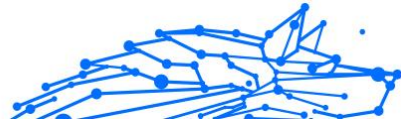


GUIDE D'UTILISATION

Bitdefender® CONSUMER SOLUTIONS

Parental Control





Bitdefender Parental Control

Manuel d'utilisation

Publication date 04/29/2024
Copyright © 2024 Bitdefender

Mentions légales

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris sous la forme de photocopies, d'enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. Il est permis d'inclure de courtes citations dans la rédaction de textes sur le produit, à condition d'en mentionner la source. Le contenu ne peut en aucun cas être modifié.

Avertissement et clause de non-responsabilité. Le présent produit et sa documentation sont protégés par le droit d'auteur. Les informations contenues dans le présent document sont fournies « telles quelles », sans garantie. Bien que toutes les précautions aient été prises lors de l'élaboration du présent document, ses auteurs ne sauraient être tenus pour responsables envers toute personne ou entité, des pertes ou dommages directs ou indirects consécutifs à l'utilisation des informations qu'il contient.

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

Marques. Des noms de marques peuvent apparaître dans le présent document. Toutes les marques, déposées ou non, citées dans le présent document, sont la propriété exclusive de leurs propriétaires respectifs et sont reconnues comme telles.

Bitdefender®



Table des matières

À propos de ce guide	1
Objectifs et destinataires	1
Comment utiliser ce guide	1
Conventions utilisées dans ce guide	1
Normes typographiques	1
Avertissement	2
Commentaires	2
1. Pour démarrer	4
1.1. Configurer le contrôle parental	4
1.2. Installer le contrôle parental de Bitdefender sur les appareils de votre enfant	5
1.2.1. Sur les appareils Windows :	5
1.2.2. Sur les appareils macOS :	5
1.2.3. Sur les appareils Android :	6
1.2.4. Sur les appareils iOS :	7
2. Fonctionnalités & Capacités	10
2.1. Profils	10
2.2. Statistiques	11
2.3. Code PIN parental	12
2.3.1. Vous avez oublié le code PIN ?	12
2.3.2. Modifier votre code PIN	13
2.4. Filtrage du contenu	13
2.4.1. Recherche sécurisée et accès limité à YouTube	14
2.4.2. Bloquer et autoriser des catégories de sites Internet	14
2.4.3. Exceptions	15
2.5. Temps passé sur Internet au quotidien	15
2.5.1. Système de récompense	16
2.6. Désactiver Internet sur l'appareil de votre enfant	17
2.7. Routines	18
2.7.1. Définir des routines	19
2.8. Suivre les déplacements de votre enfant	20
3. Désinstaller le contrôle parental	22
4. Obtenir de l'aide	23
4.1. Demander de l'aide	23
4.2. Ressources En Ligne	23
4.2.1. Centre de support Bitdefender	23
4.2.2. Communauté des experts Bitdefender	24
4.2.3. Bitdefender Cyberpedia	24
4.3. Pour nous joindre	25



4.3.1. Distributeurs locaux	25
Glossaire	26



À PROPOS DE CE GUIDE

Objectifs et destinataires

Le présent guide est destiné à tous les utilisateurs de Bitdefender ayant choisi le contrôle parental de Bitdefender comme solution de prédilection pour la sécurité, la surveillance et la protection continue des appareils et de la présence en ligne de leurs enfants.

Vous y découvrirez comment installer, configurer et tirer le meilleur parti du contrôle parental de Bitdefender, pour des fonctionnalités améliorées et un meilleur contrôle sur les activités en ligne de vos enfants.

Nous vous souhaitons un apprentissage agréable et utile.

Comment utiliser ce guide

Ce guide couvre plusieurs thèmes essentiels :

[Pour démarrer \(page 4\)](#)

Commencez par configurer le contrôle parental de Bitdefender selon vos besoins.

[Fonctionnalités & Capacités \(page 10\)](#)

Découvrez comment utiliser le contrôle parental de Bitdefender et toutes ses fonctionnalités.

[Obtenir de l'aide \(page 23\)](#)

Où chercher et à qui demander de l'aide en cas d'imprévu

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.



Style	Description
sample syntax	Les exemples de syntaxe sont écrits dans une police à espacement fixe.
https://www.bitdefender.com	Les liens URL renvoient vers un emplacement externe comme un serveur http ou ftp.
documentation@bitdefender.com	Les adresses email sont insérées dans le texte pour plus d'informations sur les contacts.
À propos de ce guide (page 1)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
Nom de fichier	Les noms de fichiers et de répertoires sont écrits dans une police à espacement fixe.
Option	Toutes les options du produit sont écrites en caractères gras .
Mot-clé	Les mots-clés et les expressions importantes sont mis en évidence à l'aide de caractères gras .

Avertissement

Les avertissements sont des notes mises en évidence pour attirer votre attention sur des informations complémentaires relatives au paragraphe dans lequel elles se trouvent.



Note

Les notes sont de courtes observations. Vous pouvez les survoler, mais elles comportent des informations intéressantes, comme des précisions sur des fonctions spécifiques ou un lien vers un thème proche.



Important

Le texte précédé de cette icône requiert votre attention et nous vous recommandons de ne pas l'ignorer. Il fournit habituellement des informations non essentielles mais utiles.



Attention

Le texte précédé de cette icône contient des informations essentielles que vous devez lire attentivement. Si vous suivez les indications, tout se passera bien. Assurez-vous de bien les comprendre, car elles décrivent des procédures dangereuses.

Commentaires

Aidez-nous à améliorer ce livret ! Nous avons testé et vérifié toutes les informations mais n'hésitez pas à nous écrire pour nous signaler



d'éventuelles erreurs ou des améliorations que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Écrivez-nous à l'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

Voici en premier lieu un guide détaillé qui vous indiquera les différentes étapes à suivre pour configurer l'abonnement au contrôle parental de Bitdefender sur votre compte Bitdefender Central. Il s'agit de la première étape d'un processus simple, qui est nécessaire pour vous assurer de pouvoir gérer et surveiller efficacement les activités en ligne de vos enfants.

1.1. Configurer le contrôle parental

Lors de l'activation de votre abonnement, pour commencer la configuration du contrôle parental de Bitdefender sur votre compte :

1. Connectez-vous à votre compte Bitdefender Central et accédez à l'onglet **Contrôle parental** situé à gauche de l'écran.
2. Cliquez sur **Commencer**.
3. Définir un code PIN de l'application



Attention

Ce code PIN vous aidera à empêcher vos enfants de désactiver eux-mêmes les fonctionnalités du contrôle parental en se déconnectant de leur application enfant.

Mémo-risez-le.

4. Cliquez sur **Suivant**.
5. Poursuivez en créant un profil enfant. Saisissez le nom de l'enfant et choisissez une photo de profil. Ensuite, cliquez sur **Suivant**.
6. Sélectionnez l'âge correspondant à celui de votre enfant. Une fois cela fait, cliquez sur **Suivant**.
7. Indiquez si l'application de contrôle parental doit être installée sur l'appareil que vous utilisez actuellement ou sur un autre appareil.



Attention

Si vous sélectionnez **Autres appareils**, trois options d'installation vous seront proposées. Sélectionnez la méthode qui vous convient le mieux :

- Scanner le code QR.
- Copier le lien fourni et l'ouvrir dans le navigateur de l'appareil de l'enfant.
- Envoyer le lien d'installation par e-mail.

8. Attendez la fin du téléchargement, puis exécutez le programme d'installation sur l'appareil en question.

À partir de là, le processus d'installation commencera. Les étapes à suivre varient en fonction du type d'appareil et du système d'exploitation sur lesquels l'installation est effectuée.

1.2. Installer le contrôle parental de Bitdefender sur les appareils de votre enfant

1.2.1. Sur les appareils Windows :

Une fois que vous avez exécuté le programme d'installation que vous venez de télécharger :

1. Cliquez sur **Oui** si une boîte de dialogue « Contrôle du compte de l'utilisateur » vous invite à autoriser le fichier d'installation à apporter des modifications à l'appareil.
2. Connectez-vous à l'aide des identifiants associés à votre compte Bitdefender Central si l'on vous y invite.

1.2.2. Sur les appareils macOS :

Une fois le téléchargement du programme d'installation terminé, double-cliquez sur le fichier Bitdefender afin de lancer le processus d'installation :

1. Vous serez guidé-e à travers les étapes nécessaires à l'installation du contrôle parental pour macOS. Cliquez sur **Autoriser** si vous y êtes invité-e.
2. Cliquez sur les deux boutons **Continuer** consécutifs.



3. Pour poursuivre l'installation, vous devez accepter les conditions générales du contrat d'abonnement au logiciel.
4. Cliquez sur **Continuer**. Ensuite, cliquez sur **Installer**.
5. Lorsque vous y êtes invité-e, saisissez un nom d'administrateur et un mot de passe, puis appuyez sur le bouton **Installer le logiciel**.

Patientez jusqu'à ce qu'une notification apparaisse, indiquant qu'*une extension système a été bloquée*. Il s'agit d'un phénomène normal au cours de cette procédure. Pour poursuivre, vous devez autoriser l'extension système du contrôle parental conformément aux instructions ci-dessous :

1. Cliquez sur le bouton **Ouvrir les paramètres système**.



Attention

Sur les versions les plus anciennes de macOS, ce bouton affiche **Ouvrir les préférences sécurité**.

2. Cliquez sur le bouton **Autoriser** dans la fenêtre qui apparaît à l'écran, puis saisissez un nom d'administrateur et un mot de passe pour déverrouiller les paramètres.



Attention

Sur macOS 11 (Big Sur) et macOS 12 (Monterey), avant de pouvoir cliquer sur le bouton **Autoriser**, vous devrez d'abord cliquer sur l'icône en forme de cadenas située dans le coin inférieur gauche de la fenêtre **Sécurité & Confidentialité**, puis saisir un nom d'administrateur et un mot de passe pour apporter des modifications.

3. La fenêtre contextuelle **Filtrer le contenu réseau** apparaîtra. Cliquez sur le bouton **Autoriser** dans cette fenêtre.
4. Ensuite, cliquez sur le bouton **Ouvrir les paramètres systèmes**.
5. Cliquez une nouvelle fois sur le bouton **Autoriser**.

1.2.3. Sur les appareils Android :

Vous trouverez l'application de contrôle parental sur la page Google Play Store de Bitdefender :



1. Appuyez sur le bouton **Installer**. Le téléchargement et l'installation de l'application commenceront.
2. Une fois l'installation terminée, vous verrez un bouton **Ouvrir**. Appuyez dessus pour lancer l'application de contrôle parental de Bitdefender.

Après avoir ouvert l'application, suivez les étapes décrites à l'écran pour configurer le contrôle parental sur l'appareil Android de votre enfant :

1. Appuyez sur **Continuer**.
2. Connectez-vous à l'application à l'aide des identifiants de votre compte Bitdefender Central.
3. Sélectionnez le profil enfant que vous souhaitez attribuer à l'appareil Android.
4. Vous devez accorder les autorisations nécessaires à l'application pour que celle-ci fonctionne correctement. Pour ce faire, appuyez sur **Suivant**, puis :
 - a. Autorisez l'accès VPN, puis choisissez **Autoriser tout le temps** pour filtrer le contenu en ligne sur l'appareil de votre enfant.
 - b. Pour faciliter la localisation de l'appareil Android de votre enfant, appuyez sur **Suivant**, puis sur **Autoriser**, et choisissez l'option **Autoriser tout le temps**.
 - c. Les autorisations « VPN » et « Localisation » afficheront une coche verte. Appuyez sur **Terminer la configuration**, puis appuyez sur **Suivant**.
 - d. À ce stade, il existe 3 autres autorisations permettant de bloquer des applications et l'accès Internet sur l'appareil de l'enfant. Appuyez sur **Définir l'autorisation** dans le panneau **Droits d'administrateur de l'appareil**.
 - e. Appuyez sur le bouton **Terminer** une fois que vous avez terminé la configuration de l'application de contrôle parental de Bitdefender.

1.2.4. Sur les appareils iOS :

Vous trouverez l'application de contrôle parental sur la page App Store de Bitdefender :



1. Appuyez sur l'icône en forme de nuage avec une flèche pointant vers le bas. Le téléchargement et l'installation de l'application commenceront.
2. Une fois l'installation terminée, vous verrez un bouton **Ouvrir**. Appuyez dessus pour lancer l'application de contrôle parental de Bitdefender.
3. Si des profils de gestion des appareils mobiles sont trouvés sur l'appareil iOS de l'enfant, il vous sera demandé de les supprimer. Appuyez sur **Suivant** et choisissez **Supprimer les profils**.
4. Dans l'application **Réglages** d'iOS, allez dans **Général**, puis faites défiler vers le bas jusqu'à la section **VPN et gestion de l'appareil**.
5. Appuyez sur chaque entrée dans la section **GESTION DES APPAREILS MOBILES** et choisissez **Supprimer la gestion** pour chacune d'entre elles.
Répétez ce processus jusqu'à ce qu'il ne reste plus aucune entrée dans la section « GESTION DES APPAREILS MOBILES ».

Rouvrez l'application installée sur l'appareil de l'enfant et suivez les étapes décrites à l'écran pour configurer le contrôle parental de Bitdefender :

1. Appuyez sur **Continuer**.
2. Connectez-vous à l'application à l'aide des identifiants associés à votre compte Bitdefender Central.
3. Sélectionnez le profil enfant que vous souhaitez attribuer à l'appareil.
4. Vous devrez ensuite accorder les autorisations nécessaires à l'application pour que celle-ci fonctionne correctement. Appuyez sur **Suivant**.
5. Autorisez l'accès VPN afin de filtrer le contenu en ligne sur l'appareil de votre enfant. Appuyez sur **Autoriser** deux fois de suite pour ajouter les configurations VPN.
6. Appuyez sur **Suivant**, puis choisissez **Autoriser** afin de faciliter la localisation de l'appareil iOS de votre enfant.
7. Procédez ensuite à la configuration du contrôle parental d'Apple pour bloquer des applications et l'accès Internet sur l'appareil de l'enfant.



Attention

Vous pouvez appuyer sur **Comment faire** pour être guidé-e pas à pas dans ce processus.

8. Après avoir configuré le contrôle parental d'Apple sur votre propre appareil et sur celui de votre enfant, sélectionnez **J'ai configuré le contrôle parental d'Apple** afin de continuer.
9. Ensuite, autorisez l'accès au temps d'écran pour filtrer le contenu en ligne sur l'appareil iOS de votre enfant.
- 10 Appuyez sur **Terminer la configuration**.

Une fois ces étapes achevées sur le ou les appareils de votre enfant, le processus de configuration est terminé. En tant que parent, vous pouvez désormais surveiller les activités en ligne de votre enfant et consulter ses statistiques d'utilisation dans votre compte Bitdefender Central, dans le tableau de bord du contrôle parental, que nous présenterons en détail dans les chapitres suivants.



2. FONCTIONNALITÉS & CAPACITÉS

2.1. Profils

Les profils enfants sont des ensembles de règles personnalisées qui permettent à l'application de contrôle parental de Bitdefender de gérer et de surveiller les activités en ligne des enfants. Ces profils sont basés sur des paramètres adaptés à l'âge des enfants, tels que des filtres de contenu et des restrictions de temps. Grâce au compte Bitdefender Central, les parents peuvent créer, modifier et supprimer ces profils, et leur attribuer ou leur ôter des appareils, garantissant ainsi à leurs enfants une expérience en ligne sûre et appropriée.

Pour créer un profil enfant :

1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Dans le menu de gauche, cliquez sur l'onglet **Contrôle parental**.
3. Cliquez sur **Nouveau profil** pour créer un nouveau profil enfant.
4. Saisissez le nom et la date de naissance de l'enfant, et sélectionnez une photo de profil.



Attention

En fonction de l'âge de l'enfant, Bitdefender bloquera automatiquement certaines catégories telles que « chat », « réseaux sociaux », « contenu explicite », etc. Vous pourrez ajuster les catégories bloquées plus tard.

5. Cliquez sur le bouton **Enregistrer**.

Le nouveau profil est maintenant créé ; il apparaîtra sur la page.

Pour modifier un profil enfant :

1. Cliquez sur le bouton **Afficher les détails** dans le profil de l'enfant.
2. Pour modifier le profil de votre enfant, allez dans **Modifier le profil**.
3. Utilisez le champ correspondant pour modifier le nom, la date de naissance et/ou la photo de profil de l'enfant.
4. Cliquez sur **Enregistrer les modifications** après avoir effectué les modifications nécessaires.



Pour supprimer un profil enfant :

1. Cliquez sur le bouton **Afficher les détails** dans le profil de l'enfant.
2. Allez dans **Modifier le profil**.
3. Cliquez sur le bouton **Supprimer le profil** et confirmez la suppression.

Pour attribuer des appareils à un profil enfant :

Si votre enfant possède plusieurs appareils (Windows, macOS, Android ou iOS), vous pouvez les affecter au même profil enfant.

1. Cliquez sur le bouton **Afficher les détails** dans le profil de l'enfant.
2. Cliquez sur le nombre d'appareils répertoriés sous son nom.
3. Cliquez sur le bouton **Attribuer des appareils**.
4. Sélectionnez le nom de l'appareil, puis cliquez sur le bouton **Attribuer**.



Attention

Si l'appareil n'apparaît pas dans la liste, cliquez sur **Installer un nouvel appareil**, puis suivez les instructions qui s'affichent à l'écran pour installer et configurer le contrôle parental de Bitdefender sur le nouvel appareil.

Pour supprimer des appareils d'un profil enfant :

Lorsque vous supprimez un appareil d'un profil enfant, celui-ci ne sera plus soumis à la gestion opérée par le contrôle parental de Bitdefender. Les règles et paramètres spécifiés dans le profil enfant ne s'appliqueront plus à cet appareil. Bien que l'application de contrôle parental reste installée sur l'appareil, elle cessera de fonctionner.

1. Cliquez sur le bouton **Afficher les détails** dans le profil de l'enfant.
2. Cliquez sur le nombre d'appareils répertoriés sous son nom.
3. Localisez l'appareil de l'enfant, puis cliquez sur l'option **Annuler l'attribution de l'appareil**.
4. Appuyez sur le bouton **Oui, annuler l'attribution de l'appareil** pour confirmer l'action.

2.2. Statistiques

Le contrôle parental fournit des informations sur la façon dont les enfants utilisent Internet et leurs appareils. Dans ce guide, nous vous



présenterons les diverses statistiques accessibles dans Bitdefender Central, qui permettent aux parents de prendre des décisions éclairées et de garantir une expérience en ligne sûre et équilibrée à leurs enfants.

Pour consulter les statistiques :

1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Une fois connecté·e, cliquez sur l'onglet **Contrôle parental** dans le menu de gauche.
3. Cliquez sur le profil de l'enfant dont vous souhaitez consulter les statistiques.

Après avoir sélectionné le profil de votre enfant, vous serez redirigé·e vers un tableau de bord présentant divers panneaux de statistiques. Tous font référence aux autres fonctionnalités décrites un peu plus loin dans ce guide.

2.3. Code PIN parental

Le code PIN parental est une fonctionnalité de sécurité accessible depuis le tableau de bord du contrôle parental de la plateforme Bitdefender Central. Elle permet aux parents de conserver le contrôle sur l'accès de leur enfant à l'application de contrôle parental de Bitdefender installée sur ses appareils. Vous trouverez ci-dessous des instructions détaillées sur la façon de définir, de trouver et de gérer votre code PIN parental.

Le code PIN parental empêche les déconnexions non autorisées de l'application de contrôle parental de Bitdefender sur l'appareil de votre enfant. Si votre enfant tente de se déconnecter, il sera invité à saisir ce code PIN. Cela garantit que vous seul·e, en tant que parent ayant accès au compte Bitdefender Central, pouvez contrôler les paramètres de l'application.



Attention

Lors de la première configuration de l'application de contrôle parental, il vous sera demandé de définir un code PIN parental comprenant 4 à 8 caractères.

2.3.1. Vous avez oublié le code PIN ?

Si vous oubliez votre code PIN parental, vous pouvez facilement le récupérer depuis votre compte Bitdefender Central :



1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Une fois connecté·e, cliquez sur l'onglet **Contrôle parental** dans le menu de gauche.
3. Dans le coin supérieur droit de la page, cliquez sur **Code PIN**.
4. Cliquez sur l'icône en forme d'œil pour trouver votre code PIN parental.

2.3.2. Modifier votre code PIN

Si vous pensez que votre code PIN a été compromis ou si vous souhaitez simplement le mettre à jour pour des raisons de sécurité :

1. Dans la section « Contrôle parental » de votre compte Bitdefender Central, cliquez sur l'option **Code PIN**.
2. Cloisissez l'option **Modifier le code PIN** et suivez les instructions qui s'affichent à l'écran pour définir un nouveau code PIN.

2.4. Filtrage du contenu

Le filtrage du contenu permet aux parents de restreindre l'accès de leur enfant à certains contenus en ligne, soit en bloquant des catégories entières de sites Internet, soit en créant des exceptions sur la base d'URL ou de sujets spécifiques.



Attention

La fonctionnalité de filtrage du contenu du contrôle parental de Bitdefender n'empêche pas votre enfant d'utiliser des applications de sites Internet hors ligne ; elle ne gère que le trafic Internet en ligne des appareils qu'il utilise.

Pour accéder au filtrage du contenu :

1. Connectez-vous à votre compte Bitdefender Central.
2. Dans le menu de gauche, cliquez sur l'onglet **Contrôle parental**.
3. Accédez au profil de votre enfant, puis cliquez sur **Plus** en haut à droite. Ensuite, sélectionnez **Filtrage du contenu**.



2.4.1. Recherche sécurisée et accès limité à YouTube

Dans la section **Confidentialité et sécurité** située à droite de l'écran, vous pouvez activer les commutateurs « Recherche sécurisée » et « Accès limité à YouTube ».

- **Recherche sécurisée** : lors de l'utilisation de moteurs de recherche, la recherche sécurisée empêche l'affichage de contenus jugés dangereux par Google dans les résultats de recherche.
- **Accès limité à YouTube** : fournit à l'enfant des vidéos adaptées à son âge sur YouTube.



Attention

La **recherche sécurisée** et le mode **accès limité à YouTube** redirigent toutes les requêtes DNS de **google.com** vers **safe.google.com**. Le filtrage du contenu est effectué par Google. Le contrôle parental de Bitdefender ne filtre pas le contenu proposé par la recherche sécurisée ou par Google. De la même façon, YouTube peut ne pas contrôler efficacement les tags associés aux vidéos, ce qui peut conduire à l'exposition des enfants à des contenus inappropriés.

2.4.2. Bloquer et autoriser des catégories de sites Internet



Attention

Dans la section **Catégories**, les types de sites Internet que votre enfant peut voir en ligne sont autorisés ou bloqués par défaut, en fonction de l'âge défini lors de la création du profil de l'enfant.

Vous pouvez bloquer ou autoriser divers types de sites Internet à tout moment :

1. Sélectionner une catégorie.
2. Pour bloquer l'accès à cette catégorie, choisissez **Bloqué** dans le menu déroulant. Pour autoriser l'accès, choisissez **Autorisé**.



Important

Si vous bloquez la catégorie **Partage de fichiers** pour le profil de votre enfant, la mise à jour de macOS ne fonctionnera pas. Nous vous recommandons d'autoriser temporairement le partage de fichiers lors de la mise à jour de macOS.



2.4.3. Exceptions

Dans l'onglet **Exceptions**, vous pouvez définir des exclusions de sites Internet et d'applications :

○ **Exceptions relatives aux sites Internet :**

1. Cliquez sur le bouton **Ajouter une exception**.
2. Sélectionnez **Site Internet uniquement**, puis cliquez sur le bouton **Suivant**.
3. Saisissez l'adresse du site Internet, puis choisissez de l'autoriser ou de le bloquer dans le menu déroulant.
4. Cliquez ensuite sur le bouton **Ajouter**.

○ **Exceptions relative aux applications et aux plateformes Web:**

1. Cliquez sur le bouton **Ajouter une exception**.
2. Sélectionnez **Application et plateforme Internet**, puis cliquez sur le bouton **Suivant**.
3. Choisissez la plateforme pour laquelle vous souhaitez créer une exception dans la liste fournie. Vous pouvez également utiliser la barre de recherche pour trouver ce que vous cherchez.
4. Cliquez ensuite sur le bouton **Ajouter**.

○ **Supprimer l'exceptions:**

Toutes les exceptions que vous définissez apparaîtront dans le filtrage du contenu, dans la liste des exceptions située en bas.

Pour supprimer une exception, cliquez simplement sur l'icône en forme de corbeille située à droite de l'entrée.

2.5. Temps passé sur Internet au quotidien

Dans la section « Contrôle parental » de votre compte Bitdefender Central, chaque profil créé affiche une carte « Temps passé sur Internet au quotidien ». Cette carte indique le temps total que l'enfant a passé en ligne sur l'ensemble des appareils qui lui sont attribués. Pour limiter le temps passé en ligne par un enfant :

1. Accédez au profil de l'enfant, puis cliquez sur le bouton **Définir une limite de temps** dans le panneau **Temps passé sur Internet au quotidien**. Vous pouvez également cliquer sur le menu **Plus** situé dans



le coin supérieur droit et sélectionner **Temps passé sur Internet au quotidien**.


2. Cliquez sur le bouton **Activer la limite de temps** pour activer cette fonctionnalité.



Attention

Par défaut, l'enfant dispose de 1 heure et 30 minutes d'accès Internet par jour. Si le parent n'étend pas cette limite de temps, l'accès Internet de l'enfant sera bloqué une fois la limite de 1 heure 30 minutes atteinte.

Supprimer la limite de temps quotidienne :

- Pour désactiver la limite de temps quotidienne, accédez au tableau de bord du profil de votre enfant, cliquez sur le bouton **Modifier la durée** dans le panneau **Temps passé sur Internet au quotidien**, puis appuyez sur le bouton **Pause** dans le panneau **Limite de temps**.
- Pour supprimer la limite de temps d'un jour particulier, cliquez sur le bouton  correspondant au jour de la semaine concerné dans le panneau **Emploi du temps**.

Modifier la limite de temps :

- Pour définir une limite de temps différente pour un jour spécifique de la semaine, cliquez sur le nom du jour en question dans le panneau **Emploi du temps**, sélectionnez la limite souhaitée dans le menu déroulant, puis cliquez sur le bouton **Enregistrer les modifications**. Vous pouvez sélectionner plusieurs jours à la fois.

2.5.1. Système de récompense

La fonctionnalité **Récompense** vous permet de récompenser ou de prolonger le temps d'écran de votre enfant, favorisant ainsi les bonnes habitudes en ligne. Vous pouvez utiliser le système de récompense de deux manières différentes :

○ Récompense manuelle :

1. Accédez à la section « Contrôle parental » de votre compte Bitdefender Central.



2. Accédez au profil de l'enfant, puis cliquez sur le bouton **Récompenser** dans le panneau **Temps passé sur Internet au quotidien**.
3. Sélectionnez le temps supplémentaire que vous souhaitez octroyer, puis confirmez en cliquant sur **Récompenser**.

○ **Demande de l'enfant :**

Lorsque votre enfant atteint la limite quotidienne, il peut demander du temps supplémentaire via l'application de contrôle parental installée sur son appareil mobile. En tant que parent, vous recevrez une notification dans votre compte Bitdefender Central.

1. Une fois connecté-e à votre compte Bitdefender Central, recherchez un point rouge sur la cloche de notification située dans le coin supérieur droit de l'écran, indiquant une demande en attente de la part de votre enfant.
2. Examinez la demande et décidez du temps supplémentaire à accorder.



Attention

Les enfants ont la possibilité de demander des prolongations de leur temps passé sur Internet au quotidien uniquement sur les appareils Android et iOS.

2.6. Désactiver Internet sur l'appareil de votre enfant

La gestion par les parents de l'utilisation d'Internet par un enfant peut être importante pour préserver son bien-être et sa productivité. Pour désactiver temporairement l'accès Internet sur l'appareil de votre enfant à l'aide du contrôle parental de Bitdefender :

1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Une fois connecté-e, cliquez sur l'onglet **Contrôle parental** dans le menu de gauche.
3. Sélectionnez **Afficher les détails** dans le profil de l'enfant pour lequel vous souhaitez désactiver Internet.
4. Cliquez sur le bouton **Désactiver Internet** situé dans le coin supérieur droit du tableau de bord de l'enfant.



Attention

Internet sera coupé sur tous les appareils de votre enfant. Cette action remplace tous les paramètres de contrôle parental existants, tels que les routines, les limites de temps quotidiennes ou les catégories autorisées.

5. Lorsque l'accès Internet est coupé, le bouton **Arrêter Internet** est remplacé par le bouton **Réactiver Internet**. Pour restaurer l'accès Internet, cliquez simplement sur le bouton **Réactiver Internet**.

2.7. Routines

Avec le contrôle parental de Bitdefender, vous pouvez définir jusqu'à 3 routines différentes à intégrer à l'emploi du temps de votre enfant lorsque son accès Internet est coupé. Elles offrent une approche structurée de la gestion des activités en ligne d'un enfant, encourageant les bonnes habitudes et les interactions familiales tout en garantissant sa sécurité. Ces routines sont indépendantes les unes des autres, ce qui signifie que vous pouvez décider d'en activer une, deux ou les trois, en fonction de vos préférences :

○ Routine

Créez un emploi du temps prévoyant du temps pour les devoirs, les révisions et d'autres activités.

○ Coucher

Utilisez la routine « Heure du coucher » pour réserver une période de repos à votre enfant.

○ Temps en famille

Utilisez la routine « Temps en famille » pour que votre enfant soit présent lors des repas en famille, par exemple.



Attention

Routines versus Temps passé sur Internet au quotidien :

Pendant une routine, le temps passé en ligne n'est pas pris en compte dans la limite de temps passé sur Internet au quotidien. Une fois la routine terminée, la fonction « Temps passé sur Internet au quotidien » reprend le suivi de l'utilisation d'Internet par l'enfant.

Pour éviter toute confusion pour les parents, lorsqu'une routine sera en cours, la carte « Temps passé sur Internet au quotidien » ne sera pas visible dans le tableau de bord du profil de l'enfant, et ce jusqu'à la fin de la routine. À la place, c'est le nom de la routine en cours qui sera affiché.

2.7.1. Définir des routines


Pour définir l'une des routines du contrôle parental :

1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Dans le menu de gauche, cliquez sur l'onglet **Contrôle parental**.
3. Accédez au profil de l'enfant, puis sélectionnez la routine souhaitée dans le menu **Plus**.
4. Cliquez sur le bouton **Activer** pour activer la routine sélectionnée.
5. Les panneaux **Emploi du temps** et **Accès Internet** s'afficheront alors.

○ **Planification:**

Pour définir une routine pour un ou plusieurs jours de la semaine :

- a. Sélectionnez les jours de votre choix.
- b. Sélectionnez les heures de début et de fin de la routine dans le menu déroulant fourni.
- c. Enfin, cliquez sur le bouton **Enregistrer les modifications** pour confirmer vos choix.

Pour supprimer la routine pour un jour particulier, cliquez sur le bouton  correspondant au jour de la semaine concerné.

○ **Accès à Internet:**

Le panneau « Accès Internet » associé à une routine offre deux fonctions principales permettant de contrôler les activités en ligne d'un enfant pendant des plages horaires spécifiques :



- **Désactivation complète d'Internet** : les parents ont la possibilité de désactiver complètement l'accès Internet de leur enfant pendant la durée de la routine programmée. Lorsque vous désactivez le commutateur **Accès Internet**, les appareils de l'enfant ne pourront pas accéder à Internet pendant la plage horaire spécifiée.
- **Catégories ou sites Internet spécifiques** : les parents ont également la possibilité de choisir d'autoriser l'accès Internet pendant les routines, tout en restreignant l'accès à certains sites Internet ou à certaines catégories de contenu. Lorsque vous activez le commutateur **Accès Internet**, deux onglets supplémentaires, à savoir les onglets **Catégories** et **Exceptions**, apparaissent, vous donnant accès à d'autres paramètres de [filtrage du contenu](#). (page 13)

2.8. Suivre les déplacements de votre enfant

Dans un contexte d'omniprésence des smartphones et autres appareils mobiles, le suivi des déplacements des enfants est devenu un outil essentiel pour de nombreuses familles. Qu'il s'agisse de savoir où ils se trouvent après l'école ou lorsqu'ils sortent avec des amis, la possibilité de surveiller leurs déplacements offre aux parents une certaine tranquillité d'esprit. Les instructions suivantes vous expliqueront en détail comment suivre les déplacements de votre enfant à l'aide de la fonctionnalité de localisation du contrôle parental de Bitdefender.

1. Accédez à Bitdefender Central et connectez-vous à votre compte.
2. Une fois connecté-e, cliquez sur **Contrôle parental** dans le menu de gauche.
3. Si vous avez plusieurs enfants, sélectionnez **Afficher les détails** dans le profil de l'enfant dont vous souhaitez suivre les déplacements.
4. Dans le panneau « Localisation », sélectionnez l'appareil Android ou iOS que vous souhaitez suivre, puis cliquez sur le bouton **Localiser**.



Attention

La fonctionnalité de localisation du contrôle parental de Bitdefender n'est pas disponible pour les appareils Windows et macOS.



5. Après quelques instants, une épingle rouge vous indiquera l'emplacement actuel de votre enfant sur la carte.



Attention

Les mises à jour de localisation ont lieu toutes les 20 minutes. Si vous tentez de localiser votre enfant moins de 20 minutes après la dernière localisation, il se peut que l'emplacement affiché ne reflète pas son emplacement en temps réel.



3. DÉINSTALLER LE CONTRÔLE PARENTAL

Désinstaller le contrôle parental de Bitdefender sur des appareils Windows :

1. Supprimez l'appareil du profil de votre enfant dans Bitdefender Central.
2. Ouvrez le panneau de contrôle sur l'appareil en question et localisez le contrôle parental de Bitdefender dans la liste **Programmes et fonctionnalités**.
3. Désinstallez le contrôle parental de Bitdefender.

Désinstaller le contrôle parental de Bitdefender sur des appareils macOS :

1. Supprimez l'appareil du profil de votre enfant dans Bitdefender Central.
2. Cliquez sur l'icône **Finder** sur l'appareil macOS.
3. Accédez à vos applications, puis localiser le dossier Bitdefender.
4. Ouvrez-le, puis exécutez le **Programme de désinstallation de Bitdefender**.
5. Choisissez le contrôle parental de Bitdefender dans la liste des produits à désinstaller.
6. Saisissez vos identifiants d'administrateur, puis attendez la fin de la désinstallation.

Désinstaller le contrôle parental de Bitdefender sur des appareils Android ou iOS :

1. Supprimez l'appareil du profil de votre enfant dans Bitdefender Central.
2. Désinstallez le contrôle parental de l'appareil mobile comme n'importe quelle autre application ou via Google Play Store ou AppStore, respectivement.



4. OBTENIR DE L'AIDE

4.1. Demander de l'aide

Bitdefender offre à ses clients une assistance sans égale, rapide et précise. Si vous rencontrez des difficultés ou si vous avez la moindre question au sujet de votre produit Bitdefender, nous mettons à votre disposition plusieurs ressources en ligne dans lesquelles vous trouverez sûrement une solution ou une réponse. Vous pouvez également contacter le service client Bitdefender. Nos représentants vous répondront dans les plus brefs délais et vous fourniront toute l'aide dont vous avez besoin.

4.2. Ressources En Ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à trouver des réponses à vos questions et résoudre les problèmes liés à Bitdefender.

- Centre de Support Bitdefender :
<https://www.bitdefender.fr/consumer/support/>
- Communauté des experts Bitdefender :
<https://community.bitdefender.com/fr/>
- Bitdefender Cyberpedia:
<https://www.bitdefender.com/cyberpedia/>

Vous pouvez également utiliser le moteur de recherche de votre choix pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

4.2.1. Centre de support Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention contre les menaces, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est ouverte au public et consultable gratuitement. Cet ensemble d'information est une autre



manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'information ou les rapports de bug venant de clients de Bitdefender trouvent une réponse en cherchant dans la base de données de Bitdefender, comme les rapports de bugs, travaux associés, feuillet ou article d'information venant compléter les fichiers d'aide des produits.

Le centre de support Bitdefender est accessible à tout moment à l'adresse suivante : <https://www.bitdefender.fr/consumer/support/>.

4.2.2. Communauté des experts Bitdefender

La communauté des experts est un espace dans lequel des utilisateurs et des amateurs des produits Bitdefender peuvent échanger, s'entraider et partager leurs connaissances et leurs solutions. C'est aussi un espace propice à l'émergence d'idées et de commentaires précieux pour nos développeurs. Les membres de la communauté sont des utilisateurs expérimentés heureux de donner un peu de leur temps pour aider les autres. Grâce à leurs généreux efforts, nous avons créé une base de connaissances dans laquelle tous les utilisateurs peuvent une aide et un peu de convivialité.

Vous pourrez avoir des conversations riches avec des personnes qui utilisent vraiment les produits Bitdefender. Cette communauté permet aux membres d'établir des liens et de faire entendre leurs voix. Ils sont encouragés à y participer en sachant que leurs opinions et leurs contributions sont respectées et appréciées. En tant que fournisseur reconnu, nous nous efforçons d'offrir à nos clients une assistance rapide et précise et nous voulons nous rapprocher d'eux. C'est dans cette optique nous avons créé cette communauté.

Vous pouvez rejoindre la communauté des experts ici :

<https://community.bitdefender.com/fr/>

4.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent des conseils et des astuces sur la protection contre les pirates, les violations de données et l'usurpation d'identité, notamment sur les réseaux sociaux.

La page Bitdefender Cyberpedia se trouve ici :

<https://www.bitdefender.com/cyberpedia>.



4.3. Pour nous joindre

Une communication efficace est la clé d'une relation professionnelle réussie. Depuis 2001, BITDEFENDER s'est bâti une réputation irréprochable en cherchant sans cesse à améliorer sa communication pour dépasser les attentes de ses clients et de ses partenaires. Si vous avez la moindre question, n'hésitez pas à nous contacter directement via **Bitdefender Support Center**.

<https://www.bitdefender.fr/consumer/support/>

4.3.1. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Rendez-vous sur <https://www.bitdefender.com/partners/partner-locator.html>.
2. Choisissez vos pays et ville à l'aide des options correspondantes.



GLOSSAIRE

Code d'activation

Clé unique qui peut être achetée chez un revendeur et utilisée pour activer un produit ou service spécifique. Un code d'activation permet l'activation de l'abonnement valide pour un certain laps de temps et pour certains appareils, et peut également être utilisé pour prolonger un abonnement avec pour seule condition d'être utilisé pour le même produit ou service.

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer 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 poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. ActiveX est connu pour son manque total de contrôles de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Menaces persistantes avancées

Les Menaces persistantes avancées exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par cette menace. L'objectif d'une menace persistante avancée est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter la menace dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

Adware

Les publiciels sont souvent associés à des applications gratuites qui exigent 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 recueillies peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des conditions de l'accord de licence.

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.

Porte dérobée

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

Secteur de démarrage

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.

Virus de démarrage

Menace 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 la menace active en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez la menace active en mémoire.

Botnet

Le terme « botnet » est un mot composé de robot et de network (réseau). Les botnets sont des appareils connectés à Internet infectés par une menace et pouvant servir à envoyer des pourriels, voler des données, contrôler à distance les appareils vulnérables ou diffuser des logiciels espions, rançongiciels, ou tout autre type de menace. Leur objectif est d'infecter autant d'appareils connectés que possible, comme les PC, serveurs, mobiles ou autres objets connectés appartenant à des grandes entreprises.



Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les principaux navigateurs comprennent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce 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 (plugiciels) pour certains formats.

Attaque par force brute

Les attaques qui essaient de pénétrer un système informatique en saisissant toutes les combinaisons de mots de passe possible, ce en commençant par les mots de passe les plus faciles à deviner.

Ligne de commande

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

Cookies

Sur Internet, les témoins 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 témoins est encore en développement. Son but est de cibler directement les intérêts que vous avez exprimés. 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 "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Cyberharcèlement

Lorsque des camarades ou des inconnus mènent des actions abusives envers des enfants dans le but de les blesser physiquement. Pour leur nuire sur le plan émotionnel, les assaillants envoient des messages malveillants ou des photos peu flatteuses, provoquant l'isolation de leurs victimes ou un sentiment de frustration.



Attaque par dictionnaire

Les attaques qui essaient de pénétrer un système informatique en saisissant une combinaison de mots communs pour générer des mots de passe potentiels. La même méthode est utilisée pour deviner les clés de chiffrements des messages ou documents chiffrés. Les attaques par dictionnaire fonctionnent car de nombreuses personnes ont tendance à choisir des mots de passe simples à deviner et ne contenant qu'un seul mot.

Lecteur de disque

C'est un appareil qui lit et écrit des données sur un disque. Une unité de disque dur lit et écrit sur un disque dur. Un lecteur de disquette accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

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.

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.

Exploits

Une manière de tirer profit des bugs et vulnérabilités (logicielles ou matérielles) qui sont présents sur un ordinateur. Les pirates peuvent ainsi prendre le contrôle des ordinateurs ou réseaux.

Faux positif

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



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

Heuristique

Méthode basée sur des règles permettant d'identifier de nouvelles menaces. Cette méthode d'analyse ne s'appuie pas sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'une menace existante. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

Pot de miel

Un faux système informatique est créé pour attirer les pirates informatiques afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques utilisées pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de pots de miel pour améliorer leur état de sécurité global.

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.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement 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.

Enregistreur de frappe

Un enregistreur de frappe est une application qui enregistre tout ce qui est saisi avec le clavier. 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).

Virus macro

Type de menace codée 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.

Client de messagerie

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

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.

Non-heuristique

Cette méthode d'analyse s'appuie sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être une menace et ne génère donc pas de fausses alertes.

Prédateurs en ligne

Individus cherchant à discuter avec des mineurs et des adolescents dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l'endroit idéal pour traquer les enfants vulnérables et les séduire dans le but de les faire se livrer à des activités sexuelles, en ligne ou en face à face.



Programmes compressés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. 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.

Chemin

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

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

Phishing

Action d'envoyer un courriel 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 courriel. Cet courriel 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.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la solution de sécurité sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Virus polymorphe

Menace qui change de forme avec chaque fichier qu'elle infecte. Ces menaces n'ayant pas de forme unique bien définie, elles sont plus difficiles à identifier.



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.

Ransomware

Les ransomwares sont des programmes malveillants qui tentent de soutirer de l'argent aux utilisateurs en bloquant leurs systèmes vulnérables. CryptoLocker, CryptoWall, et TeslaWall ne sont que des variantes qui traquent les systèmes personnels des utilisateurs.

L'infection peut se répandre via courriel, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblés par les pirates derrière les rançongiciels.

Fichier de rapport

Un fichier qui enregistre les actions qui surviennent. 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.

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 trousseaux administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications



cachent des fichiers sensibles en utilisant des trousseaux administrateur. Cependant, ils sont principalement utilisés pour camoufler des menaces ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les trousseaux administrateur pirates 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 journaux et passer inaperçus.

Script

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

Spam

Message électronique ou envoi de messages souvent répertoriés comme des e-mails « non sollicités ».

Spyware

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 logiciels gratuits et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des 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.

Éléments de démarrage



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

Abonnement

Achetez une licence qui donne à l'utilisateur le droit d'utiliser un produit ou service particulier sur un nombre spécifique d'appareils et pour un certain laps de temps. Un abonnement expiré peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

Barre d'état

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.

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 normes pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Menace

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des menaces peuvent également se répliquer. Toutes les menaces informatiques sont créées par des personnes. Une menace simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même une menace simple comme celle décrite est dangereuse puisqu'elle remplit vite la mémoire et bloque le système. Une menace plus dangereuse encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.



Mise à jour des informations sur les menaces

La signature binaire de la menace, utilisée par la solution de sécurité pour détecter et éliminer la menace.

Cheval de Troie

Programme destructeur qui prétend être une application normale. À la différence des programmes malveillants comme les vers, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout autant destructeurs. L'un des types les plus pernicioeux de chevaux de Troie est un programme qui, sous couvert de supprimer les menaces de votre ordinateur, en installe en fait de nouvelles.

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.

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.

Réseau privé virtuel (VPN)

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

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.