Bitdefender

# DIGITAL IDENTITY PROTECTION

## GUIDE D'UTILISATION

# Bitdefender Digital Identity Protection

**Guide de l'utilisateur**

Date de publication : 21/11/2022


## Mention légale



Bitdefender

# Table des matières

# À PROPOS DE CE GUIDE

## Objectifs et destinataires

Le présent guide est destiné à tous les utilisateurs de Bitdefender qui ont choisi Bitdefender Digital Identity Protection comme outil logiciel dédié pour se protéger contre un nombre toujours croissant de violations de données en ligne. Accessibles à tous, les informations présentées dans ce guide ne sont pas réservées aux personnes ayant des connaissances informatiques.

Vous découvrirez comment commencer à contrôler votre vie privée en ligne en demandant à Bitdefender Digital Identity Protection d'analyser le Web à la recherche de divulgations non autorisées de vos données personnelles, de vérifier si vos comptes ont été exposés et de vous proposer des mesures simples à mettre en œuvre avant qu'une catastrophe se produise. Vous apprendrez à tirer le meilleur parti de Bitdefender.

Nous vous souhaitons un apprentissage agréable et utile.

## Comment utiliser ce guide

Ce guide couvre plusieurs thèmes essentiels :

Pour démarrer (page 6)

Commencez à utiliser Bitdefender Digital Identity Protection et son interface utilisateur.

Violations de données (page 11)

Découvrez comment protéger convenablement votre identité numérique. Commencez par bien comprendre ce que sont les violations de données et comment les examiner afin de prendre des mesures appropriées pour la protection de votre vie privée en ligne.

Obtenir de l’aide (page 17)

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

# Conventions utilisées dans ce guide

## Normes typographiques

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

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

## Avertissement

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

### Note

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

### Important

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

### Attention

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

## Commentaires

Aidez-nous à améliorer ce livret ! Nous avons testé et vérifié toutes les informations mais n'hésitez pas à nous écrire pour nous signaler d'éventuelles erreurs ou des améliorations que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Écrivez-nous à l'adresse documentation@bitdefender.com. Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

# 1. QU'EST-CE QUE BITDEFENDER DIGITAL IDENTITY PROTECTION

De nos jours, la confidentialité et la sécurité en ligne font partie des principales préoccupations des internautes, et à très juste titre. En effet, d'importantes violations de données se produisent fréquemment. Vous devez donc impérativement vous assurer que vos informations personnellement identifiables (PII) sont protégées et sécurisées.

Mais que sont les informations personnellement identifiables ? Autrefois, seules les informations sensibles, telles que le nom complet, le numéro de sécurité sociale, le numéro de permis de conduire, l'adresse e-mail ou les informations de cartes de crédit, étaient considérées comme des PII. Des informations moins sensibles, telles que les codes postaux, les adresses IP ou les identifiants de connexion, ont finalement elles aussi été incluses à la catégorie des PII. Avec le temps, votre empreinte numérique, autrement dit, les données que vous laissez derrière vous suite à vos activités de navigation sur Internet, peut finir par contenir certaines de ces données.

Bitdefender Digital Identity Protection constitue un moyen privé d'accéder à la liberté en ligne, en vous permettant de reprendre le contrôle de votre vie numérique. Et la solution ne requiert que votre nom, l'adresse e-mail que vous utilisez le plus et votre numéro de téléphone. Sur la base de ces informations, elle parcourt le Web surfacique et le Dark Web à la recherche d'informations personnelles ayant été divulguées.

Avantages de Bitdefender Digital Identity Protection:

- **Services de surveillance et de détection :** la solution surveille plus de 100 informations personnellement identifiables telles que votre numéro de sécurité sociale, vos informations de cartes de crédit ou votre adresse personnelle et affiche toutes les données détectées en lien avec votre empreinte numérique.

  > **Note**
  > Bitdefender ne stocke ni ne traite aucune information personnellement identifiable. Seules sont conservées les références à de potentielles violations de données, sans inclure de données sensibles.

- **Alertes en temps réel :** vous recevez des notifications relatives aux violations de données et aux données exposées sur le Dark Web, aux

informations personnelles divulguées sur le Web surfacique et aux potentiels usurpateurs d'identité sur les réseaux sociaux.

- **Solutions :** notre service vous suggère des actions claires nécessaires pour résoudre les problèmes et vous envoie des rappels si un problème n'est pas complètement résolu. Notre solution peut également vous fournir des instructions sur la façon de supprimer les publicités personnalisées, d'exporter vos données ou de désactiver le suivi.

# 2. POUR DÉMARRER

## 2.1. Activer la protection de l'identité numérique

Activez votre abonnement Bitdefender Digital Identity Protection une fois votre commande finalisée et réglée.

1. Ouvrez l'e-mail de confirmation que vous avez reçu peu après avoir passé votre commande et cliquez sur **COMMENCER**.
2. Vous serez redirigé(e) vers https://central.bitdefender.com.
   Connectez-vous à votre compte Bitdefender Central. Si vous ne possédez pas de compte, créez-en un.
3. Une fois que vous serez connecté(e), votre abonnement sera automatiquement rattaché à votre compte Central et déclenchera le processus d'intégration.

Autre option :

- Accédez au panneau **Mes abonnements** de votre compte Central, situé sur le côté gauche de la fenêtre, puis cliquez sur **+ Activer à l'aide d'un code**.
- Saisissez la clé à 10 chiffres qui vous a été communiquée dans l'e-mail de confirmation et appuyez sur **ACTIVER**.
- Si vous y êtes invité(e), sélectionnez la façon dont vous souhaitez utiliser le code, puis cliquez sur **ACTIVER**.

## 2.2. Configurer la protection de l'identité numérique

1. Rendez-vous sur https://central.bitdefender.com/ et connectez-vous à votre compte.
   Si vous n'avez pas encore de compte, cliquez sur **CRÉER UN COMPTE**, puis saisissez votre nom complet, une adresse e-mail et un mot de passe.
2. Sélectionnez le panneau Protection de l'identité numérique.
   Un écran de bienvenue s'affiche.
3. Cliquez sur **COMMENCER**.
4. Vous allez maintenant être informé(e) des informations que vous devez fournir. Vos données seront toujours chiffrées et sécurisées.

Cliquez sur **SUIVANT**.

5. Saisissez votre prénom, votre second prénom (le cas échéant) et votre nom de famille dans les cases correspondantes, puis cliquez sur **SUIVANT**.
6. Saisissez votre adresse e-mail, puis cliquez sur **SUIVANT**.
   Assurez-vous de saisir une adresse e-mail valide à laquelle vous pouvez accéder.
7. Un code de sécurité est envoyé à l'adresse que vous avez fournie.
   Ouvrez votre e-mail, copiez le code et collez dans le champ correspondant.
   Ensuite, cliquez sur **VÉRIFIER**.
8. Sélectionnez votre pays et saisissez votre numéro de téléphone, puis cliquez sur **SUIVANT**.
9. Vous devriez recevoir un code de sécurité peu après.
   Saisissez le code, puis cliquez sur **VÉRIFIER**.
10. Une fois la première vérification effectuée, cliquez sur **TERMINER**.

> **Note**
> Vous serez informé(e) si des violations, des informations personnellement identifiables ou de potentielles tentatives d'usurpation d'identité sont détectées lors de cette première vérification.

La solution Bitdefender Digital Identity Protection est maintenant configurée.

## 2.3. Analysez votre empreinte numérique et vérifiez l'absence de violations de données et d'éventuelles usurpations d'identité

Une fois la configuration terminée, Bitdefender Digital Identity Protection effectue une vérification en ligne afin de détecter d'éventuelles usurpations d'identité, violations de données et informations personnellement identifiables sur le Web ouvert. Nous vous recommandons d'examiner toutes les informations figurant dans les onglets **EMPREINTE NUMÉRIQUE**, **VIOLATIONS DE DONNÉES** ET **USURPATIONS D'IDENTITÉ**.

❍ Examinez votre empreinte numérique (page 10)

- Examiner les violations de données (page 11)
- Examiner d'éventuelles usurpations d'identité (page 12)

## 2.4. Améliorez vos vérifications

Nous utilisons les données que vous renseignez pour surveiller Internet et le Dark Web et pour repérer toute activité susceptible d'exposer votre vie privée ou de nuire à votre réputation.

Si vous souhaitez ajouter une autre adresse e-mail ou un autre numéro de téléphone, cliquez sur ⊕, puis cliquez sur **AJOUTER UNE ADRESSE E-MAIL** ou sur **AJOUTER UN NUMÉRO DE TÉLÉPHONE** et suivez les instructions.

# 3. TABLEAU DE BORD

Le tableau de bord regroupe les informations figurant dans les sections **EMPREINTE NUMÉRIQUE**, **VIOLATIONS DE DONNÉES** et **USURPATIONS D'IDENTITÉ**.

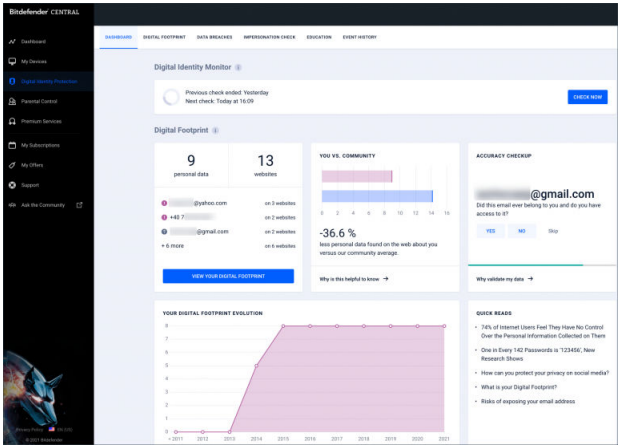
Il inclut les éléments suivants :

- Vos données exposées et leurs sources Internet
- La quantité moyenne de données exposées pour l'ensemble de la communauté
- L'évolution de votre empreinte numérique
- Des contenus en lien avec la confidentialité
- Fuites de données
- Le nombre moyen de violations de données au sein de la communauté

## 3.1. Surveillance de votre identité numérique

Sur la base d'informations vérifiées, le système de Bitdefender recherche de nouvelles informations personnelles qui seraient exposées sur le web visible et le dark web, et analyse les principaux réseaux sociaux pour y détecter toute tentative d'usurpation d'identité.

Cliquez sur **VÉRIFIER MAINTENANT** pour lancer une analyse en ligne.



# 4. EMPREINTES NUMÉRIQUES

Vos informations personnellement identifiables et leurs sources apparaissent ici. Il vous revient de déterminer si le fait que ces informations apparaissent publiquement sur Internet constitue ou non une menace.

Notre module de surveillance, basé sur l'IA, dépend fortement de l'exactitude des données fournies pour détecter de nouvelles menaces ; par conséquent, merci de nous dire si les informations sont exactes ou non.

Lorsque vous confirmez qu'une information vous appartient, nous l'ajoutons à notre système de surveillance et améliorons ainsi les chances d'en détecter d'autres à l'avenir.

## 4.1. Examinez votre empreinte numérique

Pour examiner votre empreinte numérique :

1. Rendez-vous dans l'onglet **EMPREINTE NUMÉRIQUE**.
2. Les informations qui n'ont pas encore été vérifiées apparaîtront à droite avec le texte **Vérifier**. Cliquez sur **Vérifier**, puis sélectionnez Oui ou Non, selon le cas.

> **Note**
> Chaque information confirmée est ajoutée à notre algorithme de surveillance, améliorant ainsi les résultats affichés par nos services. Les informations rejetées ne seront plus affichées. Toutefois, elles resteront accessibles sur Internet.

# 5. VIOLATIONS DE DONNÉES

Une violation se produit lorsque des pirates parviennent à contourner les mesures de sécurité d'une entreprise et à obtenir vos informations personnelles dans le but de les revendre sur le Dark Web. Généralement, les cybercriminels ciblent les données de connexion, les informations personnellement identifiables (PII), les dossiers médicaux et les informations bancaires.

Toute organisation ou tout service peut être victime d'une violation de données, mais les entités ayant un grand nombre de clients font des cibles plus attrayantes. Les violations impliquent généralement des noms, des adresses e-mail, des noms d'utilisateur, des mots de passe, des adresses postales, des numéros de téléphone, des numéros de sécurité sociale et des informations de cartes de crédit (numéro, date d'expiration, CVV).

## 5.1. Examiner les violations de données

Pour examiner les violations de données dans lesquelles vos données ont été impliquées :

1. Rendez-vous dans l'onglet **VIOLATIONS DE DONNÉES**.
2. Sous certaines entrées, vous trouverez une liste d'actions requises pour sécuriser votre compte. Une fois que vous avez effectué une action, cliquez sur la case située à côté afin de confirmer.
   Si vous n'êtes pas sûr(e) de la façon d'effectuer une tâche, cliquez sur le lien inclus dans la description de la tâche et vous serez redirigé(e) vers une page qui vous expliquera la marche à suivre, étape par étape.
   Toutes les violations ne peuvent pas être traitées de cette manière. Pour certaines d'entre elles, telles que **Collection #1**, vous ne trouverez pas d'étapes à suivre. Au lieu de ça, vous serez redirigé(e) vers des articles disponibles en ligne dans lesquels vous trouverez une aide supplémentaire.

   **Note**
   Bitdefender ne stocke ni ne traite les informations personnellement identifiables. Seules les références à d'éventuelles violations de données sont conservées, sans inclure les données sensibles.

# 6. USURPATIONS D'IDENTITÉ

Les criminels qui cherchent à extorquer des données personnelles recourent à diverses formes d'usurpation d'identité, se faisant passer pour une personne de confiance afin de tromper leurs victimes et d'accéder à des informations sensibles. Cette forme d'« extorsion d'informations » se produit lorsqu'une personne se fait passer pour quelqu'un d'autre dans le but d'amener sa victime à lui fournir des données sensibles telles que des mots de passe, des numéros de cartes de crédit ou d'autres informations confidentielles.

La solution Bitdefender Digital Identity Protection surveille 25 plateformes de réseaux sociaux et vous informe instantanément lorsqu'elle détecte un profil susceptible de dissimuler une tentative d'usurpation d'identité.

## 6.1. Examiner d'éventuelles usurpations d'identité

L'onglet **USURPATIONS D'IDENTITÉ** regroupe et affiche toutes les tentatives potentielles d'usurpation d'identité. Pour chaque détection, vous pouvez choisir entre trois options :

- C'est une tentative d'usurpation d'identité
- Il s'agit de votre profil
- Il s'agit d'un autre profil

En fonction de votre choix, Bitdefender Digital Identity Protection vous invitera à suivre une série d'étapes spécifiques qui vous permettront de régler le problème. À chaque fois que vous terminerez une étape, vous pourrez la marquer comme étant **Effectuée**.

# 7. FORMATION

L'onglet Formation fait office de base de connaissance ; l'utilisateur y trouvera davantage d'informations sur la façon de protéger son identité numérique.

Les articles listés ici peuvent être classés en plusieurs catégories :

- les violations
- Expositions
- Vérification de l'usurpation d'identité

Pour accéder à la version complète d'un article, cliquez sur le lien **Poursuivre la lecture** correspondant.

# 8. HISTORIQUE DES ÉVÉNEMENTS

La section Historique des évènements nous permet de communiquer en continu avec nos utilisateurs. Elle présente une liste d'évènements, affichés par ordre chronologique, en lien avec la protection de votre identité numérique.

Hormis pour prendre connaissance des menaces nouvellement détectées (le cas échéant), vous pouvez consulter cette page pour obtenir de précieux conseils sur les comportements à adopter en ligne pour réduire au maximum vos risques d'être confronté(e) à des problèmes de confidentialité.

Dans la section Historique des évènements, vous trouverez les informations suivantes :

- Actions effectuées
- Mises à jour des services
- Violations de données

# 9. FOIRE AUX QUESTIONS

**Pourquoi la confidentialité en ligne est-elle si importante de nos jours ?**

Assurer votre confidentialité en ligne signifie protéger vos données personnelles et financières des cybercriminels. Ces informations personnellement identifiables s'échangent à prix fort sur Internet et une fois qu'elles ont fuité, votre argent n'est plus en sécurité. Vous aurez besoin d'un service fiable pour la protection et la surveillance continues de votre identité en ligne afin d'assurer la confidentialité permanente de vos données personnelles.

**Quelle est mon empreinte numérique ?**

Votre empreinte numérique correspond à l'ensemble de vos activités en ligne. Chaque connexion à vos comptes de réseaux sociaux, chaque transaction bancaire, chaque achat que vous effectuez en ligne est susceptible de faire l'objet d'une violation de données. Vous devez savoir à tout moment comment vos données personnelles et financières sont stockées et traitées - et prendre les mesures nécessaires pour les protéger.

**Que sont les violations de données et comment affectent-elles mes comptes personnels ?**

Les violations de données sont des incidents de sécurité au cours desquels des données fuitent vers des environnements non sécurisés. Ces données peuvent être exploitées par des cybercriminels du monde entier pour accéder à votre identité en ligne. Les violations de données peuvent affecter votre capacité à prendre un crédit, vos assurances, le financement de vos études ou votre épargne.

**Comment Bitdefender Digital Identity Protection peut-il contribuer à ma confidentialité en ligne ?**

Bitdefender Digital Identity Protection surveille en continu vos informations personnelles et vous alerte en temps réel en cas de violation de données. Ainsi, vous pouvez modifier vos mots de passe et sécuriser vos comptes afin de prévenir toute perte financière ou toute usurpation d'identité sur les réseaux sociaux.

**Où Bitdefender Digital Identity Protection recherche-t-il des données ?**

Bitdefender Digital Identity Protection recherche des données sur le web (réseaux sociaux, billets, blogs, forums, courtiers en données, publications, bases de données hors ligne), mais également sur les places de marché

du Dark Web, où les cybercriminels échangent des informations collectées lors de violations de données.

**En quoi Bitdefender Digital Identity Protection est-il différent des autres services (gratuits) ?**

Bitdefender Digital Identity Protection dispose de capacités inégalées qui lui permettent de contrôler des volumes considérables de données - de meilleure qualité - issues du Dark Web. Les informations issues du Dark Web sont collectées et dédupliquées afin que nous puissions réduire les alertes de faux positifs.

**Comment puis-je utiliser ce service ? Dois-je télécharger quelque chose ?**

Vous n'avez pas besoin de télécharger quoi que ce soit, dans la mesure où Bitdefender Digital Identity Protection est un service en ligne. Cette fonctionnalité vous permet d'accéder à un tableau de bord à partir duquel vous pouvez contrôler tous vos comptes personnels en temps réel.

**Comment puis-je recevoir des alertes relatives aux futures violations de données ?**

Pour recevoir des alertes relatives aux futures violations de données, il vous suffit de vous inscrire aux alertes e-mail à partir de votre tableau de bord et Bitdefender Digital Identity Protection commencera à vous envoyer des alertes concernant la confidentialité et des rapports de sécurité.

# 10. OBTENIR DE L'AIDE

## 10.1. 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.

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

## 10.2. 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.

### 10.2.1. 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/.

### 10.2.2. 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

### 10.2.3. 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.

## 10.3. 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/

### 10.3.1. 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.