GUIDE DE L'UTILISATEUR

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security pour iOS

Guide de l'utilisateur

Date de parution 02/10/2023

Mention légale

Bitdefender

Table des matières

À PROPOS DE CE GUIDE

Objectif et public visé

Ce guide est destiné à tous les utilisateurs d'iOS qui ont choisi Bitdefender Mobile Security pour iOS comme solution de sécurité pour leurs appareils mobiles. Les informations présentées dans ce livre conviennent non seulement à ceux qui ont une formation technique, elles sont accessibles à tous ceux qui sont capables de travailler avec des appareils mobiles Apple.

Vous découvrirez comment configurer et utiliser Bitdefender Mobile Security pour iOS pour vous protéger contre les menaces et autres applications malveillantes. Vous apprendrez comment tirer le meilleur parti de Bitdefender.

Nous vous souhaitons une conférence agréable et utile.

Comment utiliser ce guide

Ce guide est organisé autour de plusieurs grands thèmes :

Commencer (page 5)

Démarrez avec Bitdefender Mobile Security pour iOS et son interface utilisateur.

Caractéristiques et fonctionnalités (page 9)

Apprenez à utiliser Bitdefender Mobile Security pour iOS pour vous protéger contre les menaces et les applications malveillantes en découvrant ses caractéristiques et leurs fonctionnalités.

Obtenir de l’aide (page 29)

Où chercher et où demander de l'aide si quelque chose d'inattendu apparaît.

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 MOBILE SECURITY POUR IOS

Les activités en ligne telles que le paiement de factures, la réservation de vacances ou l'achat de biens et de services sont pratiques et sans tracas. Mais comme de nombreuses activités ont évolué sur Internet, celles-ci comportent des risques élevés et, si les détails de sécurité sont ignorés, des données personnelles peuvent être piratées. Et quoi de plus important que de protéger les données stockées dans les comptes en ligne et sur le smartphone personnel ?

Bitdefender Mobile Security pour iOS vous permet de :

- Bénéficiez de la protection la plus puissante contre les menaces avec le moins d'impact sur la batterie
- Protégez vos données personnelles : mots de passe, adresse, informations sociales et financières
- Vérifiez facilement la sécurité de votre téléphone pour détecter et corriger les erreurs de configuration qui pourraient l'exposer
- Évitez l'exposition accidentelle des données et l'utilisation abusive de toutes les applications installées
- Analysez votre appareil pour obtenir des paramètres de sécurité et de confidentialité optimaux
- Obtenez des informations sur l'utilisation de votre activité en ligne et l'historique des incidents évités
- Vérifiez vos comptes en ligne contre les violations de données ou les fuites de données
- Crypter le trafic Internet avec le VPN inclus

Bitdefender Mobile Security pour iOS est fourni gratuitement et nécessite une activation avec un Compte Bitdefender. Cependant, certaines fonctionnalités importantes de Bitdefender, telles que notre module 'Web Protection', nécessitent un abonnement payant pour être accessibles à nos utilisateurs.

2. COMMENCER

2.1. Configuration requise pour l'appareil

Bitdefender Mobile Security pour iOS fonctionne sur tout appareil exécutant iOS 12 ou des versions ultérieures du système d'exploitation et a besoin d'une connexion Internet active pour être activé et pour détecter si une fuite de données s'est produite dans vos comptes en ligne.

2.2. Installation de Bitdefender Mobile Security pour iOS

- **De Bitdefender Central**
  - Sur iOS
    1. Accès Centrale Bitdefender.
    2. Sélectionnez le **Mes appareils** panneau.
    3. Robinet **INSTALLER LA PROTECTION**, puis appuyez sur **Protégez cet appareil**.
    4. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
    5. Vous êtes redirigé vers le **Magasin d'applications** application. Dans l'écran App Store, appuyez sur l'option d'installation.
  - Sur Windows, macOS, Androïd
    1. Accès Centrale Bitdefender.
    2. Sélectionnez le **Mes appareils** panneau.
    3. Presse **INSTALLER LA PROTECTION**, puis appuyez sur **Protégez d'autres appareils**.
    4. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
    5. Presse **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.

6. Saisissez une adresse e-mail dans le champ correspondant et appuyez sur **ENVOYER UN COURRIEL**. Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.
7. Sur l'appareil que vous souhaitez installer Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis appuyez sur le bouton de téléchargement correspondant.

- **À partir de l'App Store**
  Recherchez Bitdefender Mobile Security pour iOS pour localiser et installer l'application.

Une fenêtre d'introduction contenant des détails sur les fonctionnalités du produit s'affiche la première fois que vous ouvrez l'application. Appuyez sur Commencer pour passer à la fenêtre suivante.

Avant de passer par les étapes de validation, vous devez accepter le contrat d'abonnement. Veuillez prendre le temps de lire le Contrat d'abonnement car il contient les termes et conditions selon lesquels vous pouvez utiliser Bitdefender Mobile Security pour iOS.

Robinet **Continuer** pour passer à la fenêtre suivante.

2.3. Connectez-vous à votre compte Bitdefender

Pour utiliser Bitdefender Mobile Security pour iOS, vous devez lier votre appareil à un compte Bitdefender, Facebook, Google, Apple ou Microsoft en vous connectant au compte depuis l'application. La première fois que vous ouvrez l'application, vous êtes invité à vous connecter à un compte.

Pour lier votre appareil à un compte Bitdefender :

1. Saisissez l'adresse e-mail de votre compte Bitdefender dans le champ correspondant, puis appuyez sur **SUIVANT**. Si vous n'avez pas de compte Bitdefender et que vous souhaitez en créer un, sélectionnez le lien correspondant, puis suivez les instructions à l'écran jusqu'à ce que le compte soit activé.
   Pour vous connecter à l'aide d'un compte Facebook, Google, Apple ou Microsoft, appuyez sur le service que vous souhaitez utiliser à partir du **Ou connectez-vous** avec zone. Vous êtes redirigé vers la page de connexion du service sélectionné. Suivez les instructions pour lier votre compte à Bitdefender Mobile Security pour iOS.

> **Note**
> Bitdefender n'a accès à aucune information confidentielle telle que le mot de passe du compte que vous utilisez pour vous connecter ou les informations personnelles de vos amis et contacts.

2. Tapez votre mot de passe, puis appuyez sur **S'IDENTIFIER**.

De là, vous pouvez également accéder à la politique de confidentialité de Bitdefender.

2.4. Tableau de bord

Appuyez sur l'icône Bitdefender Mobile Security pour iOS dans le tiroir d'applications de votre appareil pour ouvrir l'interface de l'application.

La première fois que vous accédez à l'application, vous êtes invité à autoriser Bitdefender à vous envoyer des notifications. Robinet **Permettre** pour rester informé chaque fois que Bitdefender doit vous communiquer quelque chose concernant votre application. Pour gérer les notifications de Bitdefender, accédez à Paramètres > Notifications > Mobile Security.

Pour accéder à la section dont vous avez besoin, appuyez sur l'icône correspondante en bas de l'écran.

Protection Internet

Restez en sécurité lorsque vous naviguez sur le Web et chaque fois que des applications moins sécurisées tentent d'accéder à des domaines non approuvés. Pour plus d'informations, reportez-vous à Protection Internet (page 11).

VPN

Préservez votre confidentialité quel que soit le réseau auquel vous êtes connecté en cryptant vos communications Internet. Pour plus d'informations, reportez-vous à VPN (page 13).

Confidentialité du compte

Découvrez si vos comptes de messagerie ont été divulgués ou non. Pour plus d'informations, reportez-vous à Confidentialité du compte (page 16).

Pour voir des options supplémentaires, appuyez sur le ••• icône sur votre appareil lorsque vous êtes dans l'écran d'accueil de l'application. Les options suivantes s'affichent :

- **Restaurer les achats** - à partir de là, vous pouvez restaurer les abonnements précédents que vous avez achetés via votre compte iTunes.
- **Paramètres** - à partir d'ici vous avez accès à :
  - **Paramètres VPN**
    - **Accord** - vous pouvez lire les conditions d'utilisation du service VPN Bitdefender. Si vous touchez **je ne suis plus d'accord**, vous ne pourrez pas utiliser Bitdefender VPN au moins tant que vous n'aurez pas appuyé sur **Je suis d'accord**.
    - **Ouvrir l'avertissement Wi-Fi** - vous pouvez activer ou désactiver la notification du produit qui s'affiche chaque fois que vous vous connectez à un réseau Wi-Fi non sécurisé.
      Le but de cette notification est de vous aider à garder vos données privées et sécurisées en utilisant Bitdefender VPN.
  - **Paramètres de protection Web**
    - **Accord** - vous pouvez lire les conditions d'utilisation du service Bitdefender Web Protection. Si vous touchez **je ne suis plus d'accord**, vous ne pourrez pas utiliser Bitdefender VPN au moins tant que vous n'aurez pas appuyé sur **Je suis d'accord**.
    - **Activer la notification de protection Web** - Vous avertit que la protection Web peut être activée après avoir terminé une session VPN.
  - **Rapports sur les produits**
- **Retour** - à partir de là, vous pouvez lancer le client de messagerie par défaut pour nous envoyer vos commentaires sur l'application.
- **Informations sur l'application** - à partir d'ici, vous avez accès aux informations sur la version installée et aux conformités du contrat d'abonnement, de la politique de confidentialité et des licences open-source.

3. CARACTÉRISTIQUES ET FONCTIONNALITÉS

3.1. Analyse

Bitdefender Mobile Security pour iOS vous permet d'analyser votre appareil à la recherche de vulnérabilités de sécurité et de menaces potentielles sur votre appareil. L'exécution de l'analyse vérifiera :

- **Version du système d'exploitation :** Vérification de votre version iOS pour les dernières mises à jour.
- **Code d'accès/Biométrie :** Vérification du niveau de sécurité en ce qui concerne l'accès à votre appareil.
- **Protection Internet :** Vérification de l'état du module Web Protection
- **Confidentialité du compte :** Vérification de la présence de comptes surveillés répertoriés dans le module Confidentialité des comptes.
- **Scan Wi-Fi :** Vérification de l'état de sécurité du réseau actuellement connecté.

L'état de la protection est déterminé après l'exécution d'une analyse manuelle.

Après avoir exécuté la première analyse, vous rencontrerez les informations de Bitdefender Recommandations du pilote automatique. Il s'agit de votre conseiller en sécurité personnel, fournissant des recommandations contextuelles basées sur l'utilisation et les besoins de votre appareil. De cette façon, vous bénéficierez de tout ce que votre application a à offrir.

> **Note**
> Lors de la première entrée dans l'application, vous serez invité à exécuter une analyse.

3.2. Alerte aux arnaques

La fonctionnalité Scam Alert disponible dans Bitdefender Mobile Security pour iOS protège de manière proactive les utilisateurs Apple contre les escroqueries par phishing. Scam Alert pour iOS comprend deux niveaux de protection qui surveillent les escroqueries transmises via des messages SMS/MMS et des invitations d'agenda :

- **Filtre de messages texte (SMS, MMS)**
  Cette fonctionnalité identifie et filtre les messages SMS et MMS indésirables.
  Un SMS/MMS (Short Message Service/Multimedia Messaging Service) malveillant fait référence à un type de message envoyé à des appareils mobiles dans un but nuisible. Ces messages sont conçus pour exploiter les vulnérabilités, tromper les destinataires ou nuire à l'appareil, aux informations personnelles ou à la sécurité de la cible.
- **Scanner de liens d'invitation de calendrier**
  Cette fonctionnalité détecte les calendriers de spam et les événements contenant des liens dangereux. Le virus du calendrier est un type de spam qui affecte l'application Calendrier de votre iPhone, ce qui peut être ennuyeux et potentiellement dangereux :
  - Vous recevez des invitations de calendrier ou des notifications d'événements indésirables lorsque vous acceptez accidentellement une fausse invitation de calendrier envoyée à votre adresse e-mail par des pirates ou des spammeurs.
  - Lorsque vous cliquez sur le lien dans l'invitation, vous vous abonnez sans le savoir au calendrier de l'expéditeur, ce qui lui permet de vous envoyer davantage d'événements de spam.
  - Les événements de spam peuvent contenir des liens ou des pièces jointes qui pourraient vous conduire vers des pages de phishing ou d'autres cybermenaces si vous les ouvrez.

3.2.1. Comment configurer une alerte d'arnaque

Pour activer l'alerte d'arnaque, vous devez accorder à l'application Bitdefender Mobile Security l'accès aux notifications du calendrier et aux messages SMS :

Comment activer le filtrage SMS :

Pour que Bitdefender commence à filtrer les messages, vous devez activer manuellement l'option Filtrer les expéditeurs inconnus dans les paramètres de l'application Messages :

1. Ouvrez le **Paramètres** application sur votre iPhone ou iPad.
2. Faites défiler vers le bas et sélectionnez **messages** dans la liste.
3. Appuyez sur le **Inconnu et spam** section.

4. Basculer **Filtrer les expéditeurs inconnus** en position marche.
5. Sélectionner **Sécurité mobile** dans la section Filtrage SMS puis choisissez **Activer**.

Bitdefender sera désormais capable de filtrer les messages indésirables sur votre iPhone/iPad.

> **Note**
> En raison des restrictions iOS, le filtrage SMS de Bitdefender ne peut être utilisé que pour les messages SMS et MMS provenant de personnes que vous n'avez pas enregistrées dans vos contacts. Cela signifie qu'il ne filtrera pas les messages des personnes déjà présentes dans votre liste de contacts ni les messages iMessage de quiconque.

Comment activer l'analyse du calendrier :

1. Ouvrez le **Sécurité mobile Bitdefender** application installée sur votre iPhone ou iPad.
2. Allez au **Alerte aux arnaques** option dans la barre de navigation inférieure et appuyez sur **Configurer maintenant**.
3. Robinet **Continuer**, puis appuyez sur **Activer**.
4. Choisir **D'ACCORD** pour accorder à Bitdefender l'accès à votre calendrier. Une analyse du calendrier commencera immédiatement.

3.3. Protection Internet

Bitdefender Web Protection garantit une expérience de navigation sécurisée en vous alertant sur les pages Web malveillantes potentielles et lorsque des applications installées moins sécurisées tenteront d'accéder à des domaines non approuvés.

Lorsqu'une URL pointe vers un site Web de phishing ou frauduleux connu, ou vers un contenu malveillant tel qu'un logiciel espion ou un virus, la page Web est bloquée et une alerte s'affiche. La même chose se produit lorsque des applications installées tentent d'accéder à des domaines malveillants.

> **Important**
> Si vous vous trouvez dans une zone où l'utilisation d'un service VPN est restreinte par la loi, la fonctionnalité de la protection Web ne sera pas disponible.

Pour activer la protection Web :

1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Je suis d'accord**.
3. Activez le commutateur de protection Web.

> **Note**
> La première fois que vous activez la protection Web, vous serez peut-être invité à autoriser Bitdefender à configurer des configurations VPN qui surveilleront le trafic réseau. Robinet **Permettre**, continuer. Si une méthode d'authentification (empreinte digitale ou code PIN) a été définie pour protéger votre smartphone, vous devez l'utiliser. Pour pouvoir détecter l'accès à des domaines non approuvés, Web Protection travaille en collaboration avec les services VPN.

> **Important**
> La fonction de protection Web et le VPN ne peuvent pas fonctionner en même temps. Chaque fois que l'un d'eux est activé, l'autre (s'il est actif à ce moment-là) sera désactivé.

3.3.1. Alertes Bitdefender

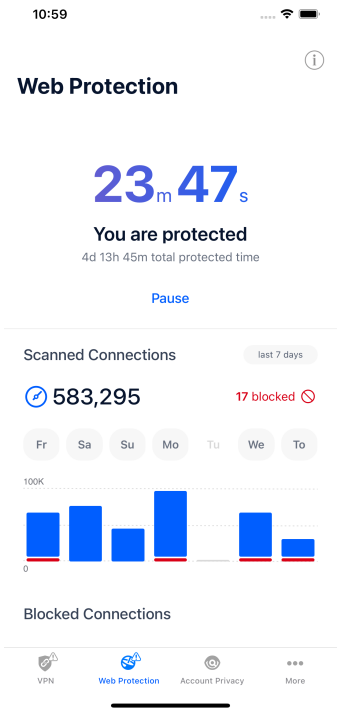
Chaque fois que vous essayez de visiter un site Web classé comme dangereux, le site Web est bloqué. Pour vous informer de l'événement, vous êtes averti par Bitdefender dans le centre de notification et dans votre navigateur. La page d'avertissement contient des informations telles que l'URL du site Web et la menace détectée. Vous devez décider quoi faire ensuite.

De plus, vous êtes averti dans le centre de notification chaque fois qu'une application moins sécurisée tente d'accéder à des domaines non approuvés. Appuyez sur la notification affichée pour être redirigé vers la fenêtre où vous pouvez décider quoi faire ensuite.

Les options suivantes sont disponibles dans les deux cas :

- Quittez le site Web en appuyant sur **RAMENEZ-MOI EN SÉCURITÉ**.
- Accédez au site Web, malgré l'avertissement, en appuyant sur la notification affichée, puis **Je veux accéder à la page**.

Confirmez votre choix.



3.4. VPN

Avec le VPN Bitdefender vous pouvez assurer la confidentialité de vos données lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les aéroports, les commerces, les cafés ou les hôtels. Vous pouvez de cette manière éviter le vol de données personnelles ou les tentatives d'accès des pirates à l'adresse IP de votre appareil.

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 sur Internet et, par conséquent, l'utilisation de VPN sur leur territoire a été interdite par la loi. Pour éviter des conséquences juridiques, un message d'avertissement peut apparaître lorsque vous essayez d'utiliser l'application Bitdefender VPN pour la première fois. En continuant à utiliser l'application, vous confirmez avoir pris connaissance des réglementations nationales applicables et des risques auxquels vous pourriez être exposé.

Pour activer Bitdefender VPN :

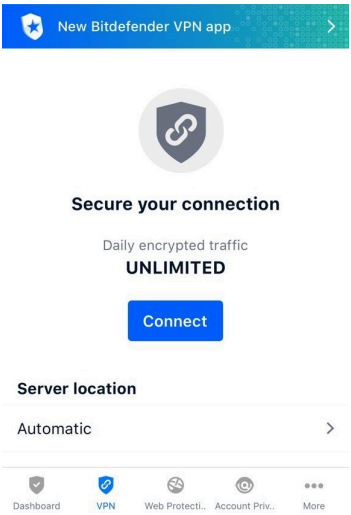
1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Connecter** chaque fois que vous souhaitez rester protégé lorsque vous êtes connecté à des réseaux sans fil non sécurisés.
   Robinet **Déconnecter** chaque fois que vous souhaitez désactiver la connexion.

> **Note**
> La première fois que vous activez le VPN, vous êtes invité à autoriser Bitdefender à configurer les configurations VPN qui surveilleront le trafic réseau. Robinet **Permettre**, continuer. Si une méthode d'authentification (empreinte digitale ou code PIN) a été définie pour protéger votre smartphone, vous devez l'utiliser.

Le VPN L'icône apparaît dans la barre d'état lorsque le VPN est actif.

Pour économiser la batterie, nous vous recommandons de désactiver le VPN lorsque vous n'en avez pas besoin.

Si vous avez un abonnement premium et que vous souhaitez vous connecter à un serveur à votre guise, appuyez sur Automatique dans l'interface VPN, puis sélectionnez l'emplacement souhaité. Pour plus de détails sur les abonnements VPN, reportez-vous à Abonnements (page 15).



3.4.1. Abonnements

Bitdefender VPN offre gratuitement un quota de trafic quotidien de 200 Mo par appareil pour sécuriser votre connexion à chaque fois que vous en avez besoin et vous connecte automatiquement à l'emplacement optimal du serveur.

Pour obtenir un trafic illimité et un accès illimité au contenu dans le monde entier en choisissant un emplacement de serveur à votre guise, passez à la version premium.

Vous pouvez mettre à niveau vers la version Bitdefender Premium VPN à tout moment en appuyant sur le bouton **Activer le VPN Premium** bouton disponible dans la fenêtre VPN. Vous avez le choix entre deux types d'abonnements : annuel et mensuel.

L'abonnement Bitdefender Premium VPN est indépendant de l'abonnement gratuit Bitdefender Mobile Security pour iOS, ce qui signifie que vous pourrez l'utiliser pendant toute sa disponibilité. En cas d'expiration de l'abonnement Bitdefender Premium VPN, vous reviendrez automatiquement au forfait gratuit.

Bitdefender VPN est un produit multiplateforme, disponible dans les produits Bitdefender compatibles avec Windows, macOS, Android et iOS. Une fois que vous aurez mis à niveau vers le plan premium, vous pourrez

utiliser votre abonnement sur tous les produits, à condition que vous vous connectiez avec le même compte Bitdefender.

> **Note**
> Bitdefender VPN fonctionne également comme une application autonome sur tous les systèmes d'exploitation pris en charge, à savoir Windows, macOS, Android et iOS.

3.5. Confidentialité du compte

Bitdefender Account Privacy détecte si une fuite de données s'est produite dans les comptes que vous utilisez pour effectuer des paiements en ligne, faire des achats ou vous connecter à différentes applications ou sites Web. Les données qui peuvent être stockées dans un compte peuvent être des mots de passe, des informations de carte de crédit ou des informations de compte bancaire et, si elles ne sont pas correctement sécurisées, un vol d'identité ou une atteinte à la vie privée peut se produire.

Le statut de confidentialité d'un compte s'affiche juste après la validation.

Pour vérifier si l'un des comptes a été divulgué, appuyez sur **Rechercher les fuites**.

Pour commencer à protéger les informations personnelles :

1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Ajouter un compte**.
3. Saisissez votre adresse e-mail dans le champ correspondant, puis appuyez sur **Suivant**.
   Bitdefender doit valider ce compte avant d'afficher des informations privées. Par conséquent, un e-mail avec un code de validation est envoyé à l'adresse e-mail fournie.
4. Vérifiez votre boîte de réception, puis tapez le code reçu dans le **Confidentialité du compte** zone de votre application. Si vous ne trouvez pas l'e-mail de validation dans le dossier Boîte de réception, vérifiez également le dossier Spam.
   L'état de confidentialité du compte validé s'affiche.

Si des fuites sont constatées dans l'un de vos comptes, nous vous recommandons de changer son mot de passe dès que possible. Pour créer un mot de passe fort et sécurisé, tenez compte de ces conseils :

- Faites-en au moins huit caractères.
- Inclure les caractères minuscules et majuscules.
- Ajoutez au moins un chiffre ou un symbole, tel que #, @, % ou !.

Une fois que vous avez sécurisé un compte qui faisait partie d'une violation de la vie privée, vous pouvez confirmer les modifications en marquant la ou les fuites identifiées comme **Résolu**. Pour faire ça:

1. Robinet ··· à côté de la brèche que vous avez résolue.
2. Robinet **Marquer comme résolu**.

Lorsque toutes les fuites détectées sont marquées comme résolues, le compte n'apparaîtra plus comme ayant fui, du moins jusqu'à ce qu'une nouvelle fuite soit détectée.

4. À PROPOS DE BITDEFENDER CENTRAL

Bitdefender Central est la plate-forme sur laquelle vous avez accès aux fonctionnalités et services en ligne du produit et pouvez effectuer à distance des tâches importantes sur les appareils sur lesquels Bitdefender est installé. Vous pouvez vous connecter à votre compte Bitdefender depuis n'importe quel ordinateur ou appareil mobile connecté à Internet en allant sur https://central.bitdefender.com, ou directement depuis l'application Bitdefender Central sur les appareils Android et iOS.

Pour installer l'application Bitdefender Central sur vos appareils :

- **Sur Androïd** - recherchez Bitdefender Central sur Google Play, puis téléchargez et installez l'application. Suivez les étapes requises pour terminer l'installation.
- **Sur iOS** - recherchez Bitdefender Central sur l'App Store, puis téléchargez et installez l'application. Suivez les étapes requises pour terminer l'installation.

Une fois connecté, vous pouvez commencer à effectuer les opérations suivantes :

- Téléchargez et installez Bitdefender sur les systèmes d'exploitation Windows, macOS, iOS et Android. Les produits disponibles en téléchargement sont :
  - Bitdefender Mobile Security pour iOS
  - Bitdefender Mobile Security pour Android
  - Bitdefender Antivirus pour Mac
  - La gamme de produits Bitdefender Windows
- Gérez et renouvelez vos abonnements Bitdefender.
- Ajoutez de nouveaux appareils à votre réseau et gérez-les où que vous soyez.

4.1. Accéder à Bitdefender Central

Il existe deux façons d'accéder à Bitdefender Central

- Depuis votre navigateur Web :

1. Ouvrez un navigateur Web sur n'importe quel appareil avec accès à Internet.
2. Aller à: https://central.bitdefender.com.
3. Connectez-vous à votre compte à l'aide de votre adresse e-mail et de votre mot de passe.

- Depuis votre appareil Android ou iOS :
  Ouvrez l'application Bitdefender Central que vous avez installée.

  Note
  Dans ce matériel, nous avons inclus les options que vous pouvez trouver sur l'interface Web.

4.2. Authentification à 2 facteurs

La méthode d'authentification à 2 facteurs ajoute une couche de sécurité supplémentaire à votre compte Bitdefender, en exigeant un code d'authentification en plus de vos identifiants de connexion. De cette façon, vous empêcherez la prise de contrôle de compte et éloignerez les types de cyberattaques, telles que les enregistreurs de frappe, les attaques par force brute ou par dictionnaire.

4.2.1. Activation de l'authentification à 2 facteurs

En activant l'authentification à 2 facteurs, vous rendrez votre compte Bitdefender beaucoup plus sécurisé. Votre identité sera vérifiée chaque fois que vous vous connecterez à partir de différents appareils, que ce soit pour installer l'un des produits Bitdefender, vérifier l'état de votre abonnement ou exécuter des tâches à distance sur vos appareils.

Pour activer l'authentification à 2 facteurs :

1. Accès Centrale Bitdefender.
2. Appuyez sur le icône dans le coin supérieur droit de l'écran.
3. Robinet **Compte Bitdefender** dans le menu des diapositives.
4. Sélectionnez le **Mot de passe et sécurité** languette.
5. Robinet **COMMENCER**.
   Choisissez l'une des méthodes suivantes :

- **Application d'authentification** - utilisez une application d'authentification pour générer un code chaque fois que vous souhaitez vous connecter à votre compte Bitdefender.
  Si vous souhaitez utiliser une application d'authentification, mais que vous ne savez pas quoi choisir, une liste des applications d'authentification que nous recommandons est disponible.
  a. Robinet **UTILISER L'APPLICATION D'AUTHENTIFICATION** commencer.
  b. Pour vous connecter sur un appareil Android ou iOS, utilisez votre appareil pour scanner le code QR.
  Pour vous connecter sur un ordinateur portable ou un ordinateur, vous pouvez ajouter manuellement le code affiché.
  Robinet **CONTINUER**.
  c. Insérez le code fourni par l'application, ou celui affiché à l'étape précédente, puis appuyez sur **ACTIVER**.

- **E-mail** - chaque fois que vous vous connectez à votre compte Bitdefender, un code de vérification sera envoyé à votre boîte de réception. Vérifiez l'e-mail, puis utilisez le code que vous avez reçu.
  a. Robinet **UTILISER LE COURRIEL** commencer.
  b. Vérifiez votre e-mail et saisissez le code fourni.
  Notez que vous disposez de cinq minutes pour vérifier votre compte de messagerie et saisir le code généré. Si le délai expire, vous devrez générer un nouveau code en suivant les mêmes étapes.
  c. Robinet **ACTIVER**.
  d. Dix codes d'activation vous sont fournis. Vous pouvez copier, télécharger ou imprimer la liste et l'utiliser au cas où vous perdriez votre adresse e-mail ou si vous ne parvenez pas à vous connecter. Chaque code ne peut être utilisé qu'une seule fois.
  e. Robinet **FAIT**.

Si vous souhaitez arrêter d'utiliser l'authentification à 2 facteurs :

1. Robinet **DÉSACTIVER L'AUTHENTIFICATION À DEUX FACTEURS**.
2. Vérifiez votre application ou votre compte de messagerie et saisissez le code que vous avez reçu.

Si vous avez choisi de recevoir le code d'authentification par e-mail, vous disposez de cinq minutes pour vérifier votre compte de messagerie et saisir le code généré. Si le délai expire, vous devrez générer un nouveau code en suivant les mêmes étapes.

3. Confirmez votre choix.

4.3. Ajout d'appareils de confiance

Pour vous assurer que vous seul pouvez accéder à votre compte Bitdefender, nous pouvons d'abord exiger un code de sécurité. Si vous souhaitez ignorer cette étape chaque fois que vous vous connectez depuis le même appareil, nous vous recommandons de le désigner comme appareil de confiance.

Pour ajouter des appareils en tant qu'appareils de confiance :

1. Accès Centrale Bitdefender.
2. Appuyez sur le icône dans le coin supérieur droit de l'écran.
3. Robinet **Compte Bitdefender** dans le menu des diapositives.
4. Sélectionnez le **Mot de passe et sécurité** languette.
5. Robinet **Appareils de confiance**.
6. La liste des appareils sur lesquels Bitdefender est installé s'affiche. Appuyez sur l'appareil souhaité.

Vous pouvez ajouter autant d'appareils que vous le souhaitez, à condition que Bitdefender soit installé et que votre abonnement soit valide.

4.4. Mes appareils

La zone **Mes Appareils** de votre compte Bitdefender vous donne la possibilité d'installer, de gérer et d'exécuter des actions à distance sur votre produits Bitdefender sur n'importe quel appareil, pourvu qu'il soit allumé et connecté à Internet. Les cartes des appareils présentent le nom de l'appareil, l'état de sa protection et s'il court un risque potentiel de sécurité.

4.4.1. Ajouter un nouvel appareil

Si votre abonnement couvre plus d'un appareil, vous pouvez ajouter un nouvel appareil et y installer votre Bitdefender Mobile Security for iOS, comme suit :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau, puis appuyez sur **INSTALLER LA PROTECTION**.
3. Choisissez l'une des deux options disponibles :
   - **Protégez cet appareil**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
   - **Protégez d'autres appareils**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
     Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER PAR E-MAIL**. Attention, le lien de téléchargement généré sera valide pendant 24 heures seulement. Si le lien expire, il vous faudra en générer un nouveau en suivant les mêmes étapes.
     Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis appuyez sur le bouton de téléchargement correspondant.
4. Attendez que le téléchargement soit terminé, puis lancez l'installation.

4.4.2. Personnalisez votre appareil

Pour identifier vos appareils facilement, vous pouvez personnaliser le nom de l'appareil :

1. Accès Centrale Bitdefender.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône ⋮ dans l'angle supérieur droit de l'écran.
4. Sélectionnez **Paramètres**.
5. Saisissez un nouveau nom dans le champ **Nom de l'appareil**, puis cliquez sur **ENREGISTRER**.

Vous pouvez créer et assigner un propriétaire pour chacun de vos appareils pour une meilleure gestion :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte d'appareil souhaitée, puis sur la ⋮ icône dans le coin supérieur droit de l'écran.
4. Sélectionnez **Profil**.
5. Cliquez sur **Ajouter un propriétaire**, puis remplissez les champs correspondants. Vous pouvez personnaliser le profil en ajoutant une photo, une date de naissance et une adresse e-mail ou un numéro de téléphone.
6. Cliquez sur **AJOUTER** pour sauvegarder le profil.
7. Sélectionnez le propriétaire souhaité dans la liste des **propriétaires d'appareils**, puis cliquez sur **ASSIGNER**.

4.4.3. Actions à distance

Pour mettre à jour Bitdefender à distance sur un appareil :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte d'appareil souhaitée, puis sur la ⋮ icône dans le coin supérieur droit de l'écran.
4. Sélectionnez **Mise à jour**.

Pour plus d'actions à distance et d'informations concernant votre produit Bitdefender sur un appareil spécifique, cliquez sur la carte appareil souhaitée.

Une fois que vous avez cliqué sur une carte appareil, les onglets suivants sont disponibles :

- **Tableau de bord.** Dans cette fenêtre, vous pouvez consulter des informations relatives à l'appareil sélectionné, vérifier l'état de sa protection, l'état du VPN Bitdefender et le nombre de menaces bloquées au cours des sept derniers jours. L'état de la protection peut s'afficher en vert (aucun problème n'affecte votre appareil), en jaune (un sujet mérite votre attention) ou en rouge (l'appareil est en danger). Si votre appareil présente des problèmes, cliquez sur la flèche située dans la zone d'état supérieure pour en savoir plus. D'ici, vous

- **Protection.** Depuis cette fenêtre, vous pouvez exécuter à distance une analyse rapide ou une analyse système de vos appareils. Cliquez sur le bouton **ANALYSER** pour lancer le processus. Vous pouvez également vérifier à quand remonte les dernières analyses sur vos appareils et obtenir les rapports correspondants, contenant les informations les plus importantes.
- **Optimizer.** Ici, vous pouvez améliorer à distance les performances d'un appareil en analysant, en détectant et en effaçant rapidement les fichiers inutiles. Cliquez sur le bouton **COMMENCER**, puis sélectionnez les zones que vous souhaiter optimiser. Cliquez de nouveau sur le bouton **COMMENCER** pour lancer le processus d'optimisation. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes résolus.
- **Antivol.** En cas de perte ou de vol de votre appareil, la fonctionnalité antivol vous permet de le localiser et de prendre des mesures à distance. Cliquez sur **LOCALISER** pour découvrir l'emplacement de l'appareil. Sa dernière position connue sera affichée, ainsi que la date et l'heure correspondantes.
- **Vulnérabilité.** Pour vérifier la présence de vulnérabilités (telles que des mises à jour Windows manquantes, des applications obsolètes ou des mots de passe faibles) sur un appareil, cliquez sur le bouton **ANALYSER** dans l'onglet Vulnérabilité. Il n'est pas possible de corriger les vulnérabilité à distance. Si une vulnérabilité est découverte, vous devez lancer une nouvelle analyse sur l'appareil concerné puis appliquer les actions recommandées. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes détectés.

4.5. Activité

Dans la zone Activité, vous avez accès à des informations sur les appareils sur lesquels Bitdefender est installé.

Une fois que vous avez accédé à la fenêtre **Activité**, les cartes suivantes sont disponibles :

- **Mes appareils.** Ici, vous pouvez visualiser le nombre d'appareils connectés ainsi que l'état de leur protection. Pour corriger les problèmes à distance sur les appareils détectés, cliquez sur **Corriger les problèmes**, puis cliquez sur **ANALYSER ET CORRIGER LES PROBLÈMES**.

Pour visualiser les détails des problèmes détectés, cliquez sur **Afficher les problèmes**.
Les informations sur les menaces détectées ne peuvent pas être récupérées sur les appareils iOS.

- **Menaces bloquées.** Vous pouvez ici voir un graphique présentant une statistique générale avec des informations sur les menaces bloquées ces dernières 24 heures et au cours des sept derniers jours. Les informations affichées sont récupérées en fonction du comportement malveillant détecté sur les fichiers, applications et URL.
- **Utilisateurs avec le plus de menaces bloquées.** Ici, vous pouvez visualiser un classement indiquant quels utilisateurs ont été le plus confrontés à des menaces.
- **Appareils avec le plus de menaces bloquées.** Vous pouvez voir ici un classement des appareils sur lesquels le plus de menaces ont été détectés.

4.6. Mes abonnements

La plateforme Bitdefender Central vous donne la possibilité de gérer facilement vos abonnements pour tous vos appareils.

4.6.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accès Centrale Bitdefender.
2. Sélectionner le panneau **Mes Abonnements**.

Vous trouverez ici des informations sur la disponibilité des abonnements que vous avez et le nombre d'appareils qui les utilisent.

Vous pouvez ajouter un nouvel appareil à un abonnement ou le renouveler en sélectionnant une carte d'abonnement.

> **Note**
> Vous pouvez avoir un ou plusieurs abonnements sur votre compte, pourvu qu'ils soient pour différentes plateformes (Windows, macOS, iOS ou Android).

4.6.2. Activer abonnement

Un abonnement peut être activé pendant le processus d'installation grâce à votre compte Bitdefender. Avec le processus d'activation, la validité de l'abonnement commence le décompte.

Si vous avez acheté un code d'activation chez l'un de nos revendeurs ou que vous l'avez reçu en cadeau, vous pouvez ajouter sa disponibilité à votre abonnement Bitdefender.

Pour activer l'abonnement avec un code d'activation, suivez ces étapes :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes abonnements** panneau.
3. Cliquez sur le bouton **CODE D'ACTIVATION**, puis saisissez le code dans le champs correspondant.
4. Cliquez sur **ACTIVER** pour continuer.

L'abonnement est désormais activé.

4.6.3. Renouveler abonnement

Si vous avez désactivé le renouvellement automatique de votre abonnement Bitdefender, vous pouvez le renouveler manuellement en suivant ces étapes :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes abonnements** panneau.
3. Sélectionnez la carte d'abonnement souhaitée.
4. Cliquez sur **RENOUVELER** pour continuer.

Une page web s'ouvre dans votre navigateur, sur laquelle vous pouvez renouveler votre abonnement Bitdefender.

4.7. Avis

L'icône vous aide à rester informé des activités des appareils associés à votre compte. Après avoir cliqué sur celle-ci, un aperçu général contenant des informations sur les activités de produits Bitdefender installés sur vos appareils.

5. QUESTIONS FRÉQUEMMENT POSÉES

Comment Bitdefender Mobile Security pour iOS me protège-t-il contre les virus et les cybermenaces ?

Bitdefender Mobile Security pour iOS offre une protection absolue contre toutes les cybermenaces et est spécialement conçu pour protéger vos données sensibles des regards indiscrets.

Vous bénéficiez d'une multitude de fonctionnalités avancées de sécurité et de confidentialité pour votre iPhone et iPad, ainsi que de nombreuses fonctionnalités bonus, notamment le VPN et la protection Web.

Bitdefender Mobile Security pour iOS réagit instantanément aux virus et malwares sans compromettre les performances de votre système.

Quels types d'appareils et de systèmes d'exploitation sont couverts par Bitdefender Mobile Security pour iOS ?

Bitdefender Mobile Security pour iOS protégera vos smartphones et tablettes exécutant iOS contre toutes les cybermenaces.

Pourquoi ai-je besoin de Bitdefender Mobile Security pour iOS sur Apple OS ?

Certaines de vos données les plus personnelles sont stockées sur votre iPhone ou iPad - et vous devez savoir qu'elles sont en sécurité à tout moment. Bitdefender Mobile Security pour iOS offre une protection absolue contre les cybermenaces et prend soin de votre vie privée en ligne et de vos informations privées sans interférer avec vos activités quotidiennes.

Est-ce que j'obtiens un VPN avec mon abonnement Bitdefender Mobile Security pour iOS ?

Bitdefender Mobile Security pour iOS est livré avec une version de base de Bitdefender VPN qui inclut une quantité généreuse de trafic (200 Mo/jour, un total de 6 Go/mois) gratuitement.

6. OBTENIR DE L'AIDE

6.1. 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.

6.2. 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.

6.2.1. 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/.

6.2.2. 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

6.2.3. 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.

6.3. 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/

6.3.1. 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.