TREND MICRO™ PC-cillin™

Internet Security

Version 11

TREND MICRO™

Guide de démarrage rapide

Trend Micro Incorporated se réserve le droit d'apporter des modifications au présent document ainsi qu'aux produits décrits sans avertissement préalable. Avant d'installer et d'utiliser le logiciel, veuillez lire les fichiers Lisez-moi, les notes de publication et la dernière version du Guide de démarrage rapide.

REMARQUE : Les licences d'utilisation des logiciels Trend Micro incluent généralement un droit d'accès aux mises à jour des produits, aux mises à jour des fichiers de signatures et au service standard d'assistance technique pour une durée d'un (1) an à partir de la date d'achat. Le contrat de maintenance peut être renouvelé sur une base annuelle, au tarif alors en vigueur chez Trend Micro.

Document n° PCEM01608/30910

Date de publication : septembre 2003

Protégé par le brevet américain n° 5,951,698

Le Guide de démarrage rapide pour Trend Micro Internet Security™ est destiné à présenter les principales fonctions du logiciel et les instructions d'installation pour votre ordinateur. Il convient de lire ce guide avant d'installer ou d'utiliser le logiciel.

Des informations détaillées sur la façon d'utiliser les fonctions spécifiques du logiciel sont disponibles dans le fichier d'aide en ligne et dans la Base de connaissances en ligne de Trend Micro.

Sommaire

Chapitre 3 : Protection de vos fichiers et de vos données

Chapitre 4 : Gestion des virus

Chapitre 5 : Protection de votre connexion Internet

Chapitre 6 : Obtenir de l'aide

Annexe

Chapitre 1

Bienvenue dans Trend Micro™ Internet Security

Trend Micro Internet Security protège votre ordinateur contre les menaces Internet telles que les virus, les programmes espions, les pirates et les courriers non sollicités. En outre, Trend Micro Internet Security vous permet de sécuriser vos informations personnelles, de bloquer les sites Web indésirables et de rechercher des virus dans le courrier électronique. Trend Micro Internet Security offre une interface simple qui permet d'accéder à des fonctions efficaces. Les nouvelles fonctions de Trend Micro Internet Security garantissent vos connexions Internet et réseau et sont entièrement sécurisées.

Les messages non sollicités appelés « spams » (« pourriel ») prennent aujourd'hui sur Internet une ampleur fâcheuse. Trend Micro Internet Security contient une fonction anti-spam efficace qui permet de filtrer ces messages.

Désormais, Trend Micro Internet Security détecte et bloque les programmes espions. Les programmes espions sont souvent installés conjointement avec des programmes téléchargés sur Internet ; ils repèrent des informations de type sites Web visités ou encore achats faits en ligne.

Trend Micro Internet Security comprend également une fonction de protection des données confidentielles. Cette fonction vous permet de spécifier d'importantes informations personnelles qui ne doivent pas être diffusées sur Internet ou via le courrier électronique. Trend Micro Internet Security bloque et enregistre toute tentative d'envoi de ces données, lesquelles peuvent inclure des éléments tels que votre numéro de carte de crédit, votre adresse personnelle ou votre numéro de téléphone.

En outre, Trend Micro Internet Security peut également scanner les courriers (SMTP) sortants. Cette fonction protège les autres utilisateurs de toute infection provenant d'un courrier de votre ordinateur en exécutant un scan de tous les messages et de leurs pièces jointes avant qu'ils ne quittent votre ordinateur.

Le système innovant d'alerte d'épidémie virale protège votre ordinateur contre les épidémies virales et les menaces les plus récentes envers la sécurité. Le système d'alerte d'épidémie vous prévient de la présence de nouvelles infections de virus de réseau et vous demande de mettre à jour votre logiciel afin d'éviter toute infection.

Ce chapitre contient les sections suivantes :

Un logiciel directement opérationnel...

Même avant la fin de son installation complète, Trend Micro Internet Security lance une détection de virus et de chevaux de Troie sur vos principaux fichiers système. Une fois l'installation terminée, Trend Micro Internet Security contribue à éviter toute infection de votre ordinateur en exécutant une série de tâches automatiques prédéfinies.

Actions de Trend Micro Internet Security dès son installation

Sans nécessiter aucune configuration, Trend Micro Internet Security exécute les tâches suivantes :

- recherche des virus à chaque ouverture, copie, déplacement ou enregistrement de fichier
- protection contre le téléchargement de fichiers infectés

- détection et nettoyage des chevaux de Troie
- blocage des programmes espions
- scan des courriers électroniques et des pièces jointes durant leur téléchargement à partir du serveur de messagerie POP3 ou envoyés via un serveur SMTP (si vous utilisez les clients de messagerie : Microsoft™ Outlook™ 2000 ou version supérieure, Outlook Express 5.5 ou version supérieure, Netscape 7.0 ou version supérieure ou encore Eudora™ Pro 5.0 ou version supérieure.) Un scan des pièces jointes aux courriers électroniques est également effectué lors de leur téléchargement du serveur de courrier Internet (l'accès à un serveur de courrier Internet est effectué via un navigateur Web, par exemple Microsoft Hotmail™, Yahoo!™, et AOL™)
- protection de votre ordinateur contre les attaques issues d'Internet à l'aide d'un pare-feu personnel
- surveillance de vos sessions Microsoft Word™ et Excel™ pour détecter la présence de virus de macro à l'aide de MacroTrap™, un système qui détecte les virus de macro par le biais des méthodes basées sur des règles d'analyse heuristique, plutôt que sur la correspondance de signatures
- recherche des virus inconnus en fonction de leur « comportement », à l'aide de la technologie heuristique avancée
- scan de tous les fichiers sur le disque conformément à la tâche de scan programmée par défaut
- scan de tous les fichiers programme conformément à la tâche de scan programmée par défaut

D'un simple clic de souris, vous pouvez :

- scanner tout fichier de votre système,
- scanner tout fichier à partir de l'Explorateur de Windows ou du Poste de travail en cliquant du bouton droit sur l'icône du fichier,
- scanner les disquettes,
- contrôler la présence de virus de macro dans tous vos fichiers Word et Excel.

Nouveautés de Trend Micro Internet Security

Les virus et autres codes malveillants étant de plus en plus forts et intelligents, Trend Micro Internet Security améliore constamment sa puissance pour assurer une protection antivirus personnelle complète et la sécurité Internet.

Fonction	Description
Protection des données confidentielles	Cette fonction vous permet de définir certains types d'informations (par exemple votre nom, adresse ou numéro de carte de crédit) dont le programme empêchera l'envoi sur Internet ou via le courrier électronique.
Anti-spam	Trend Micro Internet Security inclut un moteur anti-spam efficace et personnalisable. Les messages identifiés en tant que « spams » sont marqués pour faciliter le filtrage ou la suppression. Vous pouvez configurer une « Liste blanche » (liste de toutes les adresses ne présentant aucun danger) pour éviter que les messages importants ne soient étiquetés par inadvertance.
Profils du pare-feu personnel	Selon les paramètres de votre ordinateur et les paramètres réseau, il peut s'avérer nécessaire d'activer certains ports ou services dans certaines situations et de les désactiver dans d'autres. Grâce aux profils de pare-feu personnel, vous pouvez facilement passer d'un profil à l'autre, par exemple d'un profil de réseau domestique à un profil de réseau local sans fil, pour garder un niveau de sécurité optimal adapté à votre environnement.
Recherche de programmes espions	Trend Micro Internet Security détecte et supprime les programmes espions. Un programme espion est souvent installé clandestinement avec des programmes légitimes téléchargés sur Internet. Ce type de programme repère et enregistre vos données personnelles dans une base de données centralisée. Les informations recueillies peuvent inclure votre zone géographique, les sites Web visités et vos achats en ligne.
Scan du courrier SMTP sortant	Trend Micro Internet Security scanne également les messages et pièces jointes sortants (SMTP).

Configuration minimale requise

Pour exécuter Trend Micro Internet Security, les logiciels et les équipements informatiques suivants sont nécessaires.

Système d'exploitation :

- Microsoft™ Windows™ 98, 98SE, Me, 2000 Professionnel avec Service Pack 3 ou version supérieure, XP Édition Familiale ou Professionnel avec Service Pack 1 ou version supérieure

Unité centrale :

- Intel™ Pentium™ 166 MHz ou processeur équivalent pour Windows 98, 98SE et Me
- Intel Pentium 300 MHz ou processeur équivalent pour Windows 2000 et XP

Mémoire :

- 64 Mo de RAM (128 Mo ou plus recommandés) pour Windows 98, 98SE, Me, 2000
- 128 Mo de RAM pour Windows XP

Pour toutes les installations :

- Internet Explorer 5.5 avec Service Pack 2 ou supérieur
- 100 Mo d'espace disque disponible pour l'installation
- Clients pris en charge par le scan du courrier : Microsoft Outlook Express 5.5 ou version supérieure, Microsoft Outlook 2000 ou version supérieure, Netscape Messenger 7.0 ou version supérieure, Eudora Pro 5.0 ou version supérieure.

Remarque : Les exigences matérielles dépendent de votre environnement logiciel. Une connexion Internet est requise pour effectuer l'enregistrement en ligne, les mises à jour et d'autres services en ligne.

Tâches de mise en route principales

Cette section fournit une liste des tâches les plus importantes que vous devez accomplir pour maîtriser rapidement Trend Micro Internet Security. Pour utiliser de manière efficace Trend Micro Internet Security et démarrer la protection de votre PC, nous vous recommandons vivement d'effectuer toutes les tâches suivantes.

Tâche	Rubrique
Installer le logiciel	Voir **Installation de votre logiciel, page 1-7**.
Enregistrer Trend Micro Internet Security	Voir **Enregistrement et activation de Trend Micro Internet Security, page 1-8**, enregistrez votre logiciel pour activer les mises à jour. Trend Micro Internet Security doit mettre à jour les fichiers de signatures et programme pour arrêter les virus les plus récents (si vous devez effectuer une mise à niveau depuis une version d'évaluation de 30 jours, consultez la section *Utilisation des disquettes de secours*, page A-1 dans l'annexe.)
Exécuter une mise à jour manuelle	Voir **Mise à jour de Trend Micro Internet Security, page 1-9**. Étant donné que de nouveaux virus sont constamment libérés, nous vous recommandons vivement de mettre à jour régulièrement Trend Micro Internet Security. Activez l'option de mise à jour intelligente pour que Trend Micro Internet Security effectue sa mise à jour automatiquement.
Scanner manuellement tous les fichiers	Voir **Scan complet de votre ordinateur, page 3-3**, exécutez un scan complet de votre ordinateur pour vous assurer qu'aucun virus ou programme malveillant n'est présent sur votre PC

Installation de votre logiciel

L'installation de Trend Micro Internet Security est simple et ne dure que quelques minutes.

Important : Avant l'installation, vous devez supprimer tous les logiciels antivirus ou pare-feux existants, y compris les autres logiciels antivirus Trend Micro.

Pour installer Trend Micro Internet Security, procédez comme suit :

1. Insérez le CD-ROM du programme Trend Micro Internet Security dans votre lecteur et procédez comme suit :
   - Si le menu apparaît automatiquement, cliquez sur le bouton **Installer le programme**, puis sur **Suivant**.
   - Si le programme ne démarre pas automatiquement, cliquez sur **Démarrer** > **Exécuter** dans la barre des tâches de Windows. Dans le champ **Ouvrir**, tapez D:\setup.exe et cliquez sur **OK** (D:\ correspond à la lettre attribuée à votre lecteur de CD-ROM). Cliquez maintenant sur le bouton **Suivant**.
2. Cliquez sur **J'accepte les termes du contrat de licence** pour indiquer votre acceptation et continuer l'installation de Trend Micro Internet Security. Si vous n'acceptez pas les termes du contrat, la procédure d'installation sera abandonnée.
3. Cliquez maintenant sur le bouton **Suivant**. Avant d'installer les fichiers programme, Trend Micro Internet Security scanne la mémoire de votre système, le secteur d'amorçage et les fichiers sensibles. Si Trend Micro Internet Security détecte un fichier infecté, il le nettoie ou le supprime. L'écran **Informations relatives à l'utilisateur** apparaît. Procédez comme suit :
   - Dans le champ **Nom d'utilisateur**, entrez un nom d'utilisateur. Pour poursuivre l'installation, vous devez fournir un nom d'utilisateur.
   - Dans le champ **Organisation**, saisissez le nom de votre entreprise.

- Dans le champ **Numéro de série**, saisissez votre numéro de série. Si vous n'avez pas de numéro de série, vous pouvez installer une version d'évaluation valable pendant 30 jours. Si vous installez la version d'évaluation, un écran supplémentaire apparaît lorsque vous cliquez sur **Suivant** et vous demande si vous souhaitez installer la version d'évaluation. Cochez la case **Je veux installer la version d'évaluation valable 30 jours** puis cliquez sur **Suivant**. Cette version ne vous permet pas l'enregistrement ou la mise à jour et, après une période de 30 jours, la fonction de scan antivirus sera désactivée ; vous avez alors la possibilité d'acheter le produit ou de le supprimer.

4. Cliquez maintenant sur le bouton **Suivant**. L'écran **Dossier de destination** apparaît. Vous pouvez choisir un emplacement d'installation pour Trend Micro Internet Security ou utiliser l'emplacement par défaut. Pour modifier l'emplacement, cliquez sur **Modifier** et atteignez l'emplacement souhaité.
5. Cliquez sur **Installer** pour commencer l'installation.
6. Une fois l'installation terminée, l'assistant vous informe que l'installation a réussi. Cliquez sur **Terminer** pour quitter le programme d'installation.

Si le programme d'installation demande le redémarrage de l'ordinateur, fermez tous les programmes en cours et cliquez sur **Oui** pour redémarrer.

Enregistrement et activation de Trend Micro Internet Security

Consacrez quelques minutes à l'enregistrement en ligne de votre logiciel. Les licences de logiciels Trend Micro incluent le droit aux mises à jour du produit, aux mises à jour des fichiers de signatures de virus et au support technique de base pendant un (1) an, à partir de la date d'achat. Le contrat de maintenance doit être renouvelé sur une base annuelle.

Important : Pour pouvoir effectuer des mises à jour du programme ou des fichiers de signatures, vous devez enregistrer votre logiciel. Les mises à jour sont nécessaires pour maintenir la protection de votre ordinateur.

Pour enregistrer Trend Micro Internet Security :

1. Connectez-vous à Internet.
2. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Mettre à jour > Enregistrement**.
3. Confirmez que le numéro de série de votre version complète existe déjà et cliquez sur **Enregistrer maintenant**.
4. Dans les champs correspondants de la page d'enregistrement Web, saisissez votre nom, votre adresse électronique ainsi que les informations requises.
5. Cliquez maintenant sur le bouton **Aperçu**. Confirmez l'exactitude des informations saisies.
6. Cliquez maintenant sur le bouton **Valider**. Vérifiez que l'adresse électronique relative à votre ID utilisateur est correcte, puis saisissez un mot de passe.
7. Confirmez l'exactitude du mot de passe, puis cliquez sur **Valider**. Votre clé de licence s'affiche.

Votre logiciel a bien été enregistré. Vous êtes désormais membre du Service Clients de Trend Micro. Vous avez la possibilité de télécharger les mises à jour de Trend Micro Internet Security.

Remarque : Si la page Enregistrement ne s'affiche pas correctement, il est conseillé de modifier la configuration de vos paramètres proxy. Consultez *Activation et configuration des paramètres proxy*, page A-3 dans l'annexe pour obtenir des instructions.

Mise à jour de Trend Micro Internet Security

Pour protéger votre ordinateur contre les dernières menaces, vous devez régulièrement mettre à jour vos fichiers programme, votre moteur de scan et vos fichiers de signatures des virus. Des mises à jour des fichiers de signatures sont publiées par Trend Micro au moins une fois par semaine. La mise à jour de votre fichier de signatures vous offre une protection optimale et permet à Trend Micro Internet Security de rechercher les virus ou autres programmes malveillants les plus récents.

Important : Étant donné que des centaines de nouveaux virus sont découverts chaque mois, il est fortement recommandé de mettre régulièrement à jour Trend Micro Internet Security.

En outre, face à l'apparition de nouveaux virus et à l'évolution des virus connus, la mise à jour de certains fichiers programme devient nécessaire, de même que l'ajout de nouvelles fonctionnalités au moteur de scan. La mise à jour du moteur de scan permet à Trend Micro Internet Security d'exécuter une détection et une suppression conformément aux nouvelles instructions des signatures.

Remarque : Pour pouvoir mettre à jour Trend Micro Internet Security, vous devez enregistrer votre logiciel.

Pour mettre à jour manuellement votre fichier de signatures de virus et votre moteur de scan :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Mise à jour**. L'écran **Mise à jour manuelle** apparaît. Si le processus de mise à jour ne démarre pas, cliquez sur **Mettre à jour**. La barre de progression présente le déroulement de la mise à jour.
2. Si vous devez interrompre la mise à jour, cliquez sur **Arrêter**. Pour poursuivre la mise à jour, cliquez sur **Mettre à jour**.

Pour rechercher et télécharger automatiquement les fichiers de signatures et les fichiers programme les plus récents à partir du serveur Trend Micro ActiveUpdate, il est recommandé de programmer la fonction de mise à jour intelligente. Cette fonction efficace garantit que Trend Micro Internet Security et tous ses composants sont à jour et vous offre ainsi une protection maximale pour une intervention minimale de l'utilisateur.

Pour programmer régulièrement une mise à jour du fichier de signatures de virus et du moteur de scan :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Mettre à jour >Paramètres de mise à jour.**
2. Assurez-vous que la case **Activer la mise à jour intelligente…** est cochée, sélectionnez la fréquence de vérification de la disponibilité des mises à jour par Trend Micro Internet Security.
3. Cliquez sur **Appliquer**.

Remarque : Pour que Trend Micro Internet Security exécute automatiquement les mises à jour sans votre intervention, cochez la case **Mettre à jour automatiquement sans notification** dans **Notification de mise à jour**.

Pratiques recommandées pour limiter les risques en informatique

Pour éviter toute infection de votre ordinateur, prenez les mesures préventives suivantes.

- **Vérifiez que le scan en temps réel est activé –** le scan en temps réel fournit une protection antivirus constante. En activant le scan en temps réel, vous réduisez de façon significative les risques d'infection pour votre ordinateur. Il est recommandé d'activer systématiquement le scan en temps réel car cette fonction est très efficace et fonctionne en arrière-plan, de manière transparente.
- **Mettez à jour Trend Micro Internet Security –** Enregistrez votre logiciel et téléchargez les dernières versions des fichiers de signatures, du moteur de scan et des composants programme de Trend Micro Internet Security pour vous assurer que le logiciel utilise la technologie antivirus la plus récente. Programmez également Trend Micro Internet Security de sorte que le logiciel exécute automatiquement les mises à jour à l'aide de la mise à jour intelligente.
- **Méfiez-vous des pièces jointes suspectes –** La messagerie électronique représente le mode de propagation le plus courant pour les virus et codes malveillants. Si vous recevez un message d'un inconnu, veillez à ne pas enregistrer ni exécuter les fichiers joints. Cependant, quel que soit l'expéditeur, méfiez-vous des pièces jointes contenant des fichiers exécutables (.exe, .com).
- **Définissez des tâches de scan programmées –** Les tâches de scan constituent un moyen rapide et simple de programmer différents scans manuels. Les tâches vous permettent de configurer le type de fichiers à scanner ainsi que la fréquence du scan. Par exemple, vous pouvez créer une tâche de scan pour scanner tous les types de fichiers sur votre ordinateur, chaque vendredi à 22 h.
- **Restez informé –** Visitez régulièrement le site Web de Trend Micro (www.trendmicro-europe.com) afin d'y découvrir les dernières informations sur les virus et les alertes de sécurité. L'encyclopédie des virus en ligne de Trend Micro vous permet en outre de vous documenter sur les virus.
- **Mettez à jour Microsoft Windows –** Microsoft répond aux problèmes de sécurité en publiant des correctifs ou des mises à jour sur son site Web. Les systèmes d'exploitation Microsoft Windows offrent une fonction de mise à jour Windows qui vous permet de télécharger et de mettre à jour facilement ces fichiers.

Mise à niveau de votre version d'évaluation

Le passage de la version d'évaluation valable 30 jours à la version complète, suivi de son enregistrement, vous permet d'utiliser toutes les fonctionnalités de Trend Micro Internet Security.

En outre, après avoir procédé à la mise à niveau et à l'enregistrement en ligne de votre logiciel, vous profiterez des avantages suivants : droit de recevoir les mises à jour des fichiers de signatures et de bénéficier d'un support technique de Trend Micro ou d'un revendeur agréé pendant une période d'un (1) an. Par la suite, vous devez renouveler votre contrat de maintenance sur une base annuelle et vous acquitter des frais demandés par Trend Micro à ce moment pour pouvoir continuer à bénéficier de ces services.

Si vous continuez à utiliser la version d'évaluation après la période de 30 jours, toutes les fonctions seront désactivées.

Si vous utilisez une version d'évaluation, cliquez sur **Acheter** sur l'écran de démarrage et suivez les instructions affichées à l'écran.

Pour passer à la version complète depuis votre version d'évaluation, si vous n'avez pas saisi de numéro de série durant l'installation :

1. Dans la fenêtre principale, cliquez sur **Mettre à jour > Enregistrement.**
2. Dans le champ Étape 1 de l'écran Enregistrement, entrez votre numéro de série valide.
3. Cliquez sur **Mettre à niveau**.

Vous venez de passer de la version d'évaluation à la version complète. Vous pouvez désormais passer à l'étape suivante, à savoir l'enregistrement de votre logiciel. Voir Enregistrement et activation de Trend Micro Internet Security, page 1-8.

Chapitre 2

Apprentissage de Trend Micro Internet Security

Ce chapitre contient des sections qui vous aident à vous familiariser avec Trend Micro Internet Security. En outre, il présente les alertes d'épidémie virales et décrit comment accéder à l'aide en ligne de Trend Micro Internet Security.

Ce chapitre contient les sections suivantes :

Comment Trend Micro Internet Security protège-t-il votre PC ?

Trend Micro Internet Security est conçu pour protéger l'ordinateur à la fois contre les menaces externes et internes.

Menace	Protection Trend Micro Internet Security
Externe : virus et autres programmes malveillants (par ex. chevaux de Troie et vers), e-mail infectés	Le scan en temps réel est conçu pour détecter et scanner les fichiers téléchargés, copiés ou déplacés. Le scan du courrier offre une protection contre les messages électroniques et les pièces jointes présentant des signes d'infection en entrée ou en sortie et contre les pièces infectées jointes aux courriers Internet (Hotmail, AOL, Yahoo!) .
Interne (ordinateur local) : virus et autres programmes malveillants (par ex. chevaux de Troie et vers)	Le scan manuel (à la demande) et le scan programmé vérifient votre ordinateur local. Trend Micro Internet Security peut détecter l'activité des programmes de type cheval de Troie, récupérer les fichiers système que ces derniers ont modifiés, interrompre leurs processus et supprimer les fichiers qu'ils génèrent.
Épidémies virales	Le système d'alerte d'épidémie virale vous informe, de manière proactive, sur l'arrivée d'une épidémie ou sur une autre situation à haut risque et vous conseille une mise à jour de Trend Micro Internet Security.
Pirates	Le pare-feu de Trend Micro Internet Security fournit une solide protection contre les intrusions externes ainsi que des règles d'exception pour une meilleure flexibilité.
Sites Web inappropriés	Le filtrage des URL bloque le chargement de sites Web inappropriés.

Menace	Protection Trend Micro Internet Security
Courriers électroniques non sollicités (« spam »)	Le moteur anti-spam de Trend Micro Internet Security identifie les messages non sollicités et les marque de façon à les filtrer aisément.
Données confidentielles	La protection des données confidentielles vous permet de spécifier des informations personnelles (telles que le numéro de votre carte de crédit ou l'adresse de votre domicile) dont Trend Micro Internet Security bloquera la transmission via le Web ou via un message électronique.

Ouverture de la fenêtre principale de Trend Micro Internet Security

L'interface à onglet de Trend Micro Internet Security fournit un accès rapide à tous les domaines de programme antivirus et des paramètres de sécurité Internet.

Pour visualiser la fenêtre principale de Trend Micro Internet Security :

- Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Trend Micro Internet Security** > **Trend Micro Internet Security**.

Conseil : Dans la barre d'état système, cliquez avec le bouton droit sur l'agent en temps réel  et cliquez sur **Ouvrir l'écran principal**. (La barre d'état système se situe à côté de l'horloge, sur le côté inférieur droit de l'écran.)

- La fenêtre principale de Trend Micro Internet Security s'affiche :

Utilisation de Trend Micro Internet Security

La nouvelle conception de l'interface vous permet d'accéder rapidement aux paramètres et aux informations récapitulatives de Trend Micro Internet Security. En haut de la fenêtre principale, des liens offrent un accès rapide aux fonctions fréquemment utilisées :

Lien d'accès rapide	Description
Mettre à jour	Ce lien interroge immédiatement le serveur Trend Micro ActiveUpdate pour connaître les dernières mises à jour disponibles des fichiers de signatures des virus et des fichiers programme. Le serveur ActiveUpdate est un serveur Internet où se situent le fichier de signatures et les mises à jour de tous les produits Trend Micro. Pour bénéficier de la fonction de mise à jour, vous devez être connecté à Internet.
Scanner	Scanne votre système selon les paramètres de scan manuel spécifiés.
Aide	Permet de visualiser l'Aide en ligne, l'Encyclopédie des virus, le Centre d'informations sur les virus et la page d'accueil de Trend Micro.

Chaque bouton situé dans la partie droite de l'interface vous permet de visualiser ou de gérer les paramètres d'un domaine de sécurité ou d'un domaine antivirus spécifique.

Pour effectuer l'action suivante :	**Cliquez sur :**
Afficher l'état du système et les journaux d'événements.	
Afficher vos paramètres antivirus et les fichiers en quarantaine ou effectuer une tâche de scan.	
Afficher vos paramètres de scan du courrier, de scan Internet et anti-spam.	
Afficher les paramètres de votre filtre URL et de votre protection des données confidentielles.	
Afficher les paramètres du profil de votre pare-feu personnel.	
Afficher vos paramètres de mise à jour ou effectuer une mise à jour manuelle. Enregistrer votre logiciel.	

Utilisation de l'agent en temps réel

L'agent en temps réel est le programme qui assure une protection en temps réel de votre ordinateur. Il représente le moyen le plus rapide d'accéder à certaines fonctions, par exemple pour afficher la fenêtre principale.

Démarrage de l'agent en temps réel

L'agent en temps réel est configuré de manière à démarrer automatiquement et à apparaître dans la barre d'état système à chaque démarrage de votre ordinateur. Si ce n'est pas le cas, nous vous conseillons de le démarrer manuellement.

Pour démarrer l'agent en temps réel :

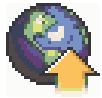
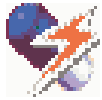
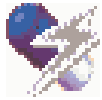
- Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Trend Micro Internet Security** > **Agent en temps réel**.

Avec l'agent en temps réel, un seul coup d'œil vous permet de savoir si le scan en temps réel est activé ou désactivé.

Pour :	**Procédez comme suit :**
Ouvrir la fenêtre principale	Double-cliquez sur l'agent en temps réel.
Arrêter l'agent en temps réel	Cliquez avec le bouton droit de la souris sur l'agent en temps réel, puis sur **Quitter**. **Important :** Si vous désactivez l'agent en temps réel, le scan en temps réel sera également désactivé.
Interrompre tout le trafic Internet	Cliquez avec le bouton droit de la souris sur l'agent en temps réel, puis sur **Verrouillage d'urgence**.
Exécuter une mise à jour	Cliquez avec le bouton droit de la souris sur l'agent en temps réel, puis sur **Mettre à jour**.

Identification des icônes de l'agent en temps réel

Utilisez le tableau ci-dessous pour connaître la signification des icônes de l'agent en temps réel.

Icône	Description
	Le trafic Internet entrant et sortant est entièrement interrompu (pour autoriser le trafic Internet, consultez *Utilisation du Verrouillage d'urgence*, page 5-3)
	Connexion au serveur Trend Micro pour télécharger les dernières mises à jour
	Le scan en temps réel est activé (éclair rouge)
	Le scan en temps réel est désactivé (éclair gris). Pour activer le scan en temps réel, consultez *Confirmation de l'activation du scan en temps réel*, page 3-1

Affichage des informations système

Des informations récapitulatives et détaillées sur votre antivirus et la sécurité Internet sont disponibles via Trend Micro Internet Security. Vous pouvez afficher des informations récapitulatives pour vérifier rapidement les paramètres actifs, ou les journaux pour obtenir des détails sur les événements de sécurité, antivirus et programme.

Affichage des informations sur le produit

Il est important de vous assurer que vos fichiers de signatures et votre moteur de scan sont à jour. L'utilisation de la version la plus récente de ces composants vous permet de bénéficier d'une protection antivirus optimale. Pour être certain de disposer des dernières mises à jour, vous pouvez afficher la version en cours de votre moteur de scan et de votre fichier de signatures.

Pour afficher les informations importantes relatives au produit :

- Cliquez sur **Aide** > **À propos du produit**> **Informations relatives à la version**.

Votre numéro de série s'affiche également. Si vous contactez le support technique ou un revendeur agréé pour obtenir une assistance ou pour réinstaller Trend Micro Internet Security, vous devez fournir votre numéro de série.

Vous pouvez consulter le Centre d'informations sur les virus de Trend Micro pour obtenir les dernières versions du fichier de signatures et du moteur de scan.

Pour visiter le Centre d'informations sur les virus de Trend Micro :

- Cliquez sur **Aide** > **Centre d'informations sur les virus.**

Affichage de l’état de la sécurité Internet

La fenêtre État de la sécurité Internet fournit un aperçu de l’état de la sécurité Internet. Vous pouvez ainsi rapidement évaluer le niveau de sécurisation du système dans les domaines suivants : pare-feu personnel, filtrage des URL, protection des données confidentielles et anti-spam.

Pour afficher l’état de la sécurité Internet :

- Cliquez sur **État** > **État de la sécurité Internet**.

État actuel fournit une vue d’ensemble de l’état de la sécurité Internet.

État actuel	Signification
Normal	Les fonctions de pare-feu personnel, de protection des données confidentielles et anti-spam sont activées.
Attention	Certains des paramètres de Trend Micro Internet Security sont désactivés. Cochez la case État des paramètres pour obtenir plus d’informations.
Danger	Certains des paramètres de Trend Micro Internet Security sont désactivés. Le système n’est pas sécurisé. Cochez la case **État des paramètres** pour afficher et réactiver les paramètres désactivés.

La case **Informations relatives à la dernière attaque** affiche la dernière tentative d’attaque ou de scan. Ces informations sont accessibles uniquement si le pare-feu personnel est activé.

La case **État des paramètres** fournit des informations sur l’état actuel des paramètres de sécurité Internet (activé/désactivé). Cliquez sur le lien pour afficher la fenêtre de configuration de chaque paramètre.

La case **Surveillance du trafic Internet** fournit les données chiffrées du trafic entrant et sortant. Si vous observez une augmentation du trafic entrant ou sortant alors que vous n’utilisez pas les services Internet, il se peut que l’ordinateur soit infecté par un cheval de Troie ou un virus.

Affichage de l’état antivirus

La fenêtre État antivirus fournit un récapitulatif des paramètres de scan antivirus et de mise à jour. Utilisez cette page pour vérifier l’état global de vos paramètres et afficher des statistiques relatives aux activités antivirus.

Pour afficher l’état antivirus :

- Cliquez sur **État** > **État antivirus**.

État actuel fournit une vue d’ensemble de l’état de vos paramètres antivirus.

État actuel	Signification de l'icône
Normal	Les fonctions Scan en temps réel, Scan du courrier entrant, Scan du courrier sortant, Scan du courrier Internet et Mise à jour intelligente sont activées.
Attention	Un ou plusieurs paramètres antivirus est (sont) désactivé(s). Cochez la case **Paramètres de mise à jour et de scan** pour obtenir plus d’informations.
Danger	Tous les paramètres antivirus sont désactivés. Le système n’est pas sécurisé. Cochez la case **Paramètres de mise à jour et de scan** pour afficher et réactiver les paramètres désactivés.

La case **État du scan et des virus** fournit des informations sur les derniers virus et fichiers infectés détectés, le dernier fichier scanné et l’heure du dernier scan manuel ou programmé.

La case **Paramètres de mise à jour et de scan** fournit des informations sur l’état actuel des paramètres de sécurité antivirus (activé/désactivé). Cliquez sur le lien pour afficher la fenêtre de configuration de chaque paramètre.

Affichage des journaux d'événements

Trend Micro Internet Security conserve des journaux de tous les événements relatifs aux mises à jour, aux virus, au filtrage des URL, à la fonction Damage Cleanup Services, à la protection des données confidentielles, à la fonction anti-spam et au pare-feu personnel. Ces journaux peuvent être affichés à partir de l'écran Journaux d'événements et constituent une véritable source d'informations. Par exemple, vous pouvez visualiser le type de virus pour savoir s'il s'agit d'un cheval de Troie ou d'un ver et s'il convient de le supprimer plutôt que de le mettre en quarantaine.

Outre l'affichage de la date et de l'heure de chaque journal enregistré, les divers types de journaux fournissent des informations spécifiques.

Journal	**Des entrées sont créées lorsque :**
Mise à jour	vous tentez de télécharger les composants les plus récents. Les entrées des journaux de mise à jour contiennent également des informations sur le ou les fichier(s) téléchargé(s) et installé(s), ainsi que sur l'état du téléchargement (réussite ou échec).
Virus	un virus ou un programme malveillant est détecté. Les entrées des journaux des virus contiennent également des informations sur l'heure de la détection, le type de scan – en temps réel ou manuel – qui a permis de détecter le virus, le nom du virus, le nom du fichier qui contient le virus, l'état de la première action et, le cas échéant, l'état de la deuxième action.
Damage Cleanup Services	Un cheval de Troie est détecté par la fonction Trend Micro Damage Cleanup Service (DCS). La fonction DCS détecte et élimine les chevaux de Troie. Les entrées des journaux DCS contiennent des informations sur l'heure de la détection, le nom du cheval de Troie et le résultat de l'action de nettoyage.
Filtrage des URL	un site Web est bloqué ou un contenu de site Web malveillant est détecté. Les entrées des journaux de filtrage des URL contiennent également des informations sur l'heure de la tentative d'accès à un site restreint, l'URL ou l'adresse Internet bloqué(e) et l'action exécutée.

Journal	Des entrées sont créées lorsque :
Pare-feu personnel	votre ordinateur fait l'objet d'une attaque depuis Internet. Les entrées des journaux du pare-feu personnel incluent également des informations sur le type de défense, l'heure de l'attaque, la direction du trafic réseau, le type de protocole utilisé, l'adresse IP source, le numéro de port source, l'adresse IP de destination, le numéro de port de destination et la raison pour laquelle le trafic a été bloqué.
Protection des données confidentielles	votre ordinateur tente d'envoyer des données confidentielles via Internet. Les entrées des journaux de la protection des données confidentielles contiennent des informations sur l'heure de la tentative d'envoi des données confidentielles, le type de données et le site Web ou l'adresse électronique de destination.
Anti-spam	un courrier non sollicité est identifié et marqué. Les journaux de la fonction anti-spam contiennent des informations sur l'heure de la détection, l'objet du courrier et l'expéditeur.

Pour vérifier vos journaux :

1. Dans la fenêtre principale, cliquez sur **État** > **Journaux d'événements.**
2. Cliquez sur le type de journal à afficher.
3. Cliquez sur **Journaux**.
4. Sélectionnez la date du journal à afficher.

Remarque : Pour trier les journaux (ordre croissant ou décroissant) en fonction d'un en-tête de colonne (par exemple : Heure), cliquez sur le titre de la colonne.

Introduction au système d'alerte d'épidémie virale

Trend Micro Internet Security comprend un service innovant pour éviter les dernières épidémies virales et autres menaces malveillantes. Grâce à l'exploitation des recherches et des connaissances de Trend Micro TrendLabs, Trend Micro Internet Security est en mesure de vous avertir à l'avance de l'existence de menaces, ce qui vous laisse le temps de mettre votre logiciel à jour pour éviter une infection. (TrendLabs est le réseau international de centres de recherche antivirus et de centres de support technique Trend Micro, qui fournit une assistance 24 h sur 24, 7 jours sur 7 aux clients de Trend Micro dans le monde entier.)

Le système d'alerte d'épidémie virale doit être activé avant que vous puissiez recevoir les alertes d'épidémie.

Pour activer le système d'alerte d'épidémie virale :

1. Dans la barre des tâches de Windows, cliquez sur **Démarrer > Programmes > Trend Micro Internet Security > Paramètres d'avertissement lors d'une épidémie**.
2. Cochez la case **Permettre à l'agent d'épidémie de donner des conseils préventifs**.
3. Pour afficher le dernier avertissement d'épidémie virale, cliquez sur **Afficher alerte**.
4. Cliquez sur **OK**.

Les avertissements d'épidémie sont classés en Alertes rouges et Alertes jaunes. Les alertes rouges correspondent aux épidémies définies par TrendLabs comme présentant un risque majeur et les alertes jaunes correspondent à celles qui présentent un risque moyen.

Important : Si vous recevez un avertissement d'épidémie, la première action à entreprendre est de mettre à jour votre fichier de signatures et votre moteur de scan, puis d'exécuter un scan complet de votre ordinateur.

 **Critère Risque majeur (Alerte rouge)**	 **Critère Risque moyen (Alerte jaune)**
Plusieurs rapports d'infection révèlent la présence de programmes malveillants à propagation rapide. La première procédure de réponse est mise en œuvre dans les 45 minutes suivant l'alerte rouge, comme il est d'usage dans ce secteur d'activité. La publication d'une signature officielle (OPR) est déployée et accompagnée d'une note indiquant sa disponibilité ; toutes les autres notifications d'importance vous sont également envoyées.	Les différents sites de Trend Micro reçoivent des rapports d'infection ainsi que des appels pour une assistance technique, permettant de localiser des points d'infection isolés. Une OPR est alors mise à disposition pour le téléchargement.

Accès à l'aide en ligne

L'aide en ligne de Trend Micro Internet Security détaille toutes les fonctions et caractéristiques de Trend Micro Internet Security. Utilisez-la pour trouver des réponses à vos questions sur Trend Micro Internet Security.

Pour accéder à l'aide en ligne :

- Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Aide** > **Sommaire et index**. L'aide en ligne apparaît.

De plus, lorsque vous utilisez le programme, vous pouvez également voir apparaître des boutons Aide. Cliquez sur ces boutons pour afficher une aide contextuelle (informations qui correspondent à l'affichage en cours).

Chapitre 3

Protection de vos fichiers et de vos données

Ce chapitre contient des informations sur les tâches de base à exécuter pour protéger votre ordinateur. Il contient les sections suivantes :

Confirmation de l'activation du scan en temps réel

Le scan en temps réel fournit une protection antivirus constante dans la mesure où il prend en compte tout fichier copié, téléchargé ou déplacé. Le scan en temps réel s'exécute en arrière-plan et ne nécessite aucune intervention de la part de l'utilisateur : il vous suffira donc de vous assurer que la fonction est activée.

Vous pouvez vérifier si le scan en temps réel est activé (ce qui est le cas par défaut) en consultant l'agent en temps réel dans la barre d'état système.

Activé (par défaut) – éclair rouge

Désactivé – éclair gris

Important : Si vous désactivez l'agent en temps réel, le scan en temps réel sera également désactivé.

Pour activer le scan en temps réel :

- Dans la barre d'état système, cliquez avec le bouton droit de la souris sur l'**agent en temps réel**.

Confirmation de l'activation du scan du courrier

Le courrier électronique est le moyen de propagation le plus courant pour les virus et autres programmes malveillants. L'ouverture d'un courrier infecté ou d'une pièce jointe infectée est la principale cause d'infection. Du fait de la popularité du courrier électronique, de nombreux créateurs de virus écrivent aujourd'hui des virus qui exploitent la vulnérabilité des logiciels de messagerie.

Le scan du courrier est conçu pour vérifier les messages électroniques et les pièces jointes lors de leur téléchargement et de leur envoi depuis un serveur de messagerie Internet (POP3/SMTP). Les clients de courrier électronique pris en charge sont :

- Microsoft Outlook 2000 et version supérieure
- Outlook Express 5.5 et version supérieure
- Eudora Pro 5.0 et version supérieure
- Netscape Messenger 7.0 et version supérieure

La fonction Scan du courrier peut également scanner les pièces jointes téléchargées à partir d'un compte de messagerie sur Internet (courrier électronique stocké sur un serveur et accessible grâce à un navigateur). Les comptes de courrier Internet pris en charge sont :

- Microsoft Hotmail
- Yahoo!
- AOL

La fonction Scan du courrier de Trend Micro Internet Security doit être activée pour que vos messages électroniques soient scannés.

Pour vérifier l'activation du scan du courrier :

1. Dans la fenêtre principale, cliquez sur **Courrier** > **Scan du courrier.**
2. Cliquez sur **Courrier entrant**. Vérifiez que la case **Autoriser le scan du courrier entrant** est cochée.
3. Cliquez sur **Courrier sortant**. Vérifiez que la case **Autoriser le scan du courrier sortant** est cochée.
4. Cliquez sur **Appliquer**.

Scan complet de votre ordinateur

Scannez tous les lecteurs pour rechercher d'éventuels signes d'infections sur votre ordinateur. En un seul clic, Trend Micro Internet Security offre un moyen simple et rapide de scanner tous les lecteurs connectés à l'ordinateur.

Pour scanner l'ordinateur entier :

- Dans la fenêtre principale, cliquez sur **Scanner.** La boîte de dialogue Scanner les fichiers apparaît et Trend Micro Internet Security procède au scan. Pour interrompre le scan, cliquez sur **Arrêter**. Un message vous demande confirmation. Cliquez sur **Oui** pour confirmer puis sur **OK**.

Remarque : Trend Micro Internet Security scanne les types de fichiers et exécute les actions antivirus nécessaires en fonction des paramètres du scan manuel. Pour modifier ces paramètres, consultez la rubrique « Configuration des paramètres de recherche de virus » de l'aide en ligne.

Scan d'un dossier ou d'un fichier

Avec Trend Micro Internet Security, vous pouvez scanner tout le contenu d'un dossier, y compris les sous-dossiers, ou encore un fichier unique. Trend Micro Internet Security scanne les types de fichiers et exécute les actions antivirus nécessaires en fonction des paramètres du scan manuel.

Pour scanner un dossier :

- Cliquez à l'aide du bouton droit de la souris sur le dossier, puis sur **Recherche de virus**.

Conseil : Vous pouvez également « faire glisser » le dossier dans la fenêtre principale de Trend Micro Internet Security.

Pour scanner un fichier unique :

- Cliquez à l'aide du bouton droit de la souris sur le fichier, puis sur **Recherche de virus**.

Conseil : Vous pouvez cliquer avec le bouton droit de la souris sur le fichier, sélectionner **Propriétés**, puis cliquer sur l'onglet **Propriétés virales**. Il est également possible de « faire glisser » le fichier dans la fenêtre principale de Trend Micro Internet Security.

Exécution des tâches de scan

Les tâches de scan vous permettent de programmer l'exécution automatique de différents scans à une heure spécifiée. Par exemple, vous pouvez créer une tâche de scan pour vérifier tous les types de fichiers sur tous les lecteurs, chaque vendredi à 22 h. Vous pouvez toutefois exécuter manuellement, à tout moment, des tâches de scan préalablement définies.

Trend Micro Internet Security propose plusieurs tâches de scan prédéfinies. Vous pouvez non seulement exécuter ces tâches mais également les consulter pour y découvrir des astuces et créer efficacement, par la suite, vos propres tâches de scan.

Pour exécuter une tâche de scan :

1. Dans la fenêtre principale, cliquez sur **Système** > **Scan de fichiers**.
2. Sélectionnez la tâche à exécuter.
3. Cliquez sur **Scanner**. Pour interrompre le scan, cliquez sur **Arrêter**. Une boîte de dialogue de confirmation apparaît. Cliquez sur **Oui** pour confirmer puis sur **OK**.

Remarque : Pour en savoir plus sur les tâches de scan, consultez la rubrique « Gestion des tâches de scan » de l'aide en ligne.

Blocage des programmes espions

Trend Micro Internet Security bloque l'installation des programmes espions sur votre ordinateur en les incluant dans le scan en temps réel. Le programme espion est un logiciel qui est installé conjointement avec les programmes et les utilitaires officiels ou après la consultation d'un site Internet. Les partagiciels ou les logiciels gratuits téléchargés depuis Internet sont susceptibles de contenir des programmes espions. Ces derniers repèrent les informations personnelles, telles que les sites Internet que vous visitez ou les logiciels que vous installez sur votre ordinateur.

Pour activer le blocage des programmes espions :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Système** > **Paramètres de scan.**
2. Cliquez sur **Scan en temps réel**.
3. Cochez la case **Rechercher programmes espions**.
4. Cliquez sur **Appliquer**.

Recherche et suppression des chevaux de Troie

Trend Micro Internet Security détecte l'activité des chevaux de Troie, récupère les fichiers que ces derniers modifient, interrompt leur processus et supprime les fichiers qu'ils génèrent.

Les chevaux de Troie sont de petits programmes d'apparence inoffensive. Pour causer des dommages, ils doivent être installés sur votre système. Une fois installé, un cheval de Troie dispose des mêmes privilèges que l'utilisateur de l'ordinateur et peut se servir du système pour exécuter des actions indésirables. La principale différence entre les chevaux de Troie et les virus réside dans le fait que les premiers ne peuvent pas se dupliquer ou se propager d'eux-mêmes.

Trend Micro Internet Security recherche automatiquement les chevaux de Troie au cours de leur installation initiale ; il est également possible de configurer Trend Micro Internet Security pour qu'il recherche automatiquement les chevaux de Troie pendant les scans manuels et au début de chaque scan en temps réel.

Pour rechercher et supprimer automatiquement les chevaux de Troie lors des scans :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Système** > **Paramètres de scan**.
2. Cliquez sur **Scan manuel** ou **Scan en temps réel** selon le scan auquel vous voulez inclure la recherche de chevaux de Troie. Trend Micro recommande d'inclure la recherche des chevaux de Troie au scan manuel et au scan en temps réel.
3. Cochez la case **Rechercher / supprimer chevaux de Troie**.
4. Cliquez sur **Appliquer**.

Toutefois, vous pouvez également rechercher manuellement les chevaux de Troie.

Pour rechercher et supprimer manuellement les chevaux de Troie :

1. Localisez le dossier d'installation de Trend Micro Internet Security (par exemple, l'emplacement par défaut est C:\Program Files\Trend Micro\Internet Security).
2. Cliquez deux fois sur le fichier **Tsc.exe**.

Protection de vos données confidentielles

La protection des données confidentielles vous permet de définir certains types d'informations (par exemple votre nom, adresse ou numéro de carte de crédit) dont le programme empêchera l'envoi sur Internet ou via le courrier électronique.

Remarque : Pour protéger vos données confidentielles, vous devez d'abord les définir. Consultez la rubrique « Protection des données confidentielles » de l'aide en ligne pour plus d'informations.

Pour confirmer l'activation de la protection des données confidentielles :

1. Dans la fenêtre principale, cliquez sur **Internet** > **Protection des données confidentielles**.
2. Vérifiez que la case **Autoriser la protection des données confidentielles** est cochée.
3. Cliquez sur **Appliquer**.

Pour ajouter ou modifier un élément relatif à la protection des données confidentielles :

1. Dans la fenêtre principale, cliquez sur **Internet** > **Protection des données confidentielles**.
2. Choisissez l'une des actions suivantes :
   - Pour ajouter un nouvel élément, cliquez sur **Ajouter**.
   - Pour modifier un élément existant, sélectionnez-le, puis cliquez sur **Modifier**.
3. Saisissez un nom et une description pour l'élément dans les champs **Nom de l'élément** et **Description**.
4. Entrez vos données confidentielles dans le champ **Données confidentielles**. Trend Micro Internet Security établit une correspondance exacte des données au moment où vous les saisissez. Notez que les informations que vous saisissez respectent la casse, ainsi *trend*, *TREND* et *tReNd* sont considérés comme des mots différents.

5. Choisissez l'une des actions suivantes ou les deux :
   - Pour empêcher l'envoi de cet élément sur le Web, cochez la case **Vérifier le protocole Internet**.
   - Pour empêcher l'envoi de cet élément par e-mail, cochez la case **Vérifier le protocole de messagerie**.
6. Cliquez sur **OK**. L'élément est enregistré.

Réduction du spam

Les messages non sollicités appelés « spams » (également connus sous le nom de « pourriel » ou « message-poubelle ») prennent aujourd'hui sur Internet une ampleur fâcheuse. Le moteur anti-spam de Trend Micro Internet Security identifie les messages non sollicités et leur ajoute une marque de façon à les identifier ou à les filtrer aisément.

Les messages non sollicités sont marqués uniquement lorsque la fonction anti-spam est activée sur l'ordinateur.

Pour confirmer l'activation de la fonction anti-spam :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Courrier** > **Anti-spam**.
2. Vérifiez que la case **Activer la protection anti-spam** est cochée.

Vous pouvez configurer la fonction Anti-spam de Trend Micro Internet Security de sorte qu'elle fonctionne selon trois niveaux différents. Au niveau le plus élevé, les règles anti-spam sont très strictes. En d'autres termes, davantage de messages importuns sont correctement identifiés mais des messages légitimes risquent d'être marqués par erreur. Le niveau le plus faible présente des règles anti-spam beaucoup moins sévères. Dans ce cas, davantage de messages non sollicités parviennent à passer mais il est peu probable que les messages légitimes soient marqués par erreur.

Lorsqu'un message est identifié comme étant un courrier non sollicité, le champ Objet du message indiquera « SPAM: » en préfixe. Définissez une règle dans votre logiciel de messagerie afin de filtrer ces messages et de les isoler dans un dossier spécial « spam », où vous pourrez régulièrement vérifier l'éventuelle présence de messages légitimes marqués par erreur. (Consultez la documentation de votre client de messagerie pour plus d'informations sur la configuration des règles.)

La fonction Anti-spam présente également une liste blanche, qui vous permet de spécifier des adresses électroniques connues. Tout message issu d'une adresse électronique de la liste blanche ne sera pas étiqueté comme un message non sollicité.

Pour configurer les paramètres anti-spam :

1. Dans la fenêtre principale, cliquez sur **Courrier > Anti-spam.**
2. Sélectionnez un paramètre dans la barre de défilement **Niveau de protection anti-spam**.
3. Pour ajouter des adresses électroniques à la liste blanche, cliquez sur **Modifier la liste blanche...**
   - Pour ajouter une nouvelle adresse électronique à la liste blanche, cliquez sur **Ajouter**. Saisissez l'adresse électronique, puis cliquez sur **OK**.
   - Pour supprimer une adresse électronique de la liste blanche, sélectionnez-la et cliquez sur **Supprimer**.
4. Cliquez sur **OK**.

Remarque : Les courriers électroniques dont la taille dépasse la limite définie pour le scan du courrier entrant (POP3) ne bénéficieront pas de filtrage anti-spam.

Chapitre 4

Gestion des virus

Devant la quantité de virus déjà en circulation et le nombre de nouveaux virus, il est probable que vous y soyez confronté un jour. Ce chapitre contient les sections suivantes :

Fonctionnement des chevaux de Troie

Les chevaux de Troie sont de petits programmes d'apparence inoffensive. Pour causer des dégâts, ils doivent être installés sur votre système. Dès qu'il est installé, le cheval de Troie dispose d'un accès complet à vos fichiers de données et peut prendre le contrôle de votre système. La principale différence entre les chevaux de Troie et les virus est que les premiers ne peuvent pas se reproduire ou se propager d'eux-mêmes.

Fonctionnement des virus

En termes simples, un virus informatique est un programme qui se reproduit. À cet égard, il se greffe à d'autres fichiers programme (par exemple, .exe, .com, .dll) et s'exécute à chaque exécution du programme hôte. Au-delà de la simple reproduction, le virus vise presque toujours un autre objectif : causer des dégâts.

La partie active du virus, appelée routine de destruction, exécute des actions aussi diverses que l'écrasement de données essentielles stockées dans la table de partition du disque dur ou le brouillage des nombres dans vos feuilles de calcul, en passant par la production d'images ou de sons irritants, voire d'effets insupportables.

Pour obtenir plus d'informations sur un virus en particulier ou sur les virus en général, vous pouvez accéder à l'Encyclopédie des virus en ligne de Trend Micro ou visiter notre site Web à l'adresse :

`www.trendmicro-europe.com`

Que faire lorsqu'un virus est détecté ?

Il n'y a aucune raison de paniquer. Lorsque Trend Micro Internet Security détecte un virus, que ce soit via le scan en temps réel, le scan manuel ou le scan du courrier, Trend Micro Internet Security vous informe de la présence du virus et de l'action exécutée.

Dans le cadre du scan en temps réel et du scan du courrier, un message s'affiche et décrit le fichier infecté ainsi que l'action exécutée.

Les actions du scan en temps réel, du scan manuel ou du scan du courrier dépendent des paramètres configurés pour chacun. Toutefois, l'action par défaut de tous les types de scan est Nettoyer.

En d'autres termes, si un fichier est infecté, Trend Micro Internet Security tente d'abord de nettoyer le fichier. La deuxième action par défaut pour le scan en temps réel et le scan manuel est la mise en quarantaine.

Il est possible que Trend Micro Internet Security détecte un programme malveillant qui ne peut être nettoyé. Certains programmes malveillants (comme les chevaux de Troie et les vers) n'infectent pas les fichiers, ils ne peuvent par conséquent pas être nettoyés. Il existe également certains types de virus qui écrasent les données existantes, ce qui rend le nettoyage impossible. Par défaut, Trend Micro Internet Security déplace ces fichiers « non nettoyables » vers un dossier de quarantaine (la deuxième action par défaut pour le scan du courrier est Supprimer.)

Action sur les fichiers non nettoyables

Étant donné leur nature, il n'est pas possible de nettoyer des programmes malveillants en quarantaine. En effet, il ne s'agit pas d'une infection de fichier par un virus ; il s'agit d'un programme, qui impliquerait d'être « nettoyé » dans son intégralité. Les programmes malveillants placés en quarantaine doivent être supprimés.

Pour plus d'informations sur les modalités de traitement des fichiers dans le dossier Quarantaine, consultez le guide de quarantaine interactif.

Pour afficher le guide de quarantaine :

1. Dans la fenêtre principale, cliquez sur **Système** > **Quarantaine.**
2. Cliquez sur **Guide de quarantaine** et suivez les instructions.

Pour connaître le type du virus, consultez les journaux de virus. Les informations suivantes fournissent davantage de détails sur la façon d'identifier différents types de virus en fonction de leur nom.

Type de programmes malveillants	Préfixe de nom	Exemple
Chevaux de Troie	TROJ_<nom>	TROJ_QAZ.A
Vers	WORM_<nom>	WORM_KLEZ
Virus à base de script	VBS_<nom> JS_<nom>	VBS_BRITNEYPIC.A
Fichiers contagieux	PE_<nom>	PE_VETTIKINS.A
Programmes espions	SPYW_<nom>	SPYW_NARGON.A

Éradication des virus du secteur d'amorçage

Les virus de secteur d'amorçage sont particulièrement gênants (et dangereux) car ils se logent dans une zone sensible du disque dur, le secteur d'amorçage, et se chargent en mémoire à chaque démarrage du système. À partir de la mémoire, ils peuvent aisément infecter tout fichier ouvert et toute disquette utilisée.

Trend Micro Internet Security recherche automatiquement les virus du secteur d'amorçage pendant un scan manuel ou programmé. Si un virus de secteur d'amorçage est détecté, Trend Micro Internet Security exécute l'action de scan spécifiée pour le scan actuel.

Remarque : Les virus de secteur d'amorçage se propagent facilement. Si Trend Micro Internet Security a détecté un virus de secteur d'amorçage, il est très probable qu'une ou plusieurs disquettes soient également infectées. Veillez à scanner toutes vos disquettes.

Chapitre 5

Protection de votre connexion Internet

Ce chapitre contient des instructions sur la sécurisation de votre connexion Internet contre les pirates malveillants. Il décrit également comment empêcher la visualisation de certains sites Web à l'aide du filtrage des URL.

Ce chapitre contient les sections suivantes :

Introduction au pare-feu personnel

Le pare-feu personnel de Trend Micro Internet Security protège votre ordinateur contre des attaques provenant d'Internet. Un pare-feu crée une barrière entre votre ordinateur et le réseau (réseau local, Internet). Ce rempart examine et filtre le trafic Internet entrant et sortant. Grâce à ce filtrage, le pare-feu empêche les pirates malveillants de s'introduire dans votre ordinateur et de causer des dégâts.

Le pare-feu Trend Micro Internet Security est un pare-feu « dynamique » ; en d'autres termes, il suit et surveille l'état de chaque connexion pour vérifier qu'aucune action anormale ne se produit. Par exemple, l'inspection dynamique remarquerait si le port 80 laissait passer autre chose que le trafic HTTP.

Un pare-feu à inspection dynamique fait le suivi de chaque « session » et sait si la session est déjà active. Le pare-feu utilise cette information ainsi qu'une liste de règles pour déterminer si un paquet (correspondant à l'unité de base des données transmises par le réseau) doit être bloqué ou transféré.

Le filtrage est basé non seulement sur des règles définies mais également sur le contexte établi par les précédents paquets qui ont traversé le pare-feu.

Le pare-feu personnel inclut les fonctions suivantes :

- Capacité à autoriser ou à refuser le trafic en fonction d'un port ou d'un protocole spécifié
- Affichage d'un avertissement relatif à un accès dynamique sortant lorsqu'un programme ne figurant pas dans la liste des exceptions tente de se connecter à Internet (niveau de sécurité Élevé uniquement). Cet avertissement a pour but d'empêcher les programmes non autorisés, comme les chevaux de Troie, de voler des données ou une personne tierce de contrôler votre ordinateur à distance.
- Utilisation d'un IDS (Intrusion Detection System – système de détection d'intrusion) pour empêcher les attaques de pare-feu connues
- Règles de pare-feu et règles IDS avec possibilités de mise à jour
- Capacité à filtrer les chaînes HTTP de serveur à serveur pour empêcher les attaques combinées telles que Nimda et Code Red

Activation du pare-feu personnel

Pour pouvoir vous connecter à Internet sans vous soucier d'éventuelles intrusions dans votre ordinateur, activez votre pare-feu personnel. Le pare-feu personnel vous protège des pirates qui tentent d'endommager vos fichiers, de voler vos informations confidentielles ou de causer des dégâts.

Pour vérifier l'activation du pare-feu personnel :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Pare-feu > Profils de pare-feu.**
2. Vérifiez que la case **Activer le pare-feu personnel** est cochée.
3. Cliquez sur **Appliquer**.

Compréhension des profils du pare-feu personnel

Trend Micro Internet Security vous permet de configurer divers profils de pare-feu personnel pour différentes situations. Selon les paramètres de votre ordinateur et les paramètres réseau, il peut s'avérer nécessaire parfois d'activer certains ports ou services. Grâce aux profils de pare-feu personnel, vous pouvez facilement passer d'un profil à l'autre, par exemple d'un profil de réseau domestique à un profil de réseau local sans fil, pour garder un niveau de sécurité optimal adapté à votre environnement. La préconfiguration du pare-feu personnel inclut tout un ensemble de configurations réseau communes. Vous pouvez utiliser ces configurations sans modification, ou encore créer et personnaliser votre propre profil.

Remarque : Consultez la rubrique « Gestion des profils du pare-feu personnel » de l'aide en ligne pour obtenir plus d'informations.

Utilisation du Verrouillage d'urgence

Le contrôle intégral de votre trafic Internet est une condition primordiale pour faire face à des épidémies virales ou à d'autres tentatives d'intrusion. Le Verrouillage d'urgence interrompt immédiatement l'ensemble du trafic Internet entrant et sortant ; cette fonction est particulièrement utile lorsqu'un individu tente de s'introduire à distance dans votre ordinateur ou en cas d'alerte d'épidémie virale.

Pour activer le Verrouillage d'urgence :

- Dans la fenêtre principale, cliquez sur **État > État de la sécurité Internet**, puis sur **Verrouillage d'urgence**. Le trafic Internet est entièrement interrompu, il vous sera donc impossible de naviguer sur le Web ou de consulter votre courrier électronique tant que le Verrouillage d'urgence est activé.

Pour désactiver le Verrouillage d'urgence :

- Cliquez une nouvelle fois sur **Verrouillage d'urgence**.

Conseil : Dans la barre d'état système, cliquez avec le bouton droit de la souris sur l'agent en temps réel, puis sur **Verrouillage d'urgence** ou cliquez sur **Verrouillage d'urgence** dans la boîte de dialogue qui apparaît lorsque le scan en temps réel détecte un virus.

Blocage des virus de réseau

Les virus de réseau, tel NIMDA, se propagent rapidement sur Internet et les réseaux locaux. Trend Micro Internet Security permet de protéger votre ordinateur contre les virus de réseau ou d'empêcher votre ordinateur d'infecter d'autres postes. En cas de détection d'un virus de réseau, Trend Micro Internet Security peut exécuter les actions suivantes :

- Interrompre immédiatement tout le trafic Internet
- Afficher un message d'alerte rouge

Pour afficher les informations relatives aux virus de réseau :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Pare-feu > Centre d'urgence contre les virus de réseau.**
2. Cliquez sur le lien pour obtenir davantage d'informations sur un virus de réseau spécifique.

Pour modifier les paramètres des virus de réseau :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Pare-feu > Centre d'urgence contre les virus de réseau.**
2. Choisissez l'une des actions suivantes :
   - Pour interrompre immédiatement le trafic Internet lorsqu'un virus de réseau est détecté, cochez la case **Interrompre tout le trafic Internet lorsqu'un virus de réseau est détecté**.
   - Pour afficher une alerte lorsqu'un virus de réseau est détecté, cochez la case **Afficher un message Alerte rouge**.
3. Cliquez sur **Appliquer**.

Filtrage du contenu de pages Web indésirables

Pour garantir une protection contre un contenu de page Web indésirable, Trend Micro Internet Security propose le filtrage des URL. Cette fonction vous permet d'interdire aux autres utilisateurs de l'ordinateur l'accès à certains sites Web.

Le filtrage des URL peut fonctionner selon deux modes différents :

- Activation de l'accès à tous les sites Web par défaut. Vous spécifiez alors une liste de sites auxquels l'accès est INTERDIT. Cette liste d'URL est connue sous le nom de Liste restreinte.
- Désactivation de l'accès à tous les sites Web par défaut. Vous spécifiez alors une liste de sites auxquels l'accès est AUTORISÉ. Cette liste d'URL est connue sous le nom de Liste autorisée.

Pour filtrer le contenu de pages Web indésirables :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Internet > Filtrage des URL**.
2. Cochez la case **Activer le filtrage des URL**.
3. Cliquez sur **Appliquer**.

Trend Micro Internet Security affiche le message « URL bloqué » lorsqu'un utilisateur tente d'accéder à un site Web non autorisé.

Pour ajouter un URL à la liste restreinte ou autorisée ou encore pour modifier un URL existant :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Internet > Filtrage des URL**.
2. Choisissez l'une des actions suivantes :
   - Pour autoriser l'accès, cliquez sur **Autoriser l'accès...**.
     Votre liste restreinte est alors opérationnelle.
   - Pour bloquer l'accès, cliquez sur **Bloquer l'accès...**.
     Votre liste autorisée est alors opérationnelle.

3. Choisissez l'une des actions suivantes :
   - Pour ajouter un nouvel URL : cliquez sur **Ajouter**.
   - Pour modifier un URL : sélectionnez l'URL, puis cliquez sur **Modifier**.
4. Vous pouvez ajouter un URL manuellement ou récupérer des URL à partir des favoris ou de l'antémémoire de votre navigateur. L'importation des URL depuis l'antémémoire de votre navigateur constitue un moyen rapide d'ajouter tous les sites récemment visités à la liste autorisée. Pour ajouter manuellement un URL :
   - Dans **Ajouter l'URL**, saisissez l'URL du site Web bloqué (Liste restreinte) ou permis (Liste autorisée). Par exemple, www.pageweb.com.
5. Pour ajouter tous les URL de l'antémémoire du navigateur :
   - Cliquez sur **Importer les URL de l'antémémoire du navigateur Web**. Si vous préférez importer les URL à partir des favoris du navigateur, cliquez sur **Importer mes favoris**.
6. Pour bloquer la totalité d'un site Web, y compris les pages secondaires, cochez la case **Inclure l'ensemble des pages...**.
7. Cliquez sur **OK**. Si vous avez coché la case **Inclure l'ensemble des pages...**, une petite croix apparaît sur l'icône de l'URL.
8. Cliquez sur **Appliquer**.

Chapitre 6

Obtenir de l’aide

Trend Micro s’engage à fournir un service et une aide qui dépassent les attentes de ses utilisateurs, quel que soit leur pays de résidence. Ce chapitre contient des informations sur la façon d’obtenir une assistance technique. Vous devez enregistrer votre produit pour pouvoir bénéficier de l’assistance.

Cette section présente les rubriques suivantes :

Avant de contacter le support technique

Consultez la documentation : l'aide en ligne et le manuel fournissent des informations détaillées sur Trend Micro Internet Security et contiennent peut-être la solution à votre problème.

Consultez le site Web de notre support technique : ce site contient les informations les plus récentes sur tous les produits Trend Micro. Le site Web du support technique inclut également les archives des questions déjà posées par les utilisateurs ainsi que les réponses apportées.

Visite du Service Clients

Le Service Clients contient les dernières informations sur Trend Micro Internet Security. En tant qu'utilisateur enregistré, vous pouvez accéder à des informations exclusives.

Pour visiter le Service Clients de Trend Micro :

- Dans la fenêtre principale, cliquez sur **Aide** > **Service Clients**.

Visite du site Web du support technique

Consultez le site Web du support technique de Trend Micro pour rechercher les réponses à vos questions. Ce site contient les informations les plus récentes sur nos produits. Des nouvelles solutions sont ajoutées quotidiennement. Si, cependant, vous ne trouvez pas les réponses que vous recherchez, vous pouvez poser votre question en ligne où des experts TrendLabs vous fourniront des réponses ou vous contacteront pour plus d'informations.

Pour visiter le site Web du support technique :

- Dans la fenêtre principale, cliquez sur **Aide** > **Page d'accueil du support technique**.

Contacter le support technique

Les licences d'utilisation des logiciels Trend Micro incluent généralement un droit d'accès aux mises à jour des produits, aux mises à jour des fichiers de signatures et au service standard d'assistance technique pour une durée d'un (1) an à partir de la date d'achat. Le contrat de maintenance peut être renouvelé sur une base annuelle, au tarif alors en vigueur chez Trend Micro.

Afin d'accélérer la résolution de votre problème, veuillez fournir autant d'informations que possible lorsque vous contactez notre équipe :

- Numéro de série du produit
- Numéro de version du programme Trend Micro Internet Security, du moteur de scan, du fichier de signatures, du numéro de version
- Nom et version du système d'exploitation, type de connexion Internet
- Texte exact de tout message d'erreur obtenu
- Étapes permettant de reproduire le problème

TrendLabs™

TrendLabs est le réseau international Trend Micro de centres de recherche antivirus et de centres de support technique, qui fournit une assistance 24 h sur 24 et 7 jours sur 7 aux clients de Trend Micro dans le monde entier.

Composés d'une équipe de plus de 250 ingénieurs et agents d'assistance qualifiés, les centres de service TrendLabs situés à Paris, Munich, Manille, Taïpeh, Tokyo et Irvine, CA. assurent une réponse rapide en cas d'épidémie virale ou en cas de problème support urgent avec un client, n'importe où dans le monde.

Le quartier général de TrendLabs, situé dans l'un des plus grands parcs technologiques de Manille, a gagné sa certification ISO 9002 en 2000 pour ses procédures de gestion qualité et représente ainsi l'un des premiers services de recherche antivirus et d'assistance à être accrédités de la sorte. Nous sommes certains que TrendLabs est leader de l'industrie de l'antivirus de par son service et son équipe de support.

Pour plus d'informations sur TrendLabs, consultez le site :

`http://fr.trendmicro-europe.com/enterprise/security_info/trendlabs.php`

Envoi des fichiers infectés à Trend Micro

Si vous avez un fichier susceptible d'être infecté par un virus et que votre moteur de scan ne parvient ni à le détecter, ni à le nettoyer, nous vous recommandons de nous envoyer ce fichier à l'adresse suivante :

`http://subwiz.trendmicro.com`

Pensez à joindre une brève description des symptômes ressentis dans un message texte. Notre équipe d'ingénieurs en technologie antivirus « disséquera » le fichier pour identifier et définir les caractéristiques de tous les virus qu'il contient et vous retournera le fichier nettoyé généralement sous 48 heures.

Annexe

Cette annexe contient des informations susceptibles de ne pas s'appliquer à tous les utilisateurs. Il contient les sections suivantes :

Utilisation des disquettes de secours

Certains types de virus du secteur d'amorçage peuvent empêcher le démarrage normal de l'ordinateur. Pour nettoyer ces virus, vous devez démarrer votre ordinateur à partir d'une disquette non infectée et non pas à partir du disque dur infecté. Une « disquette de secours » est une disquette de démarrage que Trend Micro Micro Internet Security peut créer si vous êtes équipé de Microsoft Windows 98 ou Windows Millenium.

Les disquettes de secours Trend Micro Internet Security requièrent un environnement DOS natif pour fonctionner correctement ; toutefois, Windows 2000 et XP ne prennent plus en charge ce type d'environnement.

Pour Windows 2000 et XP, il est recommandé de créer une disquette de réparation d'urgence. Pour obtenir des instructions, reportez-vous à la documentation de Microsoft pour Windows.

Pour créer un jeu complet de disquettes de secours, plusieurs disquettes sont nécessaires.

Remarque : Les disquettes de secours doivent être protégées en écriture après leur création. La protection en écriture est effective lorsque vous pouvez voir à travers les deux carrés des coins supérieurs.

- Disquette de démarrage d'urgence (Disquette 1) : contient les fichiers nécessaires au démarrage de l'ordinateur. Utilisez-la pour démarrer l'ordinateur si un virus d'amorce l'a infecté et vous empêche de démarrer normalement.
- Disquette des fichiers PCSCAN (Disquette 2) : contient le moteur de scan. Utilisez-la avec les disquettes des fichiers de signatures pour détecter et supprimer les virus du secteur d'amorçage de l'ordinateur.
- Disquettes des fichiers de signatures (Disquette 3 et suivantes) : contient les fichiers de signatures permettant de détecter les virus les plus récents. Utilisez-les avec la disquette des fichiers PCSCAN pour détecter et supprimer les virus du secteur d'amorçage de l'ordinateur.

Remarque : Ne redémarrez pas votre ordinateur à l'aide de disquettes de secours créées pour une version antérieure de Trend Micro PC-cillin ; vous risqueriez de perdre des données.

Avant de créer votre jeu de disquettes de secours, munissez-vous de l'équipement nécessaire pour étiqueter les disquettes. Pour créer un jeu complet de disquettes de secours, au moins sept disquettes seront nécessaires.

Si vous disposez déjà d'un jeu de disquettes de secours issu d'une version antérieure du logiciel Trend Micro, vous devez créer un nouveau jeu après l'installation de Trend Micro Internet Security. De la même manière, si vous avez créé des disquettes de secours sous Windows 98 puis procédé à une mise à niveau vers Windows Millenium, vous devez créer un nouveau jeu de disquettes de secours. Vous pouvez bien sûr réutiliser vos anciennes disquettes pour créer les nouvelles. Toutes les données des anciennes disquettes seront perdues lors de la création des nouvelles.

Pour créer des disquettes de secours :

1. Procurez-vous des disquettes, insérez-en une dans le lecteur de votre ordinateur.
2. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Trend Micro Internet Security** > **Créer les disquettes de secours**. La fenêtre Création de disquettes de secours s'ouvre.
3. Cliquez sur **Jeu complet de disquettes de secours**, puis cliquez sur **Suivant**.

4. Assurez-vous que le lecteur cible est correct et cliquez sur **Suivant**. La boîte de dialogue Formater apparaît.
5. Choisissez le type de formatage (formatage Complet recommandé) et cliquez sur **Démarrer**. Le formatage commence.
6. Lorsque l'opération est terminée, cliquez sur **Fermer**. La boîte de dialogue Formater se ferme et Trend Micro Internet Security commence à copier les fichiers sur le disque.
7. Lorsqu'une disquette est prête, retirez-la du lecteur et étiquetez-la immédiatement. Faites glisser vers le haut l'encoche en plastique située dans le coin supérieur droit, à l'arrière de la disquette, pour protéger cette dernière en écriture. La protection en écriture est effective lorsque vous pouvez voir à travers les deux carrés des coins supérieurs. La création des disquettes de secours dure environ 10 minutes.
8. Répétez la procédure pour chaque disquette, en commençant par l'étape de formatage.
9. Cliquez sur **Terminer**.

Remarque : Vous ne pouvez pas créer de disquettes de secours sur un ordinateur infecté par un virus de secteur d'amorçage. Assurez-vous que vous avez bien nettoyé (ou supprimé) tous les virus détectés.

Activation et configuration des paramètres proxy

Un serveur proxy est utilisé pour assurer la sécurité et augmenter l'efficacité d'utilisation de la bande passante du réseau. La plupart des particuliers n'utilisent pas de serveur proxy, contrairement à un grand nombre d'entreprises, bureaux et écoles. Si vous rencontrez des problèmes de connexion à Internet pour l'enregistrement, le téléchargement des mises à jour du programme, il est possible que vous utilisiez un serveur proxy qui n'a pas été identifié ou qu'une erreur se soit glissée dans l'adresse/les informations d'identification.

Si vous utilisez un serveur proxy sur votre réseau, vous devez saisir l'adresse IP (numéro) et le port de ce serveur proxy.

De plus, si les utilisateurs du serveur proxy doivent se connecter, vous devez fournir leurs informations d'identification.

Pour activer et configurer les paramètres proxy :

1. Dans la fenêtre principale, cliquez sur **Mettre à jour** > **Paramètres de mise à jour**.
2. Dans le champ **Informations proxy**, cochez la case **Utiliser le serveur proxy**.
3. Cliquez sur **Paramètres proxy**, puis procédez comme suit :
   - Dans **Adresse proxy**, saisissez l'adresse IP du serveur proxy ou le nom de domaine (par exemple, proxy.votresociété.com).
   - Dans **Port**, saisissez le numéro de port du serveur proxy (par exemple, 80).
   - Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de votre serveur proxy.
4. Cliquez sur **OK**. Cliquez sur **Appliquer**.

Index

TREND MICRO SA
6, Rue de l'Abbé Hazard
92000 NANTERRE
Tel: +33 (0) 1 56 38 26 62
Fax: +33 (0) 1 56 38 26 86
www.trendmicro-europe.com

Item code:PCEM01608/30910