Dr.WEB

Light pour Android

Manuel Utilisateur

Dr.Web Light pour Android
Version 12.2
Manuel Utilisateur
08/05/2024

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 Moscou, Russie

Site web : https://www.drweb.com/

Téléphone : +7 (495) 789-45-87

Vous pouvez trouver les informations sur les bureaux régionaux sur le site officiel de la société.

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

Doctor Web propose des solutions antivirus et antispam efficaces pour les institutions publiques, les entreprises, ainsi que pour les particuliers.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des programmes malveillants et leur conformité aux standards internationaux de sécurité.

Les certificats et les prix attribués, ainsi que l'utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

Nous remercions tous nos clients pour leur soutien !

Contenu

1. Introduction

Dr.Web Light protège les appareils mobiles fonctionnant sous le système d'exploitation Android™ contre les menaces créées spécialement pour infecter ces appareils.

L'application utilise les technologies de Doctor Web permettant de détecter et neutraliser les objets malveillants qui représentent une menace pour le fonctionnement de l'appareil et pour sa sécurité informatique.

Dr.Web Light utilise la technologie Origins Tracing™ for Android qui détecte les programmes malveillants créés spécialement pour la plateforme Android. Cette technologie permet de dépister de nouveaux virus en utilisant la base de connaissances sur les menaces connues. Origins Tracing™ for Android sait reconnaître des virus recompilés, comme Android.SMSSend, Spy, ainsi que les applications infectées par Android.ADRD, Android.Geinimi, Android.DreamExploid. Les noms des menaces détectées à l'aide d'Origins Tracing™ for Android sont basés sur le modèle «Android.*VirusName*.origin».

Dr.Web Light utilise Dr.Web Mobile Engine SDK - outil de création des applications pour Android avec un niveau de sécurité élevé. Grâce aux diverses méthodes de détection des menaces, il assure la sécurité contre les menaces connues et les menaces nouvelles pour les plateformes mobiles.

À propos du manuel

Ce Manuel est destiné à aider les utilisateurs des appareils fonctionnant sous l'OS Android à installer, à configurer l'application et à découvrir ses fonctions principales.

Les styles utilisés dans ce manuel :

Style	Commentaire
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
Réseau antivirus	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<*IP-address*>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
`Internal storage/Android/`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

1.1. Fonctions de Dr.Web

Dr.Web Light possède les fonctions suivantes :

- Suit des modifications dans le système de fichiers en temps réel (des fichiers enregistrés, des applications installées, etc.).
- Analyse tous les fichiers dans la mémoire ou les fichiers et les dossiers particuliers à la demande de l'utilisateur.
- Analyse des archives.
- Surveille les modifications dans la zone système.
- Supprime ou met en quarantaine des menaces détectées.
- Débloque l'appareil s'il a été bloqué par un ransomware.
- Permet de débloquer l'appareil de l'ami.
- Effectue des mises à jour régulières des bases virales Dr.Web par Internet.
- Enregistre des statistiques sur les menaces détectées et sur les actions de l'application, écrit le journal d'événements.

Dr.Web Light peut fonctionner dans le mode Multi-Window, ce qui permet de lancer plusieurs applications dans des fenêtres séparées. Le fonctionnement dans ce mode est possible uniquement sur les appareils Samsung Galaxy S III ou supérieur et Samsung Galaxy Note 2 ou supérieur.

2. Pré-requis système

Avant l'installation, assurez-vous que votre appareil possède les pré-requis système suivants :

Paramètre	Pré-requis
Système d'exploitation	Android en version 4.4 - 14.0
Processeur	x86/x86-64/ARMv7/ARMv8
Mémoire vive disponible	512 Mo au minimum
Espace disque disponible	35 Mo au minimum (pour le stockage de données)
Résolution de l'écran	800x480 au minimum
Autre	Connexion Internet (pour la mise à jour des bases virales)

Sur les appareils ayant des firmwares personnalisé et sur les appareils avec l'accès root ouvert (rootés), le fonctionnement correct de Dr.Web Light n'est pas garanti.

Par défaut, l'application est installée dans la mémoire interne de l'appareil. Pour un fonctionnement correct de Dr.Web Light ne déplacez pas l'application installée sur des supports amovibles.

3. Installation de Dr.Web

Installation depuis Google Play

Pour installer Dr.Web depuis Google Play, assurez-vous que :

- Vous avez un compte Google.
- Votre appareil est associé au compte Google.
- L'appareil possède une connexion Internet.
- L'appareil satisfait aux pré-requis système.

Pour installer l'application

1. Ouvrez Google Play sur votre appareil, trouvez l'application Dr.Web Light dans la liste d'applications et appuyez sur **Installer**.

   

   Si vous n'arrivez pas à trouver Dr.Web Light dans Google Play, il est possible que votre appareil ne satisfait pas aux pré-requis système.

2. Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Installation depuis Xiaomi GetApps

Pour installer Dr.Web depuis Xiaomi GetApps, assurez-vous que :

- Vous avez un compte Xiaomi.
- Votre appareil est associé au compte Xiaomi.
- L'appareil possède une connexion Internet.
- L'appareil satisfait aux pré-requis système.

Pour installer l'application

1. Ouvrez Xiaomi GetApps sur votre appareil, trouvez l'application Dr.Web Light dans la liste des applications et appuyez sur **Télécharger**.

   

   Si vous n'arrivez pas à trouver Dr.Web Light dans Xiaomi GetApps, votre appareil ne satisfait pas aux pré-requis système.

2. Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

4. Mise à jour et suppression de Dr.Web

Mise à jour de Dr.Web

Si la mise à jour automatique n'est pas configurée pour les applications de Google Play, vous pouvez lancer la mise à jour manuellement :

1. Ouvrez l'application **Play Store**.
2. Appuyez sur l'icône de votre profil Google.
3. Sélectionnez l'élément **Gérer les applications et l'appareil**.
4. Ouvrez l'onglet **Gérer**.
5. Appuyez sur la liste **Mise à jour disponible** et effectuez l'une des actions suivantes :
   - Sélectionnez **Dr.Web Light** et appuyez sur **Mettre à jour**.
   - Cochez la case contre **Dr.Web Light** et appuyez sur l'icône .

   L'application figure dans la liste **Mise à jour disponible** si la nouvelle version de l'application est déjà sortie.
6. De nouvelles autorisations peuvent être requises lors de la mise à jour. Dans ce cas, la fenêtre de confirmation va s'ouvrir.

   Appuyez sur **Accepter** pour autoriser l'accès aux fonctions de l'appareil nécessaires pour l'application.

   Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Suppression de Dr.Web

Pour supprimer Dr.Web

1. Dans les paramètres de l'appareil, sélectionnez **Applications** ou **Gestionnaire d'applications**.
2. Dans la liste des applications installées, sélectionnez **Dr.Web Light** et appuyez sur **Supprimer**.

Le dossier de la quarantaine et les fichiers journaux ne sont pas supprimés automatiquement. Vous pouvez les supprimer manuellement du dossier `Android/data/com.drweb/files` de la mémoire interne de l'appareil.

Sur les appareils tournant sous Android 11 ou une version supérieure, les journaux sont enregistrés dans le dossier `Download/DrWeb`.

5. Mise en route

Après l'installation de Dr.Web Light, vous pourrez prendre connaissance de l'interface et du menu principal de l'application, configurer le panneau de notifications et ajouter le widget Dr.Web sur l'écran d'accueil de l'appareil.

5.1. Contrat de licence

Au premier démarrage de l'application, vous serez invité à lire le Contrat de Licence. Vous devez l'accepter pour continuer à utiliser l'application.

Dans la même fenêtre, vous serez invité à accepter l'accord sur l'envoi des statistiques de fonctionnement du logiciel et des menaces détectées sur les serveurs de Doctor Web, Google et Yandex. L'option d'envoi des données statistiques ne peut être désactivée que dans la version avancée de Dr.Web.

5.2. Autorisations

A partir de la version 6.0, dans l'OS Android, il existe une option permettant d'autoriser ou d'interdire aux applications l'accès aux fonctions de l'appareil ainsi qu'aux données personnelles.

Après avoir installé Dr.Web Light et accepté les termes du contrat de licence, accordez à l'application les autorisations nécessaires. Dr.Web Light demande les autorisations obligatoires suivantes :

- Sur les appareils fonctionnant sous Android en version 10.0 ou antérieure : l'accès aux photos, aux médias et aux fichiers.
- Sur les appareils tournant sous Android 11.0 ou une version supérieure : l'accès à tous les fichiers.

Il est impossible d'utiliser Dr.Web Light sans accorder les autorisations nécessaires. Les autorisations seront demandées à chaque ouverture de l'application jusqu'à ce que vous accordiez les autorisations en suivant les instructions ci-dessous ou celles de l'écran de demande.

Sur les appareils fonctionnant sous Android 13.0 ou une version supérieure, Dr.Web Light demande l'autorisation d'envoyer des notifications. L'autorisation est nécessaire pour que Dr.Web Light puisse utiliser le panneau de notifications pour afficher les messages sur le statut de protection de l'appareil. Si vous n'accordez pas l'autorisation, Dr.Web Light ne pourra pas vous signaler la détection de menaces et la nécessité d'analyser des fichiers suspects avant que vous ouvriez l'application.

Si vous refusez la demande d'accorder les autorisations obligatoires, vous serez invité à passer sur l'écran de paramètres :

- Sur les appareils tournant sous Android 9.0 ou une version antérieure :
  1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
  2. Sélectionnez l'élément **Mémoire** ou **Stockage** et accordez l'autorisation à l'aide de l'interrupteur.
- Sur les appareils fonctionnant sous Android 10.0 :
  1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
  2. Sélectionnez l'élément **Mémoire** ou **Stockage** dans la catégorie **Accès refusé**, puis sélectionnez l'option **Autoriser**.
- Sur les appareils tournant sous Android 11.0 ou une version supérieure :
  1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
  2. Sélectionnez l'élément **Fichiers et contenus multimédias** ou bien **Stockage** dans la catégorie **Accès refusé** et puis sélectionnez l'option **Autoriser la gestion de tous les fichiers**. En utilisant cette option, vous accordez un accès aux photos et fichiers multimédia ainsi qu'à tous les fichiers.

Pour consulter la liste de toutes les autorisations pour Dr.Web Light

1. Ouvrez les paramètres de l'appareil .
2. Appuyez sur **Applications** ou **Gestionnaire d'applications**.
3. Trouvez Dr.Web Light dans la liste des applications installées et appuyez dessus.
4. Sur l'écran **À propos de l'application**, sélectionnez l'élément **Autorisations**.
5. Dans le menu se trouvant en haut à droite, sélectionnez **Toutes les autorisations**.

5.3. Interface

Écran d'accueil

À la première ouverture de l'application, l'écran contient la barre d'état, les informations sur la version complète de l'application, le menu du Scanner Dr.Web et le panneau de navigation Dr.Web (voir Figure 1).

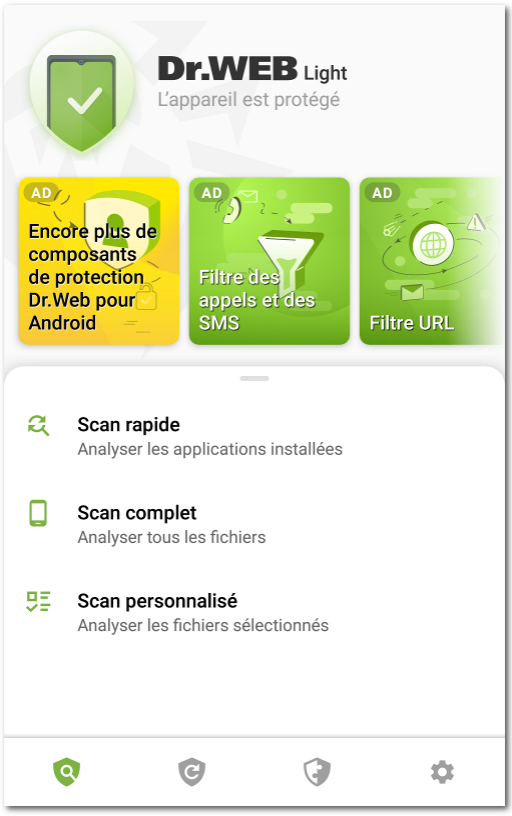

Figure 1. Écran d'accueil de Dr.Web

Barre d'état

Dans la partie supérieure de l'écran d'accueil de Dr.Web se trouve la barre d'état avec l'identificateur qui représente l'état actuel de la protection de l'appareil (voir Figure 2).

Figure 2. Barre d'état

- L'indicateur vert signifie que l'appareil est protégé. Aucune intervention n'est requise.
- L'indicateur jaune signifie que Dr.Web a détecté des problèmes de sécurité, tels que de nouveaux fichiers ajoutés sur l'appareil ou les bases virales obsolètes. Appuyez sur le panneau pour lancer un scan personnalisé de l'appareil.

Informations sur la version complète de l'application

Au-dessous de la barre d'état se trouvent les diapositives portant les informations sur les fonctionnalités de la version complète de l'application. Les diapositives fournissent les

informations sur l'antivirus Dr.Web Security Space pour Android et permettent de le télécharger sur Google Play.

Appuyez sur la première diapositive pour ouvrir la page Dr.Web Security Space pour Android dans Google Play. Appuyez sur une des diapositives suivantes pour prendre connaissances des fonctionnalités de chaque composant disponible dans Dr.Web Security Space pour Android. Le bouton **En savoir plus** sur la diapositive permet d'ouvrir la page Dr.Web Security Space pour Android sur le site de la société Doctor Web. Faites défiler la diapositive à gauche pour aller à la diapositive suivante.

Panneau de navigation

En bas de l'écran se trouve le panneau de navigation Dr.Web qui vous permet de basculer entre les onglets des composants.

- L'onglet Scanner permet de lancer un scan du système à la demande de l'utilisateur. Trois types de scan sont possibles : scan rapide, scan complet et scan personnalisé.
- Bases virales informe sur le statut actuel des bases virales et permet de lancer manuellement la mise à jour des bases virales.
- L'onglet **Outils** contient les composants suivants :
  - Statistiques permet de consulter les statistiques sur les menaces détectées et les actions appliquées à ces menaces.
  - Quarantaine permet de consulter la liste des menaces placées en quarantaine et de les traiter.
  - Aide à l'ami permet de débloquer l'appareil de l'ami bloqué par l'Antivol Dr.Web.
- L'onglet Paramètres permet de configurer les composants et l'application Dr.Web.

5.4. Notifications

Sur les appareils tournant sous Android 7.0 ou une version supérieure, toutes les notifications Dr.Web sont groupées dans une seule notification déroulante.

Sur les appareils tournant sous Android 8.0 ou une version supérieure, les notifications de Dr.Web sont divisées en catégories ou en chaînes. Vous pouvez gérer chaque catégorie de notifications dans les paramètres de l'appareil. Si vous désactivez une catégorie, vous ne recevrez plus les notifications de cette catégorie. Toutes les catégories sont activées par défaut.

Catégories de notifications

Catégorie	Notifications
Détection d'une menace	Notifications de menaces détectées par le Scanner Dr.Web.

Catégorie	Notifications
Statut de la protection antivirus	Si le panneau de notifications est désactivé, cette catégorie contient les notifications suivantes : • **L'appareil est protégé**. Elle s'affiche si l'analyse du Scanner Dr.Web n'est pas lancée. • Notification sur le type de scan du Scanner Dr.Web. Elle s'affiche si un scan rapide, complet ou personnalisé est lancé. Si le panneau de notifications est activé, une notification s'affiche vous informant de l'analyse en cours, si une des analyses du Scanner Dr.Web est lancée.
Notifications des amis	Notifications reçues des amis.
Autres	• **Les permissions sont requises**. Elle s'affiche lors de l'ouverture de l'application si l'accès aux photos, multimédias et fichiers a été refusé.
Grouper les notifications	Cette catégorie ne contient pas de notifications particulières, mais elle permet de grouper toutes les notifications Dr.Web dans une seule notification déroulante.

Panneau de notifications

Le panneau de notifications Dr.Web (voir Figure 3) affiche rapidement les notifications sur les modifications suspectes dans la zone système et les menaces potentielles.

Le panneau de notifications affiche l'indicateur de l'état actuel de la protection — sur les appareils sous Android 11.0 ou une version antérieure, — sur les appareils Android 12.0 ou une version supérieure. Si Dr.Web détecte de nouveaux fichiers sur l'appareil ou des modifications suspectes dans la zone système, l'indicateur dans le panneau de notifications devient jaune. Si Dr.Web détecte des menaces, l'indicateur devient rouge.

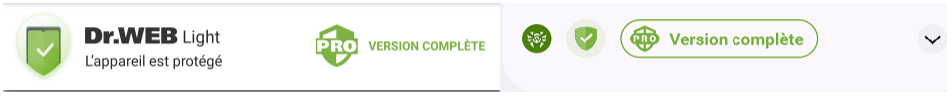

Figure 3. Panneau de notifications sous Android 11.0 (à gauche) et Android 12.0 (à droite)

Pour activer le panneau de notifications Dr.Web

1. Appuyez sur l'icône dans le panneau de navigation Dr.Web.
2. Sélectionnez **Paramètres généraux**.
3. Activez l'option **Panneau de notifications**.

Sous Android 5.0 ou 5.1, si Dr.Web détecte une modification suspecte dans la zone système ou une menace, le panneau de notifications s'affiche par-dessus toutes les applications jusqu'à ce qu'une action ne soit appliquée à l'objet détecté ou que vous fassiez défiler la notification de menace du panneau de notifications.

Avec le panneau de notifications, vous pouvez effectuer les actions suivantes :

- Ouvrir l'écran d'accueil de l'application si l'indicateur est vert et l'état actuel de la protection est le suivant : **L'appareil est protégé**. Pour ce faire, appuyez sur l'indicateur.
- Lancer un scan personnalisé si l'indicateur est jaune et l'état actuel de la protection est le suivant : **Lancez un scan**. Pour ce faire, appuyez sur l'indicateur.
- Ouvrir les résultats du scan si l'indicateur est rouge et l'état actuel de la protection est le suivant : **Résolvez les problèmes**. Pour ce faire, appuyez sur l'indicateur.
- Consulter les informations sur l'application Dr.Web Security Space pour Android et la télécharger pour une période gratuite de 14 jours. Pour ce faire, appuyez sur le texte **Version complète**.

Pour voir l'état de la protection, les actions actuelles et recommandées sur les appareils tournant sous Android 12.0 ou une version supérieure, appuyez sur ⌄.

5.5. Widget

Pour rendre la gestion de Dr.Web Light plus facile, vous pouvez ajouter sur l'écran d'accueil de votre appareil un widget spécial permettant de contrôler l'état de protection de l'appareil.

Pour ajouter un widget Dr.Web

1. Ouvrez la liste des widgets disponibles sur votre appareil mobile.
2. Dans la liste, sélectionnez le widget Dr.Web.

Le widget affiche l'état actuel de la protection (voir Figure 4).

- Le widget sans indicateur vous informe de l'absence de menaces. Aucune action n'est requise.
- Le widget avec un indicateur jaune signale la détection de nouveaux fichiers et applications sur l'appareil. Appuyez sur le widget pour lancer le scan de nouveaux objets.
- Le widget avec un indicateur rouge signale la nécessité de neutraliser les menaces détectées. Appuyez sur le widget pour ouvrir l'écran de résultats de scan et sélectionner les actions à appliquer aux menaces détectées.

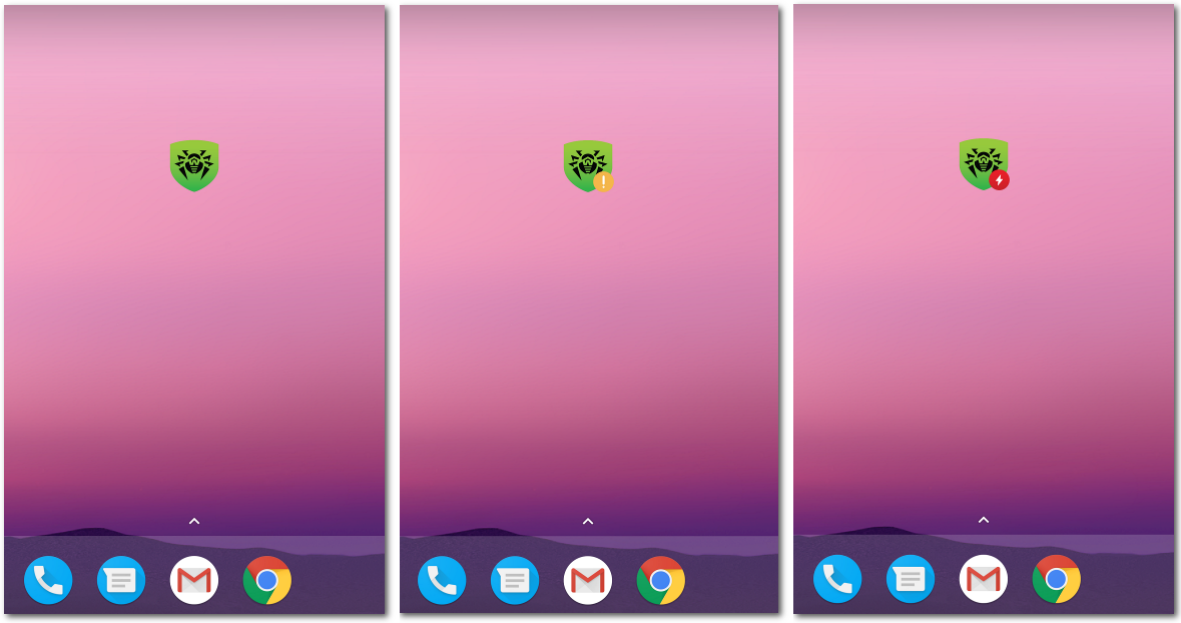

Figure 4. Widget Dr.Web

6. Composants de Dr.Web

Vous pouvez accéder au composant Dr.Web par le panneau de navigation en bas de l'écran.

- Scanner permet de lancer un scan du système à la demande de l'utilisateur. Trois types de scan sont possibles : scan rapide, scan complet et scan personnalisé.
- Bases virales informe sur le statut actuel des bases virales et permet de lancer manuellement la mise à jour des base virales.
- Statistiques permet de consulter les statistiques sur les menaces détectées et les actions appliquées à ces menaces.
- Quarantaine permet de consulter la liste des menaces placées en quarantaine et de les traiter.
- Aide à l'ami permet de débloquer l'appareil de l'ami bloqué par l'Antivol Dr.Web.
- Paramètres permet de configurer les composants et l'application Dr.Web.

6.1. Protection antivirus

- Le Scanner Dr.Web permet de lancer une analyse pour la présence de menaces.
- Sur l'écran Résultats du scan, vous pouvez sélectionner des actions pour neutraliser les menaces détectées.

6.1.1. Scanner Dr.Web : scan sur demande de l'utilisateur

Le composant Scanner Dr.Web effectue le scan du système sur demande de l'utilisateur. Il permet d'effectuer un scan rapide ou complet du système de fichiers, ainsi que de scanner des dossiers et des fichiers spécifiques.

Il est fortement recommandé de scanner périodiquement le système de fichiers. D'habitude, il suffit d'effectuer un scan rapide.

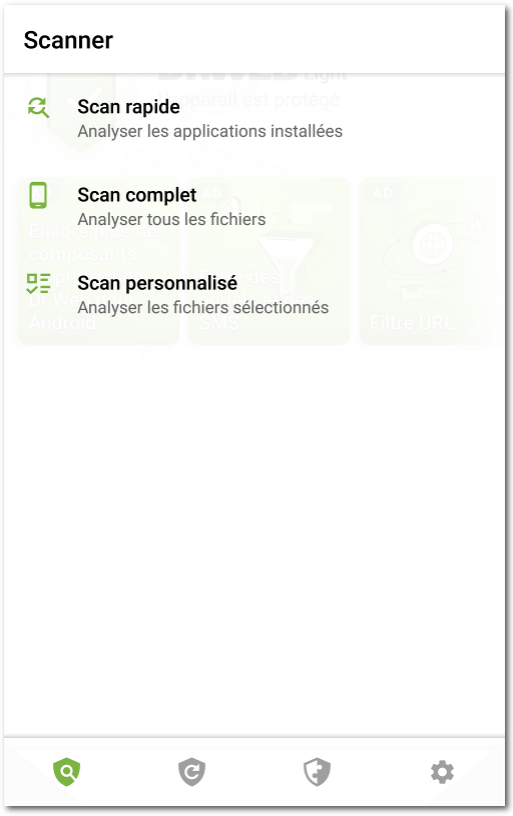

Figure 5. Scanner Dr.Web

Analyse

Pour analyser le système, appuyez sur l'icône dans le panneau de navigation Dr.Web. Ensuite, effectuez l'une des actions suivantes sur l'écran **Scanner** (voir Figure 5) :

- Pour scanner seulement les applications installées, sélectionnez l'élément **Scan rapide**.
- Pour scanner tous les fichiers, sélectionnez l'élément **Scan complet**.
- Pour analyser certains dossiers et fichiers, appuyez sur **Scan personnalisé**, puis sélectionnez les objets à scanner dans la liste des objets du système de fichiers (voir Figure 6). Pour sélectionner tous les objets, cochez la case en haut à droite de l'écran. Ensuite, appuyez sur **Scan**.

> Sur les appareils tournant sous Android 11.0 ou une version supérieure, les dossiers `/Android/data` et `/Android/obb` sont protégés par le système et ne sont pas disponibles pour l'analyse.

Si lors d'une analyse, le Scanner Dr.Web détecte des menaces, l'indicateur au centre de l'écran de scan tournera en rouge. Appuyez sur l'indicateur ou sur le nombre de menaces détectées pour ouvrir les résultats du scan (voir Figure 7) et neutraliser les menaces. Si vous avez fermé l'écran de scan ou que vous avez fermé l'application, vous pouvez ouvrir les résultats de l'analyse en appuyant sur l'icône dans le panneau de notifications.

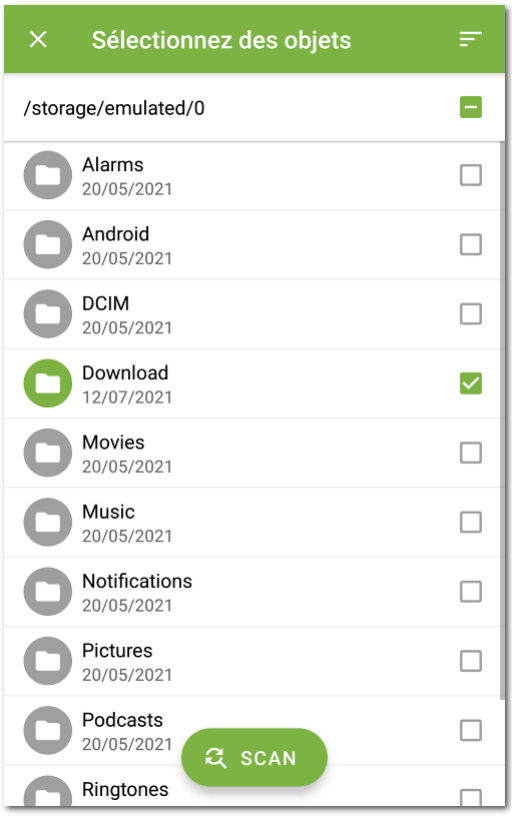

Figure 6. Analyse personnalisée

Envoi des fichiers suspects au laboratoire antivirus de Doctor Web

Vous pouvez envoyer au laboratoire antivirus de Doctor Web des archives ZIP suspectes (des fichiers ayant l'extension `.jar`, `.apk`) probablement contenant des virus, des fichiers ayant l'extension `.odex`, `.dex`, `.so` ou des archives ZIP saines provoquant un faux positif.

Pour envoyer un fichier au laboratoire

1. Appuyez et maintenez le fichier dans la liste des objets du système de fichiers (voir Figure 6), puis appuyez sur le bouton **Envoyer au Laboratoire**.
2. Sur l'écran suivant, entrez votre adresse e-mail, si vous voulez recevoir les résultats de l'analyse du fichier envoyé.
3. Sélectionnez une catégorie de votre requête :
   - **Fichier suspect**, si vous croyez que le fichier représente une menace.
   - **Faux positif**, si vous croyez que le fichier est considéré comme menace par erreur.
4. Appuyez sur **Envoyer**.

Vous pouvez envoyer au laboratoire antivirus de Doctor Web des fichiers dont la taille ne dépasse pas 250 Mo.

Paramètres du Scanner Dr.Web

Pour accéder aux paramètres du Scanner Dr.Web, ouvrez l'écran Paramètres et sélectionnez l'élément **Scanner**.

- Pour activer le scan des fichiers dans les archives, cochez la case **Fichiers archivés**.

> Par défaut, l'analyse des archives est désactivée. L'activation de l'analyse des archives peut affecter les performances du système et augmenter la consommation de la batterie. Dans ce cas, même si l'analyse des archives est désactivée, la protection reste fiable, car le Scanner Dr.Web analyse les fichiers d'installation APK indépendamment de la valeur spécifiée pour **Fichiers archivés**.

- Pour suivre les modifications dans la zone système, cochez les cases **Zone système** et **Tous les fichiers de la la zone système**. Si ces paramètres sont activés, le composant suit les modifications (ajout, modification et suppression de fichiers) et vous informe de l'ajout ou de la modification des fichiers exécutables : `.jar`, `.odex`, `.so`, fichiers au format APK, ELF, etc.
- Pour activer/désactiver l'analyse du système pour la présence des fichiers qui peuvent représenter une menace, cochez/décochez les cases correspondants :
  - Objets suspects,
  - Adwares,
  - Dialers,
  - Canulars,
  - Riskwares,
  - Hacktools,
  - Logiciels vulnérables.

Statistiques

L'application enregistre les événements liés au fonctionnement du Scanner Dr.Web (le mode et les résultats du scan, la détection des menaces de sécurité). Les actions de l'application sont affichées dans la section **Événement** de l'onglet **Statistiques**. Les actions sont triées par date (voir la rubrique Statistiques).

6.1.2. Résultats du scan

Si le Scanner Dr.Web détecte des menaces, l'écran affichera :

- L'icône dans la barre d'état d'Android en haut à gauche de l'écran :
  - — sous Android 4.4,
  - — sous Android 5.0–11.0,
  - — sous Android 12.0 ou une version supérieure.

- Un pop-up en bas de l'écran.
- Indicateur rouge sur l'écran de scan.

Pour ouvrir les résultats du scan, appuyez sur la croix en haut à gauche de l'écran du scan achevé ou sur l'indicateur de la notification ou dans la barre d'état.

Sous Android 5.0 ou une version supérieure, une notification de menace s'affiche sur l'écran de verrouillage de l'appareil. Depuis cet écran vous pouvez accéder aux résultats du scan.

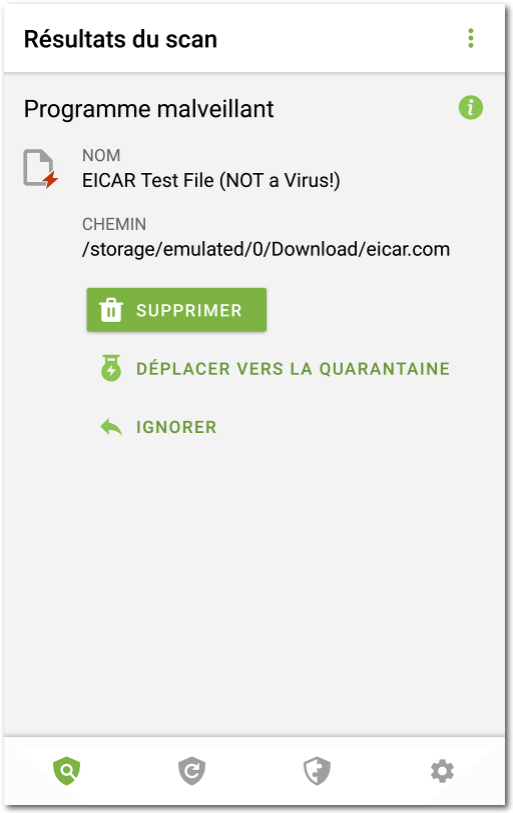

Figure 7. Résultats du scan

Neutralisation des menaces

Sur l'écran **Résultats du scan**, vous pouvez consulter la liste de menaces ou de modifications suspectes dans la zone système. Le type et le nom sont indiqués pour chaque objet.

Les objets sont marquées de couleurs différentes en fonction du niveau de danger. Types d'objets classés dans l'ordre décroissant de danger :

1. Programme malveillant.
2. Modification. Sur l'écran **Résultats de l'analyse**, le type d'objet s'affiche comme **Programme malveillant**, mais le code couleur diffère.

3. Objet suspect.
4. Adware.
5. Dialer.
6. Canular.
7. Riskware.
8. Hacktool.
9. Logiciel vulnérable.

Le niveau de danger le plus faible est attribué aux modifications dans la zone système :

- Nouveaux fichiers dans la zone système.
- Modification de fichiers système.
- Suppression de fichiers système.

Pour voir le chemin d'accès au fichier, sélectionnez l'objet correspondant. Le nom de package de l'application est également indiqué pour les menaces détectées dans les applications.

En cas de détection d'une archive contenant plusieurs menaces, sélectionnez l'objet correspondant et appuyez sur **Développer** pour ouvrir la liste complète de toutes les menaces dans l'archive.

> La détection de menaces dans l'archive est possible uniquement si l'option Fichiers archivés est activée.

Neutralisation de toutes les menaces

Pour supprimer toutes les menaces en même temps

- Sélectionnez **Menu** > **Supprimer tout** en haut à droite de l'écran **Résultats du scan**.

Pour déplacer toutes les menaces en quarantaine en même temps

- Sélectionnez **Menu** > **Mettre tout en quarantaine** en haut à droite de l'écran **Résultats du scan**.

Neutralisation de menaces une par une

Un ensemble d'options est disponible pour chaque objet. Pour ouvrir une liste d'options, sélectionnez un objet. Les options recommandées sont les premières dans la liste. Sélectionnez l'une des options suivantes :

Supprimer : pour supprimer définitivement la menace de l'appareil.

Dans certains cas Dr.Web ne peut pas supprimer les applications qui utilisent les fonctionnalités

spéciales d'Android. Si vous sélectionnez l'option **Supprimer**, mais Dr.Web ne supprime pas l'application, passez en mode sécurisé et supprimez l'application manuellement.

L'option n'est pas disponible pour les menaces se trouvant dans les applications système.

Déplacer vers la Quarantaine : pour déplacer une menace dans le dossier isolé (voir la rubrique Quarantaine).

Si la menace est détectée dans une application installée, il n'est pas possible de la placer en quarantaine. Dans ce cas, l'option **Déplacer vers la Quarantaine** n'est pas disponible.

Ignorer : pour laisser intacte pour le moment la modification de la zone système ou la menace.

Envoyer au Laboratoire ou **Faux positif** : pour envoyer le fichier pour l'analyse au laboratoire antivirus de Doctor Web. L'analyse montrera si le fichier présente un danger ou qu'il s'agit d'un faux positif. Si c'est un faux positif, il sera corrigé. Pour obtenir les résultats de l'analyse, indiquez l'adresse e-mail.

Si le fichier est envoyé avec succès au laboratoire, l'action **Ignorer** s'applique automatiquement à l'objet.

L'option **Envoyer au Laboratoire** est disponible uniquement pour les fichiers ajoutés ou les fichiers exécutables modifiés dans la zone système : `.jar`, `.odex`, `.so`, fichiers aux formats APK, ELF, etc.

L'option **Faux positif** est disponible uniquement pour les modifications des menaces et pour les menaces détectées dans la zone système.

En savoir plus sur Internet pour ouvrir la page contenant la description de l'objet détecté sur le site de Doctor Web.

6.1.2.1. Menaces dans les applications système

Les applications installées dans la zone système peuvent, dans certains cas, réaliser les fonctions typiques pour les programmes malveillants. C'est pour cette raison, Dr.Web peut considérer ces applications comme des menaces.

L'option **Déplacer vers la Quarantaine** n'est pas disponible pour les applications système et pour toutes les applications installées.

Si l'application système peut être désinfectée ou supprimée sans perte d'efficacité de l'appareil, l'option correspondante sera disponible dans la version complète de Dr.Web. Pour cela, l'accès root doit être autorisé.

Si l'application système ne peut pas être supprimée sans perte d'efficacité de l'appareil, l'option **Supprimer** ne sera pas disponible, mais vous pouvez suivre les recommandations suivantes :

- Arrêtez l'application dans les paramètres de l'appareil. Sélectionnez l'application considérée comme une menace dans la liste de l'écran **Paramètres** > **Applications**, puis sur l'écran contenant les informations sur cette application, appuyez sur **Arrêter**.

Il est nécessaire de répéter cette action à chaque fois que l'appareil est redémarré.

- Désactivez l'application dans les paramètres de l'appareil. Sélectionnez l'application considérée comme une menace dans la liste de l'écran **Paramètres** > **Applications**, puis sur l'écran contenant les informations sur cette application, appuyez sur **Désactiver**.
- Si un firmware personnalisé est installé sur votre appareil, vous pouvez restaurer les paramètres par défaut et revenir au système officiel du fabricant de votre appareil vous-même ou en s'adressant au centre de services.
- Si vous utilisez le système d'exploitation officiel, veuillez contacter le fabricant de votre appareil pour en savoir plus sur cette application.
- Si votre appareil est rooté, vous pouvez supprimer cette application à l'aide d'outils spéciaux.

Pour désactiver la notification de détection des menace dans les applications système qui ne peuvent pas être supprimées sans perte d'efficacité de l'appareil, cochez la case **Applications systèmes** dans la section **Paramètres** > **Paramètres généraux**.

6.1.2.2. Modifications dans la zone système

Zone système : une zone de mémoire qui est utilisée par les applications système et contient des données critiques pour le fonctionnement de l'appareil et des données sensibles des utilisateurs. Si votre appareil n'est pas rooté, vous ne pouvez pas accéder à la zone système.

Des applications malveillantes peuvent obtenir un accès root et modifier la zone système : supprimer, ajouter ou modifier les fichiers et les dossiers.

Vous pouvez activer l'analyse de la zone système dans les paramètres du Scanner. Si le composant détecte des modifications suspectes, il vous en informera à la fin de l'analyse.

Modification	Nom	Type
Suppression d'un dossier avec des fichiers	read-only.area.dir.deleted.threat	Suppression de fichiers système
Suppression d'un fichier	read-only.area.deleted.threat	Suppression de fichiers système
Ajout d'un dossier avec des fichiers	read-only.area.dir.added.threat	Nouveaux fichiers dans la zone système
Ajout d'un fichier	read-only.area.added.threat	Nouveaux fichiers dans la zone système
Modification d'un fichier	read-only.area.changed.threat	Modification de fichiers système

Si le Scanner détecte l'une des modifications ci-dessus, sachez que les fichiers ou dossiers ne sont pas forcément malveillants mais la modification peut être effectuée par une application malveillante.

Les options suivantes sont disponibles pour les modifications détectées :

- Ignorer.
- Envoyer au Laboratoire : disponible uniquement en cas d'ajout ou de modification de fichiers exécutables : `.jar`, `.odex`, `.so`, fichiers aux formats APK, ELF, etc.
- En savoir plus sur Internet.

Le composant vous informe simplement des modifications ci-dessus. Pour détecter une application malveillante qui aurait pu apporter des modifications dans la zone système, effectuez un scan complet de l'appareil.

6.1.3. Applications bloqueurs de l'appareil

Dr.Web Light permet de protéger l'appareil mobile contre les ransomwares. Ces logiciels représentent un danger important. Ils chiffrent les fichiers stockés dans la mémoire interne de l'appareil et sur les supports amovibles (comme, par exemple, la carte SD). Ces programmes peuvent verrouiller l'écran et afficher des messages exigeant une rançon pour le décryptage des fichiers et le déverrouillage de l'appareil.

Les ransomwares peuvent endommager vos photos, vos vidéos et vos documents. De plus, ils volent et envoient sur le serveur de malfaiteurs des données sur l'appareil infecté (y compris l'identifiant IMEI), les contacts (noms, numéros de téléphone et e-mails), ils surveillent les appels sortants et entrants et ils peuvent les bloquer. Toutes les données recueillies, y compris les informations sur les appels, sont envoyées sur un serveur de gestion.

Dr.Web Light détecte et supprime les ransomwares lors de leur tentative de pénétrer dans l'appareil protégé. Pourtant ces programmes malveillants se caractérisent par une évolution et une modification rapides, c'est pourquoi un bloqueur peut être installé sur l'appareil mobile, surtout si les bases virales Dr.Web ne sont pas mises à jour depuis un moment et elles ne contiennent pas d'informations sur de nouveaux exemplaires.

Si votre appareil mobile est bloqué par un ransomware, vous pouvez débloquer l'appareil.

Pour débloquer l'appareil

1. Dans les 5 secondes, branchez et débranchez un chargeur.
2. Dans les 10 secondes suivantes, branchez des écouteurs.
3. Dans les 5 secondes suivantes, débranchez les écouteurs.
4. Dans les 10 secondes suivantes, secouez vivement votre appareil.

5. Dr.Web Light termine tous les processus actifs sur l'appareil, y compris le processus lancé par le bloqueur, puis un court signal de vibration s'active (sur les appareils ayant cette fonction). Ensuite, l'écran Dr.Web Light s'ouvre.

   Attention ! L'arrêt des processus actifs peut causer la perte des données non sauvegardées des applications qui étaient actives au moment du blocage de l'appareil.

6. Après le déblocage de l'appareil, il est recommandé de mettre à jour les bases virales Dr.Web et de lancer le scan rapide du système, ou bien de supprimer le logiciel malveillant.

6.2. Bases virales

Afin de détecter les menaces de sécurité, Dr.Web Light utilise les bases virales spéciales qui contiennent les informations sur toutes les menaces informatiques créées pour infecter les appareils tournant sous Android connues par les spécialistes de Doctor Web. Les bases nécessitent la mise à jour périodique, car de nouveaux logiciels malveillants apparaissent régulièrement. C'est pourquoi, l'application possède la fonctionnalité de mise à jour des bases virales via Internet.

Mise à jour

Les bases virales sont mises à jour automatiquement par Internet quelque fois par jour. Si les bases virales ne sont pas mises à jour depuis plus de 24 heures (par exemple, en cas d'absence d'une connexion Internet), vous devez lancer la mise à jour manuellement.

Pour savoir si une mise à jour manuelle est requise

1. Appuyez sur dans le panneau de navigation.
2. Dans la fenêtre qui s'ouvre, vous verrez le statut des bases virales et la date de la dernière mise à jour. Si la dernière mise à jour a eu lieu plus de 24 heures auparavant, vous devez effectuer une mise à jour manuelle.

Pour lancer une mise à jour

1. Appuyez sur dans le panneau de navigation.
2. Dans la fenêtre qui s'affiche, appuyez sur **Mise à jour**.

   Il est fortement recommandé d'effectuer la mise à jour des bases virales juste après l'installation de l'application pour que Dr.Web Light puisse utiliser les dernières informations sur les menaces connues. Dès que les experts du laboratoire antivirus de Doctor Web découvrent de nouvelles menaces, les signatures virales, les caractéristiques des virus et leurs modes d'actions sont mis à jour. Dans certains cas, les mises à jour peuvent être éditées plusieurs fois par heure.

Paramètres des mises à jour

Par défaut, les mises à jour sont téléchargées automatiquement quelques fois par jour.

Pour autoriser ou interdire l'utilisation du réseau mobile pour le téléchargement des mises à jour

1. Appuyez sur dans le panneau de navigation (voir Figure 12).
2. Sélectionnez la section **Bases virales**.
3. Pour ne pas utiliser le réseau mobile pour le téléchargement des mises à jour, cochez la case **Mise à jour par Wi-Fi**.

Si des réseaux Wi-Fi actifs ne sont pas détectés, on vous proposera d'utiliser l'Internet mobile. La modification de ce paramètre n'influence pas l'utilisation du réseau mobile par d'autres fonctions de l'application et de l'appareil mobile.

> Les mises à jour sont téléchargées sur Internet. Des frais supplémentaires de transmission de données peuvent s'appliquer. Pour plus de détails, contactez votre opérateur de téléphonie mobile.

6.3. Statistiques

Dr.Web Light enregistre les statistiques des menaces détectées et des actions effectuées par l'application.

Pour voir les statistiques de fonctionnement de l'application, appuyez sur l'icône dans le panneau de navigation et sélectionnez l'élément **Statistiques**.

Voir les statistiques

L'onglet **Statistiques** contient deux sections d'informations (voir Figure 8) :

- **Total**. Contient les informations sur le nombre total des fichiers scannés et sur le nombre des menaces détectées et neutralisées.
- **Événement**. Contient les informations sur les résultats de l'analyse effectuée par le Scanner Dr.Web, le statut de mise à jour de bases virales, les menaces détectées et les actions appliquées pour les neutraliser.

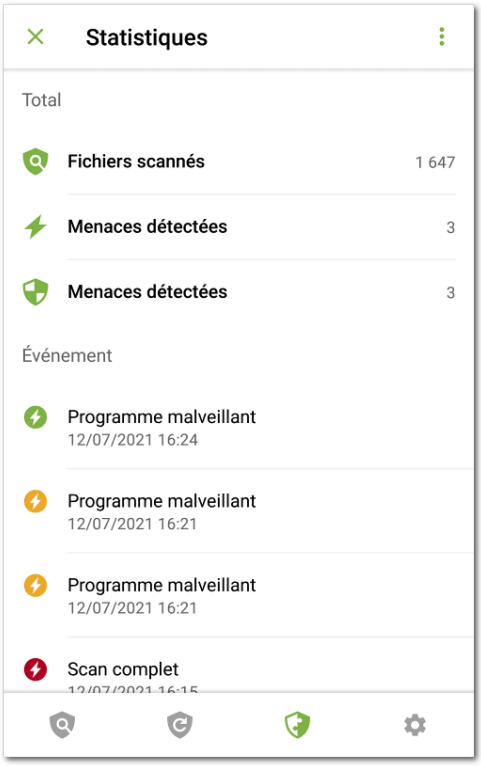

Figure 8. Statistiques

Pour effacer les statistiques

Pour effacer toutes les statistiques recueillies de l'application, appuyez sur **Menu** ⋮ dans l'onglet **Statistiques** et sélectionnez l'élément **Effacer les statistiques**.

Sauvegarder le journal des événements

Vous pouvez enregistrer le journal des événements de l'application pour l'analyse si vous rencontrez des problèmes lors de l'utilisation de l'application.

1. Appuyez sur **Menu** ⋮ dans l'onglet **Statistiques** et sélectionnez **Sauvegarder les journaux**.
2. Le journal est enregistré dans les fichiers `DrWeb_Log.txt` et `DrWeb_Err.txt` situés dans le dossier `Android/data/com.drweb/files` dans la mémoire interne de l'appareil.

> ⚠ Sur les appareils tournant sous Android 11 ou une version supérieure, les journaux sont enregistrés dans le dossier `Download/DrWeb`.

6.4. Quarantaine

Il existe une option permettant de déplacer les menaces détectées en quarantaine, dossier spécial destiné à isoler et à stocker les fichiers en toute sécurité (voir Figure 9).

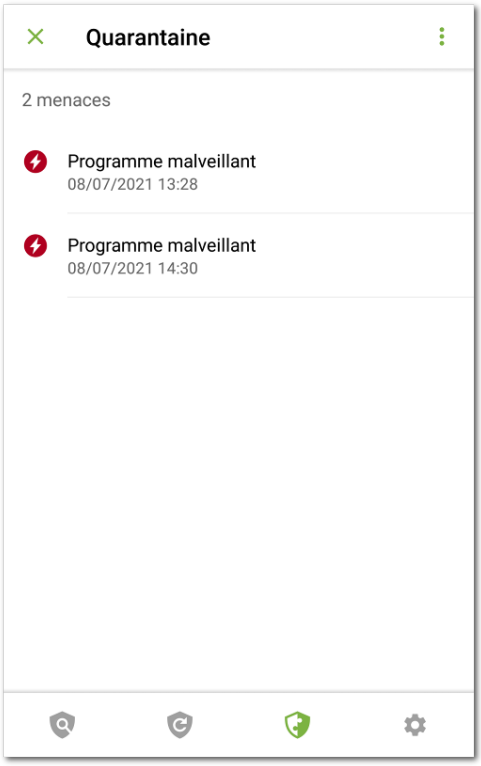

Figure 9. Quarantaine

Consulter la liste des objets en quarantaine

Pour consulter la liste des menaces placées en quarantaine, appuyez sur l'icône dans le panneau de navigation et sectionnez l'élément **Quarantaine**.

Consulter les informations sur les menaces

Pour consulter les informations sur une menace, appuyez sur son nom dans la liste.

Pour chaque menace, vous pouvez voir les informations suivantes :

- nom de fichier ;
- chemin d'accès au fichier ;
- heure et date de la mise en quarantaine.

Vous pouvez ouvrir la fiche d'informations sur la menace en la faisant défiler en haut. Faites défiler la fiche en bas pour la réduire.

Pour voir la liste de menaces dans l'archive contenant plusieurs menaces, sélectionnez l'objet correspondant et appuyez sur **Développer** contre l'élément **Menace**.

Options disponibles

Les options suivantes sont disponibles pour chaque menace :

- **En savoir plus sur Internet** : pour voir la description de la menace sur le site de Doctor Web.
- **Restaurer** : pour remettre le fichier dans le dossier où il se trouvait avant le déplacement (utilisez cette option uniquement si vous êtes absolument sûr que le fichier n'est pas dangereux).
- **Supprimer** : pour supprimer le fichier de la Quarantaine et du système.
- **Faux positif** : pour envoyer le fichier au laboratoire antivirus pour l'analyse. L'analyse montrera si le fichier présente un danger ou bien, il s'agit d'un faux positif. Si c'est un faux positif, il sera corrigé. Pour obtenir les résultats de l'analyse, indiquez votre adresse e-mail.

> L'option **Faux positif** est disponible uniquement pour les modifications des menaces.

Supprimer tous les objets de la quarantaine

Pour supprimer tous les objets placés en quarantaine :

1. Ouvrez la section **Quarantaine**.
2. Sur l'écran **Quarantaine**, appuyez sur **Menu** et sélectionnez l'élément **Supprimer tout**.
3. Appuyez sur **Supprimer**, pour confirmer l'action.
   Appuyez sur **Annuler**, pour annuler la suppression et revenir dans la section **Quarantaine**.

Taille de la quarantaine

Vous pouvez consulter les informations sur la taille de la mémoire occupée par la Quarantaine et sur l'espace libre dans la mémoire interne de l'appareil :

1. Ouvrez la section **Quarantaine**.
2. Sur l'écran **Quarantaine**, appuyez sur **Menu** et sélectionnez l'élément **Taille**.
3. Appuyez sur **OK**, pour revenir dans la section **Quarantaine**.

6.5. Aide à l'ami

Le composant **Aide à l'ami** permet de débloquer l'appareil de l'ami bloqué par l'Antivol Dr.Web.

Qu'est-ce que l'Antivol Dr.Web

L'Antivol est disponible dans l'application Dr.Web Security Space pour Android. Si l'appareil est perdue ou volé, l'Antivol bloque l'appareil. Pour le débloquer, il faut entrer le mot de passe. Si le propriétaire de l'appareil a oublié le mot de passe, vous pouvez l'aider à réinitialiser le mot de passe et débloquer l'appareil.

Comment fonctionne Aide à l'ami

Quand vous activez le composant **Aide à l'ami**, vous indiquez votre adresse e-mail et la communiquez aux utilisateurs de Dr.Web Security Space pour Android à qui vous faites confiance. Les utilisateurs de Dr.Web Security Space pour Android vous ajoutent aux amis dans l'Antivol. Vous confirmez les demandes d'ami reçues.

Si un des vos amis a besoin d'aide pour débloquer son appareil, il vous envoie une notification. Une fois la notification reçue, vous contactez votre ami pour apprendre le code de confirmation. Ensuite, vous envoyez une demande de déblocage de l'appareil d'ami. Ayant reçu la demande de déblocage, l'Antivol autorise à votre ami de réinitialiser le mot de passe. Après cela, votre ami peut continuer à utiliser l'appareil.

Pour l'interaction avec l'appareil d'ami, les deux appareils doivent être connectés à Internet. La réception de notifications peut atteindre jusqu'à 15 minutes.

Pour activer Aide à l'ami

1. Appuyez sur l'icône  dans le panneau de navigation et sélectionnez **Aide à l'ami**.
2. Sur l'écran **Aide à l'ami**, appuyez sur **Activer**.
3. Entrez votre adresse e-mail et appuyez sur **Continuer**.

Pour ajouter un ami

1. Communiquez l'adresse e-mail que vous avez indiquée à un utilisateur de Dr.Web Security Space pour Android pour qu'il puisse vous envoyer une demande d'ami.
2. Attendez la notification de demande d'ami.
3. Appuyez sur la notification pour aller à l'écran **Aide à l'ami**.
4. Appuyez sur la ligne contenant l'adresse e-mail de l'ami qui vous a envoyé la demande.
5. Appuyez sur **Confirmer** dans la fiche de l'ami pour accepter sa demande d'ami.

Si vous n'avez pas accepté ou que vous avez rejeté la demande d'ami, l'utilisateur ne pourra pas vous envoyer une demande de déblocage.

Pour changer le nom d'un ami

1. Dans la fiche d'ami (voir Figure 10), appuyez sur .
2. Entrez le nouveau nom d'ami.
3. Appuyez sur pour enregistrer les modifications.

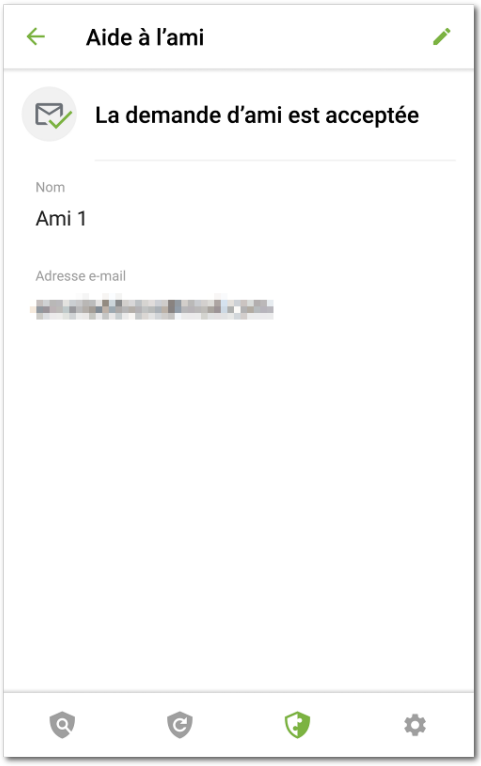

Figure 10. Fiche d'ami

Vous pouvez modifier seulement le nom d'ami. Si l'adresse e-mail de l'ami a changé ou n'est plus utilisée, vous pouvez supprimer l'ami.

Pour supprimer un ami

- Faites défiler le contact correspondant à gauche.

Si vous supprimez par erreur un contact d'ami ou une demande d'ami que vous n'avez pas encore confirmée, vous pouvez annuler la suppression en appuyant sur **Annuler**.

Pour débloquer l'appareil de l'ami

1. Appuyez sur la notification de blocage que vous avez reçue de votre ami.
2. Contactez votre ami. Il est possible que l'appareil soit perdu ou volée et la notification soit envoyée par une tierce personne.

3. S'il faut vraiment aider à débloquer l'appareil, demandez à votre ami le code de code de confirmation. Le code de confirmation est affiché sur l'écran de blocage de l'appareil de l'ami.
4. Entrez le code de confirmation et appuyez sur **Débloquer** (voir Figure 11).

Si vous avez ignoré ou fermé la notification de blocage, demandez à votre ami d'envoyer la notification encore une fois.

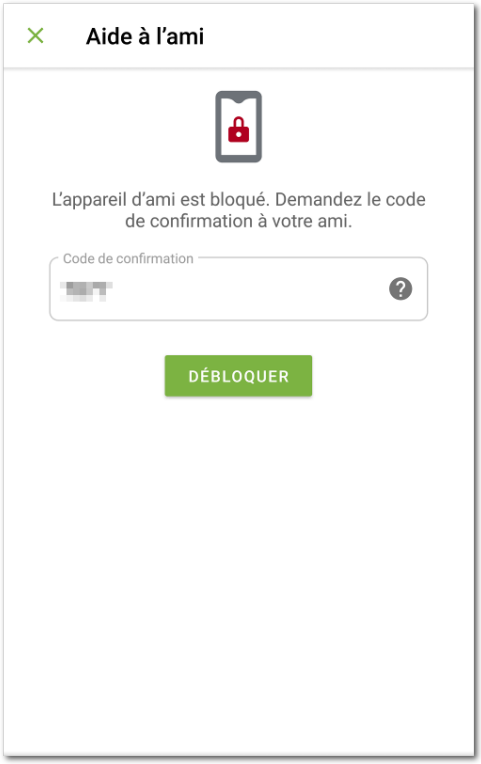

Figure 11. Code de confirmation de déblocage

Pour désactiver Aide à l'ami

1. Appuyez sur l'icône dans le panneau de navigation et sélectionnez **Aide à l'ami**.
2. Sur l'écran **Aide à l'ami**, appuyez sur **Menu** et sélectionnez **Désactiver**.

Une fois **Aide à l'ami** désactivé, tous les amis seront supprimés. Chaque ami recevra une notification l'informant que vous avez rejeté sa demande d'ami.

7. Paramètres

Pour passez aux paramètres de l'application (voir Figure 12), appuyez sur l'icône dans le panneau de navigation.

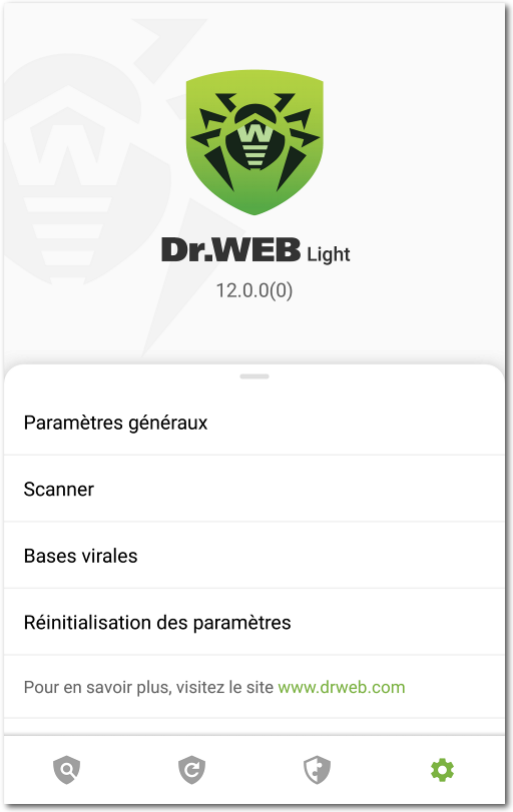

Figure 12. Paramètres

Sur l'écran **Paramètres**, les options suivantes sont disponibles :

- **Paramètres généraux** permet d'activer le mode sombre de l'application, de configurer le panneau de notifications et la notification de menaces dans les applications système, activer et désactiver les notifications sonores (voir la section Paramètres généraux).
- **Scanner**. Permet de configurer le Scanner qui effectue l'analyse sur demande de l'utilisateur (voir la section Paramètres du Scanner Dr.Web).
- **Bases virales** permet d'interdire l'utilisation de l'Internet mobile pour la mise à jour des bases virales (voir la section Bases virales).
- **Réinitialisation des paramètres**. Permet de réinitialiser les paramètres par défaut (voir la section Réinitialisation des paramètres).
- **Pour en savoir plus, visitez le site www.drweb.com** permet d'aller sur le site de la société Doctor Web et prendre connaissance des informations concernant l'application et d'autres produits de la société.

L'écran **Paramètres** permet également d'obtenir les informations sur le produit et son fabricant. La version installée du produit s'affiche dans la partie supérieure de l'écran, sous le nom du produit. Faites défiler le menu **Paramètres** en haut pour ouvrir les options d'information avancées :

- **Aide** permet de consulter la documentation de l'application Dr.Web Light.
- **Icônes de réseaux sociaux** permettent d'ouvrir la page de la société Doctor Web dans de différents réseaux sociaux.

7.1. Paramètres généraux

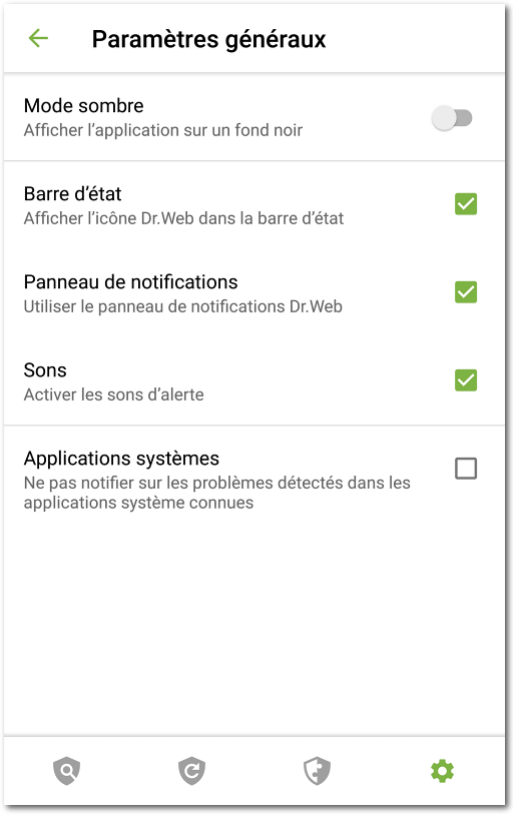

Figure 13. Paramètres généraux

Sur l'écran **Paramètres généraux** (voir Figure 13) les options suivantes sont disponibles :

- **Mode sombre** permet de choisir le mode sombre ou clair de l'application.
- **Barre d'état** : permet de configurer l'affichage de l'icône de l'application dans la barre d'état. Cette option permet également de désactiver l'affichage du panneau Dr.Web dans la zone de notification (voir la rubrique Panneau de notifications).

> Le paramètre n'est pas disponible sur les appareils tournant sous Android 8.0 ou une version supérieure.

- **Panneau de notifications** : permet de déterminer l'affichage du panneau Dr.Web dans la zone de notifications. Si l'option est activée, le panneau Dr.Web sera utilisé. Si l'option est désactivée, le panneau aura l'affichage classique du panneau de notifications Android.
- **Sons** : permet de configurer les alertes sonores de détection, suppression et déplacement des menaces en Quarantaine. Les alertes sonores sont activées par défaut.
- **Applications systèmes** permet d'activer et de désactiver la notification des menaces dans les applications système qui ne peuvent pas être supprimées sans perte d'efficacité de l'appareil. L'option est désactivée par défaut.

7.2. Réinitialisation des paramètres

Vous pouvez réinitialiser les paramètres par défaut à tout moment.

Pour réinitialiser les paramètres

1. Sur l'écran de configuration (voir Figure 12) appuyez sur **Réinitialisation des paramètres** et sélectionnez l'élément **Réinitialisation des paramètres**.
2. Confirmez la réinitialisation des paramètres par défaut.

Référence

Référence

Q

R

S

V

W

Z