Bitdefender

Bitdefender Endpoint Security Tools pour Windows

MANUEL D'UTILISATION

Bitdefender Endpoint Security Tools pour Windows
Manuel d'utilisation

Date de publication 2019.11.29

Mentions légales

Bitdefender

Table des matières

Préface

1. Objectifs et destinataires

Cette documentation est conçue pour les utilisateurs finaux d'**Bitdefender Endpoint Security Tools**, le logiciel client 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.

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 Bitdefender Endpoint Security Tools.

« Analyse antimalware » (p. 13)

Découvrez comment exécuter des analyses antimalwares.

« Mises à jour » (p. 25)

Découvrez les mises à jour Bitdefender Endpoint Security Tools.

« Événements » (p. 27)

Vérifiez l'activité de Bitdefender Endpoint Security Tools.

« Obtenir de l'aide » (p. 41)

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 meilleure lisibilité. Leur aspect et signification sont présentés dans le tableau ci-dessous.

Apparence	Description
business-docs@bitdefender.com	Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. iv)	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 consiste simplement en une courte observation. Bien que vous puissiez les ignorer, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien vers un thème proche.

Important
Cette icône requiert votre attention et il n'est pas recommandé de la passer. Elle fournit généralement des informations non essentielles mais importantes.

4. Commentaires

Écrivez-nous pour nous signifier comment ce guide pourrait être amélioré, et nous aider à vous fournir la meilleure documentation possible.

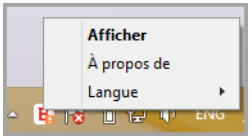
Faites le nous savoir en nous écrivant à cette adresse business-docs@bitdefender.com.

1. POUR DÉMARRER

Bitdefender Endpoint Security Tools est un programme de sécurité informatique entièrement automatisé, administré à distance par votre administrateur réseau. Une fois installé, il vous protège contre toutes sortes de malwares (virus, spywares et chevaux de Troie), attaques du réseau, phishing et vol de données. Il peut aussi être utilisé pour renforcer les politiques de sécurité vis-à-vis de l'utilisation des ordinateurs et d'Internet. Bitdefender Endpoint Security Tools prendra la plupart des décisions de sécurité à votre place et vous affichera rarement des fenêtres d'alertes. Les détails concernant les actions prises sont disponibles dans le fil des **Événements**.

1.1. Icône de la zone de notification

Lors de l'installation, Bitdefender Endpoint Security Tools place une icône B dans la zone de notification. Si vous double-cliquez sur cette icône, la fenêtre principale s'affichera. Si vous faites 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 Bitdefender Endpoint Security Tools.
- **A propos** - ouvre une fenêtre contenant des informations sur Bitdefender Endpoint Security Tools et indique où chercher de l'aide en cas de problème inattendu. Cette fenêtre comprend aussi un lien vers la Politique de confidentialité de Bitdefender.
- **Langue** - vous permet de changer la langue de l'interface utilisateur.
- **Power User** - vous permet également d'accéder et de modifier les paramètres de sécurité, après avoir saisi le mot de passe dans la fenêtre de connexion. Control Center est informé lorsqu'un endpoint est en mode Power User et l'administrateur de Control Center peut toujours écraser les paramètres de sécurité locaux.

> **Important**
> Cette option n'est valable que si elle est accordée par l'administrateur réseau via les paramètres de politiques.
> Cette option n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

L'icône Bitdefender Endpoint Security Tools de la zone de notification vous signale la présence de problèmes affectant votre ordinateur en modifiant son apparence :

Critical issues affect the security of the system.
Some issues affect the security of the system.

Note
L'administrateur réseau peut choisir de masquer l'icône de la zone de notification.

1.2. Fenêtre principale

La fenêtre principale de Bitdefender Endpoint Security Tools vous permet de consulter l'état de la protection et d'effectuer des tâches d'analyse. Tout se trouve à quelques clics. La configuration et l'administration de la protection sont réalisées à distance par votre administrateur réseau.

Pour accéder à l'interface principale de la Bitdefender Endpoint Security Tools, accédez au menu Démarrer de Windows puis suivez le chemin d'accès **Démarrer → Tous les programmes → Bitdefender Endpoint Security Tools → Open Security Console**ou, plus rapide, double-cliquez sur l'icône Bitdefender Endpoint Security Tools dans la zone de notification.

Fenêtre principale

La fenêtre est organisée en deux zones principales :

- Zone d'état
- Chronologie des événements

1.2.1. La zone d'état

La zone d'**état** fournit des informations utiles au sujet de la sécurité du système.

Zone d'état

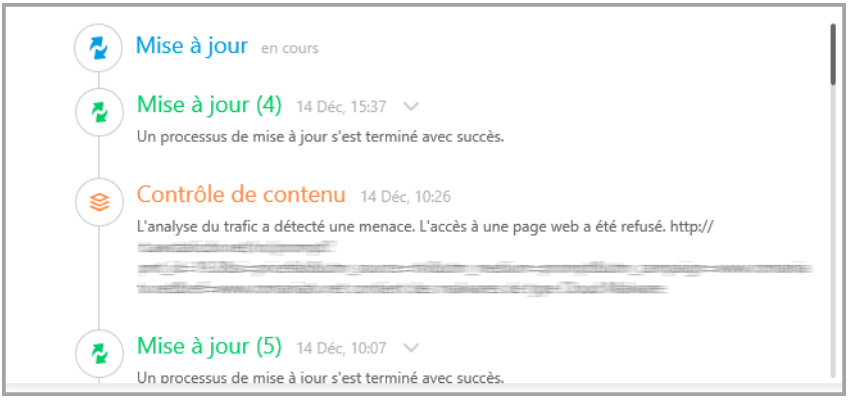
Vous pouvez identifier facilement l'état de sécurité actuel grâce au symbole d'état qui apparaît à gauche de la zone d'état :

- **Coche verte.** Il n'y a aucun problème à réparer. Votre ordinateur et vos données sont protégés.
- **Point d'exclamation jaune.** Des problèmes non critiques affectent la sécurité de votre système.
- **Croix rouge.** Des problèmes critiques affectent la sécurité de votre système.

En plus du symbole d'état, un message d'état de sécurité détaillé s'affiche à droite de la zone d'état. Vous pouvez voir les problèmes de sécurité détectés en cliquant sur la zone d'état. Les problèmes existants seront corrigés par votre administrateur réseau.

1.2.2. Chronologie des événements

Bitdefender Endpoint Security Tools tient un journal détaillé des événements concernant son activité sur votre ordinateur, comprenant les activités surveillées par le Contrôle de contenu.

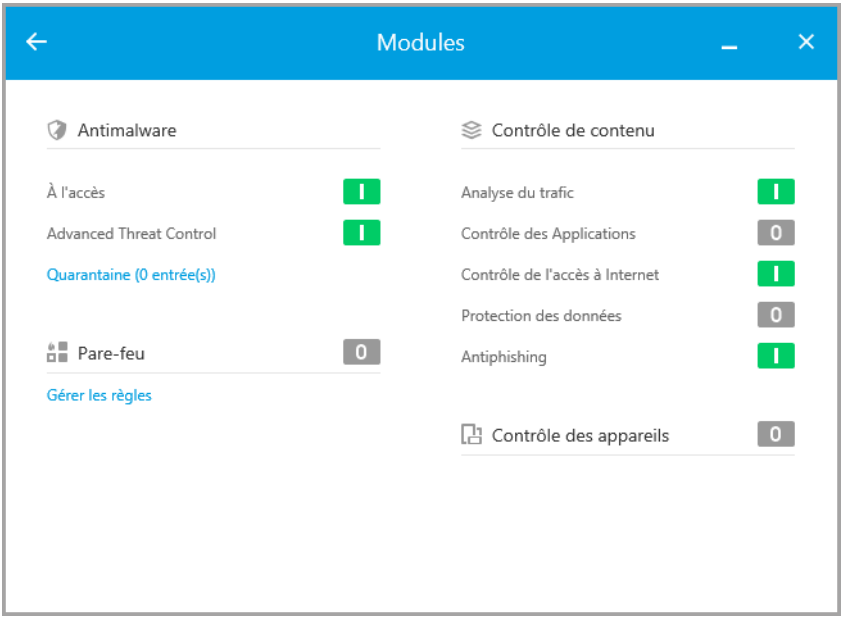


Chronologie des événements

Le fil d'actualité **Événements** sont un outil important pour la surveillance de votre protection Bitdefender. Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, ou que des malwares ont été détectés sur votre ordinateur.

1.3. La fenêtre Modules

La fenêtre **Modules** affiche des informations utiles au sujet de l'état et de l'activité des modules de protection installés. Pour ouvrir la fenêtre **Modules**, cliquez sur le bouton **Modules** dans le fenêtre principale de Bitdefender Endpoint Security Tools.



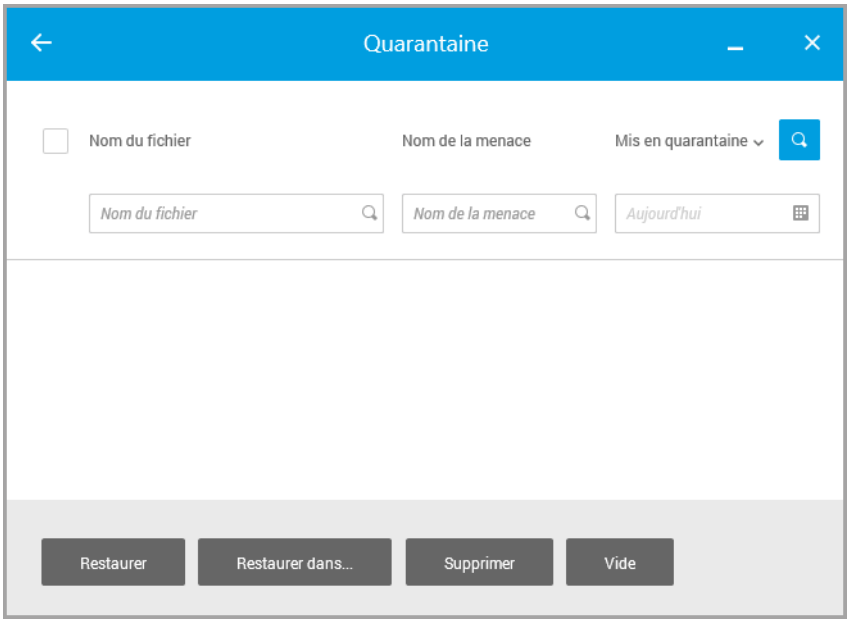
Fenêtre Modules

Antimalware

La protection antimalware est la base de votre sécurité. Bitdefender Endpoint Security Tools 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.

- **à la demande**. L'analyse à l'accès empêche que de nouveaux malwares accèdent au système en analysant les fichiers locaux et du réseau (lorsqu'ils sont ouverts, déplacés, copiés ou exécutés), les secteurs d'amorçage et les applications potentiellement indésirables.

- **HyperDetect**. HyperDetect expose les attaques avancées et les activités suspectes dès la phase de pré-exécution. Cette couche de sécurité intègre des modèles de Machine Learning et une technologie de détection avancée des attaques furtives.
- **Advanced Threat Control**. Il surveille en permanence les applications en cours dans l'endpoint, à la recherche d'actions ressemblant à du comportement de malwares. Advanced Threat Control essaiera de désinfecter automatiquement le fichier détecté.
- La **Quarantaine** affiche ici la liste des fichiers en quarantaine, leur chemin d'origine, la date et l'heure de leur mise en quarantaine et leur état de sécurité. Utilisez le bouton du bas afin de supprimer ou de restaurer le fichier désiré. Si vous désirez supprimer tous les fichiers de la quarantaine, cliquez sur le bouton **Vider**.



Quarantaine

Contrôle de contenu

Le module Contrôle de contenu vous protège lorsque vous êtes sur Internet contre les attaques de phishing, les tentatives de fraude, la divulgation de données personnelles et le contenu web inapproprié. Il comprend également un ensemble complet de contrôles utilisateur qui aident l'administrateur réseau à appliquer les politiques d'utilisation des ordinateurs et d'Internet.

- **Analyse Trafic.** Ce composant empêche le téléchargement de malwares dans l'endpoint en analysant les e-mails entrant et le trafic Web en temps réel. Les e-mails sortants sont analysés afin d'éviter que des malwares n'infectent d'autres endpoints.
- **Liste noire des applications.** Ce composant empêche d'accéder à des applications non autorisées dans votre entreprise. L'administrateur est responsable de la création des règles pour les applications autorisées dans l'entreprise.
- **Contrôle accès Web.** Ce composant vous protège contre l'accès à des sites Web dangereux grâce aux règles définies par l'administrateur.
- **La Protection des données.** Ce composant empêche la divulgation non autorisée de données sensibles grâce à des règles définies par l'administrateur.
- **Antiphishing.** Ce composant bloque automatiquement les pages web de phishing connues afin d'empêcher que les utilisateurs ne divulguent par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne.
- **Network Attack Defense.** Network Attack Defense détecte les techniques d'attaque réseau utilisée pour accéder à certains endpoints telles que les attaques par force brute, les exploits réseaux et les outils de vol de mots de passe.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

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.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

Contrôle des appareils

Il permet d'éviter la fuite de données confidentielles et les infections de malwares par des appareils externes connectés aux endpoints. Cela passe par l'application de règles de blocage et d'exclusions, via une politique, à un large éventail de types d'appareils. L'administrateur est responsable de la gestion des permissions pour les types d'appareils suivants :

- Adaptateurs Bluetooth
- Appareils CDROM
- Lecteurs de disquettes
- IEEE 1284.4
- IEEE 1284.4
- Périphériques de traitement d'images
- Modems
- Lecteurs de bande
- Mobile Windows
- Ports COM/LPT
- SCSI RAID
- Imprimantes
- Cartes réseau
- Adaptateurs réseau sans fil
- Stockage interne et externe

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

Contrôle des applications

Le module de Contrôle des applications bloque l'exécution des applications et process non autorisés Le Contrôle des applications diminue la fréquence et l'impact des incidents liés à des malwares, en réduisant la surface d'attaque et les vulnérabilités et en contrôlant le nombre d'applications non autorisées au sein de votre réseau.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

Sandbox Analyzer

Offrant une puissante couche de protection contre les menaces avancées, le module Sandbox Analyzer effectue des analyses automatiques détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender. Le Sandbox Analyzer utilise un large éventail de technologies propriétaires afin d'exécuter des charges dans un environnement virtuel confiné hébergé par Bitdefender, d'analyser leur comportement et de signaler toute modification observée au sein du système, révélatrice d'une intention malveillante.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

Chiffrement de volume

Le module de chiffrement de volume vous permet de procéder à un chiffrement complet du disque dur, via Bitlocker sur les machines Windows. Vous pouvez chiffrer et déchiffrer des volumes d'amorçage et de non-amorçage en un simple clic, tandis que GravityZone gère l'ensemble du processus, avec une intervention minime des utilisateurs. En prime, GravityZone stocke les clés de récupération nécessaires pour débloquer les volumes, lorsque les utilisateurs oublient leurs mots de passe.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

Capteur EDR

Le Capteur (Endpoint Detection and Response) collecte et gère les données sur le comportement des applications et des endpoints, et les compile sous forme de rapports. Certaines informations sont traitées en local, tandis que les ensembles de données plus complexes sont envoyés à un composant backend de GravityZone.

Le module a une faible empreinte en matière de bande passante du réseau et de consommation de ressources matérielles.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

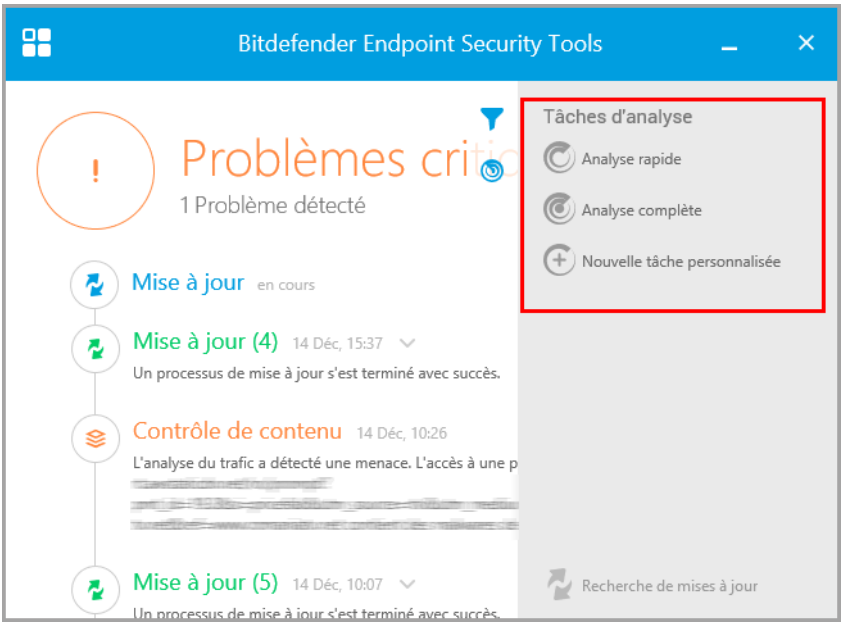
Gestion des correctifs

Patch Management veille à ce que le système d'exploitation et les applications logicielles restent à jour. Ce module comprend de nombreuses fonctionnalités, telles que l'analyse des patchs à la demande/planifiée, le patching automatique/manuel, ou l'édition de rapports sur les patchs manquants.

Note
Ce module n'est pas disponible pour Bitdefender Endpoint Security Tools for Windows Legacy.

1.4. Menu Actions

Pour définir ou exécuter une tâche d'analyse, cliquez sur le bouton **Actions** pour ouvrir le menu **Actions**. C'est également là que vous pouvez vérifier les mises à jour.



Menu Actions

Analyse rapide

Utilise l'analyse "sur le nuage" pour détecter les logiciels malveillants 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 du système

Analyse l'ensemble de votre ordinateur afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Analyse Personnalisée

Vous permet de choisir les localisations à analyser et pour configurer les options d'analyse.

Recherche de mises à jour

Si une mise à jour est détectée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour configurés par votre administrateur réseau.

2. ANALYSE ANTIMALWARE

Le principal objectif d'Bitdefender Endpoint Security Tools 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.

A tout moment durant l'analyse, vous pouvez voir le progrès dans le fil **Événements**.

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 Endpoint Security Tools**. L'analyse va commencer et vous pouvez surveiller la progression sur le fil **Événements**.

A la fin de l'analyse, vous verrez les résultats. Pour plus d'informations, cliquez sur **Voir Journal**.

2.2. Exécuter une analyse rapide

L'**analyse rapide** utilise des technologies d'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.

L'**analyse rapide** est pré-configurée pour autoriser l'analyse :

- Process en cours d'exécution, secteurs de démarrage et registre.
- Emplacements critiques de la mémoire
- Fichiers nouveaux et modifiés

- Pour les rootkits, adwares, spywares et dialers à des emplacements critiques de l'OS comme : `%windir%\\system32\\`, `%temp%`, `/etc`, `/lib`.
- Pour les applications potentiellement indésirables (PUA).

Pour effectuer une analyse rapide, suivez ces étapes :

1. Ouvrir la fenêtre Bitdefender Endpoint Security Tools.
2. Cliquez sur le bouton **Actions** dans le coin en haut à droite.
3. Cliquez sur **Analyse rapide**.
4. Patientez jusqu'à la fin de l'analyse. Vous pouvez voir la progression de l'analyse dans le fil d'actualité. Une fois terminée, cliquez sur **Voir Journal** pour voir les résultats détaillés.

2.3. Exécuter une Analyse Complète

La tâche **Analyse Complète** analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, logiciels-espions, publiciels, rootkits et autres.

Note
Parce que l'**Analyse Complète** effectue une analyse approfondie de l'ensemble du système, elle peut donc prendre un certain 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. 15).

Avant de lancer une analyse complète, assurez-vous que Bitdefender Endpoint Security Tools est à jour avec les dernières signatures de malwares. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Bitdefender Endpoint Security Tools de détecter les logiciels malveillants identifié depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à « Mises à jour » (p. 25).

L'**analyse complète** est pré-configurée pour autoriser l'analyse :

- Process en cours d'exécution, secteurs de démarrage et registre.

- Les archives d'e-mails et les fichiers réseaux de tous les disques, même amovibles.
- Pour les rootkits, adwares, spywares, keyloggers et dialers , sur tous les disques, même amovibles.
- Applications potentiellement indésirables (PUA)
- Cookies du navigateur

Pour effectuer une analyse complète, suivez ces étapes :

1. Ouvrir la fenêtre Bitdefender Endpoint Security Tools.
2. Cliquez sur le bouton **Actions** dans le coin en haut à droite.
3. Cliquez sur **Analyse complète**.
4. Patientez jusqu'à la fin de l'analyse. Vous pouvez voir la progression de l'analyse dans le fil d'actualité. Cliquez sur **Voir Détails** pour voir les détails de l'analyse en cours. Vous pouvez également mettre en pause, reporter ou arrêter l'analyse.
5. Bitdefender Endpoint Security Tools appliquera automatiquement les actions recommandées aux fichiers détectés. Une fois terminée, cliquez sur **Voir Journal** pour voir les résultats détaillés.

2.4. Configurer et exécuter une analyse personnalisée

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

1. Ouvrir la fenêtre principale Bitdefender Endpoint Security Tools.
2. Cliquez sur le bouton **Actions** dans le coin en haut à droite.
3. Cliquez sur **Nouvelle analyse personnalisée**. La fenêtre **Analyse personnalisée** va s'ouvrir.
4. Configurez les otpions d'analyse : **Agressive**, **Normale**, **Permissive**, **Personnalisée**. Reportez-vous à la description sous l'option pour identifier le niveau d'analyse le plus adapté à vos besoins.
5. Sélectionnez la cible de l'analyse sur le panneau de gauche.
6. Vous pouvez également configurer l'analyse pour exécuter la tâche avec une priorité basse en sélectionnant la case correspondante. Cela diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter

à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.

Après avoir configuré l'analyse personnalisée, vous pouvez la sauvegarder comme favorite. Pour ce faire, saisissez un nom et cliquez sur le bouton **Favorite** .

Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender Endpoint Security Tools. Pour configurer les options d'analyse en détail, cliquez sur **Personnalisée** puis **Configuration**.

Vous pouvez également configurer et réaliser une analyse personnalisée en utilisant l'utilitaire en ligne de commande du produit. Pour plus d'informations, consultez le chapitre « Utilisation de l'interface en ligne de commande » (p. 29).

2.4.1. Types de fichiers

Dans l'onglet **Types de fichiers**, spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer l'agent de sécurité afin qu'il analyse tous les fichiers (quelle que soit leur extension), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses.

L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement peut être utilisée pour effectuer une analyse plus rapide. Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques 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.

Analyser les archives de messagerie

Sélectionnez cette option si vous souhaitez permettre l'analyse de fichiers de messagerie et de bases de données de messagerie, y compris de formats de fichiers tels que `.eml`, `.msg`, `.pst`, `.dbx`, `.mbx`, `.tbb` et d'autres.

2.4.2. À analyser?

Dans l'onglet **Analyse**, cochez les cases correspondantes pour activer les options d'analyse souhaitées.

Analyser les secteurs d'amorçage

Vous pouvez paramétrer Bitdefender Endpoint Security Tools pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.

Rechercher les rootkits

Sélectionnez cette option pour rechercher des rootkits et des objets cachés 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.

Rechercher des enregistreurs de frappe
Sélectionnez cette option pour rechercher les logiciels keyloggers.

Rechercher des applications potentiellement indésirables
Un Logiciel Potentiellement Indésirable (LPI) est un programme qui peut être indésirable sur l'ordinateur et peut provenir d'un logiciel gratuit. De tels programmes peuvent être installés sans le consentement de l'utilisateur (alors appelés Adware) ou sont inclus par défaut dans le kit d'installation rapide. Les effets possibles de ces programmes sont l'affichage de pop-ups, l'installation indésirable de barre d'outils dans le navigateur par défaut ou le lancement de plusieurs programmes en arrière-plan qui ralentissent les performances du PC.

Analyser que les nouveaux fichiers et ceux modifiés
En analysant uniquement 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.

Analyser les cookies
Sélectionnez cette option pour analyser les temoins stockés par les navigateurs sur votre ordinateur.

2.4.3. Que faire ?

Dans l'onglet **Actions**, configurez l'action qui doit être exécutée sur les fichiers détectés, s'il y en a.

Fichier(s) infecté(s)
Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.

Fichiers suspects
Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

Rootkits

Les rootkits sont des logiciels spécialisés utilisés pour masquer des fichiers au système d'exploitation. Bien que n'étant pas malveillants par nature, les rootkits sont souvent utilisés pour masquer des malwares ou la présence d'un intrus dans le système.

Action automatique

Selon le type de fichiers détectés, une ou plusieurs options sont possibles :

Supprimer

Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Bitdefender Endpoint Security Tools 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.

Ignorer

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.

Déplacer en quarantaine

Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection.

Désinfecter

Supprime le code malveillant du fichier infecté et reconstruit le fichier d'origine.

2.5. 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 la fenêtre principale, une fois l'analyse terminée, en cliquant sur **Voir Journal**.

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

1. Ouvrir la fenêtre principale Bitdefender Endpoint Security Tools.

2. Cliquez sur le bouton **Filtre** pour ouvrir le menu **Filtres**.
3. Cliquez sur le bouton **Antimalware**. Ici, vous trouverez tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses récentes, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
4. 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.

3. UTILISER LE MODULE DE CHIFFREMENT DE VOLUME

Le module de chiffrement de volume vous permet de procéder à un chiffrement complet du disque sur votre système Windows grâce aux politiques définies par votre administrateur sécurité.

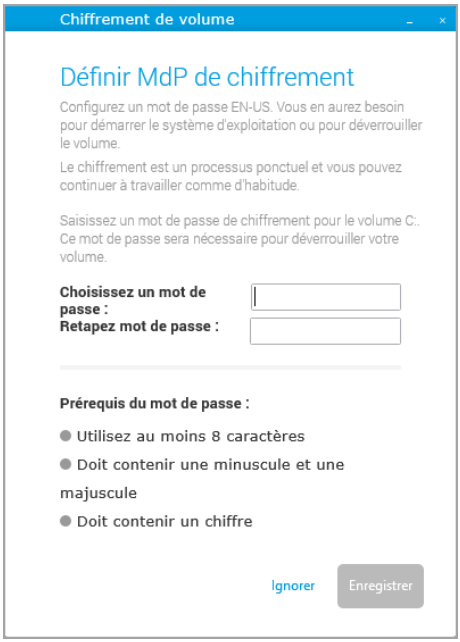
3.1. Chiffrement de votre système

Lorsqu'une politique de chiffrement est appliquée à votre système Windows :

1. Une fenêtre de configuration vous invite à saisir :
   - un numéro d'identification personnel (code PIN) si le système est équipé d'un module TPM (Trusted Platform Module). C'est notamment le cas des ordinateurs portables récents.

     Note
     Si votre système est équipé d'un module TPM, votre administrateur sécurité peut configurer une politique de chiffrement automatique des volumes (sans PIN).

   - un mot de passe si le système n'est pas équipé d'un module TPM. Le mot de passe est également requis si le module TPM n'est pas fonctionnel ou détecté par Bitdefender Endpoint Security Tools.



2. Cliquez sur le bouton **Sauvegarder**. Le chiffrement démarre immédiatement, en commençant par le volume d'amorçage.

   Vous pouvez reporter le chiffrement en cliquant sur **Reporter**. Mais après un certain temps, la fenêtre réapparaîtra pour vous inviter à configurer un code PIN ou un mot de passe de chiffrement.

Un seul code PIN ou mot de passe suffit pour chiffrer tous les volumes (volumes d'amorçage et autres) des disques fixes, des ordinateurs de bureau et des ordinateurs portables. Les disques amovibles ne sont pas chiffrés. Pour plus d'informations sur la configuration du code PIN ou du mot de passe de chiffrement, consultez cet article de la base de connaissances.

Après le chiffrement, vous pourriez avoir à saisir le code PIN ou le mot de passe à chaque démarrage du système Windows, sur l'écran d'authentification. Cela dépend de la politique de sécurité appliquée à votre système.

Si vous oubliez votre code PIN ou votre mot de passe de chiffrement, contactez votre administrateur sécurité.

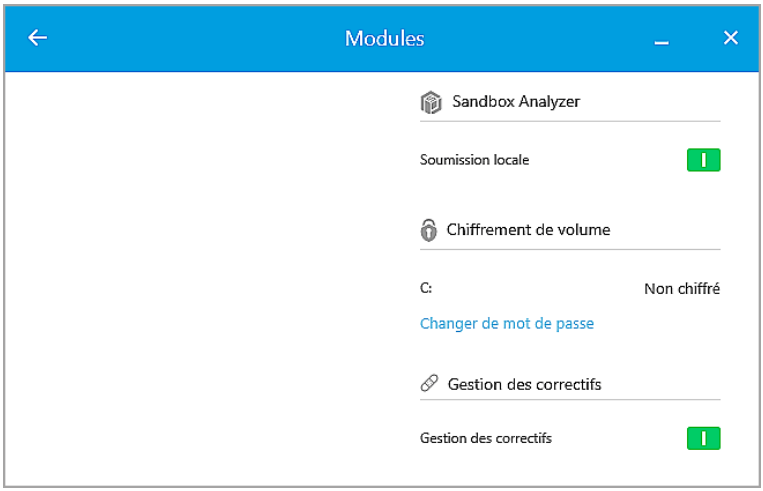
3.2. Déchiffrement de votre système

Lors de l'application d'une politique de déchiffrement les disques chiffrés sont déchiffrés automatiquement, sans aucune intervention de votre part. Toutefois vous ne pouvez pas déchiffrer le système par vous-même tant qu'une politique de chiffrement est active.

3.3. Vérification de l'état de chiffrement

Voici comment vérifier l'état de chiffrement de votre système :

1. Dans La zone de notification, double-cliquez sur l'icône pour ouvrir l'interface utilisateur Bitdefender Endpoint Security Tools.
2. Dans le coin supérieur droit, cliquez sur le bouton pour ouvrir la fenêtre **Modules**.
3. Allez dans la section **Chiffrement de volume**, qui vous permet de voir quels sont les modules chiffrés et ceux qui ne le sont pas.



3.4. Modifier le code PIN ou le mot de passe de chiffrement

Voici comment changer le code PIN ou le mot de passe de chiffrement :

1. Cliquez sur le nom du disque chiffré dans la fenêtre principale de l'interface utilisateur Bitdefender Endpoint Security Tools.
2. Cliquez sur le bouton **Changer mot de passe**.
3. Dans la fenêtre de configuration, saisissez le nouveau code PIN ou mot de passe.
4. Cliquez sur le bouton **Sauvegarder**.

4. 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 êtes connecté à Internet par câble ou DSL, Bitdefender Endpoint Security Tools s'en occupera automatiquement. Par défaut, des mises à jour sont recherchées au démarrage de votre ordinateur puis toutes les **heures** après cela.

Note

La fréquence des mises à jour automatiques par défaut peut être modifiée par votre administrateur réseau.

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. 26).

4.1. Types de mise à jour

Les Mises à jour existent sous les formes suivantes :

- **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.

4.2. Vérifier que votre protection est à jour

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

1. Faites un clic droit sur l'icône de Bitdefender Endpoint Security Tools dans la zone de notification et sélectionnez **À propos de**.
2. 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 le bouton **Filtre** pour ouvrir le menu **Filtres**.
2. Cliquez sur le bouton **Mettre à jour**. Les dernières mises à jour seront affichées dans le fil **Événements**.

   Vous pouvez voir 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.

4.3. Mise à jour en cours

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

Pour commencer une mise à jour :

- Double-cliquez sur l'icône Bitdefender Endpoint Security Tools dans la barre de lancement rapide.
- Cliquez sur le bouton **Actions** pour ouvrir le menu **Actions**.
- Cliquez **Cherchez les mises à jour**. 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 sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour configurés par votre administrateur réseau.

Important
Si nécessaire, redémarrez le système dès que possible. Il est recommandé de le faire dès que possible

5. ÉVÉNEMENTS

Bitdefender Endpoint Security Tools affiche un journal détaillé des événements concernant son activité sur votre ordinateur, comprenant les activités de l'ordinateur surveillées par le Contrôle de contenu et les applications bloquées par le Contrôle des applications. Le fil d'actualité **Événements** sont un outil 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 logiciels malveillants détectés sur votre ordinateur, etc. Pour consulter le journal des événements, procédez comme suit :

1. Ouvrir la fenêtre principale Bitdefender Endpoint Security Tools.
2. Tous les événements sont affichés dans le fil d'actualité **Événements**.
3. Cliquez sur le bouton **Filtre** pour ouvrir le menu **Filtres**.
4. Sélectionnez la catégorie d'événement dans le menu. Les événements sont regroupés dans les catégories suivantes :
   - **Paramètres généraux**
   - **Antimalware**
   - **Pare-feu**
   - **Mettre à jour**
   - **Contrôle de contenu**
   - **Contrôle des appareils**
   - **Contrôle des applications**
   - **Sandbox Analyzer**
   - **Chiffrement de volume**

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. Pour des informations détaillées sur un événement de la liste, cliquez sur **Voir Journal**.

Vous pouvez également filtrer les événements par ordre d'importance au niveau de la protection. Il existe trois types d'événements :


indique des opérations réussies.


indique des problèmes non critiques.


indique des problèmes critiques.

Quelques uns des problèmes critiques et non critiques affichés dans le fil d'actualité **Événements** sont associés avec les actions recommandées afin de les résoudre.

6. UTILISATION DE L'INTERFACE EN LIGNE DE COMMANDE

Bitdefender Endpoint Security Tools vous permet d'exécuter automatiquement des tâches d'analyse locale à la demande et des mises à jour en utilisant la Console du produit, une interface en ligne de commande qui se trouve dans le dossier d'installation du produit sur vos machines Windows.

L'interface en ligne de commande de BEST a deux modes de fonctionnement :

- **Plusieurs commandes à la fois**. Ce mode utilise sa propre interface en ligne de commande et vous permet d'entrer des commandes et de recevoir des résultats jusqu'à ce que vous le quittiez.

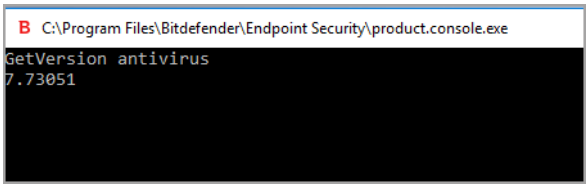
  Pour accéder à ce mode :

  1. Rendez-vous dans `c:\Program Files\Bitdefender\Endpoint Security` ou dans le dossier où BEST a été installé.
  2. Trouvez l'exécutable **product.console** et cliquez dessus. L'interface en ligne de commande s'ouvre.
  3. Exécutez la commande désirée.

     Exemple :

     ```
     GetVersion antivirus
     ```

     Le résultat représente le numéro de version des signatures antimalwares.
  4. Exécutez la commande `exit` pour fermer l'interface en ligne de commande.



- **Une commande à la fois**. Ce mode utilise l'invite de commande et retourne à l'invite du système une fois la commande exécutée.

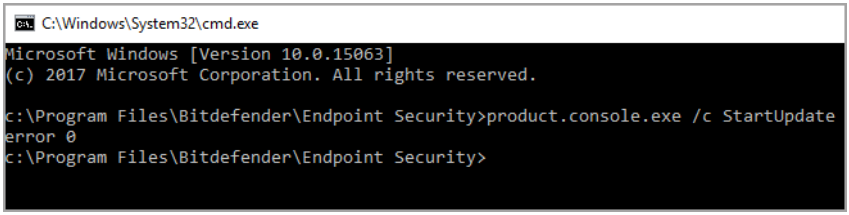
  Pour accéder à ce mode :

1. Ouvrez l'invite de commande (`cmd.exe`).
2. Utilisez la commande `cd` pour vous rendre dans le dossier d'installation de Bitdefender Endpoint Security Tools.
3. Exécutez la commande désirée.

   Exemple :

   ```
   C:\Program Files\Bitdefender\Endpoint Security>
            product.console.exe /c StartUpdate
   ```

4. Si la commande est correctement exécutée, le résultat renvoyé est `error 0`.



6.1. Commandes prises en charge

L'interface en ligne de commande prend en charge plusieurs commandes, dont certaines ont besoin de paramètres pour renvoyer des résultats valides.

Tous les exemples de cette section ont été réalisés en utilisant la Console du produit située dans le dossier d'installation de BEST.

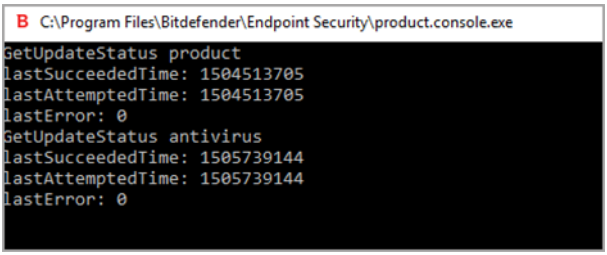
`GetUpdateStatus` `product|antivirus`

Recevoir des informations sur la/les dernière(s) mise(s) à jour.

Cette commande nécessite l'un des paramètres suivants :

- `product` – fait référence à la version de BEST.
- `antivirus` – fait référence à la version des signatures antimalwares.

Exemple :



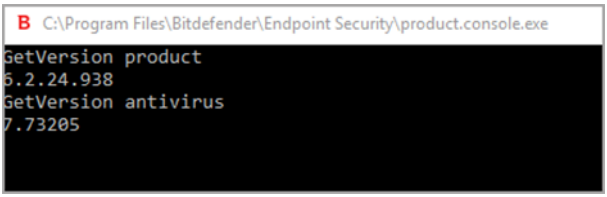
`GetVersion` `product|antivirus`

Obtenir des informations sur la version actuelle du produit.

Cette commande nécessite l'un des paramètres suivants :

- `product` – fait référence à la version de BEST.
- `antivirus` – fait référence à la version des signatures antimalwares.

Exemple :



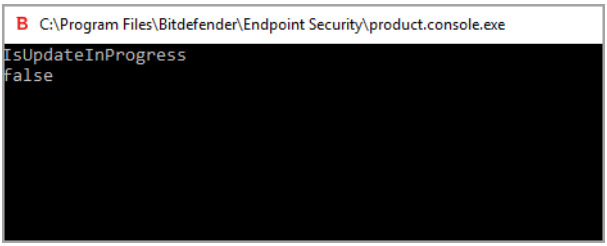
`IsUpdateInProgress`

Vérifier si une mise à jour du produit est en cours.

Valeurs de sortie :

- `true` - une mise à jour du produit est en cours.
- `false` - aucune mise à jour du produit n'est en cours.

Exemple :



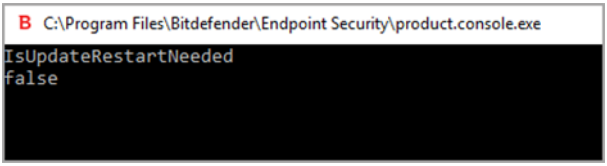
`IsUpdateRestartNeeded`

Vérifier si une machine nécessite un redémarrage du système après une mise à jour.

Valeurs de sortie :

- `true` - la machine nécessite un redémarrage du système après la mise à jour.
- `false` - la machine ne nécessite pas de redémarrage du système après la mise à jour.

Exemple :



`StartUpdate`

Commencer une mise à jour et recevoir le résultat sans attendre que la tâche ne s'achève.

Exemple :

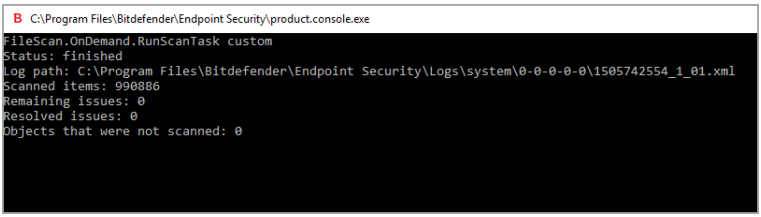
```
StartUpdate
```

Format de sortie : `error 0` (la commande a été exécutée avec succès)

`FileScan.OnDemand.RunScanTask` `custom [option]`

Commencer une analyse à la demande et afficher l'emplacement du journal et du résumé de l'analyse.

Cette commande nécessite le paramètre `custom`, suivi, si besoin, d'une option ou plus. Par exemple :



Grâce aux options, vous pouvez personnaliser une tâche d'analyse. Ces options ne sont pas obligatoires.

Chaque option a deux valeurs disponibles ou plus, mais vous ne pouvez utiliser qu'une valeur.

Lorsque la commande `FileScan.OnDemand.RunScanTask` n'est accompagnée d'aucune option, l'analyse personnalisée se lance avec la valeur par défaut de l'option. Par exemple, si vous exécutez cette commande sans mentionner l'option `scanKeyloggers`, Bitdefender Endpoint Security Tools cherchera les keyloggers, conformément à la valeur par défaut (`true`) de l'option `scanKeyloggers`.

Note

Il n'existe aucune commande spécifique pour l'**Analyse rapide** ou l'**Analyse du système**. Vous pouvez néanmoins configurer `FileScan.OnDemand.RunScanTask` de sorte à analyser uniquement

l'emplacement du système d'exploitation ou l'intégralité du système, avec toutes les options activées, en fonction de vos besoins.

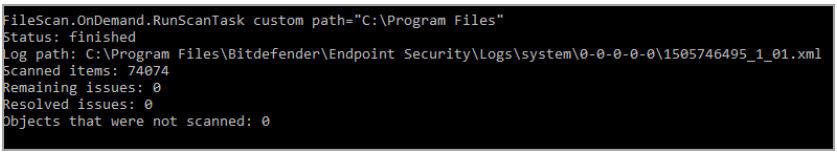
Options

`path="<path>"`

Saisissez l'emplacement de la cible de l'analyse. En cas de multiples emplacements, utiliser : `path="<path1>" path="<path2>"`.

Exemple :

```
FileScan.OnDemand.RunScanTask custom path="C:\Program
          Files"
```

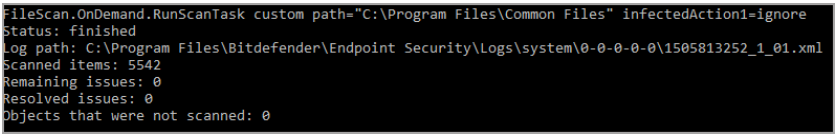


`infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine`

Sélectionner la première action réalisée lorsqu'un fichier infecté est détecté :ignorer, désinfecter, supprimer ou déplacer en quarantaine. Vous pouvez utiliser cette action en parallèle à `infectedAction2`.

Valeur par défaut : `disinfect`

Exemple :



`infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine`

Sélectionner la seconde action réalisée lorsqu'un fichier infecté est détecté si la première action n'a pas fonctionné.

Valeur par défaut : `quarantine`

Exemple :

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`suspiciousAction1=ignore|delete|quarantine`

Sélectionner la première action réalisée lorsqu'un fichier suspect est détecté. Vous pouvez utiliser cette action en parallèle à `suspiciousAction2`.

Valeur par défaut : `ignore`

Exemple :

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`suspiciousAction2=ignore|delete|quarantine`

Sélectionner la seconde action réalisée lorsqu'un fichier suspect est détecté si la première action n'a pas fonctionné.

Valeur par défaut : `ignore`

Exemple :

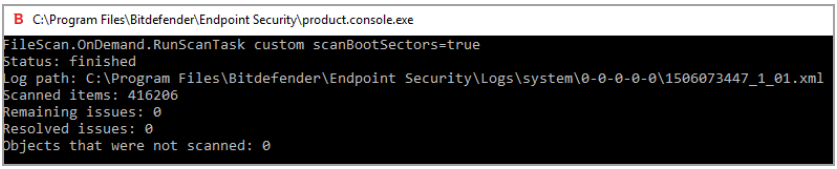
```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanBootSectors=true|false`

Analyser les secteurs d'amorçage de votre disque dur.

Valeur par défaut : `false`

Exemple :

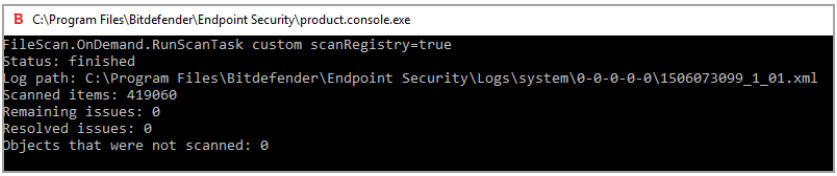


`scanRegistry=true|false`

Analyser les clés de registre de votre machine.

Valeur par défaut : `false`

Exemple :

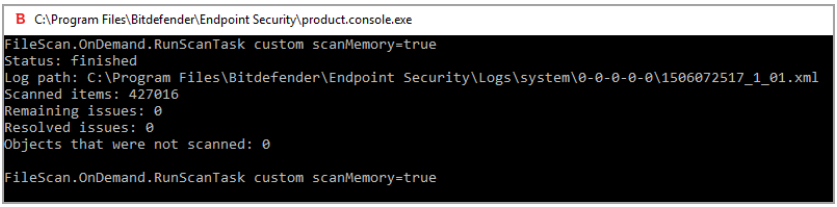


`scanMemory=true|false`

Analyser les programmes en cours d'exécution dans la mémoire de votre système.

Valeur par défaut : `false`

Exemple :

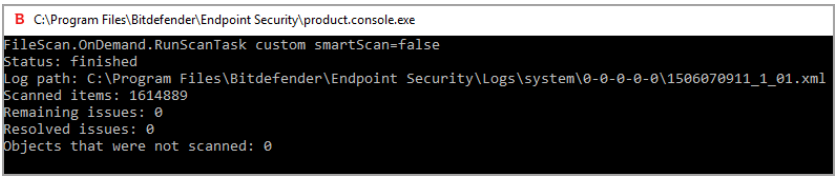


`smartScan=true|false`

Analyser uniquement les nouveaux fichiers et les fichiers modifiés.

Valeur par défaut : `true`

Exemple :

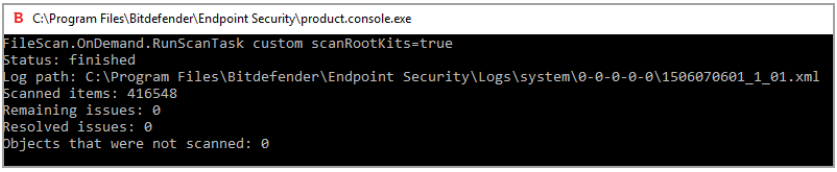


`scanRootKits=true|false`

Rechercher les rootkits et les objets cachés à l'aide de logiciels de ce type.

Valeur par défaut : `false`

Exemple :

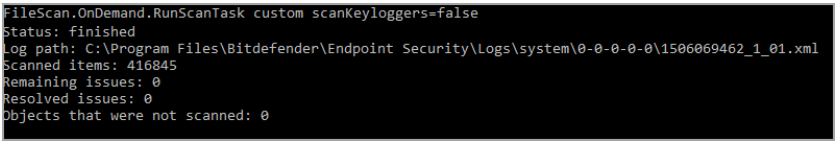


`scanKeyloggers=true|false`

Rechercher les keyloggers.

Valeur par défaut : `true`

Exemple :

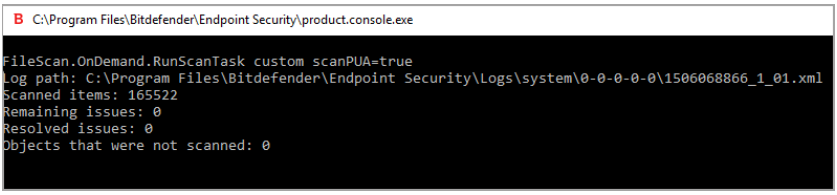


`scanPUA=true|false`

Rechercher des applications potentiellement indésirables (PUA).

Valeur par défaut : `false`

Exemple :

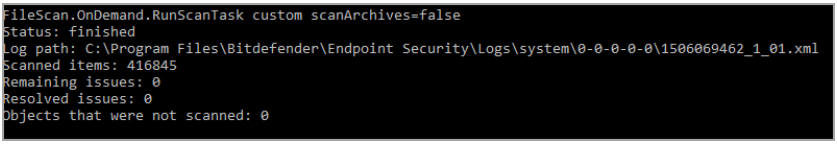


`scanArchives=true|false`

Rechercher des fichiers infectés à l'intérieur des archives.

Valeur par défaut : `true`

Exemple :

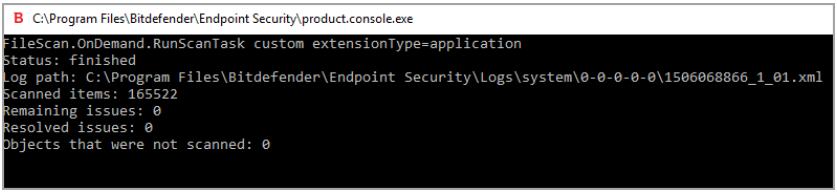


`extensionType=all|application|custom|none`

Analyser les fichiers en fonction de leur extension : tous les fichiers, les fichiers exécutables uniquement, les fichiers avec les extensions indiquées uniquement ou n'analyser aucun fichier.

Valeur par défaut : `all`

Exemple :

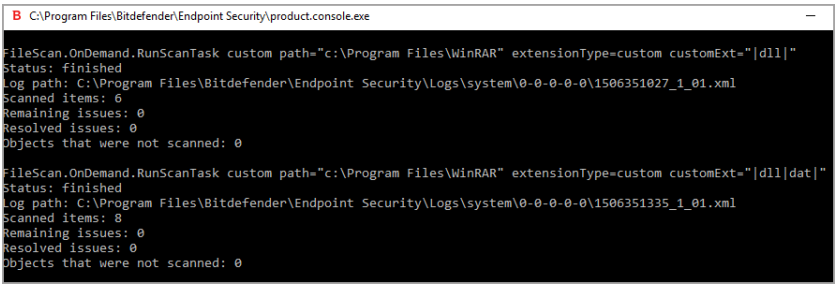


`customExt="<string>"`

Cette option vous permet de n'analyser que les fichiers présentant les extensions de votre choix. Elle doit être accompagnée d'une chaine de caractère avec toutes les extensions séparées par des barres verticales

(« `|exe|ini|txt|` »). Cette option n'est valide que si accompagnée de l'option `extensionType=custom`.

Exemple :

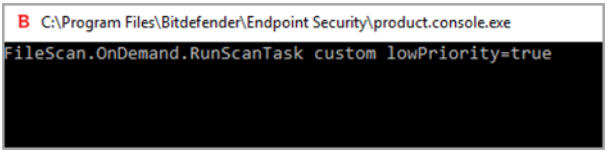


`lowPriority=true|false`

Exécuter la tâche en priorité basse.

Valeur par défaut : `false`

Exemple :



Ces options sont des alternatives aux options disponibles dans la console BEST. Pour plus d'informations, reportez-vous à « Configurer et exécuter une analyse personnalisée » (p. 15).

6.2. Codes d'erreurs des lignes de commande

L'utilitaire en ligne de commande peut renvoyer les codes erreurs suivants :

Code d'erreur	Description
0	Command executed successfully (commande exécutée avec succès).

Code d'erreur	Description
87	Invalid Parameter (Paramètre invalide).
160	Bad Arguments (Arguments incorrects)
1627	Function Failed – an error occurred while executing the command (Échec de la fonction – une erreur est survenue pendant l'exécution de la commande).

7. OBTENIR DE L'AIDE

Pour des problèmes ou des questions concernant Bitdefender Endpoint Security Tools, veuillez contacter votre administrateur réseau.

Pour trouver des informations sur le produit ou pour nous contacter, faites un clic droit sur l'icône Bitdefender Endpoint Security Tools dans la barre d'outils et sélectionnez **A propos de** pour ouvrir la fenêtre **A propos de**.

Glossaire

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.

Attaques ciblées

Les cyberattaques qui visent essentiellement des avantages financiers ou l'atteinte à une réputation. La cible peut être un individu, une société, un logiciel ou un système, minutieusement étudié avant que l'attaque ne survienne. Ces attaques s'étalent sur la durée et par étapes, via un ou plusieurs points d'infiltration. Ils passent presque inaperçus et sont détectés, généralement, lorsque le mal est déjà fait.

Bootkit

Un bootkit est un programme malveillant qui a la capacité d'infecter le master boot record (MBR), le volume boot record (VBR) ou le secteur de démarrage. Un bootkit reste actif même après un redémarrage.

Conflit de ressources d'analyse antimalware

Utilisation intensive des ressources système se produisant lorsque le logiciel antivirus analyse simultanément plusieurs machines virtuelles sur un seule hôte physique.

Cookie

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant

au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Downloader Windows

Il s'agit d'un nom générique donné à un programme ayant comme fonction principale de télécharger des contenus à fin malveillante ou indésirable.

Enregistreur de frappe

Application qui enregistre tout ce qui est tapé.

Les enregistreurs de frappe 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 les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

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 le manque de mémoire.

Exploits

Par exploit, on entend généralement toute méthode utilisée pour gagner un accès non autorisé à des ordinateurs ou une vulnérabilité dans la sécurité d'un système qui le rend susceptible d'être attaqué.

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 anciens 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)

Fichier qui enregistre les actions ayant eu lieu. La 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.

Fichiers suspects et trafic réseau

Les fichiers suspects sont ceux dont la réputation sème le doute. Ce classement repose sur de nombreux facteurs, parmi lesquels : l'existence d'une signature numérique, le nombre d'occurrences dans les réseaux informatiques, l'emballage utilisé, etc. Le trafic de réseau est considéré comme étant suspect, lorsqu'il s'écarte du modèle type. Par exemple, une source peu fiable, des demandes de connexion à des ports inhabituels, une hausse de l'utilisation de la bande passante, des horaires de connexion aléatoires, etc.

Grayware

Une classe d'applications logicielles entre les logiciels licites et les malware. Bien qu'ils ne soient pas aussi nuisibles que les malware qui affectent l'intégrité du système, leur comportement est tout de même dérangeant et provoque des situations non voulues, telles que le vol et l'usage non autorisé de données, et la publicité indésirable. Les applications graymare les plus communes sont les spyware et les adware.

Heuristique

Méthode basée sur des règles 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 les 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.

Ligne de commande

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

Malwares

« Malware » est un terme générique regroupant les logiciels conçus pour faire du tort ; il s'agit de 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.

Mettre à jour

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

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de rechercher 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.

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 sembler être un virus et ne génère donc pas de fausses alertes.

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 de l'e-mail. Cet e-mail oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des

claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

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

Portes dérobées

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Publiciels

Les publiciels sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des termes de l'accord de licence.

Ransomwares

Un malware qui vous bloque sur votre ordinateur ou bloque l'accès à vos fichiers et applications. Le ransomware exigera que vous payez une certaine somme (paiement de rançon) en échange d'une clé de déchiffrement qui vous permet de retrouver l'accès à votre ordinateur ou à vos fichiers.

Rootkit

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

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des

terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. 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, modifier des fichiers et des logs et passer inaperçus.

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 :

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur d'amorçage contient aussi un programme qui charge le système d'exploitation.

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

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des emails non sollicités.

Spywares

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des partagiciels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart

des partagiciels et logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions 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 logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison 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 - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela 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 Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus d'amorçage

Virus qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage 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

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

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

Voleur de mots de passe

Un voleur de mots de passe collecte des informations telles que les identifiants de compte et les mots de passe associés. Ces identifiants volés sont ensuite utilisés à des fins malveillantes, comme la prise de contrôle de compte.

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 : télécopieur, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.