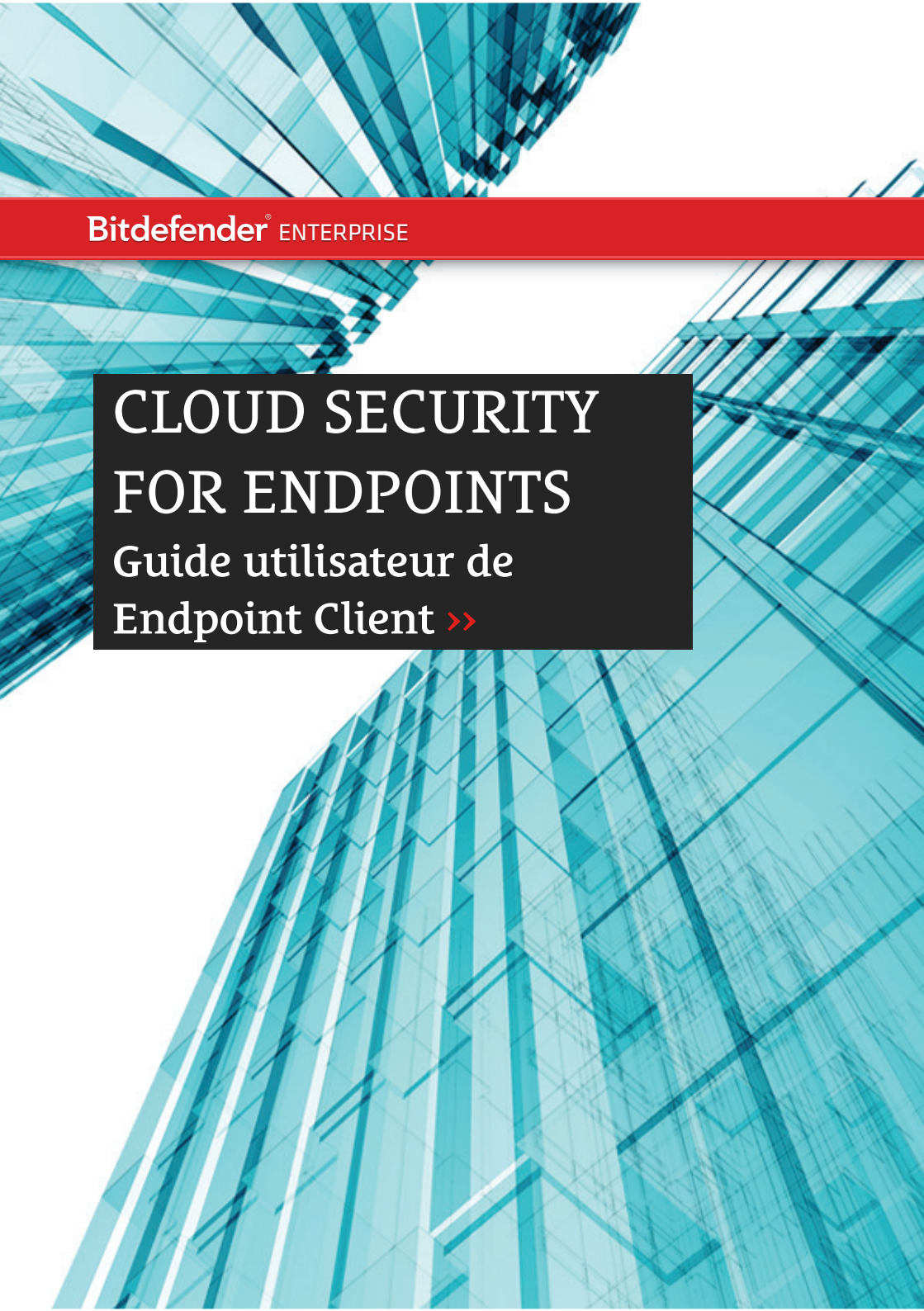

Bitdefender ENTERPRISE
CLOUD SECURITY
FOR ENDPOINTS
Guide utilisateur de
Endpoint Client ››

Cloud Security for Endpoints by Bitdefender
Guide utilisateur de Endpoint Client

Date de publication 2012.11.15


Bitdefender

Table des matières

Utilisation de ce guide

1. Objectifs et destinataires

Cette documentation est conçue pour les utilisateurs finaux de **Endpoint Client**, le logiciel client Cloud Security for Endpoints installé sur les ordinateurs et les serveurs pour les protéger contre les malwares et les autres menaces Internet et pour appliquer les politiques de contrôle utilisateur.

Les informations présentées ici devraient être faciles à comprendre pour toute personne capable de travailler sous Windows.

Nous vous souhaitons un apprentissage agréable et utile.

2. Comment utiliser ce guide

Ce guide est organisé afin de trouver facilement les informations dont vous avez besoin.

« Pour démarrer » (p. 1)
Découvrez l'interface utilisateur de Endpoint Client.

« Analyse antimalware » (p. 9)
Découvrez comment exécuter des analyses antimalwares.

« Mises à jour » (p. 18)
En savoir plus sur les mises à jour de Endpoint Client.

« Événements » (p. 20)
Vérifiez l'activité de Endpoint Client.

« Obtenir de l'aide » (p. 21)
Sachez où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

3. Conventions utilisées dans ce guide

Normes Typographiques

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

Apparence	Description
documentation@bitdefender.com	Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts.
« Utilisation de ce guide » (p. v)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
`nom de fichier`	Les fichiers et répertoires sont imprimés en utilisant des caractères `séparés d'un espace`.
option	Toutes les options du produit sont imprimées à l'aide de caractères **gras**.
mot clé	Les mots-clés et les expressions importantes sont mises en évidence à l'aide de caractères **gras**.

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 nous vous recommandons de ne pas l'ignorer. Elle fournit habituellement des informations non critiques mais significatives.

4. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutesles 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 celivret ou concernant toute amélioration que nous pourrions y apporter pour vous fournirla meilleure documentation possible.

Faites le nous savoir en nous écrivant à cette adresse documentation@bitdefender.com.Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

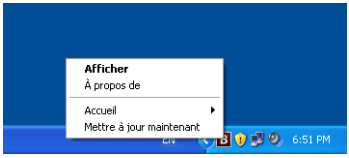
1. Pour démarrer

Endpoint Client est un programme de sécurité informatique entièrement automatisé, administré à distance par votre administrateur réseau ou fournisseur de services. Une fois installé, il vous protège contre toutes sortes de malwares (virus, spywares et chevaux de Troie), attaques réseaux, phishing et vol de données. Il peut également être utilisé pour appliquer les politiques d'utilisation d'Internet et des ordinateurs de votre entreprise.

Endpoint Client prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes pop-up.Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Événements. Pour plus d'informations, reportez-vous à « Événements » (p. 20).

1.1. Icône de la zone de notification

Lors de l'installation, Endpoint Client place une icône permanente dans la zone de notification.Si vous double-cliquez sur cette icône, la fenêtre principale du programme s'ouvrira. En faisant un clic droit sur l'icône, un menu contextuel vous fournira des options utiles.



Icône de la zone de notification

- **Afficher** - ouvre la fenêtre principale de Endpoint Client.
- **À propos de** - ouvre une fenêtre contenant des informations relatives à Endpoint Client, ainsi que des éléments d'aide si vous rencontrez une situation anormale.
- **Analyser** - vous aide à exécuter des analyses antimalwares.Vous pouvez choisir entre les trois tâches d'analyse suivantes :
  - **Quick Scan** utilise l'analyse in-the-cloud pour détecter les malwares présents sur votre système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.
  - **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.
  - L'**Analyse Complète du Système** analyse l'ensemble de votre ordinateur en vue de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Pour des informations sur l'utilisation de ces tâches d'analyse, veuillez vous référer à « Analyse antimalware » (p. 9).

- **Mettre à jour** - effectue une mise à jour immédiate.Vous pouvez suivre l'état de la mise à jour dans la fenêtre qui s'affiche.

L'icône Bitdefender de la zone de notification vous informe lorsque des problèmes affectent votre ordinateur en modifiant sa couleur comme suit :

Des problèmes critiques affectent la sécurité de votre système.

Des problèmes non critiques affectent la sécurité de votre système.

Si Endpoint Client ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : .Cela se produit généralement lorsque la clé de licence expire. Cela peut également avoir lieu lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal du programme.

Note
Si les problèmes persistent, contactez votre administrateur réseau ou votre fournisseur de services.

1.2. Ouverture de la fenêtre principale du programme

Pour accéder à l'interface principale de Endpoint Client, utilisez le menu Démarrer de Windows en suivant le chemin d'accès **Démarrer** → **Tous les programmes** → **Endpoint Client** → **Endpoint Client**ou, plus rapidement, double-cliquez sur l'icône Bitdefender dans la zone de notification.

1.3. Fenêtre principale du programme

La fenêtre principale de Endpoint Client vous permet de vérifier l'état de la protection et d'effectuer des tâches de sécurité de base (mises à jour et analyses).Tout se trouve à quelques clics. La configuration et l'administration de la protection est réalisée à distance par votre administrateur réseau ou votre fournisseur de services.

Fenêtre principale du programme

La fenêtre est organisée en deux zones principales :

Barre d'outils supérieure
: Vous pouvez vérifier ici l'état de sécurité de votre ordinateur et accéder aux tâches importantes.

Panneaux
: Vous pouvez vérifier ici l'état des modules de protection.

Vous trouverez également des options de support utiles dans la partie inférieure de la fenêtre :

Option	Description
Aide en ligne	Cliquez sur ce lien si vous avez besoin d'aide avec Endpoint Client.
	Cliquez sur cette icône pour des informations sur le produit et de contact.

1.3.1. Barre d'outils supérieure

La barre d'outils supérieure contient les éléments suivants :

- La **zone d'état de sécurité** à gauche de la barre d'outils vous indique si des problèmes affectent la sécurité de votre ordinateur. La couleur de la zone d'état de sécurité change en fonction des problèmes détectés et différents messages s'affichent :
  - **La zone est en vert.**Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.

- **La zone est en jaune.** Des problèmes non critiques affectent la sécurité de votre système.
- **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système.

Vous pouvez voir les problèmes de sécurité détectés en cliquant dans la zone d'état de sécurité.Les problèmes existants seront corrigés par votre administrateur réseau.

- **Événements** vous permet d'accéder à un historique détaillé des événements importants survenus lors de l'activité du produit. Pour plus d'informations, reportez-vous à « Événements » (p. 20).
- **Mise à jour** ouvre la fenêtre d'état de mise à jour et vous permet de requérir une mise à jour. Pour plus d'informations, reportez-vous à « Mises à jour » (p. 18).

1.3.2. Panneaux

La zone des panneaux vous permet de vérifier l'état des modules de protection. Il y a un panneau séparé pour chaque module de protection.

L'état de la protection est indiqué dans le coin supérieur droit du panneau à l'aide des icônes suivantes :

ON La protection est activée.
OFF La protection est désactivée.

Si un module de protection n'est pas installé, un message approprié s'affiche en haut du panneau correspondant.

Les panneaux disponibles dans cette zone sont :

Antimalware

La protection antimalware est la base de votre sécurité. Endpoint Client vous protège en temps réel et à la demande contre toutes sortes de malwares tels que les virus, les chevaux de Troie, les spywares, les adwares etc.

Le panneau Antimalware vous permet d'accéder facilement aux principales tâches d'analyse. Cliquez sur **Analyser** et sélectionnez une tâche dans le menu déroulant :

- **Quick Scan** utilise l'analyse in-the-cloud pour détecter les malwares présents sur votre système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.
- **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.
- L'**Analyse Complète du Système** analyse l'ensemble de votre ordinateur en vue de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Pour des informations sur l'utilisation de ces tâches d'analyse, veuillez vous référer à « Analyse antimalware » (p. 9).

Pare-feu

Le pare-feu vous protège lorsque vous êtes connecté à des réseaux et à Internet en filtrant les tentatives de connexion et en bloquant les connexions suspectes ou risquées.

Pour des informations sur la configuration du pare-feu, cliquez sur le bouton **État du pare-feu**.Voici ce que chaque paramètre signifie :

- **Type de Réseau** - le type de réseau auquel votre ordinateur est connecté. Endpoint Client applique un ensemble de paramètres pare-feu de base en fonction du type de réseau auquel vous êtes connecté.

Type de Réseau	Description
Confiance	Désactiver le Pare-feu pour l'adaptateur concerné.
Domicile/Bureau	Autoriser tout le trafic entre votre ordinateur et les ordinateurs du réseau local.
Public	Tout le trafic est filtré.
Non fiable	Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.

- **Mode Furtif** - si vous pouvez être détecté par d'autres ordinateurs.

État	Description
Activé	Le mode furtif est activé.Votre ordinateur n'est pas visible depuis le réseau local et Internet.
Désactivé	Le mode furtif est désactivé.N'importe qui sur le réseau local ou sur Internet peut détecter votre ordinateur (via la commande ping).
Distant	Votre ordinateur ne peut pas être détecté depuis Internet.Les utilisateurs du réseau local peuvent voir (Via la commande ping) et détecter votre ordinateur .

- **Partage de Connexion Internet (ICS)** - active le support du partage de connexion Internet (ICS).
- **Surveiller les connexions Wi-Fi** - si vous êtes connecté(e) à des réseaux sans fil, des informations s'affichent au sujet d'événements réseau spécifiques (par exemple lorsqu'un nouvel ordinateur rejoint le réseau).

Protection vie privée

Le module Protection Vie Privée vous aide à assurer la confidentialité de vos données personnelles importantes. Il vous protège lorsque vous êtes sur Internet contre les attaques de phishing, les tentatives de fraude, les fuites d'informations confidentielles etc.

Ce module comprend deux fonctionnalités :

- La protection antiphishing assure une navigation web sûre en bloquant les pages web de phishing et les autres pages web potentiellement dangereuses et en informant l'utilisateur.
- Protection des données : empêche la divulgation non autorisée de données sensibles.

Pour des informations sur la configuration de la Protection Vie Privée, cliquez sur le bouton **État de la Protection Vie Privée**.

Contrôle utilisateur

Endpoint Client comprend un ensemble complet de contrôles utilisateur qui aident à appliquer les politiques d'utilisation des ordinateurs et d'Internet. Votre administrateur réseau peut configurer les contrôles utilisateur suivants :

- **Contrôle Web** - permet de filtrer la navigation Web et de définir des restrictions horaires pour l'accès à Internet.À l'aide de ce contrôle, l'administrateur peut explicitement bloquer l'accès à certains sites web ou, au contraire, autoriser uniquement la consultation de sites web utilisés pour les activités professionnelles quotidiennes.
- **Contrôle des applications** - permet de bloquer ou de limiter l'accès à certaines applications.
- **Filtrage par mots-clés** - permet de filtrer l'accès à Internet et à la messagerie en fonction de mots-clés.
- **Filtrage par catégories** - pour bloquer certaines catégories de contenu Web.Par exemple, les sites web de réseaux sociaux ou de partage de fichiers.

Pour découvrir les contrôles utilisateurs configurés pour vous, cliquez sur le bouton **État du contrôle utilisateur**.

1.4. Protection navigation web

Votre administrateur Cloud Security for Endpoints peut configurer les paramètres de sécurité qui impacte votre navigation web. Ces paramètres de sécurité peuvent dépendre de :

- « Barre d'outils Bitdefender » (p. 7)
- « Search Advisor » (p. 7)
- « Pages Web bloquées » (p. 7)

1.4.1. Barre d'outils Bitdefender

Quand votre administrateur Cloud Security for Endpoints l'a installé, la barre d'outils Bitdefender vous informe sur le niveau de sécurité des pages web que vous visitez. La barre d'outils Bitdefender n'est pas votre barre d'outils de navigation web habituelle. Le seul élément qu'elle ajoute au navigateur est un petit bouton en haut de chaque page web. Cliquer sur le bouton, ouvre la barre d'outils.

En fonction de la façon dont Bitdefender classifie la page web, l'un des résultats suivants s'affiche dans la partie gauche de la barre d'outils :

- Le message "Cette page n'est pas sûre" apparaît sur un fond rouge.
- Le message "Nous vous recommandons d'être vigilant" apparaît sur un fond orange.
- Le message "Cette page est sûre" apparaît sur un fond vert.

1.4.2. Search Advisor

Quand il est installé par l'administrateur Cloud Security for Endpoints,Search Advisor évalue les résultats des recherches Google, Bing et Yahoo!, ainsi que tous les liens Facebook et Twitter en plaçant une icône devant chaque résultat. Icônes utilisées et leur signification :

Nous vous déconseillons de consulter cette page web.

Cette page web peut contenir du contenu dangereux. Soyez prudent si vous décidez de la consulter.

Cette page peut être consultée en toute sécurité.

1.4.3. Pages Web bloquées

Selon les politiques de sécurité mises en place par votre administrateur Cloud Security for Endpoints, les paramètres de sécurité spécifiques au navigateur web contre les fraudes Internet et de phishing peuvent être mis en place. Cloud Security for Endpoints peut bloquer automatiquement les pages web de phishing connues (faux site / spoofing) pour vous empêcher de divulguer par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne. En plus de faux site web, d'autres types de fraudes Internet peuvent être supprimées, comme : fraudes d'achat, les escroqueries de type "pour devenir riche rapidement" , les fraudes marketing sur Internet, etc. A la place de la page web frauduleuse, une page d'avertissement spécifique est affichée dans le navigateur pour vous informer que la page web demandée est dangereuse.

Note
Si vous avez besoin d'accéder à une page Web légitime qui est mal détecté et bloqué, merci de contacter votre administrateur Cloud Security for Endpoints pour qu'il puisse mettre en place une dérogation.

1.5. Analyse des périphériques

Endpoint Client peut être configuré pour détecter automatiquement les dispositifs de stockage (CD/DVD, supports de stockage USB, lecteurs mappés du réseau) et vous proposer de les analyser. La fenêtre d'alerte vous fournit des informations sur le périphérique détecté.

Pour analyser le périphérique, cliquez sur **Oui**.Si vous êtes sûr(e) que le périphérique est sain, vous pouvez décider de ne pas l'analyser.

Note
Si plusieurs périphériques sont détectés en même temps, des fenêtres d'alerte s'affichent, l'une après l'autre, pour chacun d'entre eux.

Votre administrateur Cloud Security for Endpoints peut choisir de supprimer les alertes et les fenêtres pop-up Endpoint Client.Dans certains cas, l'analyse du périphérique se lance automatiquement, sans que vous n'ayez à vous en occuper.

Lorsque l'analyse d'un périphérique est en cours, une icône de progression de l'analyse apparaît dans la zone de notification.Vous pouvez double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.Vous pouvez suspendre ou arrêter l'analyse du périphérique à tout moment.Pour plus d'informations, reportez-vous à « Assistant d'analyse antivirus » (p. 13).

1.6. Modifier les paramètres de protection

Endpoint Client est configuré et administré à distance par votre administrateur réseau ou votre fournisseur de services. Vous ne pouvez pas modifier les paramètres de protection.

Si vous avez des questions concernant vos paramètres de protection, veuillez les poser à la personne chargée de la sécurité de votre réseau.

2. Analyse antimalware

Le principal objectif de Endpoint Client est de maintenir votre ordinateur sans malwares. Il y parvient principalement en analysant en temps réel les fichiers à l'accès, les e-mails et tout nouveau fichier téléchargé ou copié sur votre ordinateur. Outre la protection en temps réel, il permet également d'exécuter des analyses pour détecter et supprimer les malwares de votre ordinateur.

Vous pouvez analyser l'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser.Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

2.1. Analyser un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés.Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et sélectionnez **Analyser avec Bitdefender**.L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

2.2. Exécuter une Analyse Rapide

Quick Scan utilise l'analyse 'in-the-cloud' pour détecter les malwares présents sur votre système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour effectuer une analyse rapide, suivez ces étapes :

1. Ouvrez la fenêtre Endpoint Client.
2. Allez dans le panneau **Antimalware**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Rapide** dans le menu déroulant.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.Endpoint Client appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

2.3. Exécuter une Analyse Complète du Système

La tâche d'Analyse Complète du Système analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Note

L'Analyse Complète du système effectuant une analyse approfondie de l'ensemble du système, elle peut prendre quelque temps. Il est donc recommandé d'exécuter cette tâche lorsque vous n'utilisez pas votre ordinateur.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.Pour plus d'informations, reportez-vous à « Configurer et exécuter une analyse personnalisée » (p. 10).

Avant d'exécuter une Analyse Complète du Système, nous vous recommandons ceci :

- Vérifiez que Endpoint Client dispose de signatures de malwares à jour. L'analyse de votre ordinateur à l'aide d'une base de signatures non à jour peut empêcher Endpoint Client de détecter les malwares connus depuis la dernière mise à jour.Pour plus d'informations, reportez-vous à « Mises à jour » (p. 18).
- Fermez tous les programmes ouverts.

Pour exécuter une Analyse Complète du Système, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Client.
2. Allez dans le panneau **Antimalware**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse Complète** dans le menu déroulant.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.Endpoint Client appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

2.4. Configurer et exécuter une analyse personnalisée

Pour configurer une analyse antimalware en détail et l'exécuter, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Client.
2. Allez dans le panneau **Antimalware**.
3. Cliquez sur **Analyser** et sélectionnez **Analyse personnalisée** dans le menu déroulant.

4. Vous pouvez si vous le souhaitez exécuter de nouveau rapidement une analyse personnalisée antérieure en cliquant sur l'entrée correspondante dans la liste des **Analyses récentes** ou des **Analyses favorites**
5. Cliquez sur **Ajouter cible**, cochez les cases correspondant aux emplacements que vous souhaitez analyser à la recherche de malwares puis cliquez sur **OK**.
6. Cliquez sur **Options d'analyse** si vous souhaitez configurer les options d'analyse. Une nouvelle fenêtre s'affiche.Suivez ces étapes :
   a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau d'analyse souhaité.Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

      Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Endpoint Client.Pour configurer les options d'analyse en détail, cliquez sur **Personnaliser**. Vous trouverez des informations à leur sujet à la fin de cette section.
   b. Vous pouvez aussi configurer ces options générales :
      - **Exécuter la tâche en priorité basse .** Décroît la priorité du processus d'analyse. Vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.
      - **Réduire l'assistant d'analyse dans la zone de notification .** Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de l'avancement de l'analyse pour l'ouvrir.
      - Spécifiez l'action à mener si aucune menace n'a été trouvée.
   c. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
7. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

Enregistrer une analyse personnalisée dans les analyses favorites

Lorsque vous configurez et exécutez une analyse personnalisée, elle est automatiquement ajoutée à une liste limitée d'analyses récentes. Si vous pensez réutiliser une analyse personnalisée ultérieurement, vous pouvez choisir de l'enregistrer dans la liste des analyses favorites avec un nom explicite.

Pour enregistrer une analyse personnalisée exécutée récemment dans la liste des analyses favorites, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'analyse personnalisée.

a. Ouvrez la fenêtre Endpoint Client.

b. Allez dans le panneau **Antimalware**.

c. Cliquez sur **Analyser** et sélectionnez **Analyse personnalisée** dans le menu déroulant.

2. Localisez l'analyse souhaitée dans la liste des **Analyses Récentes** .
3. Placez le curseur de la souris sur le nom de l'analyse et cliquez sur l'icône pour ajouter l'analyse à la liste des analyses favorites.
4. Indiquez un nom explicite pour l'analyse.

Les analyses enregistrées en tant que favorites sont signalées à l'aide de l'icône .Si vous cliquez sur cette icône, l'analyse sera retirée de la liste des analyses favorites.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.
- **Types de fichiers.** Vous pouvez régler Endpoint Client pour analyser tous les types de fichiers ou uniquement les applications (fichiers programmes).L'analyse de tous les fichiers consultés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour que l'analyse soit plus rapide.

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes : `386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp`

- **Options d'analyse pour les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

  Note
  L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Endpoint Client pour qu'il analyse les secteurs d'amorçage de votre disque dur.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot.Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser les rootkits.** Sélectionnez cette option pour rechercher des rootkits et des objets masqués à l'aide de ce logiciel.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le Registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
- **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur votre ordinateur.
- **Analyser uniquement les fichiers nouveaux et modifiés.** En n'analysant que les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les keyloggers commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les keyloggers commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.

2.5. Assistant d'analyse antivirus

À chaque fois que vous initierez une analyse à la demande (par exemple en faisant un clic droit sur un dossier et en sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus Endpoint Client s'affichera.Suivez l'assistant pour terminer le processus d'analyse.

Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond.Recherchez l'icône de l'avancement de l'analyse dans la zone de notification.Vous pouvez double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

2.5.1. Étape 1 - Effectuer l'analyse

Endpoint Client commencera à analyser les objets sélectionnés.Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées).Pour plus d'informations, cliquez sur le lien **Plus de statistiques**.

Patientez jusqu'à la fin de l'analyse.L'analyse peut durer un certain temps, suivant sa complexité.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter** puis sur **Oui**. Vous serez alors dirigé automatiquement à la dernière étape de l'assistant.Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe.Voici les options proposées :

- **Mot de passe.** Si vous souhaitez que Endpoint Client analyse l'archive, sélectionnez cette option et entrez le mot de passe.Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.
- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe.Endpoint Client ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Sélectionnez l'option souhaitée et cliquez sur **OK** pour poursuivre l'analyse.

2.5.2. Étape 2 - Sélectionner des actions

À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

Note

Si vous lancez une analyse rapide ou une analyse complète du système, Endpoint Client appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés.Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Prendre les actions appropriées

Endpoint Client appliquera les actions recommandées en fonction du type de fichier détecté :

- **Fichiers infectés .** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Endpoint Client tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine.Cette opération est appelée désinfection.

  Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

  Important

  Pour certains types de malware, la désinfection n'est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichiers suspects.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.Les fichiers suspects n'ont pas pu être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

  Par défaut, les fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

- **Archives contenant des fichiers infectés.**
  - Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.

– Si une archive contient à la fois des fichiers infectés et des fichiers sains, Endpoint Client tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer

Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Endpoint Client tentera de supprimer les fichiers infectés et de reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Ne pas entreprendre d'action

Aucune action ne sera menée sur les fichiers détectés.Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

2.5.3. Étape 3 - Récapitulatif

Une fois que les problèmes de sécurité auront été corrigés par Endpoint Client, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre.Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

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

Important

Dans la plupart des cas, Endpoint Client désinfecte les fichiers infectés qu'il détecte ou isole l'infection. Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement.Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

2.6. Consulter les Journaux d'Analyse

À chaque fois que vous effectuez une analyse, un journal d'analyse est créé. Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter les journaux d'analyse ultérieurement, suivez ces étapes :

1. Ouvrez la fenêtre Endpoint Client.

2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Cliquez sur **Antimalware** dans le menu de gauche.Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
4. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment.Cliquez sur un événement pour afficher des informations à son sujet.
5. Pour ouvrir le journal d'analyse, cliquez sur **Journal**.Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

3. Mises à jour

Dans un monde où les cybercriminels recherchent sans cesse de nouveaux moyens de nuire, il est essentiel de maintenir sa solution de sécurité à jour afin de conserver une longueur d'avance sur eux.

Si vous disposez d'une connexion Internet haut débit ou DSL, Endpoint Client s'en occupe automatiquement. Par défaut, il recherche des mises à jour lorsque vous allumez votre ordinateur ou toutes les **heures**.Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.

Note

La fréquence des mises à jour automatiques par défaut peut être modifiée par votre administrateur réseau. Pour plus d'informations, reportez-vous à « Qu'est-ce que la fréquence de mise à jour automatique ? » (p. 19).

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

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 Bitdefender à la demande.Pour plus d'informations, reportez-vous à « Mise à jour en cours » (p. 19).

3.1. Types de mise à jour

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

- **Mises à jour des signatures de malwares** - avec l'apparition de nouvelles menaces, les fichiers contenant des signatures de malwares doivent être mis à jour pour garantir une protection permanente, actualisée.
- **Mise à jour du produit** - quand une nouvelle version du produit est mise en circulation, elle contient de nouvelles fonctionnalités et techniques d'analyse, introduites dans le but d'améliorer les performances du logiciel.

  La mise à niveau d'un produit est une version release principale.

3.2. Vérifier que votre protection est à jour

Pour vérifier que votre protection est à jour, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Client.
2. Cliquez sur le bouton **Mise à jour** de la barre d'outils supérieure.
3. Vous pouvez voir l'état de la mise à jour et l'heure de la dernière recherche et installation de mise à jour.

Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Dans la fenêtre principale, cliquez sur **Événements** dans la barre d'outils supérieure.
2. Cliquez sur **Mise à jour** dans le menu de gauche.

Vous pouvez savoir quand des mises à jour ont été lancées et obtenir des informations à leur sujet (si elles ont été ou non réussies, si elles nécessitent un redémarrage pour que leur installation se termine).Si nécessaire, redémarrez le système dès que possible.

3.3. Mise à jour en cours

Pour effectuer des mises à jour, une connexion à Internet est requise.

Pour lancer une mise à jour, choisissez l'une des options suivantes :

- Ouvrez la fenêtre Endpoint Client, cliquez sur le bouton **Mise à jour** de la barre d'outils supérieure puis sur **Mise à jour**.
- Faites un clic droit sur l'icône de Bitdefender de la zone de notification et sélectionnez **Mettre à jour maintenant**.

Le module de Mise à jour se connectera au serveur de mise à jour de Bitdefender et recherchera des mises à jour. Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.

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.

3.4. Qu'est-ce que la fréquence de mise à jour automatique ?

Pour connaître la fréquence des mises à jour automatiques, suivez ces étapes :

1. Ouvrez la fenêtre Endpoint Client.
2. Cliquez sur le bouton **Mise à jour** de la barre d'outils supérieure.
3. Consultez le champ **Mise à jour automatique** pour voir la fréquence des mises à jour automatiques.

4. Événements

Endpoint Client tient un journal détaillé des événements concernant son activité sur votre ordinateur (comprenant également les activités surveillées par le Contrôle Utilisateur).Les événements sont un outil très important pour la surveillance de votre protection Bitdefender.Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.

Pour consulter le journal des événements, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Client.
2. Cliquez sur le bouton **Événements** de la barre d'outils supérieure.
3. Sélectionnez la catégorie d'événement dans le menu de gauche. Les événements sont regroupés dans les catégories suivantes :
   - **Antimalware**
   - **Pare-feu**
   - **Protection vie privée**
   - **Contrôle utilisateur**
   - **Mise à jour**
   - **Divers**

   Une étiquette rouge indiquant le nombre d'événements critiques ou de messages d'erreurs non lus s'affiche au-dessus du nom de chaque catégorie.

Une liste d'événements est disponible pour chaque catégorie. Pour des informations sur un événement de la liste, cliquez dessus. Des détails sur l'événement s'affichent alors dans la partie inférieure de la fenêtre. Chaque événement est accompagné des informations suivantes : une brève description, l'action que Bitdefender a appliquée et la date et l'heure de l'événement.

Vous pouvez filtrer les événements en fonction de leur importance. Il y a trois types d'événements, chacun étant signalé par une icône spécifique :

Les événements **Informations** indiquent des opérations réussies.
Les événements **Avertissement** signalent des problèmes non critiques.
Les événements **critiques** signalent des problèmes critiques.

Pour vous aider à gérer facilement les événements enregistrés, chaque section de la fenêtre Événements fournit des options permettant de filtrer ou de marquer comme lus tous les événements de cette section. Les événements peuvent uniquement être supprimés par votre administrateur réseau.

5. Obtenir de l’aide

Pour des problèmes ou des questions concernant Endpoint Client, veuillez contacter votre administrateur réseau ou votre fournisseur de services.

Pour des informations sur le produit et de contact, exécutez l'une des actions suivantes :

- Ouvrez la fenêtre Endpoint Client et cliquez sur l'icône **Infos** dans le coin inférieur droit.
- Faites un clic droit sur l'icône Bitdefender de la zone de notification et sélectionnez **À propos de** dans le menu.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes tels 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 d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son 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 a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariant 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.

Applette Java

Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il 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 par le fait qu'ils sont régis par un protocole de sécurité strict.

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

Archive

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

Un 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.

Chemin

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

La connexion entre deux points, telle le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

Code malveillant

"Malware" est un terme générique regroupant les logiciels conçus pour faire du tort - la contraction de "malicious software" (logiciels malveillants". L'emploi de ce terme n'est pas encore universel, mais sa popularité pour désigner les virus, les chevaux de Troie, les vers et les codes mobiles malveillants progresse.

Cookies

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.

Disk drive

C'est une 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).

E-mail

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.

Extension de fichier

La 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 n'en supportent pas plus de trois). Exemples : "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

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

Fichier journal (Log)

Un fichier qui établit une liste des actions survenues. Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés ayant été détectés.

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 chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par des cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion et des numéros de sécurité sociale).

Ligne de commande

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

Mémoire

Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Mise à jour

Une 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 a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

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 (plugins) pour certains formats.

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.

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 placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.

Phishing

Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du mail. Cet e-mail dirige 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.

Port

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs 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.

Programmes empaquetés

Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer 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 comprime les fichiers remplace la série d'espaces par un caractère spécial série 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.

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 principal 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 réseau, s'ils incluent les logiciels appropriés.

Les Rootkits ne sont pas malveillants 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.

Scripts

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

Secteur de boot

Un 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.

Signature du malware

Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares. Les signatures sont également utilisées pour supprimer le code malveillant des fichiers infectés.

La base de données de signatures de malwares de Bitdefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares de Bitdefender.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des e-mails « 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 un tiers. Les spywares peuvent également récupérer des informations sur des adresses e-mail, des mots de passe ou même, des numéros de cartes bancaires.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière 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.

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.

Télécharger

Copier 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.

Trojan (Cheval de Troie)

Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. 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'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, 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.

Ver

Un 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.

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 capable de se copier continuellement est relativement facile à créer. Même un virus simple de ce type 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 et d'échapper aux systèmes de sécurité.

Virus de boot

Un 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.

Virus Macro

Un 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.

Virus polymorphique

Un 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.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.