouvrez la rubrique **Options du rapport** pour voir toutes les options possibles.

Option	Description
Afficher tous les fichiers analysés	Affiche tous les fichiers, infectés ou pas, et leur état dans un fichier journal. Avec cette option activée, l'ordinateur sera ralenti.
Effacer les journaux de plus de [X] jours	C'est un champ permettant de définir - quand c'est possible - combien de temps un fichier journal doit être conservé dans le dossier Analyse des journaux . Choisissez cette option et entrez une nouvelle périodicité. L'intervalle par défaut est de 180 jours.



Note

Vous pouvez voir le fichier de rapport dans la partie [Rapports](#) de la fenêtre de [Propriétés](#).



- Spécifiez les autres options. Ouvrez la catégorie **Autres Options** depuis laquelle vous pourrez sélectionner les options suivantes:

Option	Description
Soumettre les fichiers suspects aux BitDefender Labs	Il vous sera demandé de soumettre les fichiers suspects aux BitDefender Labs à la fin de l'analyse.

Si vous cliquez sur **par Défaut** vous chargerez les paramètres par défaut. Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

Autres paramètres

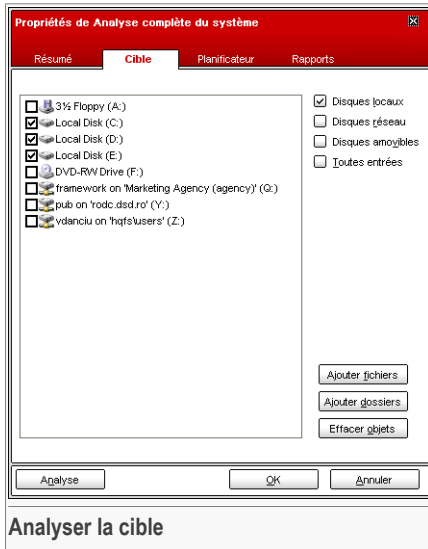
Une série d'options générales de paramétrage de l'analyse sont également disponibles:

Option	Description
Exécuter la tâche d'analyse avec une priorité basse	Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
Arrêter l'ordinateur lorsque l'analyse est terminée	L'ordinateur s'éteint à la fin de l'analyse.
Soumettre les fichiers suspects aux BitDefender Labs	Il vous sera demandé de soumettre les fichiers suspects aux BitDefender Labs à la fin de l'analyse.
Réduire la fenêtre d'analyse au démarrage dans la barre d'état système	Réduit la fenêtre d'analyse dans la barre d'état système . Double-cliquez sur l'icône de BitDefender pour l'ouvrir.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Analyser la cible

Double-cliquez sur une tâche donnée, puis cliquez sur l'onglet **Chemin d'analyse** pour entrer dans cette partie.



Vous pouvez définir les paramètres de la cible.

Cette partie contient les boutons suivants:

- **Ajouter fichiers** - ouvre une fenêtre de navigation dans laquelle vous pouvez choisir le fichier que vous voulez analyser.
- **Ajouter dossiers** - ouvre une fenêtre de navigation dans laquelle vous pouvez choisir le dossier que vous voulez analyser.



Note

Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant.

- **Effacer sélection** - efface le fichier/dossier sélectionné auparavant.



Note

Seuls les fichiers/dossiers rajoutés après peuvent être effacés, pas ceux automatiquement "proposés" par BitDefender.

Ces options permettent une sélection rapide des cibles d'analyses.

- **Disques locaux** - pour analyser les disques locaux.



- **Disques réseaux** - pour analyser tous les lecteurs réseaux.
- **Disques amovibles** - pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes les entrées** - pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

**Note**

Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Planificateur

Double-cliquez sur une tâche sélectionnée puis cliquez sur l'onglet **Planificateur** pour entrer dans cette partie.

The screenshot shows a window titled "Propriétés de Analyse complète du système" with a red header. It has four tabs: "Résumé", "Cible", "Planificateur" (selected), and "Rapports".

Propriétés
Planifié tous les 7 jours, prochaine analyse: 10/2/2006 5:13:02 PM

Planifier

non planifiée
 Une fois
 Périodiquement

Tous les: 7 jours

Date de début: 10/ 2/2006

Heure début: 5:13:02 PM

Buttons: Analyse, OK, Annuler

Planificateur

Vous pouvez voir dans cette rubrique si la tâche est programmée ou non et en modifier ses propriétés.

**Important**

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. L'utilisateur doit pour cela créer une tâche à l'avance.

Quand vous programmez une tâche, vous devez choisir une des options suivantes:

- **Non planifié** - lance la tâche uniquement à la demande de l'utilisateur.
- **Une fois** - lance l'analyse une fois seulement, à un certain moment. Spécifiez la date et l'heure de démarrage dans le champ **Démarrer Date/Heure**.
- Si vous souhaitez que l'analyse soit répétée à intervalle régulier, cochez la case **Périodiquement**.

Si vous voulez que l'analyse se répète à intervalle régulier, cochez la case **Périodiquement** et précisez dans les champs prévus minutes/heures/jours/semaines/mois/années. Vous devez également déterminer la date de début et de fin dans le champ **Date de début/Heure**.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Journaux d'analyse

Double-cliquez sur la tâche sélectionnée puis cliquez sur l'onglet **Journaux d'analyse** pour entrer dans cette rubrique.



Dans cette partie vous visualisez le rapport généré à chaque fois qu'une tâche est exécutée. Chaque fichier dispose d'informations sur son état (ok/infecté), la date et la durée de l'analyse et un récapitulatif.

Deux boutons sont disponibles:

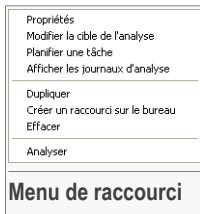
- **Afficher** - ouvre le fichier rapport sélectionné;
- **Effacer** - supprime le fichier rapport sélectionné;

Pour effacer ou visualiser un fichier, vous pouvez également faire un "clic-droit" sur le fichier et choisir l'option correspondante.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

7.2.3. Menu de raccourci

Un menu de raccourci est également disponible pour chaque tâche. Utilisez le "clic-droit" sur la tâche sélectionnée pour y accéder:



Les commandes suivantes sont disponibles dans le menu de raccourci:

- **Propriétés** - ouvre la fenêtre de **Propriétés**, l'onglet **Général** et permet de modifier les propriétés des tâches sélectionnées.
- **Changer la cible d'analyse** - ouvre la fenêtre de **Propriétés**, l'onglet **Chemin d'analyse**, où vous pouvez modifier la cible pour une tâche sélectionnée.
- **Planifier une tâche** - ouvre la fenêtre **Propriétés**, l'onglet **Planificateur**, où vous pouvez planifier la tâche sélectionnée;
- **Voir les journaux d'analyse** - ouvre la fenêtre **Propriétés**, l'onglet **Journaux d'analyse**, où vous pouvez consulter les rapports générés après l'exécution des tâches sélectionnées.
- **Dupliquer** - duplique une tâche sélectionnée.



Note

Très utile lors de la création de nouvelles tâches car cette fonction vous permet aussi d'en modifier les propriétés si besoin.

- **Créer un raccourci sur le bureau** - crée un raccourci sur le bureau vers une tâche sélectionnée.
- **Supprimer** - efface la tâche sélectionnée.



Note

Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

- **Lancer l'analyse** - démarre immédiatement la tâche d'analyse choisie.



Important

Seules les options des onglets **Propriétés** et **Voir les journaux d'analyse** sont disponibles dans la catégorie **Tâches diverses**.

7.2.4. Types d'analyse à la demande

BitDefender permet trois types d'analyse à la demande:



- **Analyse immédiate** - lance une tâche d'analyse depuis les tâches disponibles.
- **Analyse contextuelle** - faites un clic-droit sur un fichier ou répertoire et sélectionnez BitDefender Antivirus v10;
- **Analyse par glisser-déposer** - glissez & déposez un fichier ou un répertoire sur la barre d'analyse d'activité;


Analyse immédiate

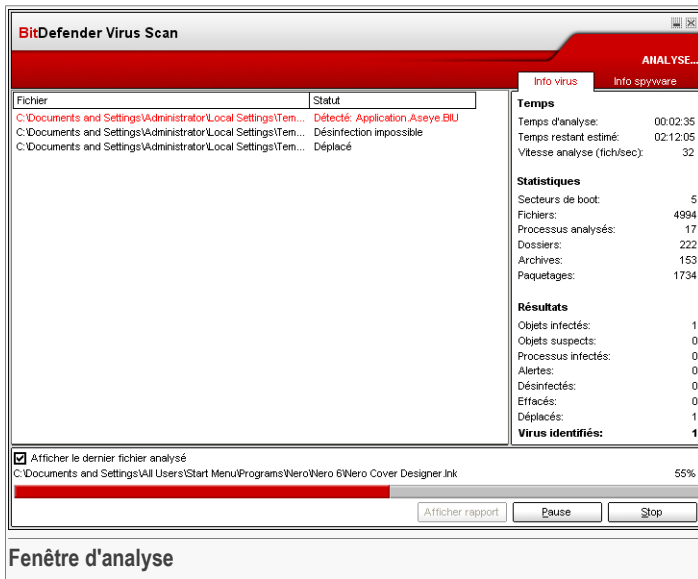
Pour lancer l'analyse d'une partie ou de la totalité de votre ordinateur vous pouvez utiliser les tâches existantes ou créer vos propres tâches. Il y a deux méthodes pour créer des tâches d'analyse:

- **Dupliquer** une règle existante: permet de la renommer et de faire les modifications nécessaires dans la fenêtre **Propriétés** ;
- **Nouvelle tâche**: permet de créer une nouvelle tâche et de **la configurer**.

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes en cours d'utilisation, tout spécialement les clients de messagerie (ex: Outlook, Outlook Express ou Eudora).

Avant de laisser BitDefender analyser votre ordinateur, vous devriez vérifier que BitDefender est à jour de ses signatures de virus, dans la mesure où de nouveaux virus apparaissent chaque jour. Vous pouvez vérifier de quand date la dernière mise à jour en bas du module **Mise à jour**.

Pour commencer l'analyse, sélectionnez la tâche désirée dans la liste et cliquez sur  **Analyser**. Vous pouvez également cliquer sur **Lancer la tâche**. La fenêtre d'analyse apparaîtra:



Fenêtre d'analyse

Une icône apparaîtra dans la **barre d'état système** pendant qu'un processus d'analyse est en cours.

Pendant l'analyse, BitDefender affiche la progression de l'analyse et vous alerte en cas de détection de menaces. Dans la partie droite, vous pouvez voir les statistiques de l'analyse en cours. Selon le choix d'analyse, des informations sur les spywares et/ou les virus sont disponibles. Si les deux sont disponibles, cliquez sur l'onglet correspondant pour en savoir plus sur l'analyse des virus ou des spywares.

Cochez la case **Afficher le dernier fichier analysé** et seules les informations sur les derniers fichiers analysés seront visibles.



Note

L'analyse peut durer un certain temps, suivant la complexité de l'analyse.

Trois boutons sont disponibles:

- **Stop** - une nouvelle fenêtre s'affichera vous permettant de stopper la vérification du système.
- **Pause** - l'analyse s'arrête temporairement – vous pouvez la reprendre en cliquant sur **Continuer**.



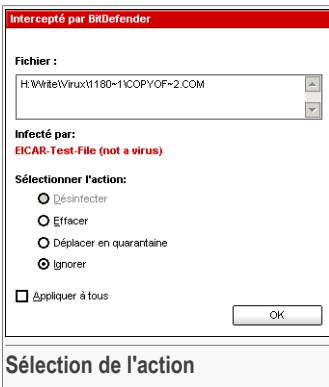
- **Afficher le rapport** - ouvre le rapport d'analyse.

Note



Vous pouvez lancer le menu contextuel en "cliquant droit" sur le raccourci d'une tâche en cours d'utilisation. Les options (**Pause / Continuer**, **Stop** et **Stop et fermer**) sont similaires à celles disponibles dans la fenêtre d'analyse.

Si l'option **Demander à l'utilisateur** est activée dans la fenêtre **Propriétés**, un message d'alerte vous demandera de choisir l'action à mener quand un fichier infecté sera trouvé.



Vous pouvez voir le nom du fichier et le nom du virus.

Vous pouvez sélectionner une des options suivantes:

- **Désinfecter** - désinfecte le fichier infecté;
- **Effacer** - efface le fichier infecté;
- **Déplacer en quarantaine** - déplace le fichier infecté dans la zone de quarantaine;
- **Ignorer** - ignore l'infection. Aucune action ne sera appliquée au fichier infecté.

Si vous analysez un répertoire, et que vous souhaitez que l'action sur les fichiers infectés soit la même pour tous, cochez l'option **Appliquer à tous**.

Note



Si l'option **Désinfecter** n'est pas activée, cela veut dire que le fichier ne peut pas être désinfecté. Le meilleur choix est alors de l'isoler en quarantaine et de nous l'envoyer, ou de le supprimer.

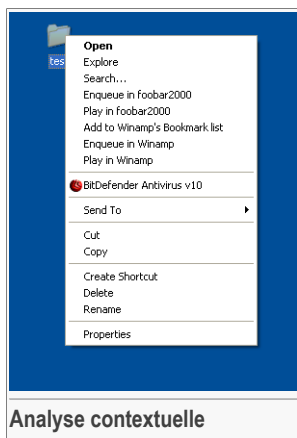
Cliquez sur **OK**.

**Note**

Le fichier rapport est sauvegardé automatiquement dans la rubrique [Rapports](#) de la fenêtre **Propriétés** de la tâche en question.

Analyse contextuelle

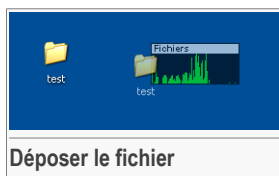
Faites un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus v10**.



Vous pouvez modifier les options d'analyse et voir les fichiers de rapport à partir de la fenêtre [Propriétés](#) de la tâche **Analyse via le menu contextuel**.

Analyse par glisser&déposer

Glissez le fichier ou répertoire que vous voulez analyser et déposez-le sur la **Barre d'analyse de l'activité**, comme sur l'image ci-dessous.



Si un fichier infecté est détecté une **fenêtre d'alerte** apparaîtra vous demandant quelle est l'action à suivre contre le fichier infecté.

Dans les deux cas (analyse contextuelle et analyse par glisser & déposer), la **fenêtre d'analyse** apparaîtra.

7.2.5. Recherche de Rootkits

BitDefender a résolu la dernière menace de sécurité en introduisant un détecteur de rootkits à ses moteurs antivirus et antispyware. BitDefender est désormais capable de détecter les rootkits en cherchant les fichiers, répertoires ou processus camouflés. De plus, il peut protéger votre système en renommant les codes malveillants qui utilisent des rootkits.

Afin de rechercher des rootkits sur votre ordinateur, lancez la tâche **Analyse contre les Rootkits** task. Une fenêtre d'analyse apparaîtra.



Important

Il est fortement recommandé lorsque vous recherchez des rootkits de paramétrer BitDefender pour qu'il ne prenne pas d'action sur les fichiers cachés.

A la fin de l'analyse, vous pouvez voir les résultats. Si des fichiers cachés ont été détectés, contrôlez les attentivement: la présence de fichiers cachés pourrait indiquer une possible intrusion.

Si vous êtes sûr que les fichiers détectés proviennent de codes malveillants, nous vous recommandons d'activer l'action **Renommer les fichiers** et de relancer la tâche **Recherche de Rootkits**. Ainsi, les fichiers cachés seront bloqués.

**Avertissement**

TOUS LES OBJETS CACHES NE SONT PAS DES MALWARES! Avant de renommer des fichiers cachés, assurez vous qu'ils n'appartiennent pas à une application valide ou au système. Renommer de tels fichiers pourrait rendre votre système inutilisable.

**Important**

Si votre système a été hacké, il n'y a qu'une seule voie sûre pour être totalement protégée de cette intrusion: réinstaller le système.

7.3. Quarantaine

Pour accéder à cette section cliquez sur l'onglet **Quarantaine** dans le module **Antivirus**.

BitDefender Antivirus v10

Résident Analyse **Quarantaine**

Dossier de quarantaine

Taille limite de la quarantaine: aucun (77 KB) Paramètres

Plus de détails

Nom du fichier	Nom	Peut être infecté par	Envoyé
eicar.com	EICAR-Test-File (not a...	Non	Non
WinRAR_v34_buildAll_...	Application.Aseye.BIU	Non	Non

Envoyer Restaurer

Quarantaine

La Quarantaine conserve les fichiers suspects pour analyse. Une fois en Quarantaine, les fichiers ne peuvent pas être exécutés ou lus. Par défaut, les fichiers suspects sont soumis pour analyse aux BitDefender Labs. Cependant, vous pouvez choisir de ne pas soumettre les fichiers à l'analyse. Pour copier un fichier suspect vers la Quarantaine, cliquez sur le bouton "Ajouter" ou glissez/déposez simplement le fichier dans la liste de Quarantaine.

Plus d'aide

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender.


La rubrique qui permet d'administrer ces fichiers isolés est la **Quarantaine**. Ce module a été conçu avec une fonction d'envoi automatique des fichiers infectés aux BitDefender Labs.




Comme vous le constaterez, la rubrique **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission. Si vous voulez voir plus d'informations à propos des fichiers en quarantaine, cliquez sur **Plus d'infos**.

**Note**

Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.


Cliquez sur le bouton  **Ajouter** pour ajouter un fichier suspect à la zone de quarantaine. Une fenêtre s'ouvrira et vous pourrez sélectionner le fichier depuis son emplacement sur le disque dur pour le copier dans la zone de quarantaine. Pour pouvoir déplacer un fichier dans la zone de quarantaine, il faut activer l'option **Effacer de l'emplacement d'origine**. Une méthode plus rapide consiste à glisser/déposer le fichier suspect dans la liste de quarantaine.

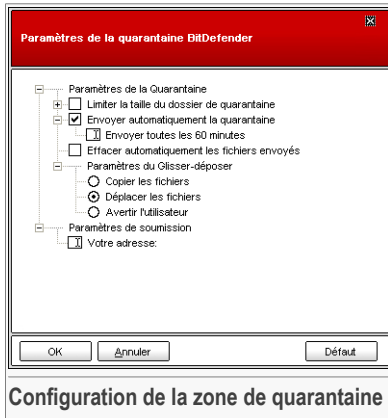
Pour effacer un fichier sélectionné dans la zone de quarantaine, cliquez sur le bouton  **Déplacer**. Si vous voulez restaurer un fichier sélectionné dans son emplacement d'origine, cliquez sur **Restaurer**.

Vous pouvez envoyer un fichier depuis la quarantaine aux BitDefender Labs en cliquant sur **Envoyer**.

**Important**

Vous devez spécifier quelques informations pour pouvoir les soumettre. Pour cela, cliquez sur **Paramétrages** et complétez les champs de la partie **Configuration de la proposition** comme décrit ci-dessous.

Cliquez sur  **Paramètres** pour atteindre les options avancées de la zone de quarantaine. La fenêtre suivante apparaîtra:



Configuration de la zone de quarantaine

Les options de quarantaine sont groupées en deux catégories:

- **Configuration de la Quarantaine**
- **Configuration de la proposition**



Note

Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Configuration de la Quarantaine

- **Limiter la taille du dossier de quarantaine** - maintient sous contrôle la taille de la quarantaine. Cette option est activée par défaut et sa taille est de 12000kbs. Si vous voulez changer cette valeur, vous pouvez en introduire une autre dans le champ prévu à cet effet. Si vous choisissez l'option **Effacer automatiquement les anciens fichiers** , les fichiers les plus anciens seront automatiquement supprimés du fichier de quarantaine pour libérer de la place pour les nouveaux fichiers.
- **Envoyer automatiquement la quarantaine** - envoie automatiquement les fichiers en quarantaine aux BitDefender Labs pour une analyse plus approfondie. Vous pouvez paramétrer le délai entre deux envois consécutifs dans le champ **Envoyer toutes les x minutes** .
- **Effacer automatiquement les fichiers envoyés** - supprime automatiquement les fichiers en quarantaine après les avoir envoyés aux BitDefender Labs pour analyse.



- **Configuration Glisser & Déposer** - si vous utilisez la méthode du glisser & déposer pour ajouter de nouveaux fichiers à la quarantaine, vous pouvez ici spécifier l'action: copier, déplacer ou demander à l'utilisateur.

Configuration de la proposition

- **Votre adresse** - entrez votre adresse e-mail dans le cas où vous souhaitez recevoir une réponse de nos experts au sujet des fichiers suspects soumis pour analyse.

Cliquez sur **OK** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.



8. Module Antispyware

La section **Antispyware** de ce manuel utilisateur contient les rubriques suivantes:

- Etat de l'antispyware
- Paramètres avancés - Contrôle de la vie privée
- Paramètres avancés - Contrôle de la base de registres
- Paramètres avancés - Contrôle des numéroteurs
- Paramètres avancés - Contrôle des cookies
- Paramètres avancés - Contrôle des scripts
- Information Système

Note



Pour plus d'informations sur le module **Antispyware** consultez la description de « *Module Antispyware* » (p. 27).

8.1. Etat de l'Antispyware

Pour accéder à cette section, cliquez sur l'onglet **Etat** dans le module **Antispyware**.



- **Contrôle des cookies** - demande votre autorisation quand un nouveau site Internet tente de déposer un cookie sur votre ordinateur.
- **Contrôle des scripts** - demande votre autorisation quand un site Internet tente d'activer un script ou tout autre contenu actif.

Pour configurer les paramètres de ces contrôles, cliquez sur  **Paramètres avancés**.

8.1.1. Niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection:

Niveau de protection	Description
Tolérant	Seul le Contrôle de la base de registre est activé.
Défaut	Le Contrôle de la base de registre et le Contrôle des numéroteurs sont activés.
Agressif	Le Contrôle de la base de registre , le Contrôle des numéroteurs et le Protection vie privée sont activés.

Vous pouvez personnaliser le niveau de protection en cliquant sur **Niveau de personnalisation**. Sélectionnez dans la fenêtre apparue les contrôles Antispyware que vous désirez activer et cliquez sur **OK**.

Cliquez sur **Niveau par défaut** pour placer le curseur sur le niveau par défaut.

8.2. Protection de la vie privée - Paramètres avancés.

Pour accéder à cette section cliquez sur le bouton  **Paramètres avancés** depuis le module **Antispyware**, dans la rubrique **Etat**.



Etape 1 sur 3 - Définition des types de règles et de données

Assistant de BitDefender Etape 1/3

Nom de la règle:

Type de règle:

Données de la règle:

Toutes les données que vous entrez sont cryptées. Pour encore plus de sécurité, n'entrez pas le champ complet des données que vous voulez protéger (ex: 12 des 16 chiffres de votre CB)

< Précédent Suivant > Annuler

Définition des types de règles et de données

Entrez le nom de la règle dans le champ correspondant.

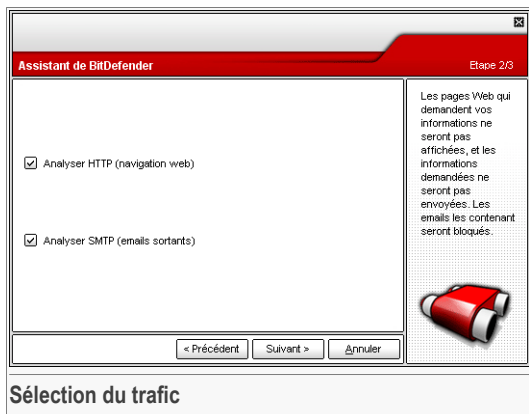
Vous devez définir les paramètres suivants:

- **Type de règle** - détermine le type de règle (adresse, nom, carte de crédit, code PIN, etc.)
- **Données de la règle** - Renseigner les données de la règle.

Toutes les données que vous enregistrez sont cryptées. Pour plus de sécurité, n'entrez pas toutes les données que vous souhaitez protéger.

Cliquez sur **Suivant**.

Etape 2 sur 3 - Sélection du trafic



Sélectionnez le type de trafic que BitDefender doit analyser. Les options suivantes sont disponibles:

- **Analyse HTTP** - Analyse le flux HTTP (web) et bloque les données qui sont prévues dans la règle de gestion des données.
- **Analyse SMTP** - Analyse le flux SMTP (mail) et bloque les emails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Cliquez sur **Suivant**.



Etape 3 sur 3 – Description de la règle

Assistant de BitDefender Etape 3/3

Description de la règle

Ma carte bancaire

Entrez une description pour cette règle. Cette description devrait vous permettre -à vous et à d'autres administrateurs- d'identifier facilement les informations qui ont été bloquées.


< Précédent Terminer Annuler


Description de la règle

Entrez une description courte de la règle dans le champ correspondant.

Cliquez sur **Terminer**.

Vous pouvez voir les règles existantes dans le tableau correspondant.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton  **Effacer**. Pour désactiver temporairement une règle sans pour autant la supprimer, décochez la case correspondante.

Pour éditer une règle, sélectionnez-la et cliquez sur le bouton  **Editer** ou double-cliquez sur la règle. La fenêtre suivante apparaîtra:

Nom de la règle:

Type de règle:

Données:

Analyse Http (web)

Analyse Smtip (emails)


Description de la règle

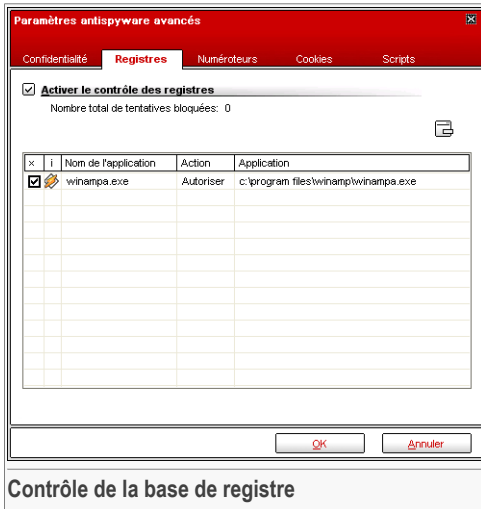
Ma carte bancaire

Dans cette rubrique, vous pouvez modifier le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez sur **OK** pour enregistrer les modifications.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

8.3. Contrôle de la base de registre -Paramètres avancés

Pour accéder à cette partie, entrez dans la fenêtre **Paramètres antispyware avancés** (allez sur le module **antispyware**, section **Etat** et cliquez sur  **Paramètres avancés**) et cliquez sur l'onglet **Registre**.

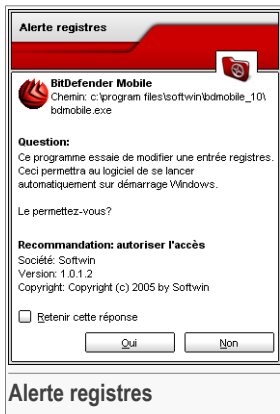


Contrôle de la base de registre

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres**. C'est l'endroit où Windows conserve ses paramètres, programmes installés, informations sur l'utilisateur et autres.

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cette fonction est souvent détournée par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle des registres** surveille les registres Windows – cette fonction est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.




Vous pouvez refuser cette modification en cliquant sur **Non** ou l'autoriser en cliquant sur **Oui**.

Si vous souhaitez que BitDefender se souvienne de votre réponse, cochez la case: **Retenir cette réponse**.



Note

Vos réponses serviront de base pour établir la liste de règles.

Pour supprimer une entrée dans les registres, sélectionnez-la et cliquez sur  **Supprimer**. Pour désactiver temporairement une entrée sans la supprimer, décochez la case correspondante.




Note

BitDefender vous alertera lors de l'installation de nouveaux logiciels nécessitant d'être lancés après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

Cliquez sur **OK** pour fermer la fenêtre.

8.4. Contrôle des numéroteurs -Paramètres avancés


Pour accéder à cette partie, entrez dans la fenêtre **Paramètres antispyware avancés** (aller au module **antispyware**, partie **Etat** et cliquez sur  **Paramètres avancés**) et cliquez sur l'onglet **Dialer**.


Chaque règle mémorisée peut être éditée dans la section **Numéroteurs** pour y ajouter des modifications ou améliorations.



Important

Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez la et cliquez sur le bouton  **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faites la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton  **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

8.4.1. Assistant de configuration

L'assistant de configuration est composé de 2 étapes.

Etape 1 sur 2 - Sélection de l'application et de l'action

Sélectionnez l'Application et l'Action Etape 1/2

Sélectionnez l'application

Tous
 Sélectionnez l'application

Sélectionnez l'action

Autoriser
 Interdire

Cliquez sur 'Tous' si vous désirez que cette règle s'applique à tous les programmes. Si vous désirez choisir une application spécifique cliquez sur [Parcourir]. Puis choisissez la règle pour cette action: Permettre ou Interdire.

Sélection de l'application et de l'action

Vous pouvez définir les paramètres:

- **Application** - sélectionnez l'application pour la règle. Vous pouvez choisir une application seule (cliquez **Choix du fichier**, puis **Parcourir** et sélectionner l'application) ou choisir toutes les applications (En cliquant sur **Tous**).



- **Action** - sélectionnez l'action liée à la règle.

Action	Description
Autoriser	L'action sera autorisée.
Interdire	L'action sera refusée.

Cliquez sur **Suivant**.

Etape 2 sur 2 - Sélection des numéros de téléphone

Sélectionnez les numéros de téléphone
Etape 2/2

Sélectionnez les numéros de téléphone

Tous
 Numéros de téléphone spécifiés

Cochez 'Tous' si vous voulez que cette règle s'applique à tous les numéros de téléphone. Vous pouvez aussi créer une règle qui permette à certains applications de composer seulement certains numéros (tels que celui de votre accès Internet).

Sélection des numéros de téléphone

BitDefender vous alertera lors de l'installation de nouveaux logiciels nécessitant d'être lancés après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.



Note

Vous pouvez utiliser des règles de redondance dans votre liste de numéros de téléphone; ex: 0825* bloquera tous les numéros de téléphone commençant par 0825.

Cochez **Tous** si vous voulez appliquer la règle à tous les numéros de téléphone. Si vous voulez supprimer un numéro, sélectionnez-le et cliquez sur **Supprimer**.




Note

Vous pouvez également créer une règle qui permet à un programme particulier de numéroté seulement certains numéros précis (comme par exemple votre numéro de connexion internet ou votre service de fax).

Cliquez sur **Terminer**.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

8.5. Contrôle des cookies - Paramètres avancés

Pour accéder à cette partie, entrez dans le module **Paramètres antispyware avancés** (aller au module **antispyware**, dans la rubrique **Etat** et cliquez sur  **Paramètres avancés**) et cliquez sur l'onglet **Cookie**.

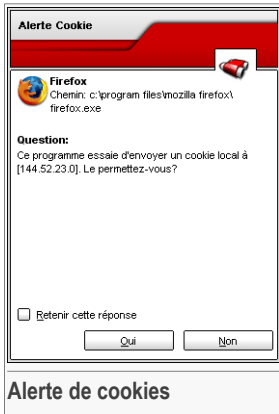


Les **Cookies** sont très communs sur Internet. Ce sont des petits fichiers stockés sur l'ordinateur. Les sites web les créent afin de connaître certaines informations concernant vos habitudes de surf.

Les Cookies sont généralement là pour vous faciliter la navigation. Par exemple, ils peuvent permettre à un site web de mémoriser votre nom et vos préférences, pour que vous n'ayez pas à les renseigner à nouveau.

Mais les cookies peuvent aussi être utilisés pour compromettre la confidentialité de vos données, en surveillant vos préférences de navigation.

C'est là que la fonction **Contrôle des cookies** est très utile. Si elle est activée, la fonction **Contrôle des cookies** vous demandera une validation à chaque fois qu'un nouveau site Web tentera de déposer un cookie.



Vous pouvez voir le nom de l'application qui tente d'envoyer un fichier de type cookie.

Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles.

Cette fonction vous aide à choisir à quels sites faire confiance et quels sites vous préférez éviter.



Note

A cause du grand nombre de cookies utilisés sur Internet, le module **Contrôle des Cookies** peut être légèrement gênant au départ. Il vous posera beaucoup de questions concernant l'acceptation de nouveaux cookies sur votre ordinateur. Au fur et à mesure que vous ajouterez vos sites Web favoris à la liste des règles, votre navigation redeviendra aussi simple qu'auparavant.

Vous pouvez éditer chaque règle mémorisée dans la section **Cookie** pour y apporter des modifications.



Important

Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez la et cliquez sur le bouton **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faites la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

8.5.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 - Selection de l'Adresse, de l'Action et de la Direction

Sélectionner l'Adresse, l'Action et la Direction Etape 1/1

Entrez le domaine

Tous
 Entrez le domaine

Sélectionnez l'action

Autoriser
 Interdire

Sélectionnez la direction

Sortant
 Entrant
 Les deux

Choisir les sites pour lesquels autoriser/refuser les cookies. Ils enregistrent vos habitudes de navigation et des informations. Note: certains sites ne fonctionnent pas sans cookies. Vous pouvez accepter les cookies mais ne pas les renvoyer.

< Précédent Terminer Annuler

Selection de l'Adresse, de l'Action et de la Direction

Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le nom de domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action liée à la règle.

Action	Description
Autoriser	Les cookies de ce domaine seront autorisés.
Interdire	Les cookies de ce domaine ne seront pas autorisés.

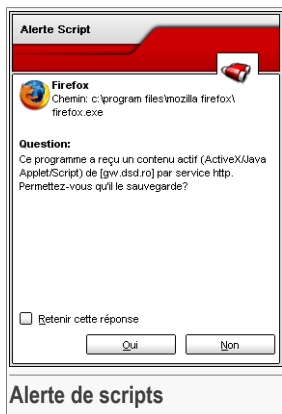
- **Direction** - sélectionne la direction du trafic.

Type	Description
Sortant	La règle s'applique seulement aux envois d'informations vers les serveurs auxquels vous accédez.
Entrant	La règle s'applique seulement aux envois d'informations en provenance des serveurs auxquels vous accédez.

vous êtes en ligne. Il est recommandé de n'accepter les contenus actifs que sur les sites que vous connaissez et auxquels vous faites parfaitement confiance.

BitDefender vous laisse le choix d'exécuter ou de bloquer ces éléments.

Avec le **Contrôle de scripts** vous pourrez définir les sites web auxquels vous faites confiance ou non. BitDefender vous demandera une validation dès qu'un site web essaiera d'activer un script ou tout type de contenu actif :



Vous pouvez voir le nom de la ressource.


Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles. Vous ne serez dès lors plus interrogé lorsque ce même site essaiera de vous envoyer un contenu actif.

Chaque règle mémorisée peut être éditée dans la partie **Scripts** pour y apporter des modifications.



Important

Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez la et cliquez sur le bouton  **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faites la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton  **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

8.6.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.



Etape 1 sur 1 - Sélection des adresses de domaine et Action

Sélectionnez l'Adresse et l'Action
Etape 1/1

Entrez le domaine

Sélectionnez l'action

Autoriser

Interdire

Choisir les domaines spécifiques pour lesquels bloquer/ permettre les scripts. Il est recommandé de bloquer ceux des domaines auxquels vous ne faites pas confiance.

Note: certains sites ne fonctionneront pas correctement sans scripts.

< Précédent
Terminer
Annuler

Sélection des adresses de domaine et Action

Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le nom de domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action liée à la règle.

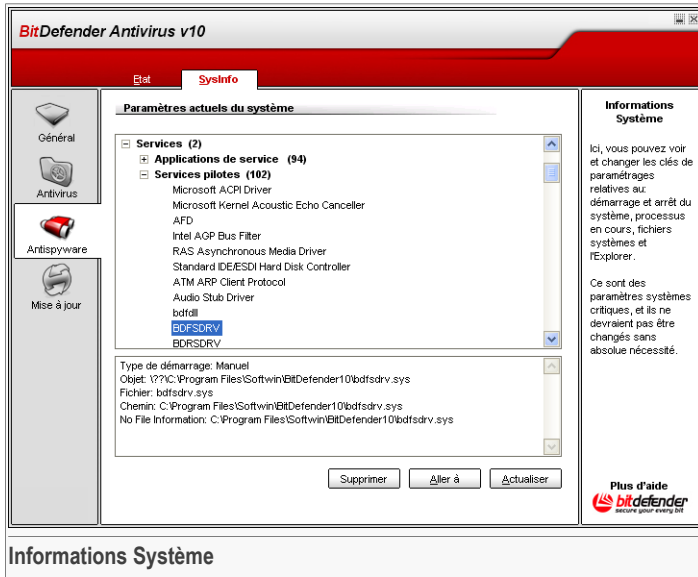
Action	Description
Autoriser	Les scripts de ce domaine seront exécutés.
Interdire	Les scripts de ce domaine ne seront pas exécutés.

Cliquez sur **Terminer**.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

8.7. Informations Système

Pour accéder à cette section, cliquez sur l'onglet **Informations Système** dans le module **Antispyware**.



Vous pouvez voir et modifier certaines informations clés du module antispyware.

La liste contient tous les éléments chargés au démarrage du système ainsi que les ceux chargés par les différentes applications.

Trois boutons sont disponibles:

- **Retirer** - supprime les objets sélectionnés.
- **Aller à** - ouvre une fenêtre dans laquelle l'objet a été placé (la **Base de Registres** par exemple).
- **Actualiser** - re-ouvre la rubrique **Informations système**.



9. Module de Mise à jour

Le chapitre **Mise à jour** de ce manuel d'utilisation contient les thèmes suivants:

- Mise à jour automatique
- Mise à jour manuelle
- Paramètres de mise à jour



Note

Pour plus de détails concernant la partie **Mise à jour** consultez la description « *Module de Mise à jour* » (p. 28).

9.1. Mise à jour automatique

Pour accéder à cette section, cliquez sur l'onglet **Mise à Jour** dans le module **Mise à Jour**.

BitDefender Antivirus v10

Mise à jour Paramètres

Mise à jour automatique activée

Dernière recherche	10/2/2006 4:15:23 PM	
Dernière	10/2/2006 4:15:34 PM	Mise à jour

Propriétés des signatures antivirales

Signatures de virus	505637	Liste des Virus
Version du moteur	7.09170	

Etat du téléchargement

Fichier:	0 %	0 ko
Mise à jour totale	0 %	0 ko

Mise à jour BitDefender

Cliquez sur 'Mise à jour' pour que BitDefender recherche maintenant une nouvelle version.

Les produits BitDefender sont capables de s'auto-réparer, si nécessaire, en téléchargeant les fichiers manquants ou endommagés, depuis les serveurs BitDefender. Il est recommandé de laisser l'option 'Mise à jour automatique' activée.

Plus d'aide
 bitdefender
 BitDefender est une marque de BitDefender Ltd.

Mise à jour automatique


Dans cette section vous pouvez lancer des mises à jour et consulter les informations relatives à ces mises à jour.

**Important**

Pour être protégé contre les dernières menaces, il est impératif de laisser la **mise à jour automatique** active.

Si vous êtes connecté à Internet par câble ou xDSL, BitDefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les heures.

Si une mise à jour est disponible, elle sera installée automatiquement ou après validation de votre part, en fonction des options choisies dans la rubrique **Paramètres de mise à jour automatique**.

La mise à jour automatique peut aussi être faite quand vous le souhaitez en cliquant sur  **Mettre à jour**. Cette mise à jour correspond à une **Mise à jour a la demande**.



Le module **Mise à jour** se connectera au serveur BitDefender pour vérifier la disponibilité d'une mise à jour. Selon les options choisies dans la partie **Paramètres de la mise à jour manuelle** une confirmation vous sera demandée ou non pour l'installer.

**Important**

Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible pour bénéficier de la meilleure protection disponible.

**Note**

Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.

Vous pouvez regarder les détails des signatures de malware de BitDefender en cliquant sur  **Afficher la liste des virus**. Un fichier HTML contenant toutes les signatures disponibles sera créé. Cliquez une nouvelle fois sur  **Afficher la liste des virus** pour voir cette liste. Vous pouvez rechercher une signature de malware spécifique en parcourant la base de données ou en cliquant sur **Liste des virus BitDefender** pour être dirigé vers la base de données en ligne BitDefender.

9.2. Mise à jour manuelle

Cette méthode permet d'installer les dernières signatures de virus. Pour installer les dernières mises à jour du produit, utilisez la **mise à jour automatique**.

**Important**

Utilisez la mise à jour manuelle quand la mise à jour automatique ne peut pas être effectuée ou quand l'ordinateur n'est pas connecté en permanence à Internet.

Il y a 2 méthodes pour effectuer une mise à jour manuelle:



- En utilisant le fichier `weekly.exe`;
- En utilisant les archives `zip`.

9.2.1. Mise à jour manuelle avec `weekly.exe`

Le fichier de mise à jour `weekly.exe` est mis à disposition chaque vendredi, il inclut toutes les signatures de virus ainsi que les derniers moteurs antivirus disponibles.

Pour mettre à jour BitDefender en utilisant le fichier `weekly.exe`, merci de suivre les étapes suivantes:

1. Téléchargez [weekly.exe](#) et sauvegardez-le sur votre disque dur.
2. Localisez le fichier d'installation et double-cliquez dessus pour lancer l'assistant de mise à jour.
3. Cliquez sur **Suivant**.
4. Cochez **J'accepte les termes de l'accord de licence** puis cliquez sur **Suivant**.
5. Cliquez sur **Installer**.
6. Cliquez sur **Terminer**.

9.2.2. Mise à jour manuelle avec des archives `zip`

Il y a deux archives sur le serveur des mises à jour, contenant les mises à jour du moteur antivirus et les définitions de virus: `cumulative.zip` et `daily.zip`.

- `cumulative.zip` est disponible chaque semaine, il inclut toutes les mises à jour de définitions des virus et du dernier moteur antivirus disponible en date.
- `daily.zip` est lancé chaque jour et il inclut toutes les mises à jour de définitions de virus et le moteur antivirus inclut dans la dernière version du fichier "cumulative".

Bitdefender utilise une architecture basée sur les services de Windows. Pour cette raison la procédure pour mettre à jour les définitions de virus peut être différente pour chaque système d'exploitation:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Étapes à suivre:

1. **Téléchargez la mise à jour appropriée.** Si vous faites une requête un lundi, merci de télécharger [cumulative.zip](#) et de le sauvegarder quelque part sur votre disque dur. Sinon, merci de télécharger le fichier [daily.zip](#) et de le sauvegarder sur votre disque dur. Si c'est la première fois que vous mettez à jour l'antivirus en utilisant la mise à jour manuelle, merci de télécharger les deux fichiers.
2. **Arrêter la protection BitDefender.**
 - **Sortez de la console de gestion.** Faites un Clic-droit sur l'icône Bitdefender de la **barre d'état système** et choisissez **Quitter**.
 - **Ouvrez les services.** Cliquez sur **Démarrer**, puis sur **Panneau de configuration**, double-cliquez sur **Outils d'administration** et cliquez sur **Services**.
 - **Arrêtez BitDefender Virus Shield service.** Sélectionnez le service **BitDefender Virus Shield** dans la liste et cliquez sur **Arrêter**.
 - **Arrêtez BitDefender Scan Server service.** Sélectionnez le service **BitDefender Scan Server** dans la liste et cliquez sur **Arrêter**.
3. **Décompressez le contenu de l'archive.** Commencez avec le fichier `cumulative.zip` quand les deux fichiers sont disponibles. Décompressez son contenu dans le dossier `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` et acceptez la réécriture des fichiers existants.
4. **Redémarrer BitDefender.**
 - **Démarrez le service BitDefender Scan Server.** Sélectionnez le service **BitDefender Scan Server** dans la liste et cliquez sur **Démarrer**.
 - **Démarrez le service BitDefender Virus Shield.** Sélectionnez le service **BitDefender Virus Shield** dans la liste et cliquez sur **Démarrer**.
 - **Ouvrez La console de gestion BitDefender.**

Windows 98, Windows Millennium

Étapes à suivre:

1. **Téléchargez la mise à jour appropriée.** Si vous faites une requête un lundi, merci de télécharger [cumulative.zip](#) et de le sauvegarder quelque part sur votre disque dur. Sinon, merci de télécharger le fichier [daily.zip](#) et de le sauvegarder sur votre disque dur. Si c'est la première fois que vous mettez à jour l'antivirus en utilisant la mise à jour manuelle, merci de télécharger les deux fichiers.
2. **Décompressez le contenu de l'archive.** Commencez avec le fichier `cumulative.zip` quand les deux fichiers sont disponibles. Décompressez son

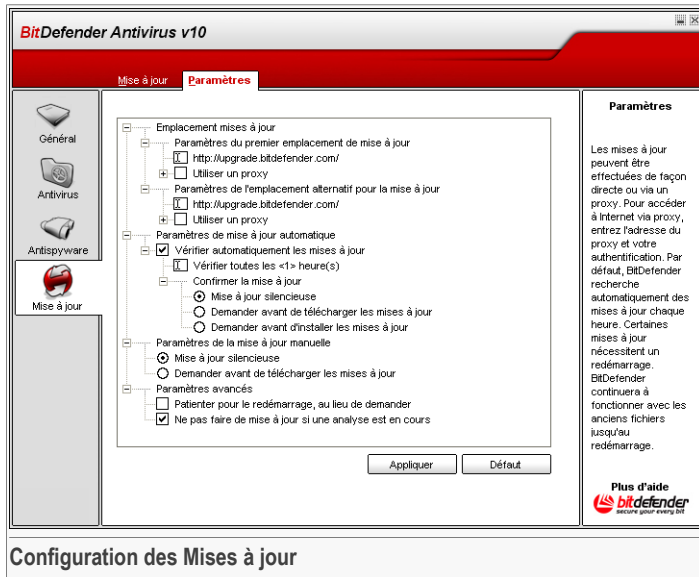


contenu dans le dossier C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\ et acceptez la réécriture des fichiers existants.

3. Redémarrer votre système.

9.3. Configuration des Mises à jour

Pour accéder à cette section cliquez sur l'onglet **Mise à Jour** dans le module **Paramètres**.



Configuration des Mises à jour

Les mises à jour peuvent être réalisées depuis un réseau local, directement depuis Internet, ou au travers d'un serveur proxy.

La fenêtre de paramètres des mises à jour contient 4 catégories d'options (**Emplacement des mises à jour**, **Options de mises à jour automatiques**, **Options de mises à jour manuelles** et **Options de l'interface**) organisées en arborescence comme dans l'explorateur de Windows.



Note

Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

9.3.1. Paramètres du choix de l'emplacement des mises à jour

Pour des mises à jour plus rapides et plus fiables, vous pouvez établir deux emplacements pour les mises à jour: un **Premier emplacement de mise à jour** et un **emplacement alternatif** . Pour les deux, vous devez paramétrer les options suivantes:

- **Emplacement des mises à jour** - Si vous êtes connectés à un réseau local sur lequel sont placées les signatures de virus de BitDefender, c'est dans cette partie que vous pouvez changer l'emplacement des mises à jour. Par défaut, l'emplacement est le suivant: <http://upgrade.bitdefender.com>.
- **Utilisez proxy** - Dans le cas où la société utilise un serveur proxy, cochez cette option. Les paramètres suivants doivent être spécifiés:
 - **Serveur proxy** - Entrez l'adresse IP ou le nom du serveur proxy et le port que BitDefender doit utiliser pour se connecter au serveur proxy.

**Important**

Syntaxe: `name:port` ou `ip:port`.

- **Utilisateur** - Entrez ici un nom d'utilisateur reconnu par le proxy.

**Important**

Syntaxe: `domain\user`.

- **Mot de passe** - tapez ici un mot de passe valide pour l'utilisateur choisi auparavant.

9.3.2. Options de mise à jour automatique

- **Vérifier automatiquement les mises à jour** - BitDefender contrôle automatiquement nos serveurs pour vérifier la disponibilité de mises à jour.
- **Vérifier toutes les x heures** - Paramétrez la fréquence de vérification des mises à jour de BitDefender. L'intervalle de temps par défaut est de 1 heure.
- **Mise à jour silencieuse** - BitDefender télécharge et installe automatiquement la mise à jour de manière transparente pour l'utilisateur.
- **Demander avant le téléchargement** - chaque fois qu'une mise à jour sera disponible, une validation sera demandée avant d'en autoriser le téléchargement.



- **Demander avant l'installation**- chaque fois qu'une mise à jour a été téléchargée, une validation vous sera demandée avant d'en autoriser l'installation.

**Important**

Si vous choisissez **Demandez avant de télécharger** ou **Demandez avant d'installer** et si vous fermez et [quittez](#) la console de gestion, la mise à jour automatique n'aura pas lieu.

9.3.3. Paramètres de la mise à jour manuelle

- **Mise à jour silencieuse** - BitDefender télécharge et installe automatiquement la mise à jour.
- **Demander avant le téléchargement** - chaque fois qu'une mise à jour est disponible, une validation vous sera demandée avant d'en autoriser le téléchargement.

**Important**

Si vous choisissez **Demandez avant de télécharger** et si vous fermez et [quittez](#) la console de gestion, la mise à jour automatique ne sera pas effectuée.

9.3.4. Paramètres avancés

- **Patiencez pour redémarrer, au lieu de le demander à l'utilisateur** - Si une mise à jour nécessite un redémarrage, le produit continuera à utiliser les anciens fichiers jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti qu'il doit redémarrer et ne sera donc pas perturbé dans son travail par la mise à jour de BitDefender.
- **Ne pas faire la mise à jour si l'analyse est en cours** - BitDefender ne se mettra pas à jour si une analyse est en cours afin de ne pas la perturber.

**Note**

Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.



Utilisation optimale



10. Utilisation optimale

La partie **Utilisation optimale** de ce manuel d'utilisation contient les sujets suivants:

- Comment protéger votre ordinateur contre les menaces de malwares
- Comment configurer une tâche d'analyse

10.1. Comment protéger votre ordinateur contre les malwares



Suivez ces étapes pour protéger votre ordinateur contre les virus, les spywares et les autres malwares.

1. **Utilisez l'assistant de démarrage dans sa totalité.** Pendant la procédure d'installation, la fenêtre de l'**Assistant** apparaîtra. Il vous aidera à vous enregistrer et à créer un compte pour pouvoir bénéficier du support technique gratuit BitDefender. Il vous aidera également à vérifier paramétrer BitDefender pour lancer d'importantes tâches de sécurité.



Important

Si vous avez le CD de secours BitDefender, lancez l'analyse de votre système avant d'installer BitDefender afin de vous assurer qu'aucun code malveillant ne soit déjà installé dans votre système.

2. **Mise à jour de BitDefender.** Si vous n'avez pas terminé l'assistant de démarrage pendant la procédure d'installation, lancez une mise à jour à la demande (aller dans la rubrique **Mise à jour**, puis dans la partie **Mise à jour**, et cliquez sur  **Mettre à jour**).
3. **Lancer une analyse complète de votre système.** Allez dans la rubrique **antivirus**, dans la partie **Résident** et cliquez sur  **Analyser**.



Note

Vous pouvez également lancer une analyse complète du système depuis la partie **Analyse**. Sélectionnez la tâche **Analyse complète du système** et cliquez sur **Lancer la tâche**.

4. **Prévenir les infections.** Dans la partie **Protection**, laissez la **protection en temps réel** active pour être protégé contre les virus, les spywares et les autres malwares.

Configurez le **niveau de protection** qui correspond le mieux à vos besoins. Vous pouvez le **personnaliser** à volonté en cliquant sur **Niveau Personnalisé**.

**Important**

Programmez une analyse de votre système au moins une fois par semaine en **planifiant** une tâche **Analyse complète du système** depuis la partie **Analyse**.

5. **Maintenir BitDefender à jour.** Dans la rubrique **Mise à jour**, partie **Mise à jour**, laissez la fonction **Mise à jour Automatique** active pour protéger votre ordinateur contre les nouvelles menaces.
6. **Programmer une analyse complète du système.** Allez dans la rubrique **Analyse** et programmez BitDefender pour **analyser votre système** au moins une fois par mois en **programmant** la tâche d'**Analyse complète du système**.

10.2. Comment configurer une tâche d'analyse

Suivez ces étapes pour créer et configurer une tâche d'analyse:

1. **Création d'une nouvelle tâche.** Allez dans la rubrique **Analyse** et cliquez sur **Nouvelle tâche**. La fenêtre de **propriétés** apparaîtra.

**Note**

Vous pouvez également créer une nouvelle tâche en **dupliquant** une tâche existante. Pour cela, faites un clic-droit sur une tâche donnée et choisissez **Dupliquer** dans les raccourcis. Double-cliquez sur la tâche dupliquée pour ouvrir la fenêtre de **Propriétés**.

2. **Choisir le niveau d'agressivité de l'analyse.** Allez dans la rubrique **Général** pour définir le **niveau d'analyse**. Si vous le souhaitez vous pouvez **personnaliser** les paramètres d'analyse en cliquant sur **Personnaliser**.
3. **Sélectionnez la cible de l'analyse.** Allez dans la rubrique **chemin d'analyse** et choisissez les **éléments que vous voulez analyser**
4. **Programmeur de tâche.** Si vous souhaitez lancer une tâche d'analyse complexe vous pouvez la programmer pour qu'elle s'exécute plus tard, quand votre ordinateur ne sera pas trop sollicité. Cela aidera BitDefender à réaliser une analyse précise de votre système. Allez dans la rubrique **Programmeur** pour **programmer la tâche**.



CD de secours BitDefender

BitDefender Antivirus v10 est fourni sur un CD bootable (CD de secours BitDefender basé sur LinuxDefender), capable d'analyser et désinfecter tous les disques durs existants avant que votre système d'exploitation ne démarre.

Il est recommandé d'utiliser le CD de secours BitDefender à chaque fois que votre système d'exploitation ne fonctionne pas correctement à cause d'une infection virale. Ceci se produit généralement quand vous n'utilisez pas un produit antivirus.

La mise à jour de la base de signatures de virus se fait automatiquement, sans intervention de l'utilisateur, à chaque fois que vous lancez le CD de secours BitDefender.

Le Live CD Linux Defender de BitDefender est basé sur une distribution Linux Knoppix. Cette solution permet à l'utilisateur de démarrer l'ordinateur directement depuis le CD dans un environnement graphique intuitif, de se connecter à Internet pour télécharger la dernière base virale à jour, puis de lancer une analyse et une désinfection de son disque dur, y compris si il est formaté en NTFS.



11. Vue d'ensemble

Fonctions principales

- Protection des messageries instantanées (Antivirus & Antispam)
- Solutions antivirusales pour votre disque dur.
- Support du NTFS en écriture
- Désinfection des fichiers infectés dans les partitions Windows XP.

11.1. Qu'est que Knoppix ?

Citation de <http://knopper.net/knoppix>:

« KNOPPIX is a bootable CD with a collection of GNU/Linux (<http://www.linux.com/>) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. »

11.2. Configuration requise

Avant de booter sur le CD LinuxDefender, vous devez d'abord vérifier que votre système remplit les conditions suivantes:

Type de processeur

x86 compatible, minimum 166 MHz pour des performances minimales, un processeur de la génération i686 à 800MHz au moins sera un meilleur choix.

Mémoire

64Mo de mémoire RAM minimum, 256Mo recommandés.

CD-ROM

LinuxDefender nécessite l'emploi d'un CD ROM et d'un BIOS capable de booter depuis ce CD.

Connexion directe à Internet

Bien que LinuxDefender puisse être exécuté sans connexion Internet, le processus de mise à jour nécessite un lien HTTP actif pour se télécharger et assurer la meilleure protection possible, même à travers un serveur proxy. La connexion Internet est donc indispensable.

Résolution graphique

Une résolution minimale de 800X600 est recommandée pour l'administration en ligne.

11.3. Logiciels inclus

Le CD de secours BitDefender inclut le package de logiciels suivant:

- BitDefender SMTP Proxy (Antispam & Antivirus)-
- La Console de gestion distante BitDefender (configuration en ligne)
- BitDefender Linux Edition (moteur antivirus) + Interface graphique (GTK)
- La documentation BitDefender (format PDF et HTML)
- Extras BitDefender (bonus, photos, série Limitée, dépliants)
- Linux-Kernel 2.6
- Le module Captive NTFS write project
- Le module LUFSS - Linux Userland File System
- Des outils pour la récupération de données et de systèmes, y compris pour d'autres systèmes d'exploitation.
- Des outils de gestion et d'analyse de sécurité du réseau pour les administrateurs réseau.
- La solution de sauvegarde Amanda
- thttpd
- Analyseur du trafic réseau Ethereal, IPTraf IP LAN Monitor
- Nessus network security auditor
- Parted, QTParted and partimage, des outils de partitionnement, de sauvegarde et de restauration.
- Adobe Acrobat Reader
- Le navigateur Internet Mozilla Firefox

11.4. Les solutions de sécurité BitDefender pour Linux

Le CD LinuxDefender inclut BitDefender SMTP Proxy Antivirus/Antispam pour Linux, BitDefender Remote Admin (une interface de type Web pour configurer BitDefender SMTP Proxy) et BitDefender Linux Edition scanner antivirus à la demande.

11.4.1. BitDefender SMTP Proxy

BitDefender for Linux Mail Servers - SMTP Proxy est une solution sûre de contrôle de contenu placée au niveau de la passerelle de messagerie, qui assure une protection antivirus et antispam pour tout le trafic email pour y trouver les malwares connus ou inconnus. Grâce à ses technologies propriétaires, BitDefender for Mail Servers est



compatible avec la majorité des plateformes de mails existantes et certifié "RedHat Ready".

Cette solution Antivirus et Antispam analyse, désinfecte et filtre le trafic email pour tous les types de serveurs de messagerie ou de systèmes d'exploitation. BitDefender SMTP Proxy se lance au démarrage et analyse tous les emails entrants. Pour configurer BitDefender SMTP Proxy, il faut utiliser la console d'administration distante de BitDefender (BitDefender Remote Admin), en suivant les instructions ci dessous.

11.4.2. Console de gestion distante de BitDefender

Vous pouvez paramétrer et administrer les services de BitDefender à distance (après avoir configuré votre réseau) ou en local, en suivant les étapes ci-après:

1. Lancer le navigateur Firefox et chargez la console de gestion BitDefender, URL: <https://localhost:8139> (ou double-cliquez sur l'icône de la console de gestion BitDefender sur votre bureau).
2. Enregistrez vous avec le nom d'utilisateur "bd" et le mot de passe "bd"
3. Choisir "SMTP Proxy" dans le menu de gauche
4. Configurez le serveur Real SMTP et le port d'écoute
5. Entrez le nom de domaine de messagerie à utiliser
6. Entrez le nom de domaine réseau à utiliser
7. Choisir "Antispam" dans le menu de gauche pour configurer les paramètres de l'antispam
8. Choisir "Antivirus" pour configurer les actions de l'antivirus BitDefender (actions à suivre en cas d'infection, emplacement de la zone de quarantaine).
9. De plus, vous pouvez paramétrer la réception d'alertes par email "Mail notifications" et les modes d'enregistrement ("Logger")

11.4.3. BitDefender pour Linux

Le moteur d'analyse antivirus est inclut dans LinuxDefender et se présente sous forme d'une interface graphique (GTK+)

Parcourez votre disque dur (ou les disques distants partagés), faites un clic-droit sur le fichier ou dossier voulu et choisissez "analyser avec BitDefender". BitDefender pour Linux analysera les éléments choisis et affichera un rapport d'état d'analyse. Pour un paramétrage avancé, se référer à la documentation BitDefender pour Linux (dans le dossier correspondant ou dans le manuel utilisateur) et au programme `/opt/BitDefender/lib/bdc`.



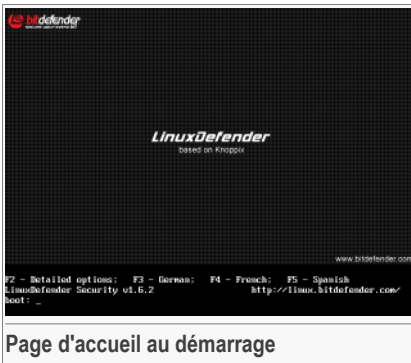
12. Fonctionnement de LinuxDefender

12.1. Démarrer et arrêter

12.1.1. Lancer LinuxDefender

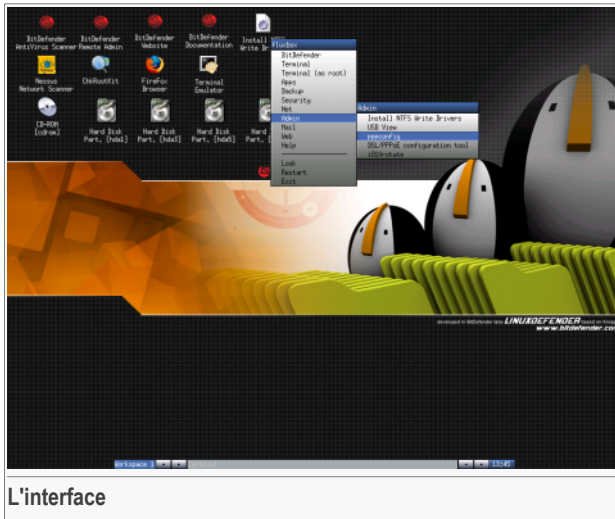
Pour lancer le CD, configurez les options de votre BIOS pour autoriser le boot sur le CD au démarrage de l'ordinateur, mettez le CD dans le lecteur et redémarrez. Vérifiez bien que votre ordinateur puisse booter sur un CD.

Patiencez jusqu'à l'apparition du prochain message et suivez les instructions pour lancer LinuxDefender



Appuyez sur la touche **F2** pour les options détaillées. Appuyez sur la touche **F3** pour les options détaillées en allemand. Appuyez sur la touche **F4** pour les options détaillées en français. Appuyez sur la touche **F5** pour les options détaillées en espagnol. Pour effectuer un démarrage rapide avec les options par défaut appuyez juste sur la touche **ENTER**.

Quand le processus de démarrage sera terminé, vous pourrez utiliser l'interface de LinuxDefender.



L'interface

12.1.2. Arrêter LinuxDefender

Pour quitter LinuxDefender de manière "propre", il est recommandé de descendre toutes les partitions utilisées avec la commande **umount** ou en cliquant droit sur les icônes des partitions disponibles sur le bureau et sélectionnez **Unmount**. Vous pouvez ensuite éteindre votre ordinateur en toute sécurité en choisissant **Exit** dans le menu LinuxDefender (faites un clic-droit pour l'ouvrir) ou en entrant la commande **halt** sur un terminal.



Quand LinuxDefender se sera fermé correctement il affichera un écran comme l'image ci-dessous. Vous pouvez retirer le CD de votre lecteur pour "booter" sur votre disque dur. Vous pouvez maintenant éteindre votre ordinateur ou le redémarrer.



```
X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb unmounted
/randisk unmounted
could not mount /KNOPPIX - trying /dev/cloop instead
/dev/root unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.
```

Patiencez jusqu'à l'apparition de ce message quand vous fermez le programme.

12.2. Configurer la connexion Internet

Si vous utilisez un réseau DHCP et une carte réseau ethernet, la connexion Internet devrait déjà être reconnue et configurée. Pour la configurer manuellement, suivez les étapes suivantes:

1. Ouvrez le menu LinuxDefender (clic-droit) et choisissez **Terminal** pour ouvrir la console.
2. Tapez la commande **netcardconfig** pour lancer les outils de configuration du réseau.
3. Si votre réseau utilise le protocole DHCP, choisissez **yes** (En cas de doute consultez votre administrateur réseau). Sinon, voir ci-dessous.
4. La configuration automatique de la connexion réseau devrait être terminée maintenant. Vous pouvez visualiser votre adresse IP et les paramètres de votre carte réseau avec la commande **ifconfig**.
5. Si vous utilisez une adresse IP statique (vous n'utilisez pas le protocole DHCP), choisissez **No** à la question concernant l'usage du protocole DHCP.
6. Suivez les instructions à l'écran. En cas de doute sur vos réponses, contacter votre administrateur réseau pour plus d'informations.

Si tout se passe correctement, vous pouvez tester votre connexion Internet en lançant une commande de "ping" sur l'adresse `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Si vous utilisez un modem RTC, choisissez **pppconfig** dans le menu de LinuxDefender / Admin menu. Puis suivez les instructions à l'écran pour paramétrer votre connexion.

12.3. Mise à jour de BitDefender

Les packages BitDefender de LinuxDefender se chargent en mémoire RAM pour les mises à jours de fichiers. De cette façon, vous bénéficiez des dernières mises à jour des signatures de virus, du moteur d'analyse ou des bases de données antispam, même si vous utilisez un média en lecture seule, comme le CD LinuxDefender.

Vérifiez que votre connexion Internet est active. Ouvrez la console de gestion distante de BitDefender et choisissez **Live! Update** dans le menu de gauche. Cliquez sur **Update Now** pour récupérer les dernières mises à jour disponibles.

Vous pouvez également taper la commande suivante sur le terminal

```
# /opt/BitDefender/bin/bd update
```

Tous les processus de mise à jour sont enregistrés dans le fichier par défaut BitDefender log. Vous pouvez les visualiser avec la commande suivante.

```
# tail -f /ramdisk/BitDefender/var/log/bd.log
```

Si vous utilisez un serveur proxy pour les connexions sortantes, il faut le paramétrer dans le menu **Live! Update**, onglet **Configuration**.

12.4. Analyse antivirus

12.4.1. Comment accéder à mes données Windows ?

Support du NTFS en écriture

Le support du NTFS en écriture est disponible en utilisant [Captive NTFS write project](#); Vous avez besoin de deux fichiers pilotes (drivers) issus de l'installation de Windows: `ntoskrnl.exe` et `ntfs.sys`. D'une manière générale, seuls les fichiers Windows XP sont supportés. Note: vous pouvez les utiliser pour accéder aussi aux partitions Windows 2000/NT/2003.

Installation des pilotes NTFS

Pour accéder à vos partitions Windows NTFS et pouvoir écrire dessus, il faut d'abord installer les pilotes NTFS. Si vous n'utilisez pas le format NTFS mais le format FAT pour vos partitions Windows, ou si vous n'avez besoin d'accéder à vos données qu'en



lecture, vous pouvez monter les disques durs directement et accéder à vos disques Windows comme avec n'importe quel disque Linux.

Pour bénéficier du support des partitions NTFS, il faut que vous installiez les pilotes NTFS depuis vos disques durs, vos partages distants, clés USB ou depuis le Windows Update. Il est recommandé d'utiliser des pilotes issus de sources sûres car les pilotes disponibles en local dans Windows peuvent parfois être corrompus ou infectés par des virus.

Double-cliquez sur l'icône du bureau **Install NTFS Write Drivers** pour lancer l'installateur **BitDefender Captive NTFS Installer**. Sélectionnez la première option si vous souhaitez installer les pilotes depuis votre disque dur local.

Si les pilotes sont dans un emplacement standard, lancez la commande **Quick search** pour les trouver.

Vous pouvez également préciser le chemin exact où se situent les pilotes. Vous pouvez aussi télécharger les pilotes depuis le Windows Update.

Les pilotes ne sont pas installés sur le disque dur, mais temporairement utilisés par LinuxDefender pour accéder aux partitions NTFS de Windows. Une fois les pilotes NTFS installés, vous pouvez double-cliquer sur les icônes des partitions NTFS sur le bureau et parcourir leur contenu. Pour utiliser un gestionnaire d'application puissant nous vous recommandons d'utiliser Midnight Commander disponible dans le menu LinuxDefender (ou tapez la commande **mc** dans une console).

12.4.2. Comment lancer une analyse antivirus ?

Parcourez vos dossiers, faites un clic-droit sur un fichier ou un dossier et choisissez **Send to**. Puis lancez l'analyse en cliquant sur **BitDefender Scanner**.

Vous pouvez également lancer les commandes suivantes depuis un terminal. Le moteur d'analyse **BitDefender Antivirus Scanner** considérera le fichier ou dossier sélectionné comme étant l'endroit à analyser par défaut.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Cliquez sur **Démarrer l'analyse**.

Si vous voulez configurer les options de l'antivirus, sélectionnez l'onglet **Configure Antivirus** sur la gauche.

12.5. Création d'un moteur de filtrage de messagerie

Vous pouvez utiliser LinuxDefender pour créer une solution de filtrage de mail, sans avoir à installer de logiciel ni à modifier le serveur de messagerie. Le concept est de placer le filtre créé avec LinuxDefender en amont de votre serveur de messagerie pour que BitDefender puisse détecter les virus et les spams dans le trafic SMTP et qu'il relaie ces informations au véritable serveur de messagerie.

12.5.1. Configuration nécessaire

Vous aurez besoin au minimum d'un processeur Pentium 3 ou équivalent avec au moins 256Mo de RAM et d'un lecteur de CD/DVD pour booter dessus. Le système LinuxDefender devra recevoir le trafic SMTP à la place du vrai serveur de messagerie. Vous pouvez le mettre en place de plusieurs manières.

1. Modifiez l'adresse IP de votre serveur de messagerie et attribuez l'ancienne adresse au système LinuxDefender
2. Changez vos enregistrements de DNS de sorte que l'entrée MX de votre domaine pointe vers le système LinuxDefender.
3. Paramétrez vos clients de messagerie pour qu'ils utilisent le système LinuxDefender comme serveur SMTP
4. Modifiez les paramètres de votre firewall pour qu'il redirige les connexions SMTP vers le système LinuxDefender au lieu du véritable serveur de messagerie.

Le guide de fonctionnement de LinuxDefender ne détaille pas les thèmes décrits plus haut. Pour plus d'informations, vous pouvez consulter l'adresse suivante [Linux Networking guides](#) ainsi que [Netfilter documentation](#).

12.5.2. Le filtre email

Bootez sur votre CD LinuxDefender et attendez jusqu'à ce que le système X Windows soit chargé et fonctionnel.

Pour configurer le proxy SMTP BitDefender, double-cliquez sur l'icône **BitDefender Remote Admin**. La fenêtre suivante apparaîtra. Utilisez le nom d'utilisateur `bd` et `bd` comme mot de passe pour vous connecter à la console de gestion distante de BitDefender.

Après vous être connecté, vous pourrez configurer le Proxy SMTP BitDefender.

Choisissez le **Proxy SMTP** pour configurer le véritable serveur de messagerie que vous souhaitez protéger contre les spam et les virus.



Sélectionnez l'onglet **domaines email** pour entrer les domaines email dont vous voulez accepter les emails.

Cliquez sur **Add Email Domain** ou **Add Bulk Domains** et suivez les instructions pour mettre en place le relais du domaine email.

Sélectionnez l'onglet **domaines Internet** pour entrer les domaines Internet dont vous voulez relayer les emails.

Cliquez sur **Add Net Domain** ou **Add Bulk Net Domains** et suivez les instructions à l'écran pour mettre en place le relais du domaine réseau.

Choisissez **Antivirus** dans le menu de gauche, pour déterminer quelle action prendre quand un virus est trouvé et pour configurer les autres options de l'antivirus.

Tout le trafic SMTP est maintenant analysé et filtré par BitDefender. Par défaut, tous les messages infectés seront nettoyés ou rejetés et tous les messages détectés par BitDefender comme étant des spams se verront attribuer la mention [SPAM] en objet. Cet entête ajouté à tous les emails (X-BitDefender-Spam: Yes/No) permet de faciliter le tri pour les utilisateurs.

12.6. Réaliser un audit de la sécurité du réseau

En plus de ses compétences de détection des malware, de récupération de données et de filtrage d'email, LinuxDefender comporte un grand nombre d'outils qui permettent de réaliser un audit approfondi de la sécurité du réseau. Les outils de sécurité de LinuxDefender permettent aussi de faire une analyse approfondie de machines déjà infectées. Lisez ce petit guide (tutorial) pour apprendre comment réaliser un audit de sécurité rapide de vos machines ou de vos réseaux.

12.6.1. Vérifier la présence de Rootkits

Avant de vous lancer dans la mise en place d'une politique de sécurité au niveau du réseau, vérifiez d'abord que votre machine hôte n'est pas contaminée. Vous pouvez lancer une analyse des virus sur les disques durs installés comme indiqué dans le guide (tutorial) **Scan for viruses** ou vous pouvez rechercher la présence de rootkits Unix.

Premièrement, montez toutes vos partitions de disques durs en double-cliquant sur leurs icônes ou en lançant la commande **mount** dans la console. Puis double cliquez sur l'icône **ChkRootKit** pour vérifier le contenu du CD ou lancer la commande **chkrootkit** dans la console, en utilisant les paramètres `-r NEWROOT` pour déterminer le nouveau répertoire de la machine hôte.

```
# chkrootkit -r /dev/hda3
```

Si un rootkit est trouvé, le module chkrootkit montrera ce qu'il a découvert en **BOLD**, utilisant des lettres capitales.

12.6.2. Le moteur d'analyse réseau - Nessus

Nessus est l'analyseur de vulnérabilités open-source le plus populaire au monde, utilisé par plus de 75 000 organisations. De nombreuses organisations internationales ont réduit significativement leurs coûts en utilisant Nessus pour auditer leur système informatique.

—www.nessus.org

Nessus peut être utilisé à distance pour analyser votre réseau d'ordinateur contre toutes sortes de vulnérabilités. Il recommande également des mesures à prendre pour limiter les risques encourus et prévenir les incidents de sécurité.

Double-cliquez sur l'icône **Nessus Security Scanner** ou lancez la commande **startnessus** dans le terminal. Attendez jusqu'à l'apparition de la fenêtre suivante. Selon les ressources dont dispose votre système, le chargement de Nessus avec ses 5000 plug-ins contenant les bases de données de vulnérabilités, peut prendre jusqu'à une dizaine de minutes. Utilisez `knoppix` comme nom d'utilisateur et `knoppix` comme mot de passe pour vous connecter.

Cliquez sur l'onglet **Target selection** pour choisir la cible et entrer l'adresse IP ou le nom de l'hôte que vous voulez analyser. Veillez à bien paramétrer toutes les options d'analyse en fonction des spécifications de votre réseau et de votre système avant de lancer l'analyse pour optimiser l'emploi de la bande passante et la pertinence des résultats obtenus. Puis cliquez sur **Start the scan** pour lancer l'analyse.

Quand l'analyse est terminée, Nessus affiche un compte rendu. Vous pouvez sauvegarder ce rapport dans plusieurs formats, y compris HTML avec des graphiques. Les rapports sauvegardés peuvent être consultés dans votre navigateur habituel.

12.7. Vérifier le bon fonctionnement de votre mémoire RAM

De manière générale, quand votre système a un comportement inhabituel (il se bloque ou redémarre de temps en temps), il s'agit d'un problème de mémoire. Vous pouvez tester vos modules de RAM avec la commande **memtest** comme décrit ci-dessous.

Démarrez votre ordinateur en bootant sur le CD LinuxDefender. Au moment du boot tapez la commande **memtest** et appuyez sur Entrée.



Le programme Memtest se lancera immédiatement et fera plusieurs tests pour vérifier l'intégrité de la mémoire RAM. Vous pouvez paramétrer quels tests doivent être lancés et d'autres options en appuyant sur `c`.

Une analyse complète de la mémoire peut prendre jusqu'à 8 heures selon la vitesse et la capacité de votre mémoire RAM. Il est recommandé de laisser Memtest aller jusqu'au bout des tests afin que ceux-ci soient exhaustifs. Vous pouvez quitter l'analyse à tout moment en appuyant sur `ESC`.

Si vous envisagez d'acheter un nouveau matériel (un ordinateur complet ou des composants) il est recommandé d'utiliser LinuxDefender et Memtest sur celui-ci afin de détecter les éventuelles erreurs ou problèmes de compatibilités.



Demander de l'aide



13. Support technique

13.1. Service de support technique

SOFTWIN fait le maximum pour apporter à leurs clients une aide rapide et efficace. Les centres de support listés ci-dessous sont continuellement mis à jour avec les nouvelles descriptions de virus et réponses aux questions communes, de manière à ce que vous obteniez les informations nécessaires aussi rapidement que possible.

Nous dédions à nos clients le temps et l'argent qu'ils méritent en accordant la plus haute importance aux nouvelles technologies. De plus, nous pensons qu'un commerce compétitif se base sur une bonne communication et un engagement à l'excellence du support.

Vous pouvez demander de l'aide à cette adresse <support@bitdefender.com> quand vous le désirez. Pour une réponse rapide, veuillez inclure votre email et autant de détails possible sur votre produit BitDefender, à propos de votre système et essayez de décrire votre problème de manière claire et précise.

13.2. Aide en ligne

13.2.1. Base de connaissances BitDefender

La base de connaissance de BitDefender est une base en ligne d'informations concernant les logiciels BitDefender. Elle contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de BitDefender. Elle contient également des articles généraux sur la prévention antivirus, la gestion des solutions BitDefender, des informations détaillées et beaucoup d'autres articles.

La base de connaissances de BitDefender est ouverte au public et consultable gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients de BitDefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou les rapports de bug venant de clients de BitDefender trouvent leur réponse en cherchant dans la base de données de BitDefender, comme les rapports de bugs, travaux associés, feuillet ou article d'informations venant compléter les fichiers d'aide des produits.

La base de connaissance BitDefender est disponible en permanence sur <http://kb.bitdefender.com>.

13.3. Contacts

Une communication efficace est la clé d'une relation réussie. N'hésitez pas à nous contacter concernant les problèmes ou questions que vous pourriez avoir.

13.3.1. Adresses Web

Département des ventes: <sales@bitdefender.com>

Support Technique: <support@bitdefender.com>

Documentation: <documentation@bitdefender.com>

Programme de Partenariat: <partners@bitdefender.com>

Marketing: <marketing@bitdefender.com>

Relations Média: <pr@bitdefender.com>

Offres d'emplois: <jobs@bitdefender.com>

Soumissions Virus: <virus_submission@bitdefender.com>

Soumissions Spam: <spam_submission@bitdefender.com>

Rapport d'Abus: <abuse@bitdefender.com>

Site web du Produit: <http://www.bitdefender.com>

Archives ftp du Produit: <ftp://ftp.bitdefender.com/pub>

Distributeurs Locaux: http://www.bitdefender.com/partner_list

Base de connaissances BitDefender: <http://kb.bitdefender.com>

13.3.2. Bureaux BitDefender

Les bureaux de BitDefender se tiennent prêts à répondre à vos questions, à propos de questions commerciales et générales. Leur adresse respective et contacts sont listés ci-dessous.

U.S.A

BitDefender LLC

6301 NW 5th Way, Suite 3500

Fort Lauderdale, Florida 33308

Support technique:

<support@bitdefender.com>

Service client: 954-776-6262

<http://www.bitdefender.com>



Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est reconnu pour un manque total de commandes de sécurité; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Adware

Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en ait accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Archive

Disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Secteur de boot

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Virus de boot

Virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Navigateur Internet

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plug-ins) pour certains formats.

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Cookie

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.

Lecteur de disque

C'est un appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

**Téléchargement**

Copie des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Email

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

Faux positif

Se produit lorsqu'une analyse détecte un fichier comme étant infecté alors qu'il ne l'est pas.

Extension de fichier

Partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Heuristique

Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP qui se charge de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser une applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'elle peut utiliser.

Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications dans le fait qu'elles sont dirigées selon un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, elles ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limitées pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Virus de Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Client de messagerie

Logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Mémoire

Zone de stockage interne dans votre ordinateur. Le terme mémoire définit le stockage de données sous forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.

Programmes compressés

Fichier dans un format compressé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de compresser un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse les fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Chemin

Directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.



Connexion entre deux points, tel le canal de communication entre deux ordinateurs.

Phishing

Action d'envoyer un email à un utilisateur en feignant d'être une entreprise connue dans le but d'obtenir frauduleusement des informations privées et qui permettront d'utiliser l'identité du destinataire du mail. Cet email oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Virus polymorphe

Virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

Port

Connectique de l'ordinateur pour périphérique. Les ordinateurs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Fichier journal (Log)

Fichier qui enregistre les actions entreprises. BitDefender établit un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principale rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseaux, s'ils incluent les logiciels appropriés.

Les Rootkits ne sont pas malicieux par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler

des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

Script

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention de la part de l'utilisateur.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des emails « non sollicités ».

Spyware

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même les numéros de cartes de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classique pour être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placés dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.

Barre d'état système

Introduit avec Windows 95, la barre d'état système se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des



accès faciles aux fonctions système: fax, imprimante, modem, volume etc.
Double-cliquez ou clic-droit sur une icône pour voir les options.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Troyen - Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se répliquent pas, mais peuvent être tout aussi destructeurs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte).

Le terme provient de la fameuse histoire de l'Illiade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Mise à jour

Nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender comporte un module spécial pour la mise à jour. Ce module vous permet de chercher manuellement les mises à jour ou de faire la mise à jour automatiquement.

Virus

Programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont créés par des personnes. Un virus simple peut faire une copie de lui-même très vite et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau par exemple.

Définition virus

"Signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

Ver Internet

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.