Bitdefender

VPN

GUIDE D'UTILISATION

Bitdefender VPN

Manuel d'utilisation

Date de publication : 21/11/2022

Mentions légales

Bitdefender

Table des matières

À propos de ce guide **1**
Objectifs et destinataires 1
Comment utiliser ce guide 1
Conventions utilisées dans ce guide 2
Normes typographiques 2
Avertissement 2
Commentaires 3
1. Qu'est-ce que Bitdefender VPN **4**
1.1. Protocoles de chiffrement 4
2. Abonnements au VPN **6**
2.1. Abonnement Basic 6
2.2. Abonnement Premium 6
2.3. Comment passer à la version Premium du VPN 6
3. Le compte Bitdefender Central **8**
3.1. Accéder à Bitdefender Central 8
4. Installation **10**
4.1. Préparation de l'installation 10
4.2. Configuration requise 10
4.3. Installation de Bitdefender VPN 11
5. Utilisation du VPN de Bitdefender **15**
5.1. Ouverture de Bitdefender VPN 15
5.2. Comment se connecter à Bitdefender VPN 16
5.3. Comment se connecter à un autre serveur 18
5.4. Tableau de bord 18
6. Bitdefender VPN Paramètres & Fonctionnalités **20**
6.1. Accéder aux paramètres 20
6.2. Fonctionnalités 20
6.2.1. Connexion automatique 20
6.2.2. Fonction Kill Switch 22
6.2.3. Segmentation du tunnel 23
6.2.4. App Traffic Optimizer 24
6.2.5. Bloqueur de publicités et Bloqueur de traceurs 25
7. Désinstallation de Bitdefender VPN **28**
8. Questions les Plus Fréquentes **30**
9. Obtenir de l'aide **32**
9.1. Demander de l'aide 32
9.2. Ressources En Ligne 32
9.2.1. Centre de support Bitdefender 32
9.2.2. Communauté des experts Bitdefender 33

9.2.3. Bitdefender Cyberpedia 33
9.3. Pour nous joindre 34
9.3.1. Distributeurs locaux 34
Glossaire 35

À PROPOS DE CE GUIDE

Objectifs et destinataires

Le présent guide est destiné à tous les utilisateurs de Bitdefender qui ont choisi Bitdefender VPN comme service de prédilection pour assurer leur anonymat en ligne en chiffrant l'intégralité du trafic entrant et sortant sur leurs PC, leurs Mac ou leurs appareils mobiles.

Vous trouverez des informations relatives à la configuration et à l'utilisation de Bitdefender VPN afin de protéger votre identité et vos activités contre les pirates, les FAI et les fouineurs. Vous découvrirez comment tirer le meilleur parti de Bitdefender.

Nous vous souhaitons un apprentissage agréable et utile.

Comment utiliser ce guide

Le présent guide couvre plusieurs thèmes essentiels :

Qu'est-ce que Bitdefender VPN (page 4)

Commencez par vous familiariser avec Bitdefender VPN et découvrez comment le produit peut vous aider à vous protéger en vous garantissant un véritable anonymat en ligne.

Utilisation du VPN de Bitdefender (page 15)

Découvrez comment interagir avec Bitdefender VPN et son interface utilisateur.

Bitdefender VPN Paramètres & Fonctionnalités (page 20)

Apprenez-en plus sur les paramètres et les fonctionnalités de Bitdefender VPN.

Obtenir de l’aide (page 32)

Où chercher de l'aide et à qui en demander si quelque chose d'inattendu se produit.

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. QU'EST-CE QUE BITDEFENDER VPN

Le VPN sert de tunnel entre votre appareil et le réseau auquel vous vous connectez pour sécuriser votre connexion, crypter les données à l'aide d'un cryptage de niveau militaire et masquer votre adresse IP où que vous soyez. Votre trafic est redirigé via un serveur séparé ; rendant ainsi votre appareil impossible à identifier par votre FAI, à travers la myriade d'autres appareils qui utilisent nos services. De plus, lorsqu'il est connecté à Internet via Bitdefender VPN, vous pouvez accéder à du contenu normalement limité à des zones spécifiques.

Note

Certains pays pratiquent la censure de l'Internet et la loi interdit donc l'utilisation de VPN. Pour éviter les conséquences juridiques, un message d'avertissement peut apparaitre lors de votre première utilisation de la fonctionnalité de Bitdefender VPN. En continuant à utiliser cette fonctionnalité, vous confirmez avoir connaissance des réglementations applicables dans le pays et des risques auxquels vous êtes susceptibles d'être exposé.

1.1. Protocoles de chiffrement

Les ensembles de suites cryptographiques activés sur le serveur et le client Hydra sont indiqués ci-dessous. Toutes les autres suites cryptographiques sont désactivées.

Suites cryptographiques du client Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Note

L'ensemble côté serveur est bien plus restrictif et le client comme le serveur Hydra rejetteront tout mode différent de GCM avec AES. Le serveur Hydra force une priorité côté serveur des suites cryptographiques les plus robustes et rejettera un handshake TLS si une suite plus faible est demandée par un client. Cette liste peut également être configurée à la volée côté serveur.

2. ABONNEMENTS AU VPN

Avec Bitdefender VPN, vous avez le choix entre deux types d'abonnement :

- L'abonnement Basic
- L'abonnement Premium

2.1. Abonnement Basic

Bitdefender VPN vous offre gratuitement 200 Mo de trafic par appareil pour sécuriser votre connexion quand vous le souhaitez et vous permet de vous connecter à un emplacement qui ne peut être changé.

L'abonnement Basic est disponible pour tous les utilisateurs qui téléchargent Bitdefender VPN.

2.2. Abonnement Premium

Passez à la version Premium pour bénéficier d'un accès illimité à toutes les fonctionnalités de Bitdefender VPN. Les utilisateurs disposant d'un abonnement Premium VPN actif bénéficient d'un trafic protégé illimité et peuvent se connecter à tous nos serveurs du monde.

Deux offres sont disponibles pour l'abonnement Premium : l'offre mensuelle et l'offre annuelle.

- Offre mensuelle : avec cette offre, vous serez facturé chaque mois pour l'utilisation des services Premium VPN. Vous pouvez arrêter l'abonnement quand vous le souhaitez.
- Offre annuelle : nécessite un paiement en une fois qui vous donne un accès aux services de notre VPN Premium pendant toute une année.

2.3. Comment passer à la version Premium du VPN

La manière la plus simple de passer à la version Premium de Bitdefender VPN est de cliquer sur le bouton **Mettre à niveau** situé en bas de l'interface principale. Choisissez le modèle d'abonnement souhaité puis suivez les instructions à l'écran.

Si vous avez déjà un code d'activation, suivez les instructions ci-dessous :

- **Pour les utilisateurs de Windows**
  1. Cliquez sur l'icône Mon compte située à gauche de l'interface du VPN.
  2. Cliquez sur **L'ajouter ici**.
  3. Saisissez le code reçu par e-mail, puis cliquez sur le bouton **Activer le code**.
- **Pour les utilisateurs d'appareils macOS**
  1. Cliquez sur la roue dentée en haut à droite de l'interface du VPN et sélectionnez **Mon compte**.
  2. Cliquez sur **Ajoutez-le ici**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.
- **Pour les utilisateurs d'appareils Android**
  1. Appuyez sur la roue dentée en haut à droite de l'interface du VPN et sélectionnez **Mon compte**.
  2. Appuyez sur **Ajouter le code**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.
- **Pour les utilisateurs d'appareils iOS**
  1. Appuyez sur la roue dentée dans le coin supérieur droit de l'interface VPN et sélectionnez **Mon compte**.
  2. Robinet **Ajouter un code**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.

3. LE COMPTE BITDEFENDER CENTRAL

Pour utiliser le VPN de Bitdefender, vous avez besoin d'un compte Bitdefender Central actif. Bitdefender Central est la plateforme depuis laquelle vous pouvez accéder aux fonctionnalités et services en ligne du produit.

Depuis ce compte, vous pourrez :

- Télécharger et installer Bitdefender VPN sur les systèmes d'exploitation macOS, Windows, iOS et Android.
- Gérer et renouveler vos abonnement Bitdefender.

3.1. Accéder à Bitdefender Central

Pour accéder à Bitdefender Central, suivez les instructions suivantes :

- **Pour les utilisateurs Windows**
  1. Cliquez sur l'icône Mon compte sur le côté gauche de l'interface VPN.
  2. Clique sur **Modifier le profil**.
- **Pour les utilisateurs de macOS**
  1. Cliquez sur l'icône Mon compte sur le côté gauche de l'interface VPN.
  2. Cliquez sur **Editer le profil**.
- **Pour les utilisateurs d'Android**
  1. Appuyez sur la roue dentée dans le coin supérieur droit de l'interface VPN et sélectionnez **Mon compte**.
  2. Appuyez sur **Modifier les informations du compte sur Bitdefender Central**.
- **Pour les utilisateurs iOS**
  1. Appuyez sur la roue dentée dans le coin supérieur droit de l'interface VPN et sélectionnez **Mon compte**.
  2. 2. Appuyez sur **Modifier les informations du compte sur Bitdefender Central**.

Sinon, vous pouvez vous rendre sur votre compte Bitdefender Central en cliquant sur le lien suivant : https://central.bitdefender.com.

4. INSTALLATION

4.1. Préparation de l'installation

Avant d'installer Bitdefender VPN, procédez comme suit pour faciliter l'installation :

- Vérifiez que l'appareil sur lequel vous prévoyez d'installer Bitdefender dispose de la configuration requise. Si l'appareil ne dispose pas de la configuration requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable.

  Pour des informations détaillées sur la configuration requise, veuillez consulter Configuration requise (page 10).
- Connectez-vous à l'appareil en utilisant un compte administrateur.
- Il est recommandé que votre appareil soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD/DVD. Si des versions plus récentes des fichiers d'applications du logiciel d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

4.2. Configuration requise

- **Pour les utilisateurs Windows**
  - **Système d'exploitation** : Windows 7 avec Service Pack 1, Windows 8, Windows 8.1 et Windows 10
  - **Mémoire (RAM):** 1 Go
  - **Espace disponible sur le disque dur :** 500 Mo d'espace libre
  - **Net Framework:** min version 4.5.2

    Important
    Les performances système peuvent être impactées sur les appareils équipés d'anciennes générations de processeurs.
- **Pour les utilisateurs de macOS**
  - **Système d'exploitation :** macOS Sierra (10.12) et versions supérieures

- **Espace disponible sur le disque dur :** 100 Mo d'espace libre

- **Pour les utilisateurs d'Android**
  - **Système d'exploitation :** Android 5.0 ou versions supérieures
  - **Stockage :** 100 Mo
  - Une connexion Internet active

- **Pour les utilisateurs iOS**
  - **Système d'exploitation :** iOS 12 et versions supérieures
  - **Stockage sur iPhone :** 50 Mo
  - **Stockage sur iPad :** 100 Mo
  - Une connexion Internet active

4.3. Installation de Bitdefender VPN

Pour débuter l'installation, suivez les instructions correspondant au système d'exploitation que vous utilisez :

- **Pour les utilisateurs Windows**

  1. Pour commencer l'installation de Bitdefender VPN sur un PC Windows, téléchargez le kit d'installation depuis https://www.bitdefender.com/solutions/vpn/download ou depuis l'e-mail que vous avez reçu suite à votre achat.
  2. Double-cliquez sur le programme d'installation que vous avez téléchargé pour l'exécuter.
  3. Choisissez Oui si une boite de dialogue du Contrôle de compte d'utilisateur apparait.
  4. Attendez la fin du téléchargement.
  5. Sélectionnez la langue du produit dans le menu déroulant de l'assistant d'installation.
  6. Cochez la case « Je confirme avoir lu et accepter les Conditions d'utilisation de l'abonnement et la Politique de confidentialité », puis cliquez sur **COMMENCER L'INSTALLATION**.
  7. Attendez que l'installation se termine.

8. **CONNECTEZ-VOUS** avec votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous pouvez en créer un en cliquant sur le bouton **CRÉER UN COMPTE**.
9. Sélectionnez **J'ai un code d'activation** si vous avez déjà acheté un abonnement Premium VPN.
   Sinon, vous pouvez choisir **COMMENCER L'ÉVALUATION** pour tester gratuitement le produit pendant 7 jours avant de vous engager à l'utiliser.
10. Saisissez le code reçu par e-mail, puis cliquez sur le bouton **ACTIVER PREMIUM**.
11. Au bout de quelques instants, Bitdefender VPN sera installé sur votre ordinateur et prêt à être utilisé.

- **Pour les utilisateurs de macOS**

1. Pour commencer l'installation de Bitdefender VPN sur macOS, téléchargez le kit d'installation depuis https://www.bitdefender.com/solutions/vpn/download ou depuis l'e-mail que vous avez reçu suite à votre achat.
2. L'assistant d'installation sera enregistré sur votre Mac. Dans le dossier Téléchargements, double-cliquez sur le package .
3. Suivez les instructions à l'écran. Sélectionnez **Continuer**.
4. Vous serez guidé(e) dans toutes les étapes de l'installation de Bitdefender VPN sur votre Mac. Cliquez deux fois sur le bouton **Continuer**.
5. Cliquez sur **J'accepte**, après avoir lu et compris les conditions du Contrat de licence du logiciel.
6. Cliquez sur **Installer**.
7. Saisissez un nom d'utilisateur et un mot de passe pour l'administrateur, puis cliquez sur **Installer le logiciel**.
8. Un message vous informe qu'une extension système signée par Bitdefender a été bloquée. Il ne s'agit pas d'une erreur, mais uniquement d'un contrôle de sécurité. Cliquez sur **Ouvrir les préférences de sécurité**.
9. Cliquez sur l'icône du verrou pour le déverrouiller.

Saisissez le nom et le mot de passe administrateur puis cliquez sur **Déverrouiller**.

10. Cliquez sur **Autoriser** pour charger l'extension système Bitdefender Bitdefender. Fermez ensuite la fenêtre Sécurité et confidentialité ainsi que l'assistant d'installation.
11. Cliquez sur l'icône en forme de boucler de la barre des menus puis **connectez-vous** à l'aide de votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous devez en créer un.
12. Choisissez J'ai un **Code d'activation** si vous avez déjà acheté un abonnement Premium VPN.
    Sinon, vous pouvez choisir **COMMENCER PROCÈS** de tester gratuitement le produit pendant 7 jours avant de s'engager à le payer.
13. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.
14. Au bout de quelques instants, Bitdefender VPN sera installé sur votre Mac et prêt à être utilisé.

- **Pour les utilisateurs d'Android**

1. Pour installer Bitdefender VPN sur Android, commencez par ouvrir l'application **Google Play Store** sur votre smartphone ou votre tablette.
2. Recherchez Bitdefender VPN et sélectionnez l'application correspondante.
3. Appuyez sur le bouton **Installer** et patientez jusqu'à la fin du téléchargement.
4. Appuyez sur **Ouvrir** pour exécuter l'application.
5. Cochez la case « J'accepte les Conditions d'utilisation de l'abonnement et la Politique de confidentialité », puis appuyez sur **Continuer**.
6. **Connectez-vous** avec votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous devez en créer un en appuyant sur **Créer un compte**.
7. Sélectionnez **J'ai un code d'activation** si vous avez déjà acheté un abonnement Premium VPN.

Sinon, vous pouvez choisir de commencer l'évaluation de 7 jours pour tester gratuitement le produit pendant 7 jours avant de vous engager à l'utiliser.

8. Saisissez le code reçu par e-mail puis appuyez sur **Code d'activation**.

- **Pour les utilisateurs iOS**

1. Pour installer Bitdefender VPN sur iOS, commencez par ouvrir l'**App Store** sur votre iPhone ou votre iPad.
2. Rechercher Bitdefender VPN et sélectionnez cette application.
3. Appuyez sur l'icône **Obtenir** et patientez jusqu'à la fin du téléchargement.
4. Robinet **Ouvrir** pour exécuter l'application.
5. Cochez la case **J'accepte les Conditions d'utilisation de l'abonnement et la Politique de confidentialité**, puis appuyez sur **Continuer**.
6. **Connectez-vous** avec votre compte Bitdefender Central. Si vous n'avez pas de compte, vous devez en créer un en appuyant sur **Créer un compte**.
7. Appuyez sur **Autoriser** si vous souhaitez recevoir des notifications de Bitdefender VPN.
8. Choisir **J'ai un code d'activation** si vous avez acheté un abonnement VPN Premium.
   Sinon, vous pouvez choisir Démarrer l'essai de 7 jours pour tester le produit gratuitement pendant 7 jours avant de vous engager à le payer.
9. Tapez le code reçu par e-mail, puis appuyez sur **Code d'activation**.

5. UTILISATION DU VPN DE BITDEFENDER

5.1. Ouverture de Bitdefender VPN

- **Pour Windows**
  Pour accéder à **l'interface principale du VPN Bitdefender**, utilisez l'une des méthodes suivantes :

  - **Depuis la zone de notification**
    Faites un clic droit sur l'icône représentant un bouclier rouge dans la zone de notification, puis sélectionnez **Afficher** dans le menu.

  - **Depuis l'interface Bitdefender**
    Si un produit de sécurité Bitdefender tel que Bitdefender Total Security ou Bitdefender Antivirus Plus (etc.) est déjà installé sur votre ordinateur Windows, vous pouvez ouvrir le VPN de Bitdefender en procédant comme suit :

    1. Cliquez sur l'icône **Vie privée** située dans le volet latéral gauche de l'interface Bitdefender.
    2. Cliquez sur **Ouvrir le VPN** dans le panneau du VPN.

  - **Depuis votre bureau**
    Double-cliquez sur l'icône Bitdefender VPN située sur votre bureau.

- **Pour macOS**
  Vous pouvez ouvrir l'application Bitdefender VPN en cliquant sur l'icône  située dans la barre de menu en haut à droite de l'écran.
  Si vous ne trouvez pas le bouclier Bitdefender dans la barre de menu, utilisez la barre de lancement ou le Finder de votre Mac pour retrouver l'icône :

  - **Depuis la barre de lancement**

    1. Appuyez sur la touche **F4** de votre clavier pour accéder à la barre de lancement de votre Mac.
    2. Cliquez sur Parcourir puis allez à l'emplacement de l'application Bitdefender VPN. Vous pouvez également saisir **Bitdefender VPN** dans la barre de lancement pour commencer à filtrer les résultats.

3. Une fois que vous voyez l'application Bitdefender VPN, cliquez sur son icône pour l'épingler à la barre de menu.

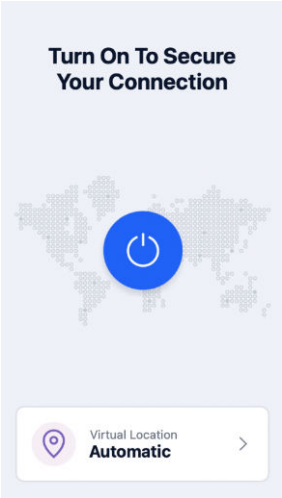
- **Depuis le Finder**

1. Cliquez sur **Finder** en bas à gauche du bureau (l'icône de Finder est celle qui ressemble à un carré bleu avec un visage souriant).
2. Ensuite, cliquez sur **Aller** en haut à gauche de l'écran, dans la barre de menu.
3. Sélectionnez **Applications** dans le menu pour accéder au dossier Applications de votre Mac.
4. Dans le dossier Applications, ouvrez le dossier **Bitdefender** puis double-cliquez sur l'application **Bitdefender VPN**.

Note
Pour accéder au VPN de Bitdefender sur vos appareils mobiles Android ou iOS, il vous suffit d'ouvrir l'application Bitdefender VPN après l'avoir installée.

5.2. Comment se connecter à Bitdefender VPN

L'interface du VPN affiche l'état de l'application : connectée ou déconnectée. Pour les utilisateurs de la version gratuite, l'emplacement du serveur le plus approprié est automatiquement défini par Bitdefender, tandis que les utilisateurs de la version Premium peuvent changer l'emplacement du serveur en le sélectionnant dans la liste des emplacements virtuels. Pour vous connecter ou vous déconnecter, il vous suffit de cliquer sur le bouton marche situé dans l'interface du VPN.



- **Pour Windows :** la zone de notification affiche une coche verte lorsque le VPN est connecté, et une coche noire lorsque le VPN est déconnecté. Lorsque vous vous connectez manuellement à un emplacement sélectionné, l'adresse IP s'affiche dans l'interface principale.
- **Pour macOS :** l'icône située dans la barre de menu s'affiche en noir lorsque le VPN est connecté, et en blanc lorsque le VPN est déconnecté. Cliquez sur le bouton rond situé au centre de l'interface et patientez le temps que la connexion soit établie.
- **Pour Android et iOS :** pour connecter le VPN de Bitdefender sur Android, iOS et iPadOS :
  - **Dans l'application Bitdefender VPN :** pour vous connecter ou vous déconnecter, appuyez simplement sur le bouton marche dans l'interface du VPN. L'état du VPN de Bitdefender s'affiche.
  - **Dans l'application Bitdefender Mobile Security :**
    1. Accédez à l'icône VPN située dans la barre de navigation inférieure de Bitdefender Mobile Security.
    2. Appuyez sur **CONNECTER** à chaque fois que vous souhaitez sécuriser une connexion à un réseau sans fil non sécurisé.Appuyez sur **DÉCONNECTER** lorsque vous souhaitez désactiver la connexion VPN.

5.3. Comment se connecter à un autre serveur

Avec un abonnement Premium, Bitdefender VPN vous permet de vous connecter à n'importe lequel de nos serveurs dans le monde, à tout moment. Pour ce faire, vous devez :

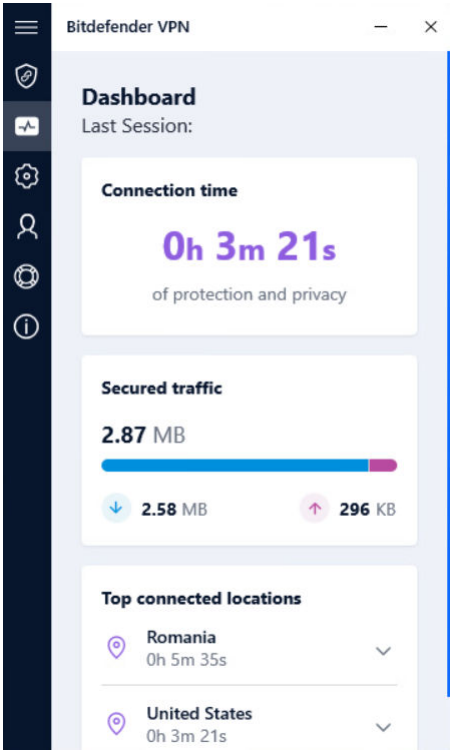
1. Ouvrir l'application Bitdefender VPN.
2. Appuyez sur le bouton **Emplacement virtuel** situé en bas de l'interface.
3. Sélectionnez le pays de votre choix.
4. Cliquez sur le bouton **Se connecter à [pays sélectionné]** situé en bas de l'interface.

5.4. Tableau de bord

Pour accéder au tableau de bord, cliquez sur l'icône dans le menu situé dans le volet latéral et sélectionnez **Tableau de bord**.

Ici, vous aurez accès à un aperçu de votre temps de connexion, de la quantité de trafic sécurisé et des principaux serveurs VPN que vous avez utilisés.

> **Note**
> Actuellement, cette fonctionnalité n'est disponible que sur les appareils Windows.


Bitdefender VPN
Dashboard
Last Session:
Connection time
0h 3m 21s
of protection and privacy
Secured traffic
2.87 MB
2.58 MB
296 KB
Top connected locations
Romania
0h 5m 35s
United States
0h 3m 21s

6. BITDEFENDER VPN PARAMÈTRES & FONCTIONNALITÉS

6.1. Accéder aux paramètres

Pour accéder aux paramètres de Bitdefender VPN, suivez les instructions suivantes :

- {1}Sur Windows{2}
  1. Ouvrez l'application Bitdefender VPN en double-cliquant sur son icône dans le système ou par un clic droit puis en sélectionnant Afficher.
  2. Cliquez sur le bouton **Paramètres** (représenté par une roue dentée) situé à gauche de l'interface.
- **Sur macOS**
  1. Ouvrez l'application Bitdefender VPN sur votre appareil macOS en cliquant sur son icône dans la barre des menus.
  2. Cliquez sur la roue dentée en haut à droite de l'interface de Bitdefender VPN et sélectionnez Paramètres.
- **Sur Android**
  1. Ouvrez l'application Bitdefender VPN sur votre appareil.
  2. Cliquez sur l'icône en forme de roue dentée située en haut à droite de l'interface de Bitdefender VPN.
- **Sur iOS**
  1. Ouvrez le Bitdefender VPN application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender VPN interface.

6.2. Fonctionnalités

6.2.1. Connexion automatique

Lorsque vous êtes en déplacement, dans un café, ou attendez à l'aéroport, la connexion à un réseau sans fil public pour effectuer des paiements,

vérifier vos courriels ou vos comptes de réseaux sociaux peut être la solution la plus rapide. Mais les regards indiscrets qui tentent de détourner vos données personnelles ne sont peut être pas loin et surveillent comment les informations fuitent du réseau.

Pour vous éviter de vous mettre en danger lorsque vous vous connectez à un réseau Wi-Fi public non sécurisé, Bitdefender VPN comprend une fonctionnalité de connexion automatique. Elle permet à Bitdefender VPN de s'activer automatiquement dans certaines situations, en fonction de vos préférences et de votre système d'exploitation.

- Sur **Windows**, la fonctionnalité de connexion automatique peut être activée dans les situations suivantes :
  - **Démarrage :** pour connecter le VPN au démarrage de Windows.
  - **Wi-Fi non sécurisé :** pour utiliser le VPN à chaque fois que vous vous connectez à un réseau Wi-Fi public ou non sécurisé.
  - **Applications de pair-à-pair :** pour vous connecter au VPN lorsque vous lancez une application de partage de fichiers en pair-à-pair.
  - **Applications et domaines :** pour utiliser systématiquement le VPN avec certaines applications et certains sites Internet.

    Note

    1. Cliquez sur le lien **Gérer**.
    2. Cliquez sur Parcourir, allez à l'emplacement de l'application avec laquelle vous souhaitez utiliser le VPN, sélectionnez le nom de l'application, puis cliquez sur **Ajouter**.

  - **Catégories de sites Internet :** pour connecter le VPN lorsque vous visitez certaines catégories de sites Internet. Le VPN de Bitdefender peut se connecter automatiquement pour les catégories de sites Internet suivantes :
    - Finance
    - Paiements en ligne
    - Santé
    - Partage de fichiers
    - Rencontres en ligne

- Contenu réservé aux adultes

> **Note**
> Vous pouvez sélectionner un serveur différent pour l'établissement de la connexion VPN pour chaque catégorie.

- Sur **macOS**, la fonctionnalité de connexion automatique peut être activée dans les situations suivantes :
  - **Démarrage :** pour connecter le VPN au démarrage de macOS.
  - **Wi-Fi non sécurisé :** Utilisez le VPN chaque fois que vous vous connectez à des réseaux Wi-Fi publics ou non sécurisés.
  - **Applications peer-to-peer :** Connectez-vous au VPN lorsque vous démarrez une application de partage de fichiers peer-to-peer.
  - **Applications:** pour utiliser systématiquement le VPN avec certaines applications.
- Sur **Android** et **iOS**, Bitdefender VPN peut être configuré pour se connecter automatiquement uniquement lorsque vous vous connectez à un réseau Wi-Fi public ou non sécurisé.

6.2.2. Fonction Kill Switch

Le Kill-Switch est une nouvelle fonctionnalité de Bitdefender VPN. Lorsqu'elle est activée, cette fonctionnalité suspend temporairement tout le trafic Internet si la connexion au VPN est perdue par accident. Dès que vous êtes de retour en ligne, la connexion VPN est rétablie.

Pour activer le Kill-Switch, suivez les instructions suivantes :

- **Sous Windows**
  1. Ouvrez l'application Bitdefender VPN sur votre appareil en double-cliquant sur son icône dans la zone de notification ou en faisant un clic droit sur l'icône et en sélectionnant **Afficher**.
  2. Clique sur le **Paramètres** bouton (représenté par une roue dentée) sur le côté gauche de l'interface.
  3. Sélectionnez **Avancé**.
  4. Activez l'option **Fonction Kill Switch**.

- **Sur Androïd**
  1. Ouvrez le Bitdefender VPN application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender VPN interface.
  3. Dans **Paramètres**, activez l'option **Kill Switch** (arrêt d'urgence).
- **Sur iOS**
  1. Ouvrez le Bitdefender VPN application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender VPN interface.
  3. Sous **Paramètres**, activez le **Antidémarreur** option.

> **Note**
> Cette fonctionnalité est également disponible pour les appareils macOS fonctionnant avec la version 10.15.4 du système (ou versions ultérieures).

6.2.3. Segmentation du tunnel

La segmentation de tunnel opérée par un réseau privé virtuel (VPN) vous permet de chiffrer le trafic lié à certaines de vos applications ou à certains de vos appareils en l'acheminant via un VPN, tandis que les autres applications et appareils conservent un accès direct à Internet. Cette fonctionnalité est particulièrement utile si vous souhaitez bénéficier de services qui fonctionnent mieux lorsqu'ils connaissent votre localisation tout en profitant d'un accès sécurisé à des communications et données potentiellement sensibles.

Lorsque vous activez la fonctionnalité **Segmentation de tunnel**, les applications et sites Internet sélectionnés contourneront le VPN et accèderont directement à Internet.

Pour gérer les applications et sites Internet qui contournent le VPN :

1. Cliquez sur le lien **Gérer** une fois la fonctionnalité activée.
2. Cliquez sur le bouton **Ajouter**.
3. Cliquez sur Parcourir, allez à l'emplacement de l'application en question ou insérez l'URL du site Internet souhaité, puis cliquez sur **Ajouter**.

Note
Lorsque vous ajoutez un site Internet, tout le domaine, y compris l'ensemble des sous-domaines, sera contourné.

Important
Sur les appareils **macOS**, la fonctionnalité de segmentation de tunnel n'est disponible que pour les sites Internet.

6.2.4. App Traffic Optimizer

La fonctionnalité App Traffic Optimizer de Bitdefender VPN vous permet de de donner la priorité au trafic des applications les plus importantes sur votre appareil sans exposer votre connexion aux risques de confidentialité. Les VPN redirigent le trafic Internet à travers un tunnel sécurisé tout en utilisant des algorithmes de cryptage puissants pour le protéger.

Cependant, cette combinaison de techniques peut présenter quelques inconvénients, particulièrement en ce qui concerne la vitesse de la connexion. Plusieurs facteurs peuvent ralentir la connexion, les plus courants étant la distance qui vous sépare du serveur auquel vous vous connectez, la congestion du réseau et l'utilisation élevée de la bande passante. Si vous remarquez que Bitdefender VPN ralentit parfois votre connexion Internet, il y a peut-être une meilleure solution que de désactiver le VPN.

Comment fonctionne App Traffic Optimizer ?

Certaines applications et services tels que les plateformes de streaming, les clients torrent et les jeux nécessitent plus de bande passante. Leur utilisation constante pourrait affecter la vitesse de votre connexion Internet. L'acheminement de votre trafic par un tunnel VPN soumet déjà votre connexion à un ralentissement relatif. Une pression supplémentaire sur votre connexion peut sérieusement dégrader votre expérience en ligne.

La fonctionnalité App Traffic Optimizer de Bitdefender VPN peut vous aider à faire face aux ralentissements de la connexion VPN en donnant la priorité à l'application de votre choix. Cette fonction vous permet de décider quelles applications doivent recevoir la majeure partie de votre trafic, puis d'allouer les ressources en conséquence. Par exemple, si vous êtes en réunion et que vous remarquez que la qualité de votre appel est médiocre, App Traffic Optimizer vous permet de donner la priorité au trafic vers l'application de vidéoconférence pour améliorer les résultats.

En général, les utilisateurs de VPN ferment tous les processus qui interfèrent sur leur appareil, voire désactivent leur connexion VPN pour obtenir une vitesse Internet plus rapide. App Traffic Optimizer vous permet de bénéficier d'une protection ininterrompue de votre vie privée sans compromettre votre vitesse de connexion.

Utiliser App Traffic Optimizer

Actuellement, la fonctionnalité est uniquement disponible sur les appareils Windows et vous permet de donner la priorité au trafic de 3 applications maximum.

Suivez ces étapes pour activer et configurer facilement App Traffic Optimizer :

1. Lancez l'application Bitdefender VPN sur votre ordinateur Windows.
2. Cliquez sur la petite roue dentée dans le volet latéral pour accéder aux paramètres du VPN.
3. Accédez à l'onglet **Généraux** et activez la fonctionnalité **App Traffic Optimizer**. La couleur de l'interrupteur passera du gris au bleu.

Pour gérer les applications priorisées par cette fonctionnalité :

1. Clique le**Gérer**lien.
2. Cliquez sur Parcourir, allez à l'emplacement de l'application que vous voulez accélérer, sélectionnez-la, puis cliquez sur **Ajouter**. L'application apparaît dans la section **Prioritaire**.

> **Note**
> Sinon, si vous avez récemment ouvert l'application que vous souhaitez prioriser, appuyez sur le bouton + situé dans la fenêtre de l'optimiseur de trafic.

3. Déconnectez et reconnectez le VPN de Bitdefender après avoir ajouté ou supprimé des applications de la liste.

Pour supprimer une application de l'optimiseur de trafic, il vous suffit de cliquer sur l'icône à côté du nom de l'application.

6.2.5. Bloqueur de publicités et Bloqueur de traceurs

Ces fonctionnalités sont conçues pour vous aider à protéger votre vie privée et à profiter d'Internet sans que des publicités agaçantes ou des

entreprises trop curieuses perturbent votre expérience. Elles contribuent à bloquer les publicités et les traceurs en ligne.

Bloqueur de publicités

Le **bloqueur de publicités** est utilisé pour bloquer les publicités, les pop-ups, les vidéos envahissantes et les bannières publicitaires pendant votre navigation. Les sites Internet se chargeront plus rapidement, seront plus agréables à consulter et seront plus sûrs.

Pour activer la fonctionnalité Ad Blocker :

1. Localisez la fonctionnalité **Bloqueur de publicités & Bloqueur de traceurs** dans les **Paramètres**.
2. Cliquez sur le lien **Gérer**.
3. Faites basculer l'interrupteur sur la position **MARCHE**.

Bloqueur de traceurs

Le **bloqueur de traceurs** permet de bloquer les traceurs utilisés par les annonceurs pour vous suivre et établir votre profil en ligne. Certains sites Internet peuvent mal fonctionner une fois les traceurs bloqués, mais il suffit d'ajouter l'URL sur la liste blanche pour corriger le problème.

Pour activer le bloqueur de traceurs :

1. Localisez le **Bloqueur de publicités et Antitracker** fonctionnalité dans **Paramètres**.
2. Clique sur le **Gérer** lien.
3. Basculez le commutateur sur **SUR** position.

Liste blanche

Certains sites ne fonctionnent pas correctement quand les traceurs et les publicités sont bloqués, Vous pouvez résoudre ce problème en ajoutant les URL des domaines concernés à la liste blanche, mais n'oubliez pas que dans ce cas vous verrez des publicités et les traceurs seront activés.

Ajoutez les sites Internet pour lesquels vous souhaitez autoriser l'affichage de publicités et l'utilisation de traceurs :

1. Localisez le **Bloqueur de publicités et Antitracker** fonctionnalité dans **Paramètres**.

2. en cliquant sur le lien **Gérer**, puis en vous rendant dans la section Liste blanche de la fenêtre et en cliquant sur le lien **Gérer** correspondant.
3. en cliquant sur **Ajouter un site Internet** et en insérant l'URL souhaitée.

7. DÉSINSTALLATION DE BITDEFENDER VPN

La procédure de suppression de Bitdefender VPN est similaire à celle que vous utilisez pour les autres programmes de votre ordinateur :

- **Désinstallation de Bitdefender VPN sur les appareils Windows**
  - Sur **Windows 7** :
    1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration** et deux fois sur **Programmes et fonctionnalités**.
    2. Trouvez **Bitdefender VPN** et cliquez sur **Désinstaller**.
       Patientez jusqu'à la fin du processus de désinstallation.
  - Sur **Windows 8** et **Windows 8.1** :
    1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
    2. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
    3. Trouver **Bitdefender VPN** et sélectionnez **Désinstaller**.
       Attendez que le processus de désinstallation soit terminé.
  - Sur **Windows 10** et **Windows 11** :
    1. Cliquez sur **Démarrer**, puis sur **Paramètres**.
    2. Cliquez sur l'icône **Système** dans les paramètres, puis sélectionnez **Applications installées**.
    3. Trouver **Bitdefender VPN** et sélectionnez **Désinstaller**.
    4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
       Attendez que le processus de désinstallation soit terminé.
- **Désinstallation sur des appareils macOS**
  1. Cliquez sur **Aller** dans la barre de menu et sélectionnez **Applications**.
  2. Double-cliquez sur le dossier **Bitdefender**.

3. Lancez **l'assistant de désinstallation de Bitdefender**.
4. Dans la nouvelle fenêtre, cochez la case située à côté de **Bitdefender VPN**, puis cliquez sur **Désinstaller**.
5. Saisissez un nom de compte administrateur et un mot de passe valide, puis cliquez sur **OK**.
6. Vous serez ensuite averti que Bitdefender VPN a bien été désinstallé. Cliquez sur **Fermer**.

- **Désinstallation sur des appareils Android**
  1. Ouvrez l'application **Play Store**.
  2. Cherchez **Bitdefender VPN**.
  3. Sur la page Bitdefender VPN du magasin d'applications, sélectionnez **Désinstaller**.
  4. Confirmez en appuyant sur **OK**.
- **Désinstallation sur des appareils iOS**
  1. Maintenez votre doigt appuyé sur l'application Bitdefender VPN.
  2. Sélectionnez **Supprimer l'application**.
  3. Appuyez sur **Supprimer**.

8. QUESTIONS LES PLUS FRÉQUENTES

Quand dois-je utiliser le VPN Bitdefender ?

Vous devez faire preuve de prudence lorsque vous accédez à des contenus ou que vous téléchargez/envoyez des données sur Internet. Pour être certain(e) de rester en sécurité pendant que vous naviguez sur le Web, nous vous recommandons d'utiliser le VPN lorsque vous voulez :

- vous connecter à des réseaux sans-fil publics
- accéder à des contenus normalement disponibles uniquement depuis certaines régions, que vous soyez ou non chez vous
- assurer la confidentialité de vos données personnelles (identifiants, mots de passe, adresses e-mail, informations bancaires, etc.)
- masquer votre adresse IP

Puis-je choisir une ville avec le VPN de Bitdefender ?

Oui. Actuellement, le VPN de Bitdefender pour Windows, macOS, Android et iOS peut être utilisé pour sélectionner une ville spécifique. Voici la liste des villes présentement disponibles :

- **États-Unis :** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada :** Montréal, Toronto, Vancouver
- **Royaume-Uni :** Londres, Manchester

Le VPN de Bitdefender peut-il être installé en tant qu'application indépendante ?

L'application VPN est installée automatiquement en même temps que votre solution de sécurité Bitdefender. Elle peut également être installée en tant qu'application indépendante depuis la page du produit (Google Play Store et App Store).

Est-ce que Bitdefender partagera mon adresse IP et mes données personnelles avec des tiers ?

Non, avec le VPN de Bitdefender, votre vie privée est protégée à 100 %. Personne n'aura accès aux journaux de vos activités en ligne (qu'il s'agisse d'agences publicitaires, de FAI, de compagnies d'assurance, etc.).

Quels algorithmes de chiffrement le VPN utilise-t-il ?

Le VPN de Bitdefender utilise le protocole Hydra sur toutes les plateformes, un chiffrement AES 256 bits ou le plus haut chiffre disponible pris en charge par le client et le serveur, avec Perfect Forward Secrecy. Cela signifie que les clés de chiffrement sont générées pour chaque nouvelle session VPN et effacées de la mémoire lorsque la session est terminée.

Puis-je avoir accès à des contenus normalement indisponibles dans ma région ?

Avec le VPN Premium vous avez accès à un vaste réseau d'emplacements virtuels dans le monde entier.

Le VPN aura-t-il une incidence négative sur l'autonomie de mon appareil ?

Le VPN de Bitdefender a été conçu pour protéger vos données personnelles, masquer votre adresse IP quand vous êtes connecté à des réseaux sans-fil non sécurisés, et accéder à des contenus normalement indisponibles dans votre pays. Pour éviter d'utiliser pour rien la batterie de votre appareil, nous vous recommandons d'utiliser uniquement le VPN quand vous en avez besoin, et de le déconnecter quand vous êtes hors ligne.

Pourquoi le VPN ralentit-il ma connexion Internet ?

Le VPN de Bitdefender a été pensé pour ne pas perturber votre navigation Web, mais la distance entre votre emplacement réel et le serveur auquel vous choisissez de vous connecter peut provoquer des ralentissements. Toutefois, ces ralentissements sont presque toujours suffisamment minimes pour que vous ne les remarquiez pas lors de vos activités en ligne habituelles. De plus, nous nous appuyons sur l'une des infrastructures VPN les plus rapides du monde. Si vous n'avez pas l'obligation de vous connecter à un serveur lointain (par exemple, des États-Unis à la France), nous vous recommandons d'autoriser le VPN à se connecter automatiquement au serveur le plus proche, ou de trouver un serveur plus proche de votre emplacement actuel.

9. OBTENIR DE L'AIDE

9.1. 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.

9.2. 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.

9.2.1. 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 donnés 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/.

9.2.2. 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

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent deq 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.

9.3. 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/

9.3.1. 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 essayent 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 essayent 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 trousses administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des trousses 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 trousses 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 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.

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 pernicieux 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.

VPN (réseau virtuel privé)

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.