Dr.WEB
Antivirus pour Windows Servers

Manuel administrateur

Antivirus Dr.Web pour Windows Servers
Version 11.0
Manuel administrateur
21/03/2017

Doctor Web, Siège social en Russie

125040

Moscou, Russie

2-12A, 3e rue Yamskogo polya

Site web : http://www.drweb.fr/

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

Antivirus Dr.Web pour Windows Servers assure une protection multiniveau de la mémoire système, des disques durs et des supports amovibles contre l'intrusion des virus, rootkits, trojans, spywares, adwares, hacktools et de tout type d'objets malveillants provenant des sources externes.

L'architecture modulaire de Dr.Web est sa caractéristique majeure. Dr.Web utilise un moteur antivirus et des bases virales communs à tous ses composants et aux différents environnements systèmes. Actuellement, en plus de Dr.Web, il existe des versions de l'antivirus pour Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian®, BlackBerry® et plusieurs systèmes basés sur Unix® (notamment Linux®, FreeBSD®, Solaris®).

Dr.Web utilise une procédure pratique est efficace de mise à jour des bases virales et des composants via Internet.

Dr.Web peut détecter et supprimer les programmes indésirables (adwares, dialers, canulars, riskwares et hacktools) de votre ordinateur. Dr.Web utilise ses composants antivirus standard pour détecter des programmes indésirables et appliquer des actions aux fichiers qu'ils contiennent.

Chaque solution antivirus Dr.Web pour les systèmes d'exploitation Microsoft® Windows® inclut l'ensemble de composants suivants :

Scanner Dr.Web – scanner antivirus avec interface graphique lancé à la demande ou selon la planification. Il scanne votre ordinateur à la recherche de virus et d'autres logiciels malveillants.

Scanner en ligne de commande Dr.Web – version en ligne de commande du Scanner Dr.Web.

SpIDer Guard – moniteur antivirus qui réside toujours en mémoire et scanne les processus lancés et les fichiers créés et détecte toute activité malveillante.

Updater Dr.Web permet aux utilisateurs enregistrés de recevoir et d'installer automatiquement les mises à jour des bases virales et des modules Dr.Web.

SpIDer Agent – module de gestion qui effectue le lancement et la configuration des composants de Dr.Web.

Protection préventive – composant contrôlant l'accès aux objets importants du système et assurant l'intégrité des applications lancées et des fichiers de l'utilisateur ainsi que la protection contre les exploits.

1.1. Contenu de ce Manuel

Ce Manuel Utilisateur décrit l'installation et l'utilisation optimale de Dr.Web.

Vous pouvez trouver une description détaillée des éléments de la GUI dans le système d'aide accessible depuis n'importe quel composant.

Ce Manuel Utilisateur décrit l'installation du logiciel et contient des conseils sur son utilisation et sur la résolution des problèmes les plus courants causés par les menaces virales. Surtout, il décrit les modes de fonctionnement standard des composants de Dr.Web (avec les paramètres par défaut).

Les Annexes contiennent des informations détaillées sur la façon de paramétrer Dr.Web.

Etant en développement constant, l'interface du logiciel peut afficher d'autres images que celles contenues dans le présent Manuel. Vous pouvez trouver une Aide toujours à jour sur http://products.drweb.fr/.

1.2. Légende et Abréviations

Les styles de texte utilisés dans ce manuel :

Styles	Description
	Avertissement sur des situations potentielles d'erreurs et sur les moments importants auxquels il faut faire attention.
Signature	Nouveau terme ou accent porté sur un terme dans des descriptions.
<fichier_clé>	Champs de remplacement des noms fonctionnels par les valeurs effectives.
Suivant	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
`C:\Windows\`	Noms des fichiers et des répertoires, fragments du code du programme.
Annexe A	Liens aux autres chapitres du manuel ou liens aux ressources externes.

1.3. Méthodes de Détection

Toutes les solutions antivirus créees par Doctor Web utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects.

Méthode de détection des menaces

Analyse de signature

Cette méthode de détection est appliquée en premier lieu. Elle est mise en oeuvre par l'examen du contenu de l'objet à la recherche des signatures de menaces connues. *Une signature* est une séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. La

comparaison du contenu de l'objet avec les signatures n'est pas effectuée directement, mais par leur sommes de contrôle ce qui permet de réduire considérablement la taille des entrées dans les bases virales tout en préservant le caractère unique de la conformité et par conséquent, l'exactitude de la détection des menaces et du traitement des objets infectés. Les entrées dans les bases virales Dr.Web sont rédigées de sorte que la même entrée peut détecter des classes entières ou des familles de menaces.

Origins Tracing

Cette une technologie unique Dr.Web permettant de détecter les nouvelles menaces ou celles modifiées et utilisant des mécanismes de contamination ou un comportement malveillant qui sont déjà connus de la base de données virale. Cette technologie intervient à la fin de l'analyse par signature et assure une protection des utilisateurs utilisant des solutions antivirus Dr.Web contre des menaces telles que Trojan.Encoder.18 (également connu sous le nom «gpcode»). En outre, l'utilisation de la technologie Origins Tracing peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Les noms des menaces détectées à l'aide d'Origins Tracing sont complétés par `.Origin`.

Émulation de l'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou très compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant l'émulateur – un modèle du processeur et de l'environnement du programme. L'Émulateur fonctionne avec un espace mémoire protégé (tampon d'émulation). Dans ce cas, les instructions ne sont pas transmises au processeur central pour exécution réelle. Si le code traité par l'émulateur est infecté, alors le résultat de son émulation est un rétablissement du code malveillant d'origine disponible pour une analyse de signature.

Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'heuristiques (hypothèses, dont la signification statistique est confirmée par l'expérience) des signes caractéristiques de code malveillant et, inversement, de code exécutable sécurisé. Chaque attribut ou caractéristique du code possède un score (le nombre indiquant l'importance et la validité de cette caractéristique). Le score peut être positif si le signe indique la présence d'un comportement de code malveillant, et négatif si le signe ne correspond pas à une menace informatique. En fonction du score total du contenu du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

L'analyseur heuristique utilise également la technologie FLY-CODE – un algorithme universel pour l'extraction des fichiers. Ce mécanisme permet de construire des hypothèses heuristiques sur la présence d'objets malveillants dans les objets, de logiciels compressés par des outils de compression (emballeurs), non seulement par des outils connus des développeurs des produits Dr.Web, mais également par des outils de compression nouveaux et inexplorés. Lors de la vérification des objets emballés, une technologie d'analyse de leur entropie structurelle est

également utilisée, cette technologie peut détecter les menaces sur les spécificités de la localisation des fragments de leur code. Cette technologie permet avec une seule entrée de la base de données de détecter un ensemble de différents types de menaces qui sont emballées du même packer polymorphe.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I (omettre une menace inconnue) ou de type II (faire un faux positif). Par conséquent, les objets marqués par l'analyseur heuristique comme « malveillants » reçoivent le statut « suspects ».

Au cours de toute analyse, tous les composants des produits antivirus Dr.Web utilisent l'information la plus récente sur tous les programmes malveillants connus. Les signatures des menaces et les informations sur leurs caractéristiques et les comportements sont mises à jour et ajoutées à la base de données de virus immédiatement, dès que les spécialistes du laboratoire antivirus Doctor Web découvrent de nouvelles menaces, parfois jusqu'à plusieurs fois par heure. Même si un nouveau malware infiltre l'ordinateur, en évitant la protection Dr.Web, il sera détectée dans la liste des processus et neutralisée après l'obtention de nouvelles bases virales.

2. Pré-requis système

Avant d'installer Dr.Web :

- supprimez tout autre antivirus installé sur votre machine afin d'éviter les incompatibilités de ses composants résidents avec les composants résidents de Dr.Web ;
- sous Windows Server 2016, désactiver manuellement Windows Defender en utilisant les stratégies de groupe ;
- installez toutes les mises à jour critiques recommandées par Microsoft. Si l'OS n'est plus supporté, migrez vers une nouvelle version de l'OS.

Dr.Web peut être installé et fonctionne sur un ordinateur possédant au minimum ces pré-requis :

Composant	**Pré-requis**
Processeur	Processeur pleinement compatible i686.
Système d'exploitation	Pour les plateformes 32-bits : • Windows Server 2003 avec Service Pack 1 ; • Windows Server 2008 avec Service Pack 2 ou supérieur. Pour les plateformes 64-bits : • Windows Server 2008 avec Service Pack 2 ou supérieur ; • Windows Server 2008 R2 ; • Windows Server 2012 ; • Windows Server 2012 R2; • Windows Server 2016.
RAM disponible	512 Mo et plus.
Espace sur le disque dur	750 Mo pour les composants Dr.Web. Les fichiers créés pendant l'installation nécessitent encore de l'espace libre.
Résolution	Résolution d'écran recommandée est au minimum de 800x600.

Antivirus Dr.Web pour serveurs n'est pas compatible avec les plugins Dr.Web pour Microsoft Exchange Server, Dr.Web pour IBM Lotus Domino, Dr.Web pour Kerio WinRoute, Dr.Web pour Kerio MailServer, Dr.Web pour Microsoft ISA Server et Forefront TMG, Dr.Web pour Qbik WinGate en version 6.0 ou version antérieure.

Pour le fonctionnement correct de Dr.Web, les ports suivants doivent être ouverts :

Destination	Direction	Numéros de ports
Pour mettre à jour (si l'option de mise à jour via https est activée)	sortant	443
Pour mettre à jour	sortant	80
Pour envoyer les notifications		25 ou 465 (ou en fonction des paramètres des notifications par e-mail)
Pour se connecter au service Dr.Web Cloud	sortants	2075 (y compris les ports UDP)

Pour d'autres pré-requis, se référer au système d'exploitation correspondant.

3. Installation, modification et suppression du logiciel

Avant l'installation de Dr.Web, faites attention aux pré-requis système, il est fortement recommandé de procéder comme suit :

- installer toutes les mises à jour critiques de Microsoft pour la version de l'OS utilisée sur votre ordinateur (elles sont disponibles sur le site de mises à jour de la société à la page : http://windowsupdate.microsoft.com) ;
- vérifier le système de fichiers en utilisant les outils système, et en cas d'erreurs détectées, résoudre le problème ;
- fermer toutes les applications en cours.

Avant de procéder à l'installation, il est nécessaire de supprimer tous les logiciels antivirus installés sur l'ordinateur afin d'éviter une éventuelle incompatibilité de leurs composants résidents.

3.1. Première installation

Il est nécessaire d'avoir les droits administrateur sur l'ordinateur pour installer Dr.Web.

Il existe les modes suivants d'installation du logiciel antivirus Dr.Web :

- en mode standard ;
- avec les paramètres de la ligne de commande.

Installation avec les paramètres de ligne de commande

Pour installer Dr.Web, entrez dans la ligne de commande le nom du fichier exécutable avec les paramètres nécessaires (ces paramètres peuvent affecter l'installation en tâche de fond, la langue d'installation et le redémarrage après l'installation) :

Paramètre	Valeur
lang	Langue utilisée pour l'installation. La valeur de ce paramètre est la langue au format ISO 639-1.
reboot	Redémarre l'ordinateur automatiquement après l'installation complète.
silent	Installation en tâche de fond.

Par exemple, pour lancer une installation de Dr.Web en tâche de fond avec un redémarrage après l'installation, exécutez la commande suivante :

```
drweb-11.0-srv-win.exe /silent yes /reboot yes
```

Installation en mode Standard

Suivez les instructions de l'assistant d'installation. A chaque étape avant la copie de fichier sur l'ordinateur, vous pouvez réaliser les fonctions suivantes :

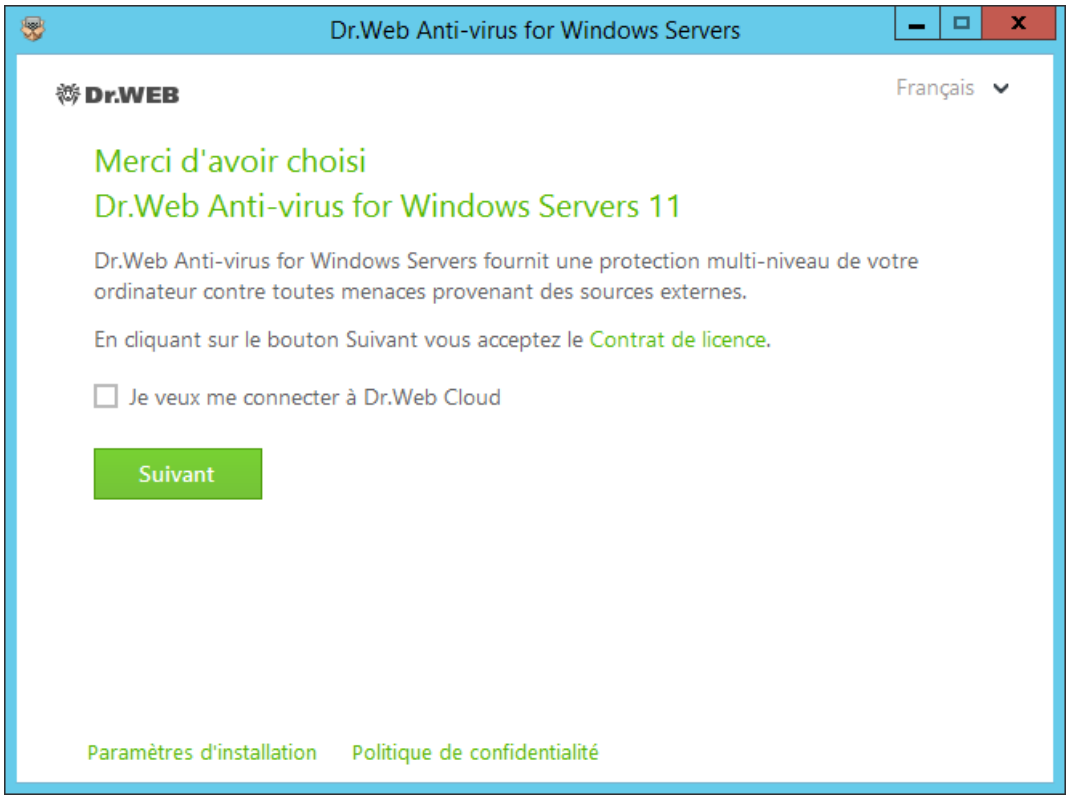
- pour revenir vers l'étape précédente de l'installation, cliquez sur **Précédent** ;
- pour passer à l'étape suivante, cliquez sur **Suivant** ;
- pour interrompre l'installation, cliquez sur **Annuler**.

Procédure d'installation

1. Si un autre antivirus est déjà installé sur votre ordinateur, l'assistant d'installation va vous alerter sur l'incompatibilité de Dr.Web avec d'autres solutions antivirus, et il vous sera proposé de les supprimer.

   Avant l'installation, le statut du fichier d'installation est vérifié. S'il existe une version plus récente du fichier d'installation, vous serez invité à la télécharger.

2. A cette étape, vous êtes invité à vous connecter aux services Cloud Dr.Web qui permettent aux composants antivirus d'utiliser les données virales les plus récentes. Ces données sont stockées et mises à jour en temps réel sur les serveurs de Doctor Web. L'option est désactivée par defaut.



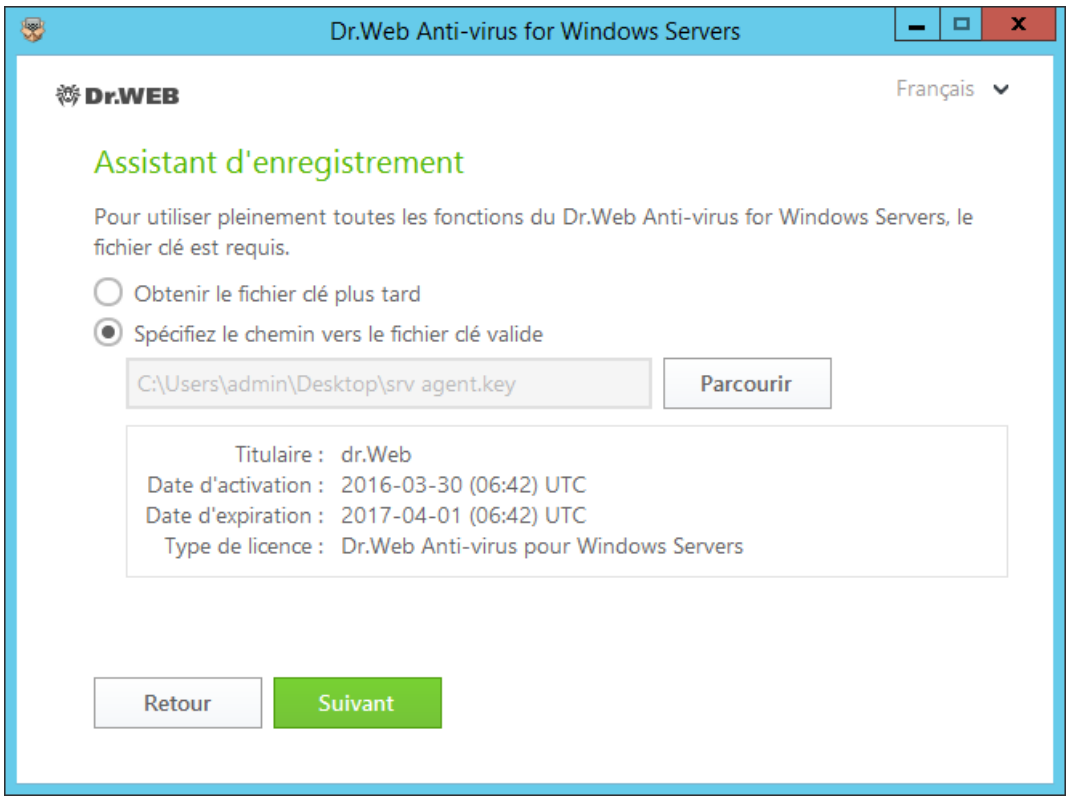
3. Pour sélectionner les composants que vous souhaitez installer, spécifiez le chemin d'installation de ces composants et d'autres paramètres puis cliquez sur **Paramètres**

d'installation. Cette option est destinée aux utilisateurs expérimentés. Si vous voulez effectuer l'installation avec les paramètres par défaut, passez à l'étape 4.

- Dans cette fenêtre, vous pouvez modifier l'ensemble de composants à installer.
- Dans cette fenêtre, vous pouvez modifier le chemin d'installation.
- Dans le troisième onglet de la fenêtre, la case **Télécharger des mises à jour pendant l'installation** est cochée afin de télécharger les mises à jour des bases virales et des composants de l'antivirus lors de l'installation. Cette fenêtre vous permet également de créer des raccourcis pour le lancement de Dr.Web.

Pour sauvegarder les modification apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**.

4. Cliquez sur **Suivant**. Ainsi vous acceptez les termes du contrat de licence.
5. Dans la fenêtre de l'**Assistant d'enregistrement,** vous êtes informé qu'une licence est requise pour que Dr.Web fonctionne. Faites une des actions suivantes :
   - si vous possédez un fichier clé sur le disque dur ou sur un support amovible, cliquez sur **Spécifier le chemin vers le fichier clé valide** et sélectionnez le fichier dans la fenêtre standard d'ouverture de fichier. Pour modifier le chemin, cliquez sur **Parcourir** et sélectionnez un autre fichier clé ;
   - pour continuer l'installation sans installer de fichier clé, sélectionnez **Obtenir la licence plus tard**. Si vous choisissez cette option, aucun des composants du logiciel ne fonctionnera avant d'avoir un fichier clé valide.



Cliquez sur **Suivant**.

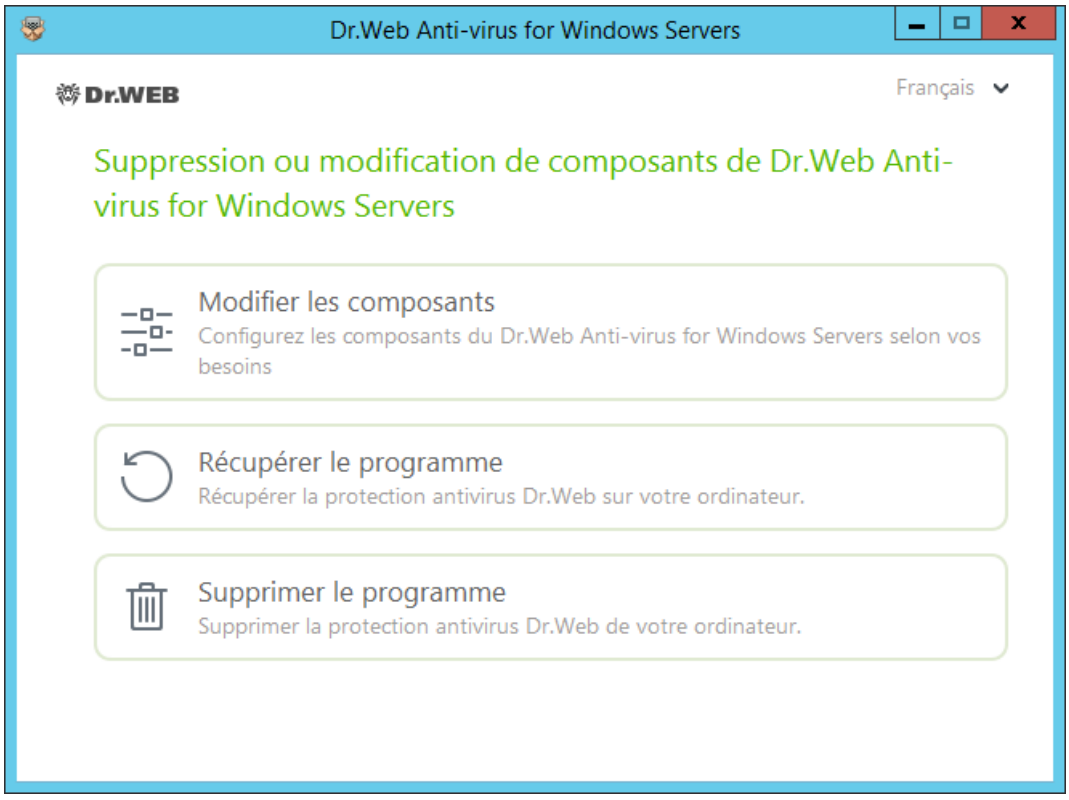
6. S'il faut spécifier manuellement les paramètres du serveur proxy, cochez la case **Configurer manuellement l'IP et le Port du proxy**. Cliquez sur **Installer**.

7. Si lors de l'installation vous avez spécifié un fichier clé valide et que vous n'avez pas décoché la case **Télécharger les mises à jour pendant l'installation**, les bases virales et d'autres composants de Dr.Web seront mis à jour. La mise à jour démarre automatiquement et ne requiert aucune action supplémentaire.
8. Pour terminer l'installation, redémarrez l'ordinateur.

3.2. Suppression ou modification du logiciel

Après la suppression de Dr.Web, votre ordinateur ne sera plus protégé contre les virus et d'autres malwares.

1. Pour supprimer ou modifier la configuration de Dr.Web en ajoutant ou supprimant des composants particuliers, lancez l'utilitaire de suppression des programmes Windows.
2. Dans la fenêtre qui apparaît, sélectionnez la ligne affichant le nom du programme. Pour supprimer définitivement le programme, cliquez sur **Désinstaller** et passez à l'étape 6. Pour modifier la configuration de Dr.Web en ajoutant ou supprimant des composants, cliquez sur **Modifier**, la fenêtre de l'Assistant de suppression/modification des composants de programme sera ouverte.



3. Pour restaurer la protection antivirus sur votre ordinateur, dans la fenêtre qui apparaît, cliquez sur **Restaurer le programme**.

4. Pour modifier la configuration de Dr.Web, sélectionnez l'élément **Modifier les composants**. Dans la fenêtre qui apparaît, cochez les cases contre les composants à ajouter et décochez les cases contre les composants à désinstaller. Dés que la configuration est déterminée, cliquez sur **Appliquer**.

   En cas de suppression des composants de Dr.Web, la fenêtre **Désactivation de l'Autoprotection** apparaît. Dans cette fenêtre, saisissez le code de confirmation, puis cliquez sur **Installer**.

5. Pour supprimer tous les composants installés, sélectionnez **Supprimer le programme**.
6. Dans la fenêtre **Paramètres sauvegardés**, cochez les cases contre les éléments à sauvegarder après la suppression du programme. Les objets et les paramètres sauvegardés peuvent être utilisés par le programme lors d'une réinstallation. Par défaut, toutes les options sont activées – **Quarantaine**, **Paramètres Dr.Web Anti-virus for Windows Servers** et **Copies de fichiers protégées**. Cliquez sur **Installer**.
7. Dans la fenêtre suivante, pour confirmer la désinstallation de Dr.Web saisissez le code affiché, puis cliquez sur **Supprimer le programme**.
8. Les modifications entrent en vigueur après le redémarrage de l'ordinateur. Vous pouvez reporter le redémarrage en cliquant sur **Plus tard**. Cliquez sur **Redémarrer maintenant** pour terminer la désinstallation et modifier l'ensemble des composants Dr.Web tout de suite.

4. Licencing

Pour utiliser Dr.Web une licence est requise. Vous pouvez acheter une licence avec un produit physique, sur le site de Doctor Web ou chez les partenaires. Une licence accorde le droit d'utiliser toutes les fonctionnalités du produit pendant toute la durée de la licence. Les droits d'utilisateur sont définis par la licence en fonction du Contrat de licence.

Fichier clé

Les droits d'utilisation de Dr.Web sont spécifiés dans le fichier spécial dit le fichier clé. Les fichiers clés reçus dans le kit de distribution du produit sont installés automatiquement et ne requièrent aucune action supplémentaire.

Le fichier clé possède l'extension .key et contient les informations suivantes :

- liste des composants antivirus fournis dans la licence ;
- durée de la licence pour le produit ;
- disponibilité du Support Technique pour l'utilisateur ;
- autres restrictions (notamment, le nombre d'ordinateurs sur lesquels vous êtes autorisé à utiliser l'antivirus).

> ⚠ Par défaut, le fichier clé est placé dans le dossier d'installation de Dr.Web. Dle logiciel vérifie le fichier régulièrement. Ne modifiez pas le fichier pour éviter de compromettre la licence.
>
> Si aucun fichier clé valide n'est trouvé, les composants de Dr.Web sont bloqués.

Un fichier clé de Dr.Web valide satisfait aux critères suivants :

- la licence n'a pas expiré ;
- l'intégrité du fichier clé n'a pas été violée.

Si l'une des conditions n'est pas respectée, le fichier clé devient invalide et Dr.Web arrête de détecter et de neutraliser les programmes malveillants et laisse passer les messages sans les analyser.

Il est recommandé de conserver le fichier clé durant toute la durée de validité de la licence.

4.1. Méthodes d'activation

Vous pouvez activer votre licence via l'un des moyens suivants :

- en obtenant le fichier clé durant l'enregistrement sur le site de Doctor Web ;
- en indiquant durant l'installation le chemin vers le fichier clé valide sur votre ordinateur ou dans la fenêtre de l'Assistant d'enregistrement.

Réactivation de la licence

Vous pourriez avoir à réactiver votre licence si vous avez perdu le fichier clé.

> ⚠ Lors de la réactivation de la licence, vous recevez le même fichier clé que durant l'enregistrement antérieur à condition que la licence n'ait pas expiré.

Si vous réinstallez le produit ou l'installez sur plusieurs ordinateurs, la réactivation du numéro de série n'est pas requise. Vous pouvez utiliser le fichier clé obtenu lors du premier enregistrement.

Le nombre de requêtes pour la réception d'un fichier clé est limité. Un numéro de série ne peut être enregistré plus de 25 fois. Si des requêtes supplémentaires sont envoyées, le fichier clé ne sera pas délivré. Dans ce cas, contactez le Support Technique en décrivant votre problème en détail, en indiquant vos données personnelles fournies lors de l'enregistrement et le numéro de série. Le fichier clé vous sera envoyé par le service de support technique par e-mail.

4.2. Renouveler la licence

Lorsque la licence expire ou que les caractéristiques du système protégé changent, vous pouvez avoir besoin de renouveler ou d'étendre votre licence Dr.Web. Si c'est le cas, vous devez remplacer le fichier clé actuel. Dr.Web assure la mise à niveau des licences en cours sans arrêter ni réinstaller Dr.Web.

Remplacer un fichier clé

1. Pour remplacer la licence actuelle, utilisez l'Assistant d'enregistrement. Vous pouvez également acheter une nouvelle licence ou renouveler une licence existante dans votre espace personnel sur le site officiel de Doctor Web. Pour visiter la page, utilisez l'option **Mon Dr.Web** dans la fenêtre du Gestionnaire de Licence ou dans le menu du SpIDer Agent.
2. Si le fichier clé actuel est invalide, Dr.Web va utiliser automatiquement le nouveau fichier clé.

4.3. Assistant d'enregistrement

Le module de gestion SpIDer Agent vérifie si vous possédez un fichier clé. Si aucun fichier clé n'est trouvé, vous êtes invité à en obtenir un sur Internet.

Vous pouvez spécifier le fichier clé durant la procédure d'installation. Pour cela, sélectionnez l'option **Spécifiez le chemin vers le fichier clé valide** à l'étape 5.

Vous pouvez également spécifier un fichier clé après l'installation du produit :

1. Ouvrez le menu de SpIDer Agent et sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher.

2. Cliquez sur **Acheter ou activer une nouvelle licence**. La fenêtre de l'Assistant d'enregistrement va s'ouvrir.

Activation de la licence

Si vous possédez un fichier clé pour l'activation d'une licence, spécifiez le chemin vers le fichier clé valide et cliquez sur **Terminer**.

Nouvelle licence

Pour acheter une nouvelle licence, renouveler ou étendre la licence actuelle avec la remise sur la boutique en ligne de Doctor Web, cliquez sur **Acheter**.

5. Mise en route

Lorsque Dr.Web est installé, l'icône de SpIDer Agent s'affiche dans la zone de notification Windows.

> Si SpIDer Agent ne fonctionne pas, sélectionnez Dr.Web puis SpIDer Agent dans le menu Démarrage de Windows.

L'icône de SpIDer Agent indique l'état de Dr.Web :

- – tous les composants nécessaires sont activés et fonctionnent correctement ;
- – l'Autoprotection Dr.Web ou un des composants est désactivé, ce qui compromet la sécurité de l'antivirus et de votre ordinateur. Activez l'autoprotection ou le composant désactivé ;
- – le lancement des composants est attendue après le démarrage du système d'exploitation, attendez le lancement des composants ; ou une erreur est survenue lors du démarrage d'un composant important de Dr.Web, votre ordinateur risque d'être infecté. Veuillez vérifier la présence d'un fichier clé valide, et si nécessaire, installez le fichier clé.

Conformément aux paramètres, au-dessus de l'icône de SpIDer Agent des notifications ou bulles d'information peuvent également être affichées.

Pour accéder au menu de SpIDer Agent, cliquez sur l'icône de SpIDer Agent dans la zone de notifications Windows.

> Pour accéder aux composants et aux paramètres de protection et pour désactiver les composants, vous devez avoir les privilèges administrateur.

Le menu de SpIDer Agent vous offre les outils principaux de gestion et de configuration de Dr.Web.

Mon Dr.Web. Ce lien ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, vous permet de renouveler votre licence, de contacter le support technique et plus encore.

Licence. Ce lien lance le Gestionnaire de licences.

Outils. Ce lien ouvre un sous-menu donnant accès :

- à la prévention de la perte de données ;
- au Réseau antivirus ;
- au Gestionnaire de quarantaine ;
- à la rubrique Support.

Composants de protection. Accès rapide à la liste des composants de protection où vous pouvez activer ou désactiver chacun des composants.

Mise à jour. Informations sur le statut des mises à jour des composants et des bases virales. Lance une mise à jour.

Scanner. Accès rapide au lancement de trois modes différents.

Mode de fonctionnement . Permet de passer du mode utilisateur au mode administrateur. Dr.Web démarre par défaut en mode (restreint) utilisateur qui ne donne pas accès à la Configuration ni aux paramètres des Composants de protection. Pour passer à un autre mode, cliquez sur le cadenas. Si l'UAC est activé, le système d'exploitation affichera une requête pour accéder aux privilèges administrateur. Vous devrez également entrer le mot de passe pour changer de mode, si vous avez activé l'option **Protéger les paramètres Dr.Web par mot de passe** dans la fenêtre Configuration.

Statistiques . Ce lien ouvre les statistiques sur les composants durant la session ouverte incluant le nombre d'objets scannés, infectés et suspects, les actions qui leur ont été appliquées.

Configuration . Ouvre la fenêtre des paramètres généraux, des paramètres des composants de protection et des exclusions.

> Pour accéder aux paramètres des composants et ouvrir votre espace personnel **Mon Dr.Web**, vous devez également entrer le mot de passe si vous avez activé l'option **Protéger les paramètres Dr.Web par mot de passe** dans la fenêtre **Configuration**.
>
> Si vous avez oublié votre mot de passe pour accéder aux paramètres de produit, veuillez contacter le support technique.

Aide . Ce lien ouvre le manuel.

5.1. Tester l'antivirus

Le fichier de test EICAR (European Institute for Computer Anti-Virus Research) permet de tester les performances des programmes antivirus utilisant la méthode de détection par signatures.

La plupart des éditeurs d'antivirus utilisent généralement un programme test.com standard. Ce programme a été spécialement conçu pour que les utilisateurs puissent tester les capacités de détection des outils antivirus nouvellement installés sans compromettre la sécurité de leur ordinateur. Bien que le programme test.com ne soit pas malveillant, il est traité par la plupart des antivirus comme un virus. Antivirus Dr.Web pour Windows Servers appelle ce « virus » de la façon suivante : `EICAR Test File (Not a Virus!)`. D'autres outils antivirus alertent les utilisateurs de la même façon.

Le programme test.com est un fichier-COM 68-bits qui affiche le message suivant sur la console lorsqu'il s'est exécuté : `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`

Le fichier test.com contient la chaîne de caractères suivante seulement :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

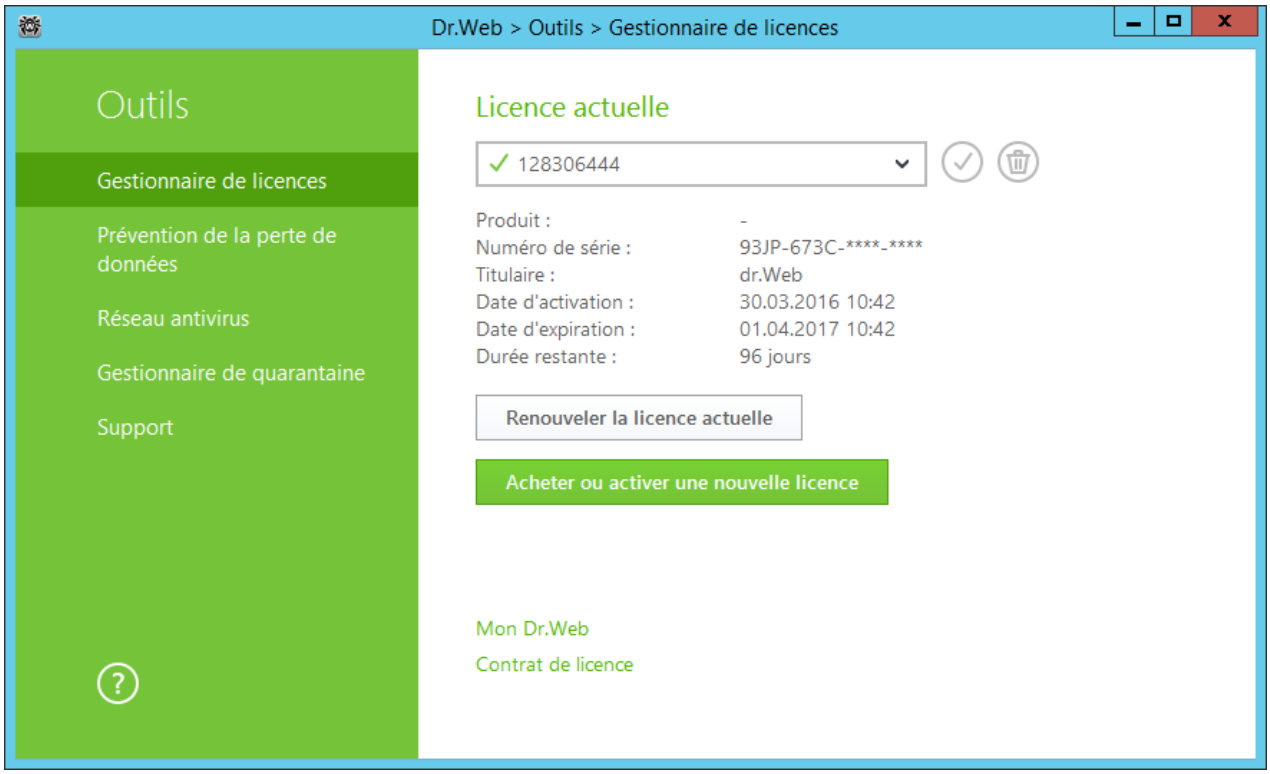
Pour créer votre propre fichier test avec le « virus », vous devez créer un nouveau fichier avec cette ligne et le sauvegarder comme test.com.

Lancé dans le mode optimal, SpIDer Guard n'interrompt pas le lancement du fichier de test EICAR et ne classe pas telle situation comme dangereuse puisque ce fichier ne représente aucun danger pour l'ordinateur. Cependant, lors de la copie ou de la création de ce fichier, SpIDer Guard le traite automatiquement comme un malware et par défaut le déplace en Quarantaine.

6. Outils

6.1. Gestionnaire de licence

Dans cette fenêtre, vous pouvez consulter toutes les informations sur toutes les licences de Dr.Web sauvegardées sur votre ordinateur ainsi que modifier la licence actuelle, la renouveler ou acheter une nouvelle licence et l'activer.



Pour voir les informations sur la licence qui n'est pas actuelle, sélectionnez la licence nécessaire dans la liste déroulante. En mode administrateur, le bouton permet de supprimer la licence consultée, tandis que le bouton permet de la designer comme actuelle. Notez qu'il est impossible de supprimer la dernière licence valide.

Si vous cliquez sur **Acheter ou activer une nouvelle licence**, le programme ouvre la fenêtre de l'Assistant d'enregistrement qui va vous suggérer les actions à accomplir.

Si vous cliquez sur **Renouveler la licence actuelle**, le programme va ouvrir la page sur le site Doctor Web sur laquelle seront affichés tous les paramètres de la licence utilisée.

Avancé

Le lien **Mon Dr.Web** ouvre votre espace personnel sur le site officiel de Doctor Web avec le navigateur utilisé par défaut sur votre ordinateur. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, et permet de renouveler la licence, contacter le support technique et plus encore.

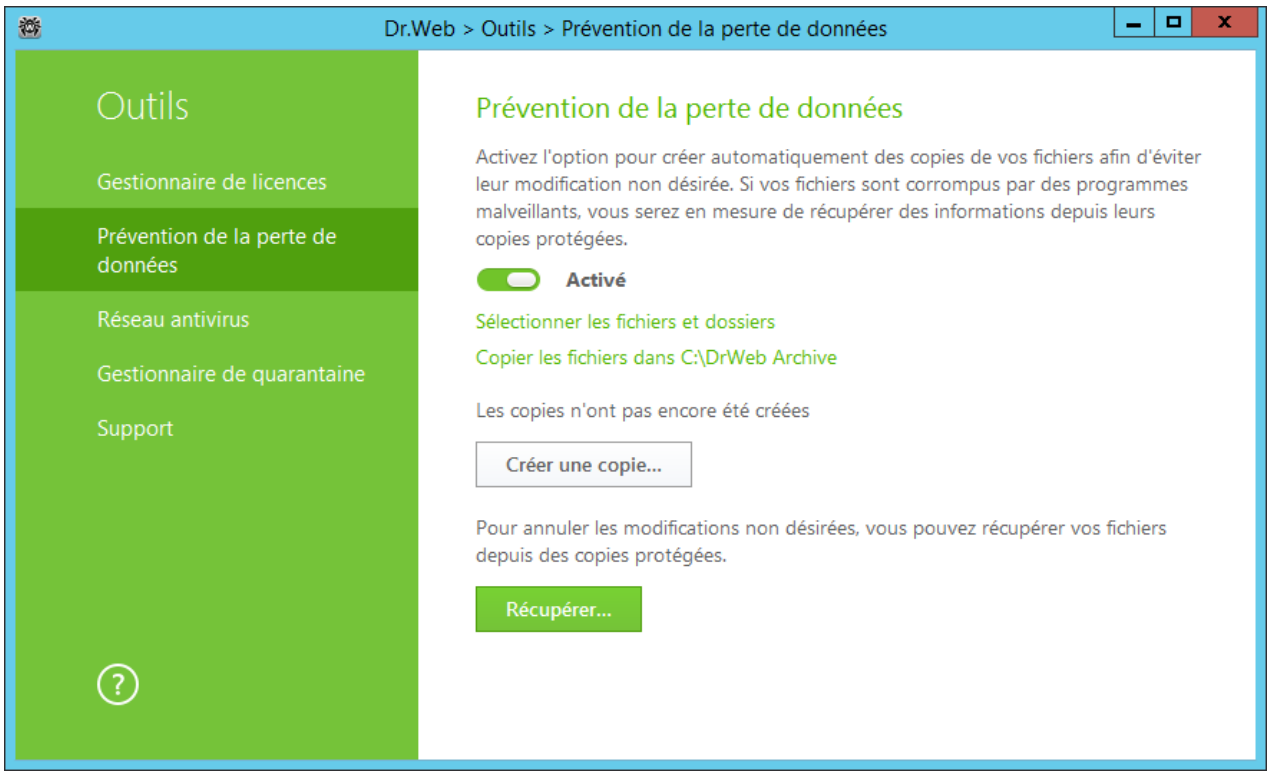
Le lien **Contrat de licence** ouvre le texte du contrat de licence sur le site de Doctor Web.

6.2. Prévention de la perte de données

> Vous ne pouvez pas modifier les paramètres de la prévention de la perte de données ou restaurer les fichiers copiés en mode utilisateur. Pour effectuer ces actions, passez en mode administrateur.

Pour protéger des fichiers importants contre leur modification par des malwares, activez la fonction **Prévention de la perte de données**. Avec cette fonction, vous pouvez faire des copies des fichiers dans les dossiers indiqués.

> Si le fichier est bloqué au moment de la création d'une copie, il ne sera pas inclus à la copie de sauvegarde.



Formation de la liste des dossier et des fichiers à protéger

Cliquez sur **Sélectionnez les dossiers et les fichiers à protéger** pour indiquer les objets pour lesquels des copies protégées seront créées :

- pour ajouter un fichier ou un dossier dans la liste, cliquez sur et sélectionnez l'objet nécessaire ;
- pour supprimer un objet de la liste, sélectionnez-le et cliquez sur .

Vous pouvez modifier cette liste à tout moment.

Paramètres de création des copies

Cliquez sur le lien **Copier les fichiers dans C:\Dr.Web Archive**. Dans la fenêtre qui s'affiche, indiquez les paramètres nécessaires.

1. Spécifiez les paramètres générales pour les copies créées :
   - sélectionnez un disque pour stocker les copies ;
   - spécifiez la périodicité de la création des copies d'objets. Dans le délai indiqué, Dr.Web analysera les objets spécifiés pour la présence des modifications et créera une copie s'il y a des modifications apportées ;
   - si nécessaire, interdisez la création des copie en fonctionnement sur batterie.
2. Spécifiez les limitations qui permettent de limiter l'espace disque utilisé :
   - spécifiez l'espace disque maximum utilise pour l'enregistrement des copies ;
   - si nécessaire, vous pouvez spécifier la limitation du nombre de copies ;
   - sélectionnez une des actions : si une des limitations indiquée est dépassée, les nouvelles copies ne seront pas créées ou bien elles écraseront les copies existantes (à commencer par la plus ancienne).

Suppression des copies créées

Vous pouvez supprimer les copies existantes pour libérer de la place sur le disque (la suppression des copies n'affecte pas les fichiers). Pour ce faire, cliquez sur **Copier les fichiers dans C:\Dr.Web Archive** et ensuite cliquez sur **Supprimer les copies**.

Restauration de fichiers

Si vos fichiers ont été corrompus, vous pouvez restaurer leurs copies depuis une certaine date. Pour cela, cliquez sur le bouton **Restaurer** dans la fenêtre principale. Dans la fenêtre qui s'affiche, sélectionnez la date requise et toutes les copies disponibles pour cette date seront restaurées dans le dossier indiqué.

Lancement manuel de la création des copies

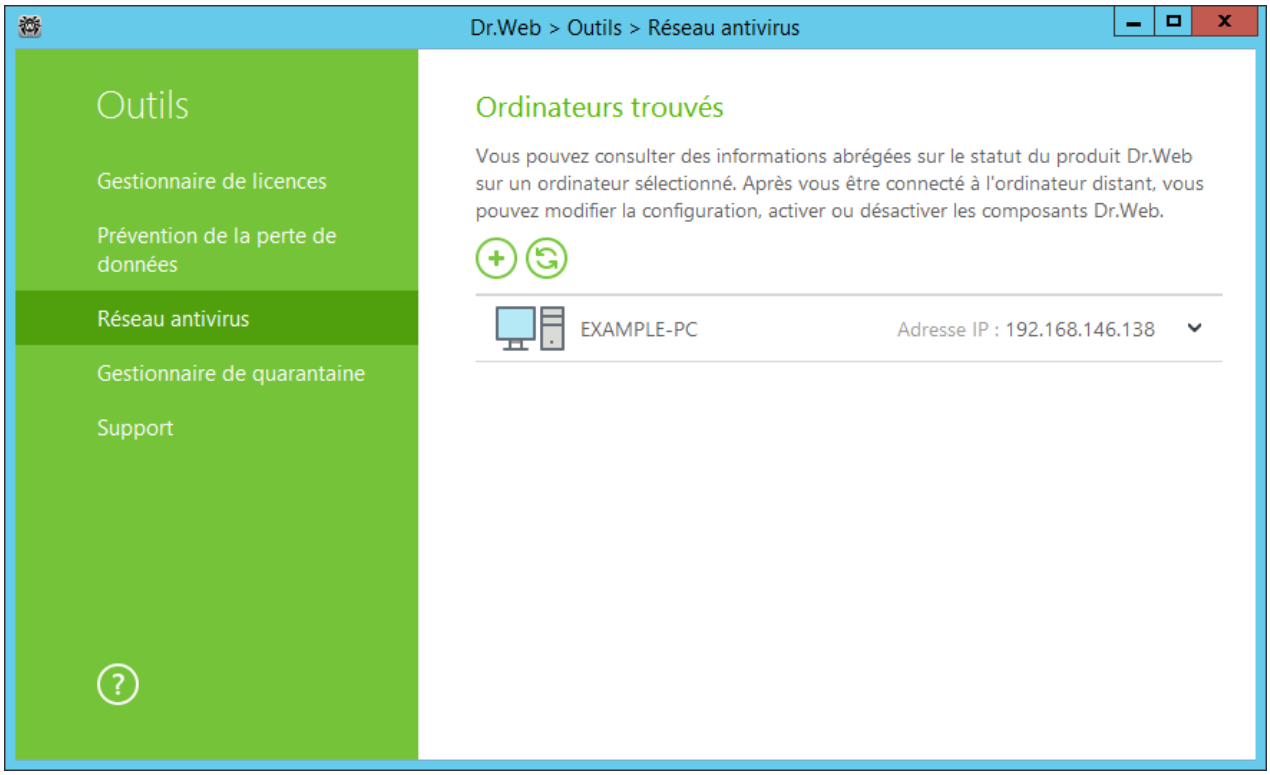
Pour démarrer la création de copies protégées manuellement, cliquez sur le bouton **Créer une copie** dans la fenêtre principale. Dans la fenêtre qui s'affiche, indiquez la description de la nouvelle copie.

Le fonctionnement du système de la **Prévention de la perte de données** nécessite au moins 20 Go d'espace libre sur le disque que vous avez sélectionné pour le stockage de copies.

6.3. Réseau antivirus

Ce composant permet de gérer les logiciels Antivirus Dr.Web pour Windows, Antivirus Dr.Web pour serveurs et Dr.Web Security Space au sein d'une version du produit sur d'autres ordinateurs au sein du même réseau local.

Pour travailler à distance avec les produits Dr.Web cliquez sur l'icône de SpIDer Agent dans la zone de notification Windows et sélectionnez **Réseau Antivirus** dans le groupe **Outils**.



Pour accéder à l'antivirus distant, sélectionnez l'ordinateur dans la liste et cliquez sur **Se connecter**. Saisissez le mot de passe spécifié dans les paramètres de l'antivirus distant. Dans la zone de notification Windows, l'icône de SpIDer Agent distant va s'afficher, ainsi que la notification de connexion réussie.

Vous pouvez consulter des statistiques, activer ou désactiver des modules et modifier leurs paramètres. Les éléments Composants, Réseau antivirus, Quarantaine et Scanner sont indisponibles. Les paramètres et les statistiques du Pare-feu Dr.Web ne sont pas disponibles non plus, cependant vous pouvez activer ou désactiver ce composant (en cas de connexion aux produits Antivirus Dr.Web pour Windows ou Dr.Web Security Space). Vous pouvez accéder à l'élément **Se déconnecter** qui vous permet de fermer la connexion établie avec un antivirus distant.

Si l'ordinateur n'est pas affiché dans le réseau, vous pouvez essayer de l'ajouter manuellement. Pour cela, cliquez sur et spécifiez ensuite l'adresse IP.

Vous pouvez établir une seule connexion avec un produit distant Dr.Web. Lorsqu'une connexion est établie, le bouton **Se connecter** devient inactif.

Les ordinateurs au sein du réseau local ne sont affichés que dans le cas où la gestion distante est autorisée dans le produit Dr.Web installé sur ces ordinateurs. Vous pouvez autoriser la connexion à Dr.Web sur votre ordinateur sur la page Réseau antivirus dans les Paramètres principaux.

6.4. Gestionnaire de quarantaine

Le Gestionnaire de quarantaine affiche l'information sur le contenu de la quarantaine qui permet d'isoler les fichiers suspectés d'être malveillants. La Quarantaine stocke également les copies de sauvegarde des fichiers traités par Dr.Web.

Utilisez les paramètres du Gestionnaire de quarantaine pour choisir le mode d'isolation des objets infectés sur les supports amovibles. Lorsque cette option est activée, les menaces détectées sont déplacées dans le dossier sur le support amovible sans être chiffrées. Le dossier de Quarantaine est créé sur les supports amovibles uniquement lorsqu'ils sont accessibles en écriture. L'utilisation de dossiers séparés et le non chiffrement sur les supports amovibles prévient la perte de données.

Pour accéder à cette fenêtre, dans le menu de SpIDer Agent, sélectionnez le sous-menu **Outils**, puis **Gestionnaire de quarantaine**.

Le tableau central liste les informations suivantes sur les objets placés en quarantaine auxquels vous avez accès :

- **Objets** – nom de l'objet placé en quarantaine ;

- **Menace** – type de malware déterminé par Dr.Web lorsque l'objet est placé en quarantaine ;
- **Date d'ajout** – la date à laquelle l'objet a été déplacé en quarantaine ;
- **Chemin** – chemin complet du fichier avant qu'il ne soit placé en quarantaine.

> Dans la fenêtre de Gestionnaire de quarantaine les fichiers sont visibles uniquement pour les utilisateurs qui ont l'accès à ces fichiers. Pour afficher les objets caches, il faut posséder les droits d'Administrateur.

Dans le menu contextuel des objets, les boutons suivants sont disponibles :

- **Récupérer** – supprimer le fichier du dossier sélectionné et donner un nouveau nom au fichier ;

> Utilisez cette option uniquement si vous êtes sûr que les objets sélectionnés ne sont pas nocifs.

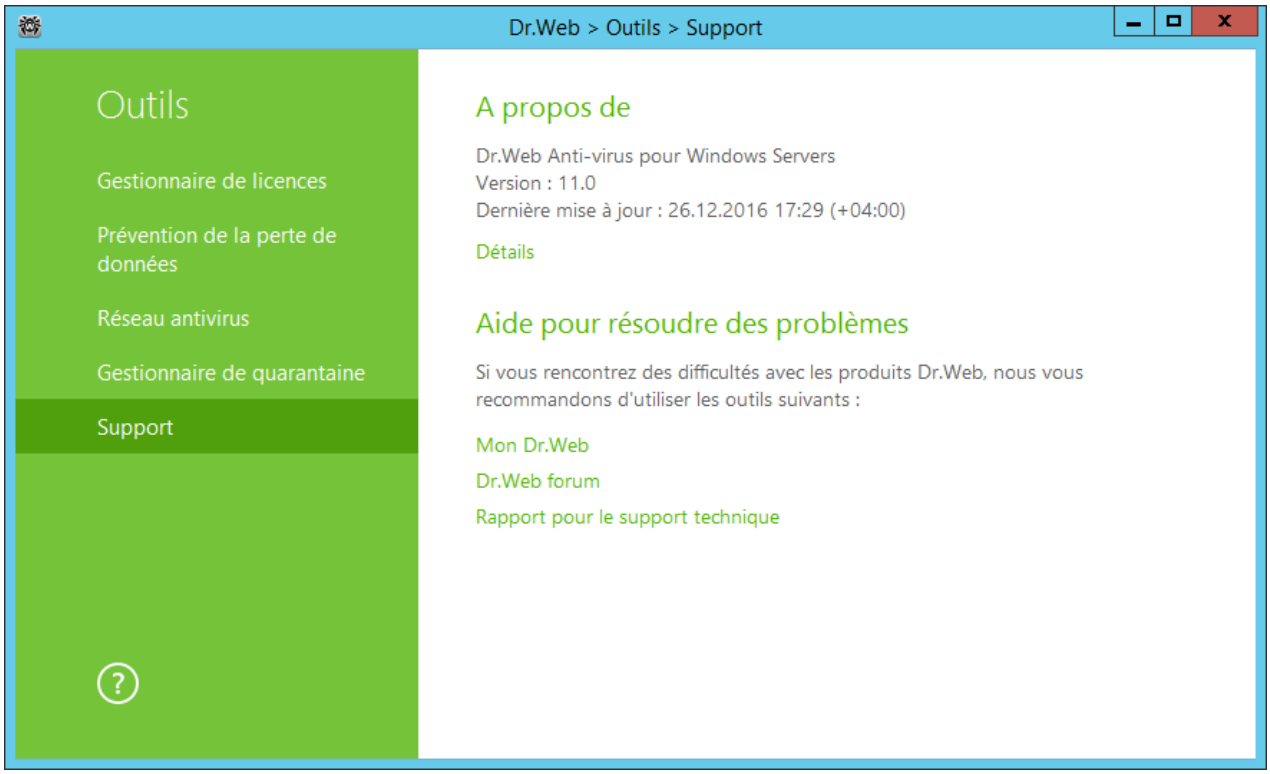
- **Rescanner** – scanner l'objet déplacé en quarantaine encore une fois ;
- **Supprimer** – supprimer les objets sélectionnés de la quarantaine et du système.

Ces actions sont également disponibles dans le menu contextuel qui s'ouvre si vous cliquez droit sur un ou plusieurs objets.

Pour supprimer tous les objets de la quarantaine, cliquez sur le bouton  et sélectionnez **Supprimer tout** dans la liste déroulante.

6.5. Support

Cette rubrique contient des informations sur la version du produit, sur les composants, la date de la dernière mise à jour et des liens utiles pour vous aider à résoudre des problèmes pouvant survenir durant l'utilisation de Dr.Web.



Si vous avez des questions, utilisez les outils suivants.

Mon Dr.Web. Ce lien ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit des informations sur votre licence y compris sa durée et son numéro de série, vous permet de renouveler votre licence, de contacter le support technique et plus encore.

Forum Dr.Web. Ce lien ouvre le forum Dr.Web à la page http://forum.drweb.com.

Rapport pour le support technique. Ce lien lance l'assistant qui vous aidera à créer un rapport contenant les informations importantes concernant la configuration de votre système et le fonctionnement de votre ordinateur.

Si vous n'avez pas trouvé de solution à votre problème, vous pouvez demander une assistance directe du support technique de Doctor Web en remplissant le formulaire sur le site du support à la page https://support.drweb.fr.

Pour en savoir plus sur les coordonnées des bureaux Doctor Web et sur les informations de contact, merci de visiter la page http://company.drweb.fr/contacts/france.

6.5.1. Créer un rapport

Pour contacter le support technique de Doctor Web, vous pouvez générer un rapport sur votre système d'exploitation et le fonctionnement de Dr.Web.

Le rapport sera sauvegardé sous forme d'archive dans le répertoire Doctor Web se trouvant dans le dossier du profil utilisateur %USERPROFILE%.

Pour créer un rapport, cliquez sur le bouton correspondant. Le rapport va inclure :

1. Informations techniques sur le système d'exploitation :
   - généralités sur l'ordinateur ;
   - sur les processus en cours d'exécution ;
   - sur les tâches programmées ;
   - sur les services et pilotes ;
   - sur le navigateur par défaut ;
   - applications installées ;
   - sur la politique de restrictions ;
   - sur le fichier HOSTS ;
   - sur les serveurs DNS ;
   - journal des événements système ;
   - liste des répertoires système ;
   - branches de la base de registre ;
   - fournisseurs Winsock ;
   - connexions réseau ;
   - rapports du débogueur Dr.Watson ;
   - indice de performances.
2. Informations sur les solutions antivirus Dr.Web.
3. Informations sur les modules ajoutables Dr.Web :
   - Dr.Web pour IBM Lotus Domino ;
   - Dr.Web pour Kerio MailServer ;
   - Dr.Web pour Kerio WinRoute.

Des informations sur les solutions antivirus Dr.Web se trouvent dans l'Observateur d'Evénements (Event Viewer) dans les **Journaux des applications et services** → **Doctor Web**.

Création du rapport depuis la ligne de commande

Pour générer le rapport, utilisez la commande suivante :

```
/auto
```

Par exemple, `dwsysinfo.exe /auto`

Le rapport sera sauvegardé sous forme d'archive dans le répertoire Doctor Web se trouvant dans le dossier du profil utilisateur %USERPROFILE%.

Vous pouvez également utiliser la commande :

`/auto/report:` [<*chemin complet vers l'archive*>]

où :

- <*chemin complet vers l'archive*> – chemin vers le fichier de rapport.

Par exemple, `dwsysinfo.exe /auto /report:C:\report.zip`

7. Mise à jour

Les solutions antivirus de Doctor Web utilisent les bases virales Dr.Web pour détecter les logiciels malveillants. Ces bases contiennent les détails pour toutes les menaces virales connues au moment du lancement du produit. Les mises à jour régulières permettent de détecter de nouveaux virus, de bloquer leur diffusion et de désinfecter parfois les fichiers infectés qui n'étaient pas curables auparavant.

Parfois, les mises à jour incluent également des améliorations des algorithmes antivirus (réalisés en tant que fichiers exécutables et bibliothèques de programme) et réparent les bugs dans le logiciel et la documentation.

Pour garantir que les bases virales et les algorithmes du logiciel sont à jour, Doctor Web publie des mises à jour régulières des bases virales et des composants du produit, distribuées par Internet. La Mise à jour vous aide à télécharger et installer les additions aux bases virales et les modules renouvelés pendant la durée de validité de votre licence.

Démarrage d'une mise à jour

Lors d'une mise à jour Dr.Web télécharge et installe automatiquement tous les fichiers mis à jour en fonction de votre version de Dr.Web, ainsi qu'une nouvelle version de Dr.Web à sa sortie.

> ⚠ Pour la mise à jour de Dr.Web une connexion à Internet ou au miroir de mises à jour (dossier local ou réseau), ou au Réseau antivirus avec le miroir de mises à jour configuré sur au moins un des ordinateurs est requise.

Vous pouvez configurer les paramètres nécessaires à la page **Mise à jour** dans les Paramètres principaux de Dr.Web.

Démarrage d'une mise à jour depuis le module de gestion SpIDer Agent

Dans le menu SpIDer Agent  sélectionnez l'élément **Mise à jour**. Une fenêtre de dialogue apparaît et affiche des informations sur les bases virales et les composants ainsi que la date de la dernière mise à jour. Pour démarrer une mise à jour cliquez sur **Mettre à jour**.

Démarrage d'une mise à jour depuis la ligne de commande

Ouvrez le dossier d'installation de Dr.Web (%PROGRAMFILES%\Common Files\Doctor Web \Updater) et lancez le fichier drwupsrv.exe. La liste des paramètres de la ligne de commande se trouve dans l'Annexe A.

Démarrage automatique d'une mise à jour

Lors du démarrage automatique, la mise à jour est effectuée en tâche de fond et le rapport est enregistré dans le fichier dwupdater.log dans le dossier %allusersprofile%\Doctor Web\Logs\.

Après une mise à jour des fichiers exécutables ou des bibliothèques, un redémarrage de la machine peut être requis. Dans ce cas, une alerte sera affichée.

8. Scanner Dr.Web

Le Scanner Dr.Web pour Windows vous permet de lancer des scans antivirus des secteurs d'amorçage, de la mémoire vive, des fichiers particuliers et des objets contenus dans des structures complexes telles que les archives, les conteneurs et les pièces jointes des e-mails. Toutes les méthodes de détection de menaces sont utilisées pour l'analyse. Par défaut, le Scanner Dr.Web scanne tous les fichiers en utilisant les bases virales et l'analyseur heuristique (une méthode basée sur les algorithmes généraux de développement de virus qui permet de détecter les virus inconnus avec une grande probabilité). Les fichiers exécutables compressés avec des outils spéciaux sont décompressés et scannés. Les fichiers contenus dans les archives de tous types (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP et d'autres), dans les conteneurs de fichiers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM etc.), et dans les boîtes e-mail (le format des e-mails doit être conforme à RFC822) sont également analysés.

Lorsqu'un objet malveillant est détecté, le Scanner Dr.Web informe seulement sur la menace détectée. Le rapport sur les résultats de l'analyse s'affiche dans un tableau où vous pouvez choisir une action nécessaire pour traiter l'objet malveillant ou suspect. Vous pouvez appliquer les actions définies par défaut à toutes les menaces détectées ou sélectionner une méthode appropriée pour traiter des objets particuliers.

Les actions par défaut sont optimales pour la plupart des cas, mais si besoin est, vous pouvez les modifier dans la fenêtre de configuration du Scanner Dr.Web. Les actions à porter sur un objet particulier peuvent être choisies après la fin de l'analyse, tandis que les paramètres généraux relatifs à la neutralisation des types différents de menaces doivent être spécifiés avant de procéder à l'analyse.

8.1. Lancement de la mise à jour

Lancer le Scanner Dr.Web

> ⚠ Si vous utilisez Windows Server 2003 ou un système d'exploitation ultérieur, il est recommandé de lancer le Scanner Dr.Web avec les droits administrateur. Sinon, les fichiers et les dossiers auxquels les utilisateurs sans droits n'ont pas accès (y compris les dossiers système) ne seront pas scannés.

1. Dans le menu SpIDer Agent sélectionnez l'élément **Scanner**. Le menu d'accès rapide aux différents modes d'analyse va s'ouvrir.
2. Sélectionnez l'élément **Personnalisée** pour scanner uniquement les objets que vous avez désignés. La fenêtre principale du Scanner Dr.Web va s'ouvrir.
3. Sélectionnez l'élément **Rapide** ou **Complète** pour lancer les types correspondants du scan.

Vous pouvez également lancer le Scanner avec la configuration par défaut pour analyser un fichier ou un dossier immédiatement : Sélectionnez **Scan Dr.Web** dans le menu du fichier ou du dossier (sur le Bureau ou dans l'explorateur Windows).

Configurer le Scanner Dr.Web

Vous pouvez configurer les paramètres de fonctionnement et les réactions du Scanner Dr.Web envers les menaces détectées dans la rubrique **Paramètres** → **Composants de protection** → **Scanner**.

Description des modes d'analyse

Analyse rapide

Dans ce mode sont analysés :

- secteurs d'amorçage de tous les disques ;
- mémoire vive ;
- dossier racine du disque de démarrage ;
- dossier système Windows ;
- dossier des Documents de l'utilisateur (« Mes documents ») ;
- fichiers temporaires ;
- points de restauration du système ;
- présence de rootkits (si le scan a été lancé en mode administrateur).

Dans ce mode les archives et les fichiers e-mail ne sont pas scannés.

Analyse complète

Dans ce mode, la mémoire vive et tous les disques durs (y compris les secteurs d'amorçage) sont scannés. La recherche des rootkit est également effectuée.

Analyse personnalisée

Lorsque vous sélectionnez l'analyse personnalisée, dans la fenêtre du Scanner Dr.Web vous pouvez spécifier les objets à vérifier : tout fichier ou dossier, ainsi que la mémoire vive, les secteurs d'amorçage etc. Pour commencer le scan, cliquez sur **Lancer l'analyse**. Pour ajouter des objets dans la liste, cliquez sur  .

Processus de l'analyse

Dès que le scan commence, les bouton **Pause** et **Stop** dans la partie droite de la fenêtre devient accessibles. Lors de toute étape de l'analyse, vous pouvez faire le suivant :

- pour suspendre le scan, cliquez sur **Pause**. Pour reprendre le scan après la pause, cliquez sur **Reprendre**.
- pour arrêter l'analyse définitivement, cliquez sur **Stop**.

> Le bouton **Pause** est indisponible lors de l'analyse de la mémoire vive et des processus.

8.2. Actions en cas de détection de menaces

Après la fin d'analyse, le Scanner Dr.Web informe seulement sur les menaces détectées et propose des actions optimales pour leur neutralisation. Vous pouvez neutraliser toutes les menaces détectées en une seule fois. Pour cela, cliquez sur le bouton **Neutraliser**, le Scanner appliquera des actions définies par défaut qui sont optimales pour toutes les menaces détectées.

> En cliquant sur **Neutraliser**, vous appliquez aux objets les actions sélectionnées dans le tableau. Tous les objets sont sélectionnés par défaut une fois le scan achevé. Si nécessaire, vous pouvez personnaliser la sélection en cochant les cases près des noms des objets ou des groupes des objets dans le menu déroulant dans le tableau principal.

Sélection d'une action

1. Dans le champ **Action** de la liste déroulante, sélectionnez une action pour chaque objet (par défaut, le Scanner Dr.Web suggère une action optimale).
2. Cliquez sur **Neutraliser**. Le Scanner Dr.Web va neutraliser toutes les menaces sélectionnées en une seule fois.

Restrictions existantes :

- il est impossible de désinfecter les objets suspects ;
- il est impossible de déplacer ou supprimer les objets qui ne sont pas des fichiers (par exemple, les secteurs d'amorçage) ;
- il est impossible d'effectuer aucune action pour des fichiers particuliers au sein des archives, des packages d'installation ou dans des e-mails. Dans ce cas, l'action sera appliquée à l'objet entier.

Le journal détaillé sur le fonctionnement du programme est enregistré sous forme du fichier de journal dwscanner.log se trouvant dans le répertoire %USERPROFILE%\Doctor Web.

Nom de colonne	Description
Objet	Cette colonne comporte le nom de l'objet suspect ou contaminé (nom du fichier – en cas de contamination d'un fichier, **Boot sector** – si un secteur d'amorçage est contaminé, **Master Boot Record** – si le MBR du disque dur est infecté).
Menace	Ici vous trouverez le nom du virus ou d'une modification virale selon la classification interne de Doctor Web (la modification d'un virus connu est un code

Nom de colonne	Description
	du virus modifié de telle manière que le scanner peut le détecter mais que les algorithmes de neutralisation appropriés au virus d'origine n'y peuvent pas être appliqués). Pour les objets suspects détectés, il est indiqué que l'objet est « probablement infecté » et le type du virus supposé selon la classification de l'analyseur heuristique est également affiché.
Action	Cliquez sur la flèche sur ce bouton pour définir l'action pour la menace sélectionnée (par défaut le Scanner Dr.Web propose la valeur optimale). Vous pouvez appliquer l'action indiquée sur le bouton séparément, sans neutraliser les menaces restantes. Pour ce faire, cliquez sur ce bouton.
Chemin	Ce colonne affiche le chemin complet vers le fichier correspondant.

Si dans les paramètres du Scanner Dr.Web, vous avez sélectionné l'option **Neutraliser les menaces détectées** pour le paramètre **Après la fin de l'analyse**, les menaces seront neutralisées automatiquement.

8.3. Lancement du Scanner avec les paramètres de la ligne de commande

Vous pouvez lancer le Scanner Dr.Web en mode de ligne de commande. Ce mode vous permet de configurer les paramètres nécessaires pour la session courante d'analyse ainsi qu'une liste des objets à scanner avec les clés correspondantes. C'est en mode de ligne de commande que vous pouvez réaliser le lancement automatique du Scanner selon la planification.

Lancement du Scanner depuis la ligne de commande

Pour lancer le Scanner avec des paramètres supplémentaires de ligne de commande, utilisez la commande suivante :

[<*chemin_vers_le_programme*>]`dwscanner` [<*clés*>] [<*objets*>]

où:

- <*objets*> – liste des objets à analyser ;
- <*clés*> – paramètres de la ligne de commande déterminant le fonctionnement du Scanner. Si aucun paramètre n'est défini, le scan est effectué avec les paramètres définis plus tôt (ou avec la configuration par défaut si vous ne l'avez pas modifiée).

La liste des objets à scanner peut être vide ou contenir plusieurs éléments séparés par des espaces. Les objets de l'analyse les plus répandus sont les suivants :

- `/FAST` – commande d'effectuer une analyse rapide du système.

- `/FULL` – commande d'effectuer une analyse complète de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage).
- `/LITE` – commande d'effectuer un scan du système en analysant la mémoire vive, les secteurs d'amorçage de tous les disques, une recherche des rootkits sera également réalisée.

Les paramètres sont les clés de la ligne de commande déterminant la configuration du programme. Si aucune clé n'est présente, le scan sera réalisé avec les paramètres enregistrés précédemment (ou avec les paramètres définis par défaut s'ils n'ont pas été modifiés). Les clés commencent par le symbole « / » et tout comme d'autres paramètres en ligne de commande, ils sont séparés pas des espaces.

8.4. Scanner en ligne de commande

Le jeu de composants Dr.Web inclut également le Scanner en ligne de commande qui permet de réaliser l'analyse en mode ligne de commande et offre à l'utilisateur des possibilités avancées de configuration.

Le Scanner en ligne de commande place les fichiers suspects pouvant contenir des objets malveillants en Quarantaine.

Lancer le Scanner en ligne de commande

Afin de lancer le Scanner en ligne de commande, utilisez la commande suivante :

[<*chemin_vers_le_programme*>]`dwscancl` [<*clés*>] [<*objets*>]

où:

- <*objets*> – liste des objets à analyser ;
- <*clés*> – liste des paramètres de la ligne de commande déterminant le fonctionnement du Scanner en ligne de commande.

La clé commence par le symbole « / », plusieurs clés sont séparées par des espaces. La liste des objets à scanner peut être vide ou peut contenir plusieurs éléments séparés par des espaces.

Pour la liste des clés du Scanner en ligne de commande, consulter l'Annexe A.

Codes de retour du Scanner en ligne de commande :

0 – l'analyse est achevée avec succès, aucun objet infecté n'est trouvé ;

1 – l'analyse est achevée avec succès, des objets infectés ont été détectés ;

10 – les clés non valides sont spécifiées ;

11 – le fichier clé est introuvable ou ne supporte pas le Scanner en ligne de commande ;

12 – Scanning Engine n'est pas lancé ;

255 – l'analyse est interrompue par l'utilisateur.

8.5. Lancement de l’analyse selon la planification

Lors de l’installation de Dr.Web, une tâche d’analyse antivirus est automatiquement créée dans le Planificateur de tâche Windows (par défaut, la tâche est désactivée).

Pour consulter les paramètres de tâche, ouvrez le **Panneau de configuration** (affichage détaillé) → **Outils d’administration** → **Planificateur de tâches**.

Dans la liste de tâches, sélectionnez la tâche d’analyse antivirus. Vous pouvez activer la tâche ainsi que configurer l’heure du démarrage et spécifier des paramètres nécessaires.

Sur l’onglet **Général** en bas de la fenêtre, des informations générales sur la tâche et les options de sécurité sont affichées. Sur les onglets **Déclencheurs** et **Conditions** vous pouvez spécifier les conditions qui déclenchent l’exécution de la tâche. Pour consulter l’historique des évènements, allez sur l’onglet **Journal**.

Vous pouvez également créer vos propres tâches d’analyse antivirus. Pour en savoir plus, consultez la rubrique d’aide et la documentation de l’OS Windows.

9. Paramètres

Pour configurer les paramètres, ouvrez le menu de SpIDer Agent, lancez la Configuration en mode administrateur.

Protection par mot de passe

Pour restreindre l'accès aux paramètres de Dr.Web sur votre ordinateur, activez l'option **Protéger les paramètres de Dr.Web par mot de passe**. Dans la fenêtre qui s'affiche, indiquez le mot de passe qui sera requis pour configurer Dr.Web, confirmez-le et cliquez sur **OK**.

Si vous avez oublié le mot de passe, contactez le Support technique.

Gérer les paramètres

Pour restaurer les paramètres par défaut, choisissez **Réinitialiser les paramètres** dans la liste déroulante.

Si vous souhaitez utiliser les paramètres de Dr.Web que vous avez déjà configurés sur un autre ordinateur, choisissez **Importer** dans la liste déroulante.

Si vous souhaitez utiliser vos paramètres sur d'autres ordinateurs, sélectionnez **Exporter** dans la liste déroulante. Ensuite, utilisez le même onglet sur un autre ordinateur.

10. Paramètres principaux

Pour configurer les paramètres principaux de Dr.Web, ouvrez le menu de SpIDer Agent, lancez la **Configuration** en mode administrateur et sélectionnez la rubrique **Général**.

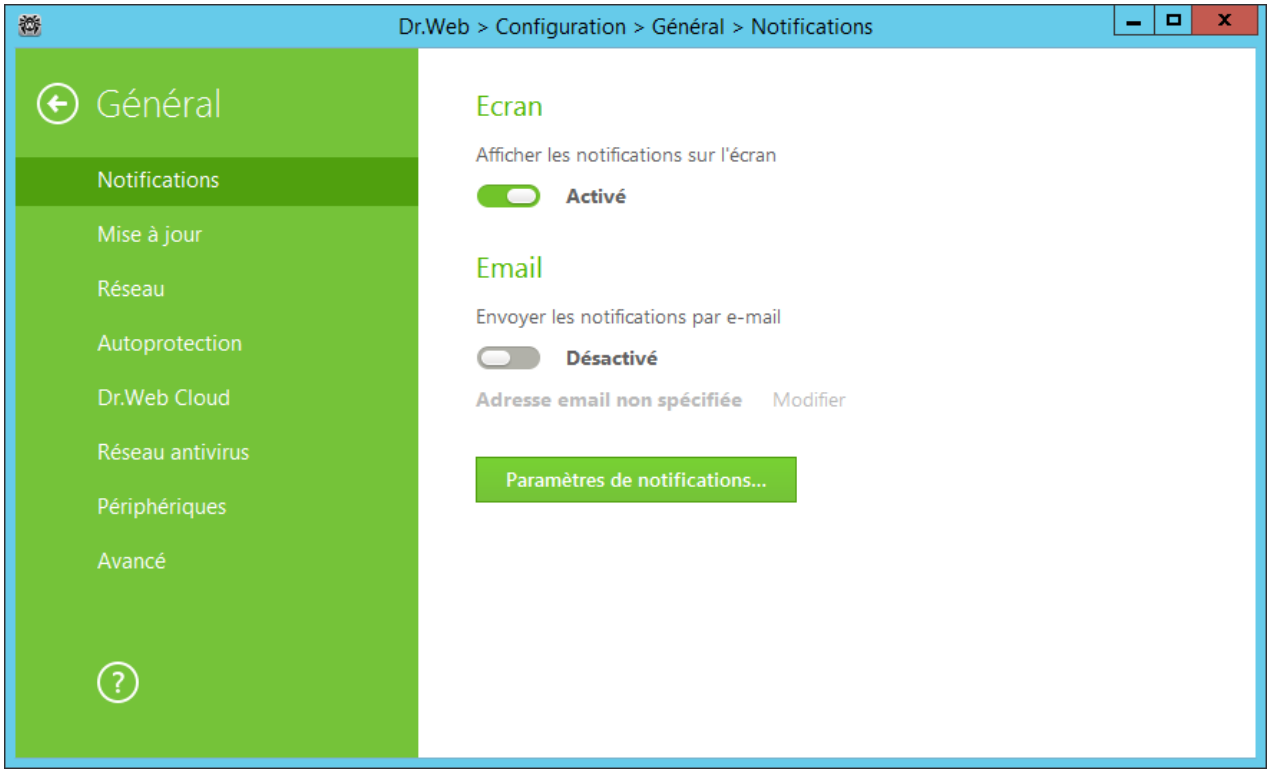
> Pour accéder aux paramètres généraux de Dr.Web, vous êtes invité à entrer le mot de passe si vous avez coché la case **Protéger les paramètres de Dr.Web par mot de passe** dans la section Paramètres.

Le centre unique de gestion des paramètres vous permet de configurer les paramètres principaux de tout l'ensemble antivirus.

10.1. Notifications

Notifications pop-up

Activez l'option pour avoir des notifications pop-up sur l'icône du SpIDer Agent dans la zone de notifications.



Notifications e-mail

Pour recevoir des notifications sur les événements par e-mail, exécutez les actions suivantes :

1. Activer l'option **Envoyer les notifications par e-mail**.
2. Dans la fenêtre qui s'affiche, spécifiez l'adresse e-mail que vous souhaitez utiliser pour recevoir les notifications. Il est nécessaire de confirmer l'utilisation de cette adresse à l'étape 7.
3. Cliquez sur **Suivant**.
4. Indiquez les données du compte depuis lequel les notifications seront envoyées.
   - Si la liste des serveurs de messagerie contient le serveur nécessaire, sélectionnez-le et indiquez le login et le mot de passe de votre compte.
   - Si la liste des serveurs de messagerie ne contient pas le serveur nécessaire, cliquez sur **Spécifier manuellement** et remplissez les champs nécessaires dans la fenêtre qui s'affiche.

Paramètre	Description
Serveur SMTP	Entrez l'adresse du serveur de messagerie qui sera utilisé par Dr.Web pour envoyer les notifications e-mail.
Port	Entrez le port du serveur de messagerie auquel Dr.Web va se connecter pour envoyer des notifications e-mail.
Login	Entrez le login pour se connecter au serveur de messagerie.
Mot de passe	Entrez le mot de passe à utiliser pour se connecter au serveur de messagerie.
Utiliser SSL/TLS	Cochez cette case si vous voulez utiliser le chiffrement SSL/TLS lors de la transmission des messages.
Authentification NTLM	Cochez cette case si vous voulez effectuer l'authentification via le protocole NTLM.

5. Cliquez sur **Envoyer un message de test** si vous voulez vérifier si le compte est indiqué correctement. Le message sera envoyé à l'adresse de laquelle les notifications doivent être envoyées (configurée à l'étape 4).
6. Cliquez sur **Suivant**.
7. Entrez le code de confirmation qui sera envoyée à l'adresse e-mail que vous avez indiquée à l'étape 2 pour recevoir les notifications. Si vous n'avez pas reçu le code pendant 10 minutes, cliquez sur **Envoyer le code encore une fois**. Si vous n'entrez pas le code de confirmation, les notifications ne seront pas envoyées à cette adresse.
8. Pour modifier l'adresse e-mail et les autres paramètres, cliquez sur **Modifier** et répétez toutes les actions à commencer par l'étape 2.
9. Cliquez sur le bouton **Paramètres de notifications** et spécifiez les types de notifications nécessaires. Par défaut tous les types des notifications envoyées par e-mail, sont désactivés.

Paramètres des notifications

1. Cliquez ensuite sur **Paramètres de notifications**.

2. Choisissez les notifications que vous souhaitez recevoir et cochez les cases correspondantes. Pour afficher les pop-ups, cochez les cases dans la colonne **Écran**. Pour recevoir les notifications par e-mail, cochez les cases dans la colonne **E-mail**.

Type de notification	Description
Menace détectée	Cochez les cases dans ce groupe pour recevoir des notifications sur les menaces détectées par les composants SpIDer Guard. Décochez les cases pour ne pas recevoir de telles notifications. Ces notifications sont activées par défaut.
Notifications critiques	Cochez les cases dans le groupe pour recevoir des notifications critiques sur les événements suivants : • erreur de création de copie de sauvegarde ont été détectées. Décochez les cases si vous ne souhaitez pas être notifié sur les sujets listés ci-dessus. Ces notifications sont activées par défaut.
Notifications majeures	Cochez les cases dans le groupe pour recevoir des notifications importantes sur les événements suivants : • le dispositif est bloqué ; • une tentative d'accès à l'objet protégé est bloquée par la Protection préventive ; • une tentative de changer la date et l'heure système a été bloquée ; • une nouvelle version de logiciel est disponible ; • les bases virales Dr.Web sont périmées. Décochez les cases si vous ne souhaitez pas être notifié sur les sujets listés ci-dessus. Ces notifications sont activées par défaut.
Notifications mineurs	Cochez les cases dans le groupe pour recevoir des notifications mineurs sur les événements suivants : • mise à jour réussie ; • erreur de mise à jour ; Décochez les cases si vous ne souhaitez pas être notifié sur les sujets listés ci-dessus. Ces notifications sont désactivées par défaut.
Licence	Cochez les cases dans le groupe pour recevoir des notifications sur les événements suivants : • la licence va expirer ; • la licence actuelle n'est pas trouvée ; • la licence actuelle est bloquée.

3. Si nécessaire, configurez des paramètres avancés de l'affichage des notifications :

Option	Description
Ne pas afficher les notifications en mode plein écran	Cochez la case pour ne pas recevoir les notifications lorsque vous travailler avec des applications en mode plein écran (affichage des filmes, graphiques etc.). Décochez la case pour recevoir toujours de telles notifications.

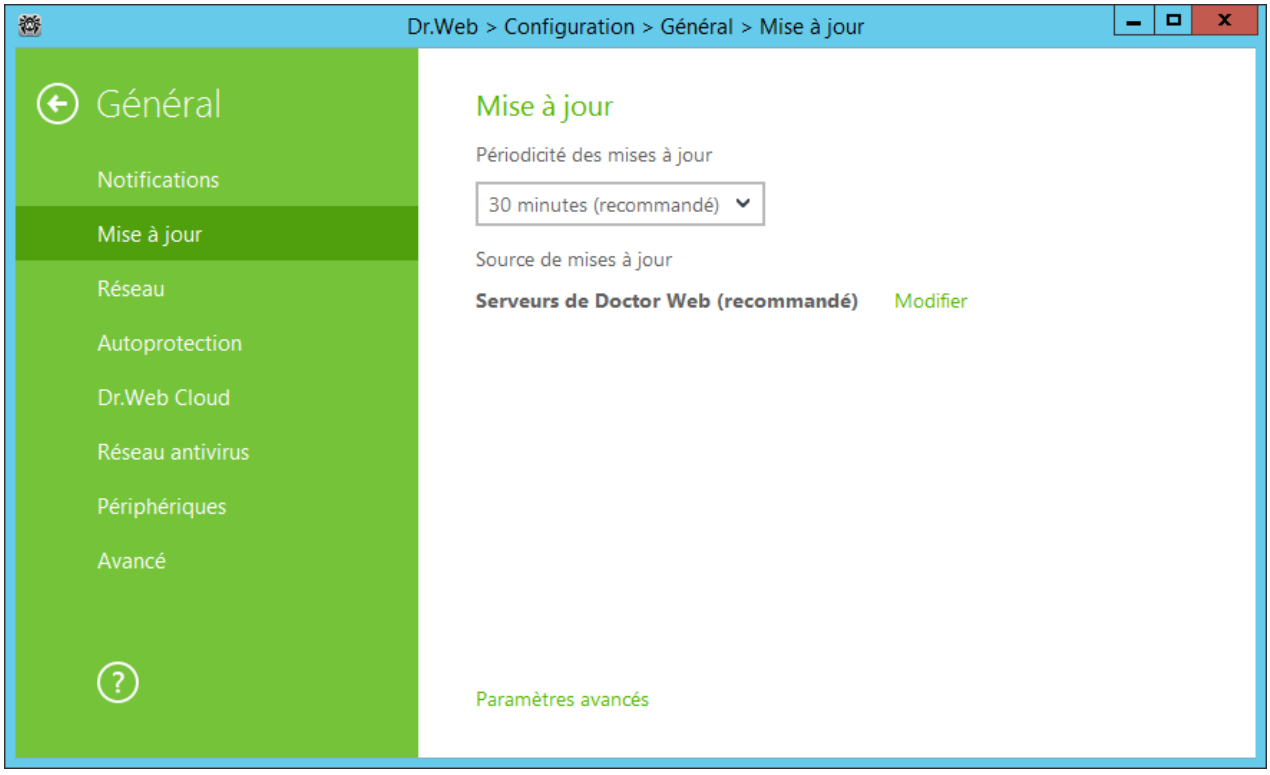
4. Si vous avez choisi une ou plusieurs notifications par e-mail, configurez l'envoi des e-mails depuis votre ordinateur.

Les notifications sur certains événements ne sont pas inclues dans les groupes listés et s'affichent toujours à l'utilisateur :

- installation des mises à jour prioritaires exigeant un redémarrage ;
- redémarrage pour achever la neutralisation des menaces ;
- redémarrage pour activer/désactiver l'hyperviseur ;
- demande de l'autorisation de modification de l'objet par le processus ;
- connexion réussie à l'ordinateur distant sur le réseau Antivirus.

10.2. Mise à jour

Dans cette rubrique, vous pouvez configurer les paramètres de mise à jour de Dr.Web. Vous pouvez spécifier une source de mises à jour, les composants à mettre à jour et la périodicité des mises à jour, vous pouvez également configurer un serveur proxy et le miroir de mises à jour.



Paramètres généraux de mise à jour

Périodicité des mises à jour. Indiquez la fréquence de vérification des mises à jour. La valeur par défaut (30 minutes) est optimale pour conserver une information à jour sur les menaces.

Source de mises à jour. Pour sélectionner une source de mises à jour, cliquez sur **Modifier**. Dans la fenêtre qui apparaît, spécifiez une source de mises à jour que vous souhaitez :

- **Serveurs de Doctor Web (recommandé)**. Cette source est sélectionnée par défaut.
- **Dossier local ou réseau** – mise à jour depuis un dossier local ou un dossier réseau vers lequel ont été sauvegardées les mises à jour. Spécifiez le chemin vers ce dossier (pour ce faire, cliquez sur **Parcourir** et sélectionnez un dossier nécessaire ou entrez le chemin manuellement), ainsi que le nom de l'utilisateur et le mot de passe si nécessaire.
- **Réseau antivirus** – mise à jour via le réseau local depuis l'ordinateur sur lequel est installé le produit Dr.Web et où un miroir de mises à jour a été créé.

Si vous voulez télécharger les mises à jour via le protocole sécurisé, activez l'option **Utiliser la connexion HTTPS**.

Paramètres avancés

Composants à mettre à jour. Vous pouvez choisir un des moyens suivants pour télécharger les mises à jour :

- **Tout (recommandé)**, dans ce mode, les mises à jour des bases virales Dr.Web ainsi que les mises à jour du noyau antivirus et d'autres composants de Dr.Web sont téléchargées ;
- **Uniquement les bases**, lorsque seules les mises à jour des bases virales Dr.Web et du noyau antivirus sont téléchargées ; les autres composants de Dr.Web ne sont pas mis à jour.

Création d'un miroir de mises à jour

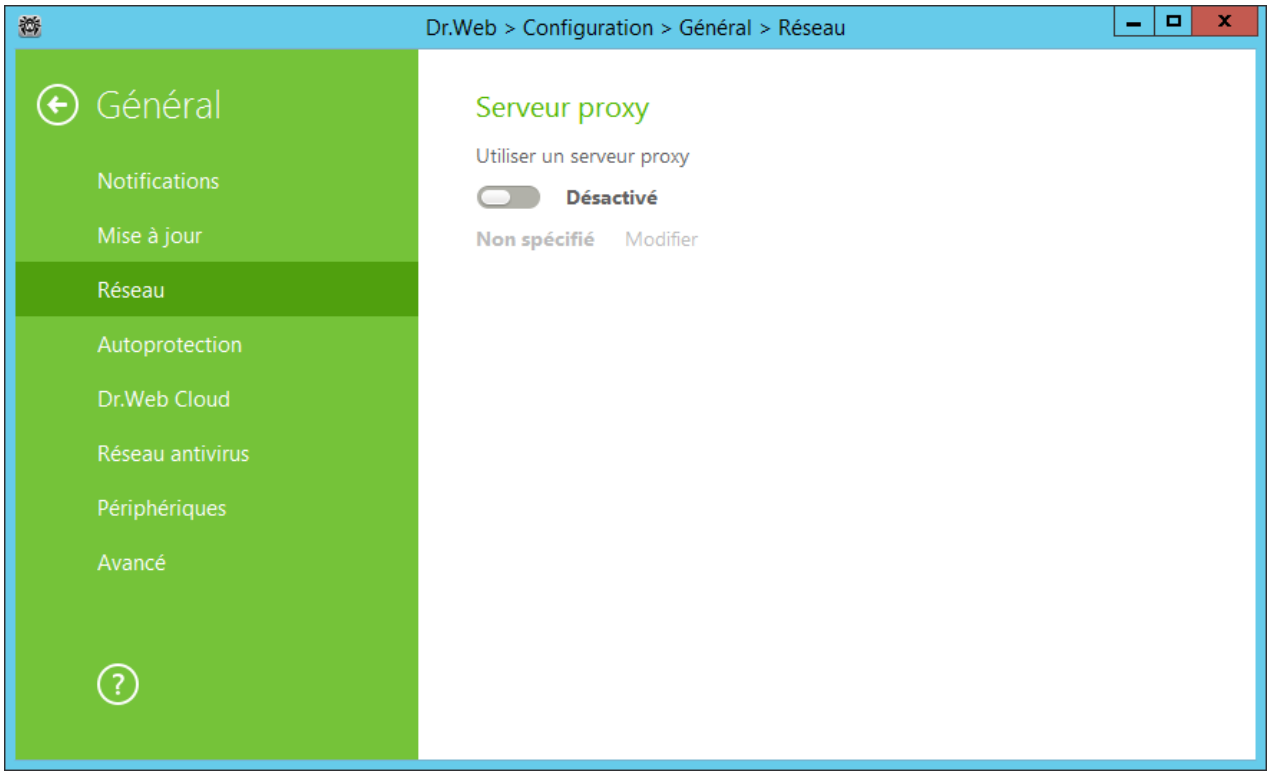
Pour autoriser d'autres ordinateurs du réseau local utilisant les produits Dr.Web à utiliser votre ordinateur comme source de mise à jour, ouvrez les **Paramètres avancés** et activez l'option correspondante. Cliquez sur **Modifier** pour indiquer le chemin vers le dossier où les mises à jour seront copiées. Si votre ordinateur est connecté à plusieurs réseaux, vous pouvez indiquer l'adresse IP disponible pour les ordinateurs d'un réseau seulement. Vous pouvez également indiquer le port pour les connexions HTTP.

10.3. Réseau

Utiliser le serveur proxy

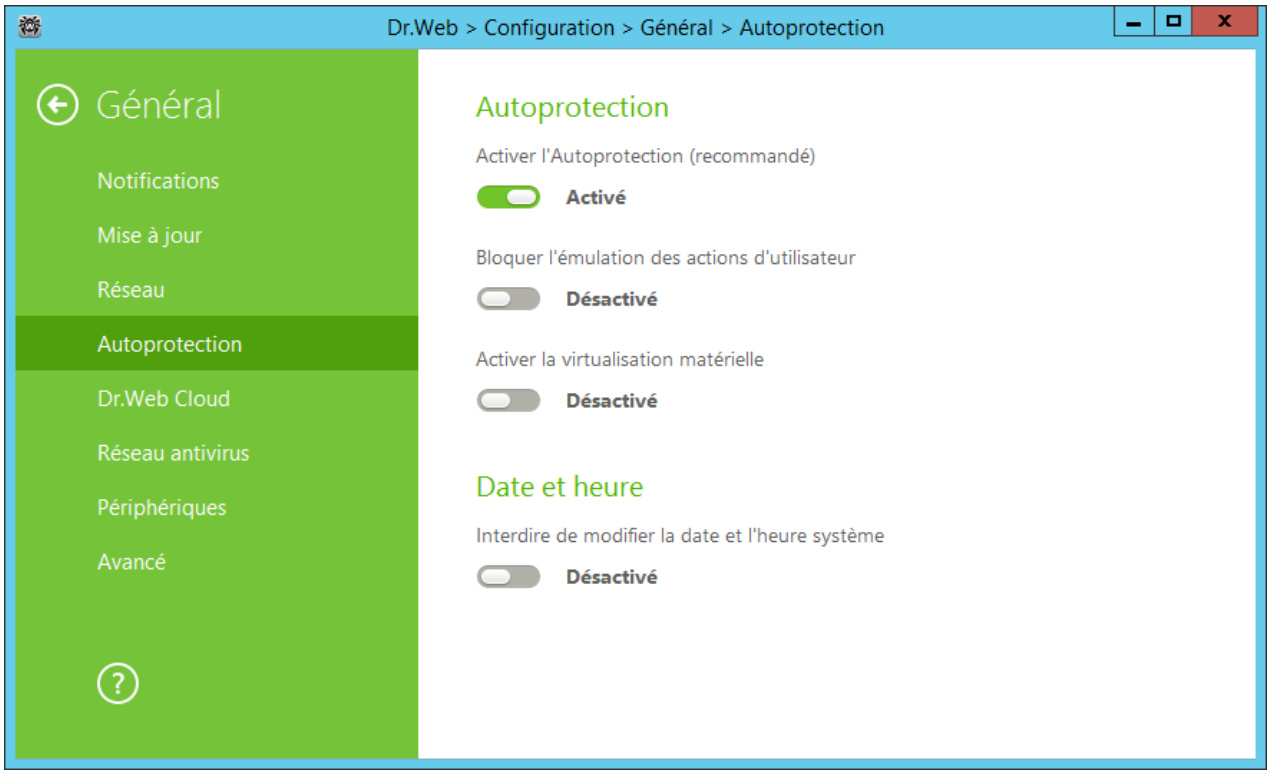
Si nécessaire, vous pouvez activer l'utilisation d'un serveur proxy et configurer ses paramètres. Cliquez sur **Modifier** pour paramétrer le serveur proxy :

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Utilisateur	Spécifiez le nom du compte pour se connecter au serveur proxy.
Mot de passe	Spécifiez le mot de passe du compte utilisé pour se connecter au serveur proxy.
Type d'authentification	Sélectionnez un type d'authentification nécessaire pour se connecter au serveur proxy.



10.4. Autoprotection

Dans cette rubrique, vous pouvez configurer l'autoprotection de Dr.Web contre les modifications non autorisées effectuées par les anti-antivirus ou contre les dommages accidentels.



Page Autoprotection

L'option **Activer l'Autoprotection** permet de protéger les fichiers et les processus de Dr.Web contre l'accès non autorisé. Il n'est pas recommandé de désactiver l'Autoprotection.

En cas de problèmes survenus lors de l'utilisation d'outils de défragmentation, il est recommandé de désactiver temporairement l'Autoprotection.

Pour réaliser un rollback vers le point de restauration du système, il est nécessaire de désactiver le module d'Autoprotection.

L'option **Bloquer l'émulation des actions d'utilisateur** permet de prévenir les modifications automatiques dans les paramètres de Dr.Web, y compris l'exécution de scripts qui imitent l'interaction de l'utilisateur avec Dr.Web et qui sont lancés par l'utilisateur (par exemple, des scripts de modification des paramètres de Dr.Web, de suppression de la licence et d'autres actions visant la modification du fonctionnement de Dr.Web).

Le paramètre **Utiliser la virtualisation matérielle** permet d'utiliser plus de fonctionnalités de l'ordinateur pour détecter et neutraliser les menaces et pour rendre l'autoprotection Dr.Web plus fiable. Pour activer cette option, le redémarrage de l'ordinateur est requis.

La virtualisation matérielle fonctionne si les particularités matérielles de votre ordinateur et le système d'exploitation supportent la virtualisation matérielle.

L'activation de cette option peut provoquer un conflit de compatibilité avec des logiciels tiers.

En cas de problèmes, désactivez cette option.

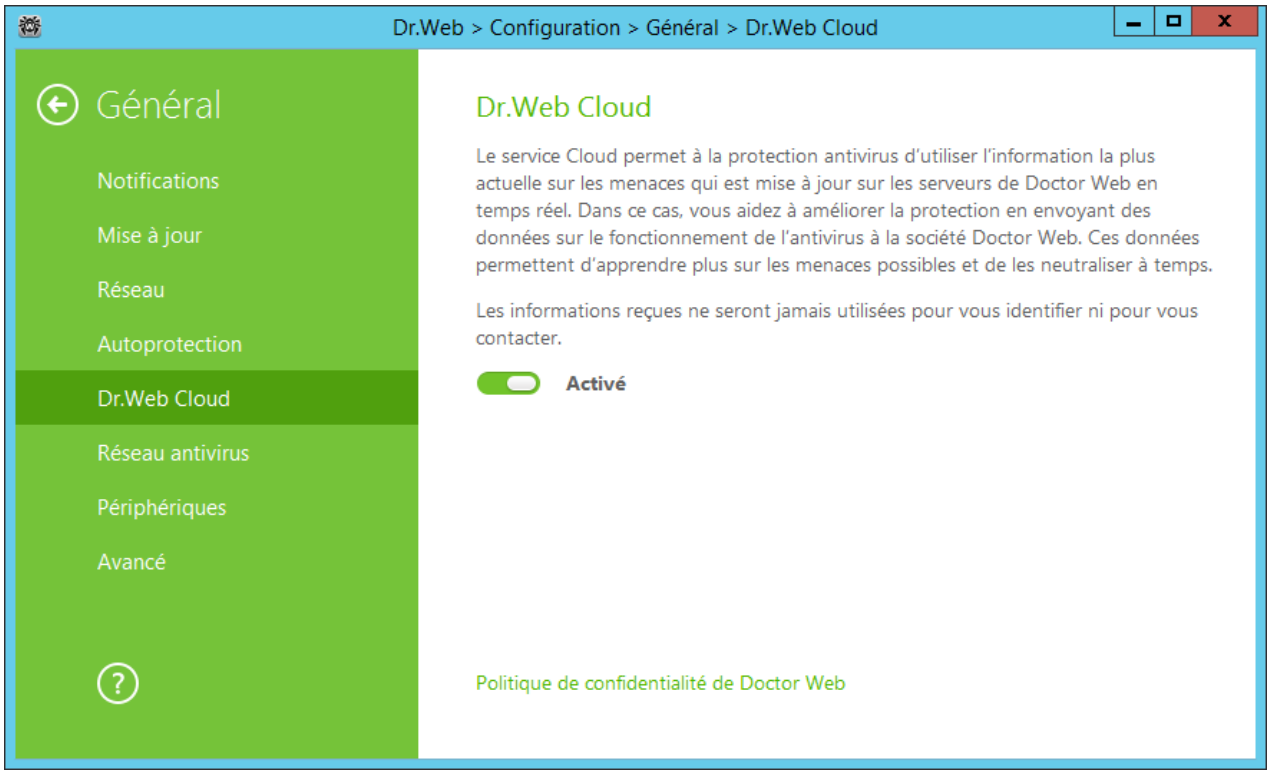
Pour les plateformes 32-bits la virtualisation matérielle n'est pas supportée.

Date et heure

L'option **Interdire de modifier la date et l'heure système** permet d'empêcher les modifications manuelles ou automatiques de l'heure et de la date système ainsi que du fuseau horaire. Cette restriction s'applique à tous les utilisateurs. Vous pouvez configurer les notifications afin d'être informé d'une tentative de modification de l'heure système.

10.5. Dr.Web Cloud

Dans cette rubrique, vous pouvez vous connecter aux services cloud de Doctor Web et participer au programme d'amélioration de la qualité des produits Dr.Web.



Services Cloud

Dr.Web Cloud permet à la protection antivirus d'utiliser des informations actuelles sur les menaces, ces informations sont mises à jour sur les serveurs de Doctor Web en temps réel.

En fonction des paramètres de mises à jour, les informations sur les menaces utilisées par les composants de la protection antivirus peuvent être obsolètes. Les services Cloud peuvent, de façon fiable, restreindre l'accès des utilisateurs de votre ordinateur aux fichiers infectés.

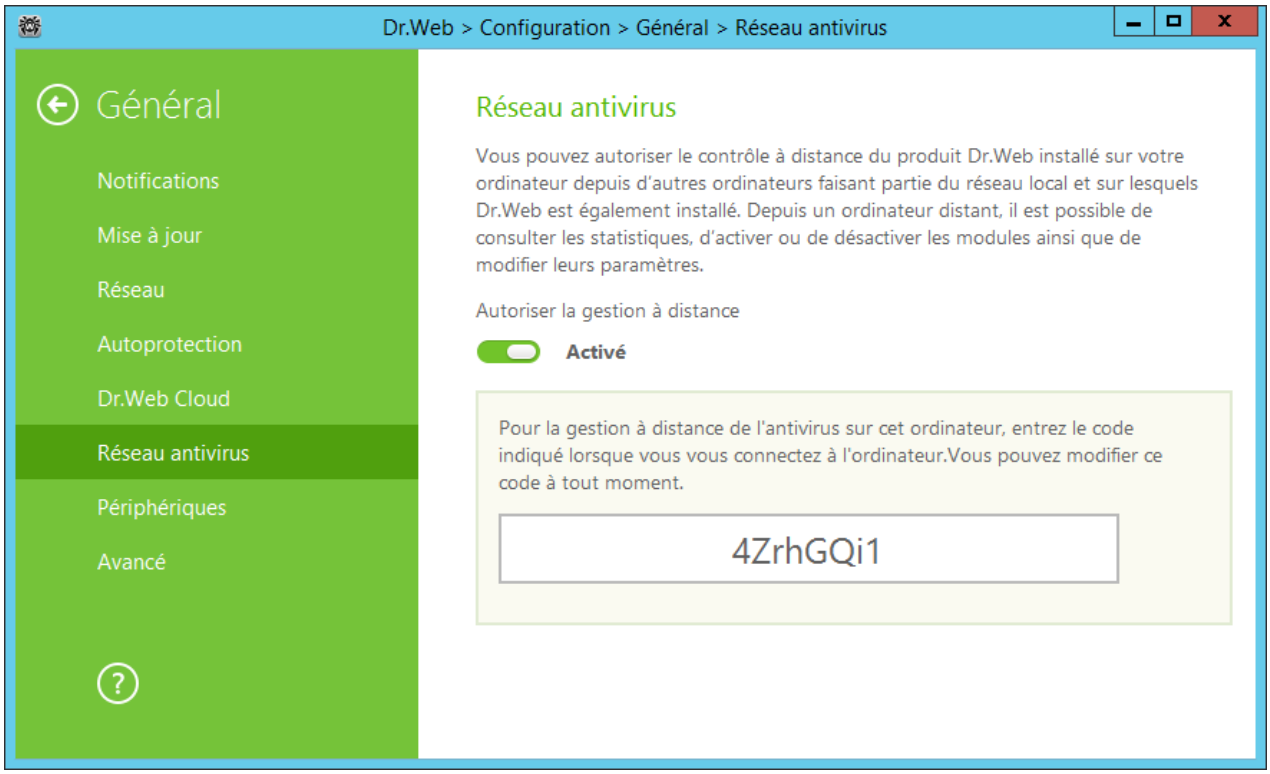
Programme d'amélioration de la qualité du logiciel

Si vous participez au programme d'amélioration de la qualité du logiciel, des données non personnelles sur le fonctionnement de Dr.Web sur votre ordinateur seront périodiquement envoyées sur les serveurs de la société. Les données reçues ne sont pas utilisées pour vous identifier ni vous contacter.

Cliquez sur le lien **Politique de confidentialité de Doctor Web** pour consulter cette politique sur le site officiel de Doctor Web.

10.6. Réseau antivirus

Dans cette rubrique, vous pouvez activer le contrôle à distance de votre antivirus depuis un autre ordinateur du réseau local grâce au composant Réseau antivirus. Si votre ordinateur est connecté à un réseau antivirus, vous pouvez contrôler l'état de la protection antivirus (consulter les statistiques, activer ou désactiver les composants de Dr.Web et modifier leur configuration) ainsi que recevoir des mises à jour via le réseau local. Pour utiliser un ordinateur comme une source de mises à jour pour les autres ordinateurs du réseau local utilisant un produit de Dr.Web, il est nécessaire de configurer sur cet ordinateur un miroir de mise à jour.

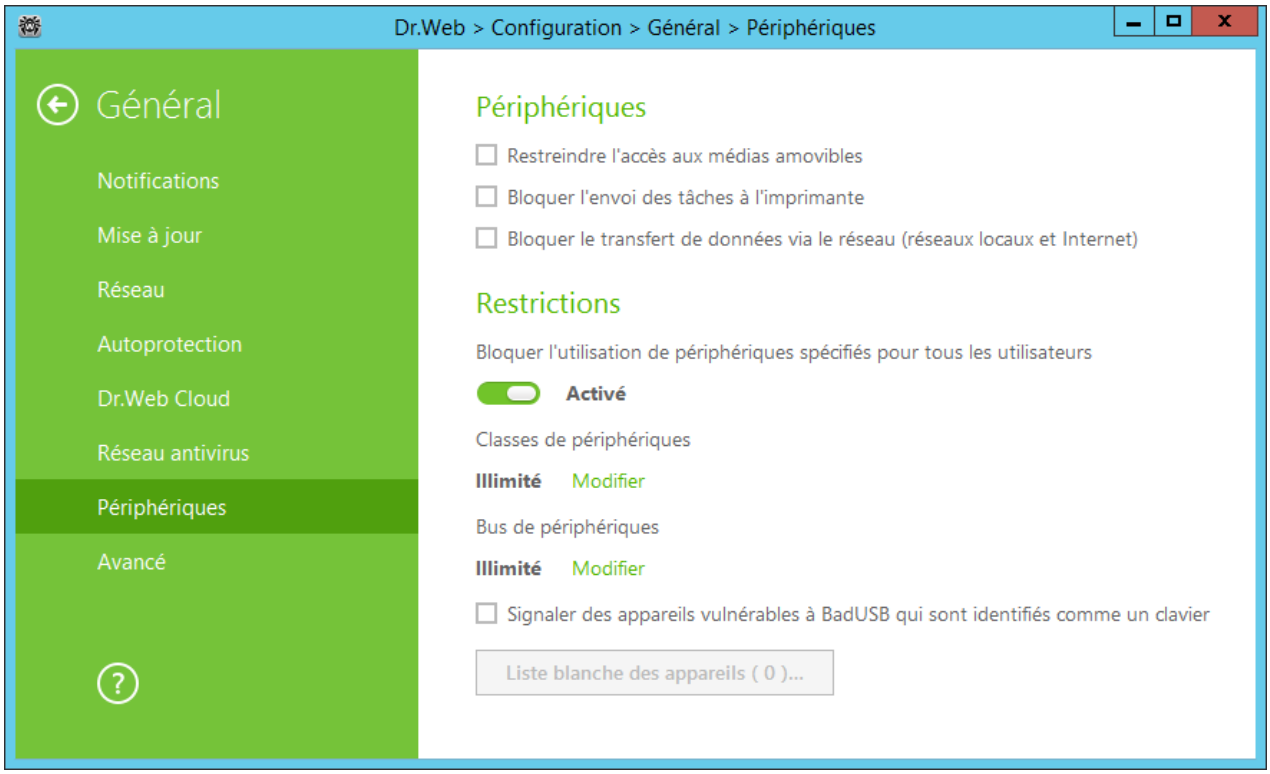


Pour gérer à distance Dr.Web sur votre ordinateur, le mot de passe sera requis. Vous pouvez utiliser le mot de passe qui est généré automatiquement au moment de l'activation de l'option ou vous pouvez spécifier votre propre mot de passe.

Vous pouvez consulter des statistiques, activer ou désactiver des modules et éditer leurs paramètres. Les éléments Quarantaine et Scanner sont indisponibles. Les paramètres et les statistiques du Pare-feu Dr.Web ne sont pas disponibles non plus, cependant vous pouvez activer ou désactiver ce composant.

10.7. Périphériques

Les règles du Contrôle d'accès sont valables pour tous les comptes Windows.



Périphériques

Pour bloquer l'accès aux données stockées sur des supports amovibles (clés USB, disquettes, CD/DVD, lecteurs ZIP, etc.), activez l'option correspondante. Pour bloquer l'envoi de tâches à l'imprimante, cochez la case **Bloquer l'envoi des tâches à l'imprimante**. Cette option est désactivée par défaut. Vous pouvez également bloquer le transfert de données via le réseau local et Internet.

Certains périphériques USB infectés peuvent être reconnus par l'ordinateur comme un clavier. Pour que Dr.Web vérifie si le périphérique connecté est vraiment un clavier, activez l'option **Signaler des appareils vulnérables à BadUSB qui sont identifiés comme un clavier**.

Périphériques et bus de périphériques

Pour bloquer l'accès aux classes sélectionnées de périphériques et de bus de périphériques, activez l'option correspondante. Cliquez sur **Modifier** pour créer la liste de tels objets. Dans la fenêtre qui s'affiche, sélectionnez les classes de périphériques et de bus de périphériques, l'accès auquel doit être bloque. Pour sauvegarder les modification apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**.

Liste blanche des appareils

Si vous avez limité l'accès à une classe de périphériques ou de bus de périphériques, vous pouvez pourtant autoriser l'accès à des périphériques concrets en les ajoutant dans la liste blanche. Vous

pouvez également ajouter un périphérique concret à la liste blanche pour ne pas le scanner à la recherche de la vulnérabilité BadUSB.

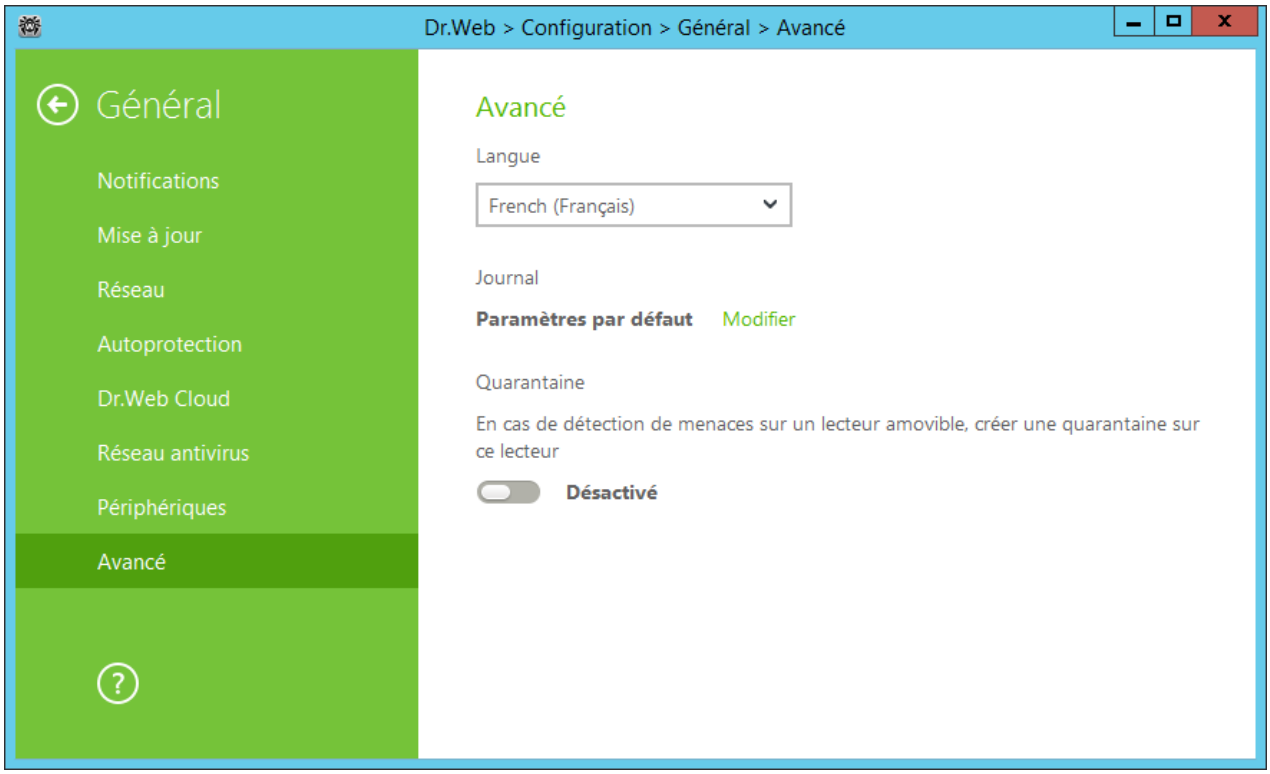
Pour ajouter un périphérique à la liste blanche, faites le suivant :

1. Cliquez sur **Liste blanche des appareils** (ce bouton devient active si les limitations sont spécifiées).
2. Assurez-vous que le périphérique est connecté à l'ordinateur.
3. Cliquez sur  . Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et sélectionnez le périphérique nécessaire. Pour plus de commodité, utilisez le filtre. Alors le tableau va contenir uniquement les périphériques connectés ou non connectés. Cliquez sur **OK**.
4. Vous pouvez configurer les paramètres d'accès pour les périphériques avec le système de fichiers. Pour ce faire, sélectionnez le mode **Autoriser tout** ou **Uniquement la lecture** dans la colonne **Règle**. Pour ajouter une nouvelle règle pour un utilisateur concret, cliquez sur le bouton  . Pour supprimer une règle, cliquez sur  .
5. Pour sauvegarder les modification apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**. Vous allez revenir à la liste blanche.
6. Pour modifier l'ensemble de règles pour un périphérique, sélectionnez-le dans la liste et cliquez sur  .
7. Pour supprimer l'ensemble de règles pour un périphérique, sélectionnez-le et cliquez sur  .

10.8. Rubrique Avancé

Sur cette page, vous pouvez choisir la langue d'interface pour les paramètres, configurer les options de journalisation et les paramètres de la Quarantaine.

Dans la liste déroulante, vous pouvez choisir une langue du logiciel. La liste de langues se complète automatiquement et à l'heure actuelle, elle contient toutes les localisations disponibles de l'interface graphique de Dr.Web pour le moment donné.



Paramètres du Journal

Pour configurer les paramètres du journal cliquez sur le bouton correspondant **Modifier**.

Par défaut, la taille des fichiers de journal est limitée à 10 Mo. Si la taille du fichier de journal excède la limite, le contenu du fichier est réduit à :

- la taille spécifiée si le fichier de journal obtenu après le scan de la session en cours n'excède pas cette limite ;
- la taille du fichier de journal obtenu après le scan de la session en cours, si le fichier de journal global excède la limite.

Par défaut pour tous les composants de Dr.Web le journal est conservé en mode standard et les informations suivantes sont enregistrées :

Composant	Information
SpIDer Guard	Les mises à jour et les démarrages/arrêts de SpIDer Guard, les événements viraux, les noms des fichiers scannés, les noms des packers et le contenu des objets complexes scannés (archives, pièces jointes d'e-mail, conteneurs de fichiers). Il est recommandé d'utiliser ce mode pour déterminer les objets les plus fréquemment scannés par SpIDer Guard. Si nécessaire, vous pouvez ajouter ces objets dans la liste d'exclusions afin d'augmenter les performances de l'ordinateur.
Scanner	Dans ce mode, les événements qui sont journalisés ce sont les mises à jour, les démarrages et les arrêts du Scanner Dr.Web, les menaces détectées, ainsi que les

Composant	Information
	informations sur les noms des packers et sur le contenu des archives scannées.
Mise à jour de Dr.Web	Liste des fichiers Dr.Web mis à jour et état de leur téléchargement, détails sur l'exécution de scripts auxiliaires, date et heure des mises à jour, détails sur le redémarrage des composants Dr.Web après la mise à jour.
Service Dr.Web	Informations sur les composants Dr.Web, modification de paramètres des composants, activation ou désactivation des composants, événements relatifs à la protection préventive, connexion au réseau antivirus.

Créer des dumps de mémoire

L'option **Créer des dumps de mémoire en cas d'erreur de scan** permet de sauvegarder les informations utiles sur le fonctionnement de plusieurs composants de Dr.Web. Cette option aide les spécialistes de Doctor Web à analyser un problème en détails et à trouver une solution. Il est recommandé d'activer cette option à la demande du support technique de Doctor Web ou lorsque des erreurs de scan ou de neutralisation surviennent. Le dump de mémoire est sauvegardé dans un fichier .dmp situé dans le dossier %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\.

Pour activer les journaux détaillés

> ⚠ Lors de la journalisation détaillée le maximum d'informations sur le fonctionnement des composants Dr.Web est fixé. Cela va désactiver la restriction de taille de fichiers de journal et augmenter la charge de Dr.Web et du système d'exploitation. Il est recommandé d'utiliser ce mode uniquement lorsque des erreurs de composants surviennent ou sur requête du Support Technique Doctor Web.

1. Pour activer les journaux détaillés pour un composant Dr.Web, cochez la case correspondante.
2. Par défaut, le mode de journal détaillé est utilisé avant le premier redémarrage de l'OS. S'il est nécessaire d'enregistrer le comportement du composant avant et après le redémarrage, cochez la case **Continuer à écrire le journal détaillé après le redémarrage (non recommandé)**.
3. Sauvegardez les modifications.

Paramètres de Quarantaine

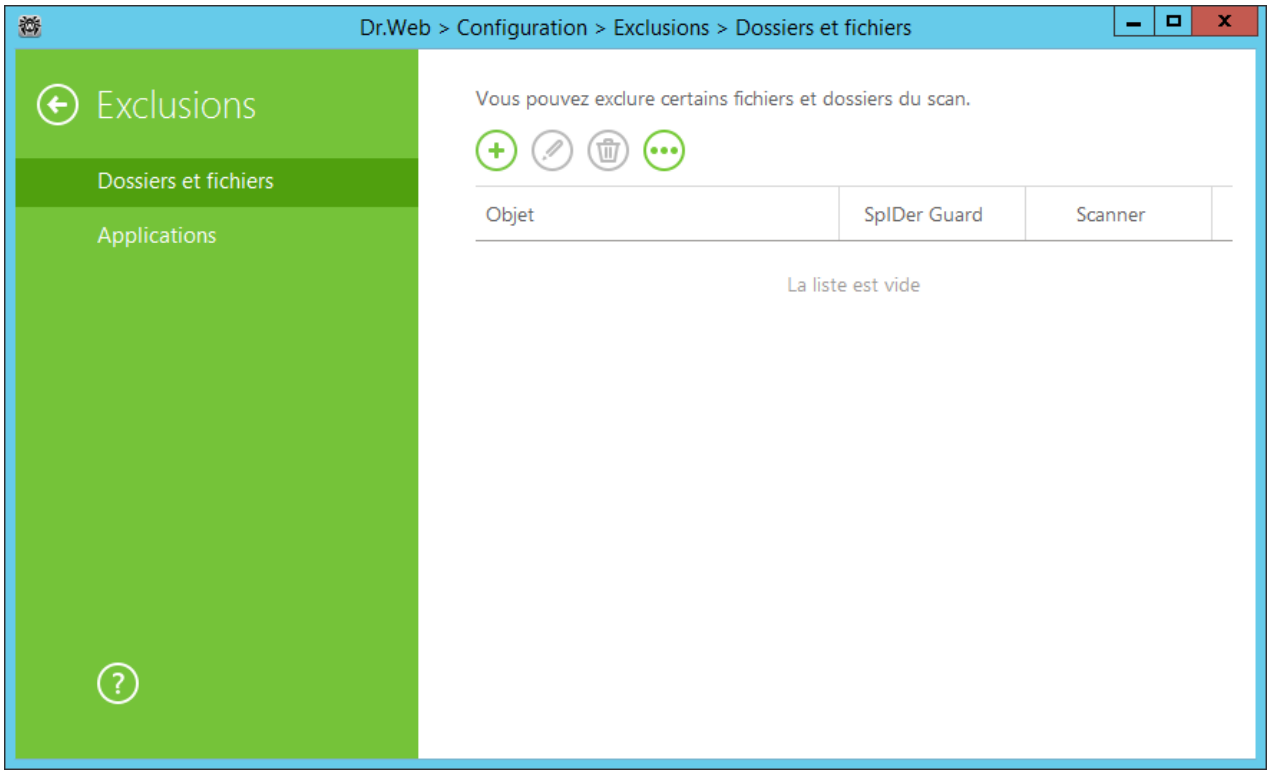
Vous pouvez choisir le mode d'isolation pour les objets infectés, détectés sur les supports amovibles. Lorsque cette option est activée, les menaces détectées sont déplacées dans le dossier sur le support amovible sans être chiffrées. Le dossier de quarantaine est créé uniquement lorsque le support amovible est accessible en écriture. L'utilisation de dossiers séparés et du non chiffrement sur les supports amovibles permet de prévenir la perte de données. Si l'option est désactivée, la menace détectée est mise en quarantaine sur le disque local

11. Exclusions

11.1. Dossiers et fichiers

Dans cette section, vous pouvez specifier la liste des fichiers et dossiers qui sont exclus du scan de SpIDer Guard et du Scanner. Vous pouvez exclure les dossiers de quarantaine, les dossiers de travail de certains programmes, les fichiers temporaires (fichiers swap), etc.

La liste est vide par défaut. Ajoutez des fichiers et dossiers aux exclusions ou utilisez des masques pour désactiver le scan de certains groupes de fichiers. Tout objet ajouté peut être exclu du scan des deux composants ou du scan de chaque composant séparément.



Pour configurer la liste des exclusions

1. Faites une des actions suivantes pour ajouter un dossier ou un fichier à la liste :
   - pour ajouter un fichier ou dossier existant, cliquez sur . Dans la fenêtre qui s'ouvre, cliquez sur **Parcourir** et choisissez le fichier ou dossier dans la fenêtre standard d'ouverture de fichier. Vous pouvez entrer manuellement le chemin complet vers le fichier ou le dossier, ou modifier le chemin dans le champ réservé à cet effet avant de l'ajouter à la liste ;
   - pour exclure de l'analyse le fichier avec un nom particulier, entrez dans le champ de saisie le nom du fichier y compris l'extension. Il n'est pas nécessaire de spécifier le chemin d'accès au fichier ;
   - pour exclure un groupe de fichiers ou de dossiers, entrez le masque qui détermine leurs noms.

2. Dans la fenêtre de configuration, indiquez les composants qui ne doivent pas scanner ce fichier.
3. Cliquez sur **OK**. Le fichier ou dossier apparaît dans la liste.
4. Pour modifier une exclusion, sélectionnez l'élément nécessaire dans la liste et cliquez sur .
5. Pour ajouter de nouveaux fichiers ou dossiers à la liste, répétez les étapes 1 et 2. Pour retirer un fichier ou un dossier de la liste, sélectionnez-le dans la liste et cliquez sur .

Un masque désigne les éléments communs aux noms des objets, ainsi :

- le caractère « * » remplace toute séquence (potentiellement vide) de signes ;
- symbole « ? » remplace n'importe quel caractère (un seul caractère) ;
- les autres symboles de masque ne remplacent aucun caractère et signifient qu'à cette place dans le nom, doit se trouver ce signe particulier.

Exemples de configuration des exclusions :

- file.txt – exclut de l'analyse tous les fichiers avec le nom file et l'extension .txt dans tous les dossiers.
- C:\folder\file.txt – exclut de l'analyse le fichier file.txt se trouvant dans le dossier C:\folder.
- file* – exclut de l'analyse tous les fichiers, dont les noms commencent pas file, avec n'importe quelle extension dans tous les dossiers.
- file.* – exclut de l'analyse tous les fichiers avec le nom file et n'importe quelle extension dans tous les dossiers.
- file – exclut de l'analyse tous les fichiers avec le nom file sans extension dans tous les dossiers.
- C:\folder\ ou C:\folder** – exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier C:\folder.
- C:\folder* – exclut de l'analyse tous les fichiers se trouvant dans le dossier C:\folder ainsi que dans tous les sous-dossiers à tout niveau d'emboîtement.
- C:\folder*.txt – exclut de l'analyse les fichiers de type *.txt se trouvant dans le dossier C:\folder. Les fichiers *.txt se trouvant dans les sous-dossiers seront scannés.
- C:\folder**.txt – exclut de l'analyse les fichiers de type *.txt uniquement dans les sous-dossier du premier niveau d'emboîtement dans le répertoire C:\folder.
- C:\folder***.txt – exclut de l'analyse les fichiers de type *.txt dans les sous-dossiers de tout niveau d'emboîtement dans le dossier C:\folder. Les fichiers *.txt se trouvant dans le dossier C:\folder seront scannés.

Gestion des objets dans la liste

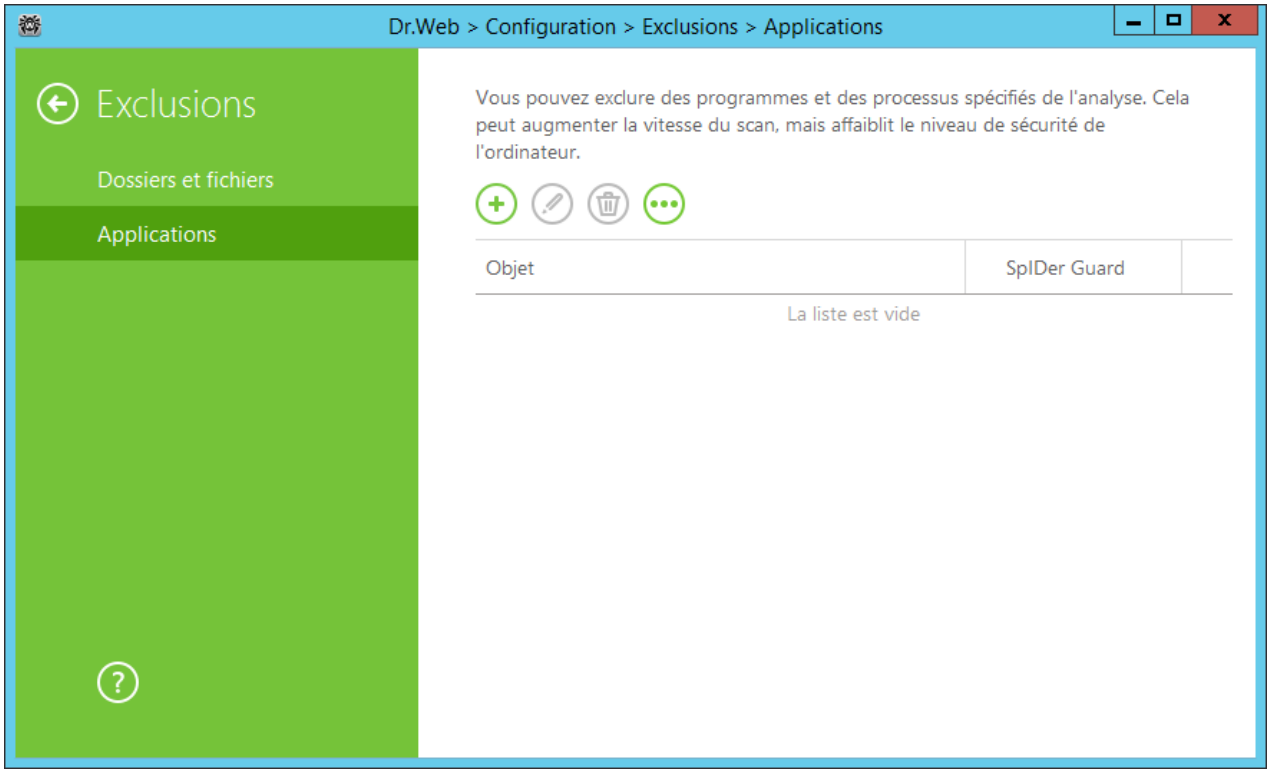
Si vous cliquez sur , les actions suivantes seront disponibles :

- **Exporter** – cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel est installé Dr.Web.
- **Importer** – cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
- **Supprimer tout** – cette option permet de supprimer tous les objets de la liste des exclusions.

11.2. Applications

Dans cette section, vous pouvez spécifier la liste des programmes et des processus à exclure de l'analyse par le composant SpIDer Guard .

Par défaut, la liste est vide.



Pour configurer la liste des exclusions

1. Pour ajouter un programme ou un processus à la liste des exclusions, cliquez sur . Exécutez une des actions suivantes :
   - dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir** et sélectionnez l'application dans la fenêtre standard d'ouverture de fichier. Vous pouvez entrer manuellement le chemin complet vers l'application dans le champ d'entrée ;
   - pour exclure une application de l'analyse, entrez son nom dans le champ de saisie. Dans ce cas, il n'est pas nécessaire de spécifier le chemin complet vers l'application (par exemple, `example.exe`) ;
   - pour exclure de l'analyse les applications d'un type particulier, entrez le masque qui les détermine dans le champ de saisie ;
   - vous pouvez exclure une application de l'analyse par le nom de variable, si dans les paramètres des variables système, le nom et la valeur de cette variable sont spécifiées.
2. Dans la fenêtre de configuration, indiquez que SpIDer Guard ne doit pas analyser l'application sélectionnée.

3. Cliquez sur **OK**. L'application sélectionnée va apparaître dans la liste.
4. Si nécessaire, reproduisez la marche à suivre pour y ajouter d'autres programmes.
5. Pour modifier une exclusion, sélectionnez l'élément nécessaire dans la liste et cliquez sur .
6. Pour supprimer une application de la liste des exclusions, sélectionnez l'élément nécessaire dans la liste et cliquez sur .

Un masque désigne les éléments communs aux noms des objets, ainsi :

- le caractère « * » remplace toute séquence (potentiellement vide) de signes ;
- le caractère « ? » remplace n'importe quel caractère (un seul caractère) ;

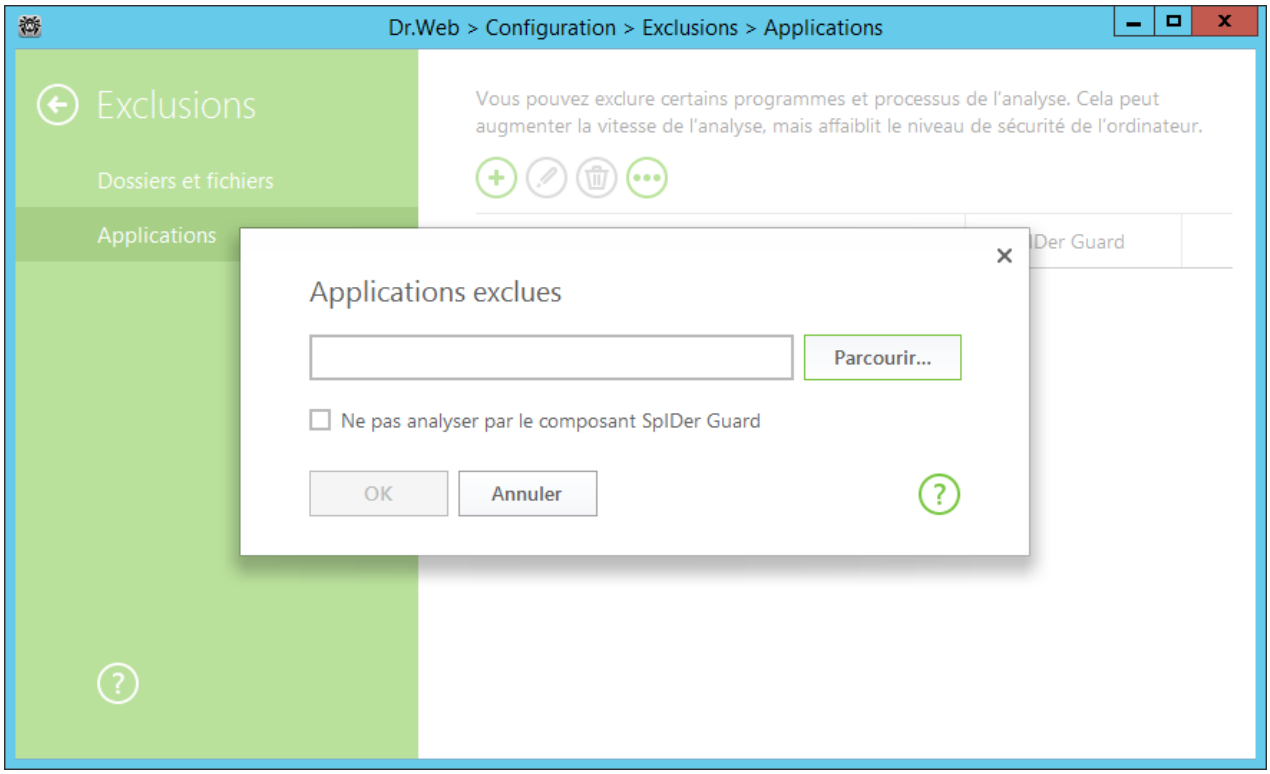
Exemples de configuration des exclusions :

- `C:\Program Files\folder\example.exe` – exclut de l'analyse l'application example.exe dans le dossier C:\Program Files\folder du scan.
- `C:\Program Files\folder\*.exe` - exclut de l'analyse les applications dans le dossier C:\Program Files\folder. Dans les sous-dossiers, les applications seront analysées.
- `C:\Program Files\*\*.exe` – exclut de l'analyse uniquement les applications dans les sous-dossiers du premier niveau d'emboîtement du dossier C:\Program Files.
- `C:\Program Files\**\*.exe` - exclut de l'analyse les applications dans les sous-dossiers de tout niveau d'emboîtement du dossier C:\Program Files. Dans le dossier C:\Program Files, les applications seront analysées.
- `C:\Program Files\folder\exam*.exe` - exclut de l'analyse toutes les applications dans le dossier C:\Program Files\folder dont les noms commencent par « exam ». Dans les sous-dossiers, ces applications seront analysées.
- `example.exe` – exclut de l'analyse toutes les applications avec le nom example et l'extension .exe dans tous les dossiers.
- `example*` – exclut de l'analyse dans tous les dossiers les applications de tout type dont les noms commencent par example.
- `example.*` – exclut de l'analyse toutes les applications avec le nom example et n'importe quelle extension dans tous les dossiers.
- `%EXAMPLE_PATH%\example.exe` – exclut de l'analyse l'application selon le nom de la variable système. Vous pouvez spécifier le nom et la valeur de la variable système dans les paramètres du système d'exploitation.

  Sous Windows 7 et supérieur : **Panneau de configuration→Système → Paramètres système avancés → Avancé → Variable d'environnement → Variables système**.

  Nom de la variable dans l'exemple :`EXAMPLE_PATH`.

  Valeur de la variable dans l'exemple :`C:\Program Files\folder`.



Gestion des objets dans la liste

Si vous cliquez sur , les actions suivantes seront disponibles :

- **Exporter** – cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel est installé Dr.Web.
- **Importer** – cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
- **Supprimer tout** – cette option permet de supprimer tous les objets de la liste des exclusions.

12. Composants de protection

12.1. SpIDer Guard

SpIDer Guard est un composant antivirus résidant en mémoire vive qui scanne les fichiers et la mémoire « à la volée » et détecte instantanément toute activité malveillante.

Avec les paramètres par défaut, SpIDer Guard réalise le scan à la volée des fichiers créés ou modifiés sur le disque dur ainsi que tous les fichiers ouverts depuis un support amovible. De même, SpIDer Guard suit constamment les processus lancés pour détecter les comportements suspects et, s'il en détecte un, bloque les processus malveillants. En cas de détection des objets infectés, SpIDer Guard applique les actions définies par les paramètres configurés.

Les fichiers en archives et les boites aux lettres ne sont pas scannés. Si un fichier en archive ou en pièce jointe d'un e-mail est infecté, l'objet malveillant sera détecté et immédiatement neutralisé par SpIDer Guard au moment de l'extraction du fichier avant que l'ordinateur soit infecté.

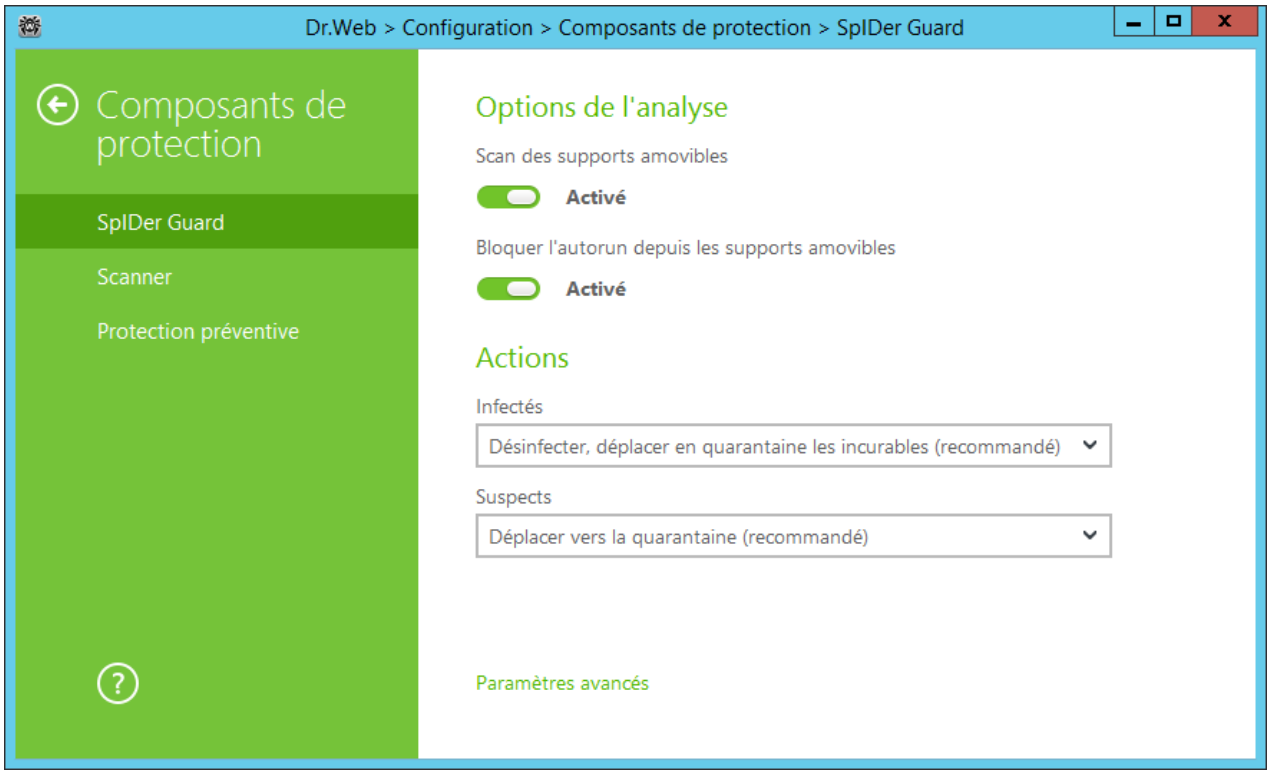
Lors de la détection d'un objet infecté, SpIDer Guard applique les actions d'après les paramètres indiqués. Vous pouvez modifier ces paramètres pour configurer des réactions automatiques à appliquer aux différents événements viraux.

Par défaut SpIDer Guard se lance automatiquement à chaque démarrage de Windows et ne peut être déchargé durant la session Windows en cours.

12.1.1. Configurer SpIDer Guard

Pour accéder aux paramètres de SpIDer Guard, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web** par mot de passe dans la fenêtre de Configuration.

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.



Options de l'analyse

SpIDer Guard analyse par défaut les objets sur les supports amovibles (disques CD/DVD, mémoires flash, etc) et bloque le lancement automatique de leur contenu actif. L'utilisation de ces paramètres permet de prévenir l'infection de votre ordinateur via les supports amovibles.

> En cas de problèmes lors de l'installation des programmes utilisant le fichier autorun.inf, il est recommandé de désactiver temporairement l'option **Bloquer l'autorun depuis les supports amovibles**.

Actions

Dans cette rubrique, vous pouvez configurer les réactions de SpIDer Guard à la détection des fichiers infectés, suspects ou des programmes malveillants.

La réaction est spécifiée séparément pour chaque catégorie des objets :

- **Objets infectés** – objets infectés par un virus connu et (supposé) curable ;
- **Objets suspects** – objets suspectés d'être infectés par des virus ou de contenir un objet malveillant ;
- Objets potentiellement dangereux. Pour afficher toute la liste, cliquez sur le lien **Paramètres avancés**.

Les réactions de SpIDer Guard vis-à-vis des logiciels malveillants sont également paramétrées séparément. Les actions disponibles dépendent du type d'événement viral.

Par défaut, SpIDer Guard essaie de désinfecter les objets infectés et supposés curables, déplace les objets les plus dangereux en Quarantaine, et ignore les canulars, hacktools et riskware. Les réactions de SpIDer Guard sont similaires à celles du Scanner Dr.Web.

Les actions suivantes sont disponibles pour appliquer aux objets détectés :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action est possible pour les virus connus seulement, sauf les Trojans et les fichiers infectés au sein des objets complexe.
Désinfecter, supprimer les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'action appliquée aux virus incurables est appliquée. Cette action est possible pour les virus connus seulement, sauf les Trojans et les fichiers infectés au sein des objets complexe.
Supprimer	Supprimer l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.

SpIDer Guard n'analyse pas les objets complexes. Aucune action ne leur est appliquée.

Des copies de sauvegarde de tous les objets traités sont stockées dans la Quarantaine.

Mode d'analyse

Dans cette partie, vous pouvez déterminer quels objets requièrent une analyse « à la volée » par SpIDer Guard.

Paramètre	Description
Optimal (recommandé)	Ce mode de scan est utilisé par défaut. Dans ce mode, SpIDer Guard analyse les objets dans les cas suivants : • pour les objets sur les disques durs, lorsqu'il y a une tentative d'exécuter un fichier, de créer un nouveau fichier ou d'écrire sur un fichier existant ou sur le secteur d'amorçage ; • pour les objets sur les supports amovibles - à chaque tentative d'accéder à un fichier ou à un secteur d'amorçage (écrire, lire, exécuter).
Paranoïde	Dans ce mode, SpIDer Guard analyse les fichiers et les secteurs d'amorçage sur les disques durs ou réseau et sur les supports amovibles en cas de tentative d'y accéder (créer, écrire, lire, exécuter).

Lancé dans le mode optimal, SpIDer Guard n'interrompt pas le lancement du fichier de test EICAR et ne classe pas telle situation comme dangereuse puisque ce fichier ne représente aucun danger pour l'ordinateur. Cependant, lors de la copie ou de la création de ce fichier, SpIDer Guard le traite automatiquement comme un malware et par défaut le déplace en Quarantaine.

Le mode **Optimal** est recommandé après une analyse de tous les disques durs effectuée par le Scanner Dr.Web. Lorsque ce mode est activé, SpIDer Guard prévient la pénétration de nouveaux virus et d'autres programmes malveillants dans votre ordinateur via les supports amovibles sans analyser de nouveaux les objets déjà scannés.

Le mode **Paranoïde** assure une protection maximum mais réduit les performances de la machine.

Dans tous les modes, SpIDer Guard analyse les objets en réseau et les supports amovibles uniquement si les options correspondantes sont activées dans l'onglet **Options de l'analyse**.

Le système d'exploitation peut reconnaitre certains supports amovibles comme des disques durs (notamment les disques durs externes à l'interface USB). Veuillez utiliser ces dispositifs avec beaucoup de précautions et analysez-les avec le Scanner Dr.Web lorsqu'ils sont connectés à l'ordinateur.

SpIDer Guard ne contrôle pas les archives ni les courriers électroniques par défaut. Ceci n'affecte pas la sécurité de votre ordinateur lorsqu'il est protégé en permanence par SpIDer Guard. Si un fichier contenu dans une archive ou une pièce jointe d'e-mail est infecté, l'objet malveillant sera détecté et immédiatement neutralisé par SpIDer Guard lorsque vous tenterez d'extraire le fichier archivé ou de télécharger la pièce jointe.

Options supplémentaires

Ce groupe de paramètres vous permet de configurer les options du scan à la volée qui seront appliquées dans tous les modes de fonctionnement de SpIDer Guard. Vous pouvez activer :

- l'utilisation de l'analyseur heuristique ;
- l'analyse des programmes et modules en cours de démarrage ;
- l'analyse des fichiers d'installation ;
- l'analyse des fichiers en réseau local (non recommandé) ;
- l'analyse de l'ordinateur pour la présence des rootkits (recommandé).

Analyse heuristique

Par défaut SpIDer Guard réalise l'analyse en utilisant l'analyseur heuristique. Si l'option est désactivée, il réalise l'analyse uniquement par signatures de virus connus.

Scan Anti-rootkit en tâche de fond

Le composant Anti-rootkit intégré à Dr.Web permet d'analyser le système d'exploitation en tâche de fond pour la présence des menaces complexes et de traiter des infections actives lorsque c'est nécessaire. Par défaut, cette option est activée.

Si cette option est activée, Anti-rootkit Dr.Web réside en mémoire de manière permanente. A la différence du scan à la volée des fichiers effectué par SpIDer Guard, le scan des rootkits inclut la vérification du BIOS de l'ordinateur et des zones critiques de Windows, tels que les objets autorun, les processus et les modules en cours, la mémoire vive (RAM), les disques MBR/VBR, etc.

Une des fonctionnalités principales de Anti-rootkit Dr.Web est sa faible consommation des ressources système ainsi que sa prise en considération des capacités hardware.

Lorsque Anti-rootkit Dr.Web détecte une menace, il notifie l'utilisateur et neutralise l'activité malveillante.

Durant le scan en tâche de fond à la recherche de rootkits, les fichiers et dossiers indiqués dans l'onglet correspondant sont exclus du scan.

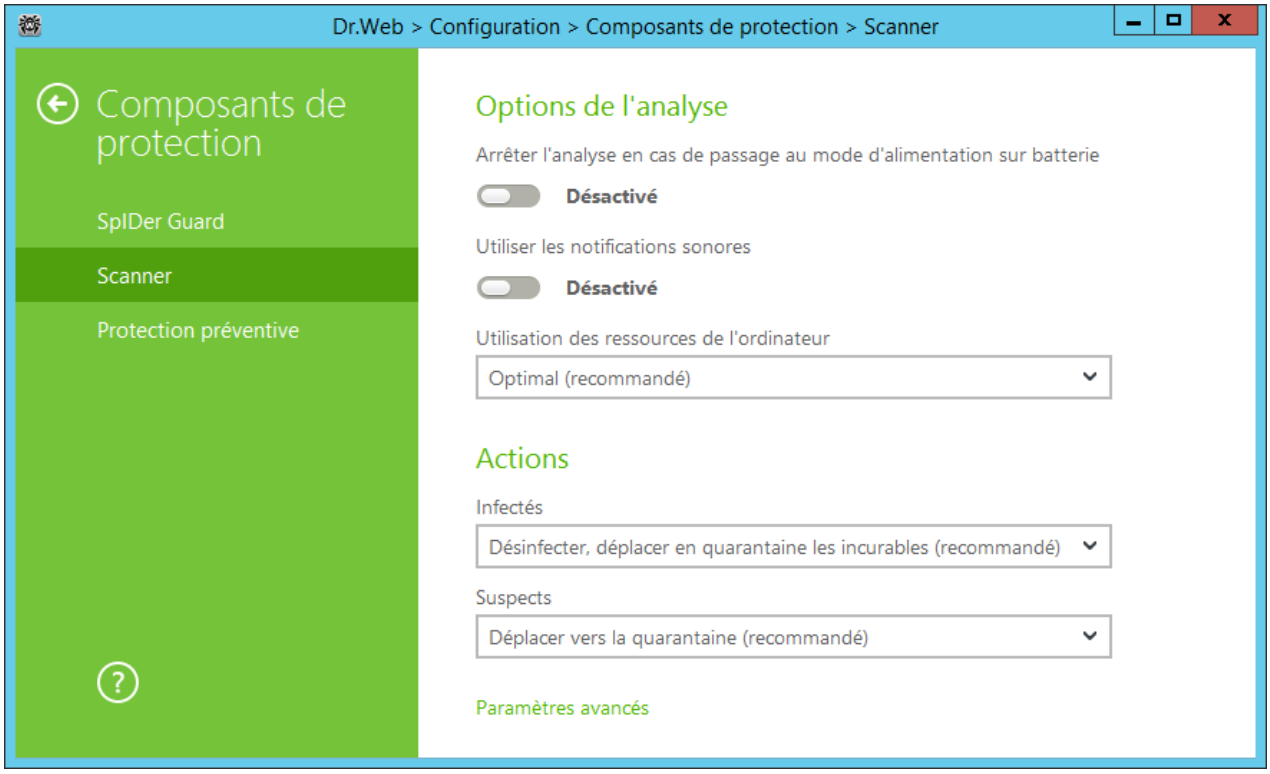
Le scan Anti-rootkit en tâche de fond est activé par défaut

La désactivation de SpIDer Guard n'a pas d'impact sur l'analyse en tâche de fond. Si le paramètre est activé, l'analyse en tâche de fond est effectuée indépendamment du statut de SpIDer Guard.

12.2. Scanner

Pour accéder aux paramètres du Scanner, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la fenêtre de Configuration.

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.



Options de l'analyse

Dans cette rubrique, vous pouvez configurer les paramètres généraux du Scanner Dr.Web :

- **Arrêter l'analyse en cas de passage au mode d'alimentation sur batterie**. Cochez la case pour arrêter le scan en cas de passage vers le mode d'alimentation de la batterie. Cette option est désactivée par défaut.
- **Utiliser les notifications sonores**. Cochez la case pour commander au Scanner Dr.Web d'accompagner chaque événement d'un signal sonore. Cette option est désactivée par défaut.
- **Limitation d'utilisation des ressources de l'ordinateur**. Cette option limite l'utilisation des ressources de l'ordinateur par le **Scanner Dr.Web**. La valeur optimale est utilisée par défaut.

Actions

Dans cette rubrique, vous pouvez configurer la réaction du Scanner lors de la détection d'objets infectés ou suspects et de programmes malveillants.

La réaction est spécifiée séparément pour chaque catégorie des objets :

- **Objets infectés** – objets infectés par un virus connu et (supposé) curable ;
- **Objets suspects** – objets suspectés d'être infectés par des virus ou de contenir un objet malveillant ;
- objets potentiellement dangereux.

Vous pouvez modifier séparément la réaction du Scanner vis-à-vis de chaque type d'objets. Les actions disponibles dépendent du type de menace.

Par défaut, le Scanner essaie de désinfecter les fichiers qui sont infectés par un virus connu et potentiellement curable, tandis que les autres objets qui sont considérés comme les plus dangereux sont placées en Quarantaine.

Les actions suivantes sont disponibles pour appliquer aux objets détectés :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action est possible pour les virus connus seulement, sauf les Trojans et les fichiers infectés au sein des objets complexe.
Désinfecter, supprimer les incurables	Indique de restaurer l'objet dans son état original avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'action appliquée aux virus incurables est appliquée. Cette action est possible pour les virus connus seulement, sauf les Trojans et les fichiers infectés au sein des objets complexe.
Supprimer	Supprimer l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.

Si un virus ou un code suspect est détecté au sein des objets complexes, les actions sur les menaces contenues dans tels objets sont appliquées à l'objet entier et non seulement à sa partie infectée.

Options supplémentaires

Vous pouvez désactiver le scan des packages d'installation, des archives et des fichiers de messagerie. Le scan de ces objets est activé par défaut.

Vous pouvez configurer le comportement du Scanner après le scan :

1. **N'appliquer aucune action**. Le Scanner va afficher le tableau contenant la liste des menaces détectées.
2. **Neutraliser les menaces détectées**. Le Scanner va appliquer automatiquement les actions aux menaces détectées.
3. **Neutraliser les menaces détectées et arrêter l'ordinateur**. Le Scanner va appliquer automatiquement les actions aux menaces détectées et après, l'ordinateur sera arrêté.

12.3. Protection préventive

Dans cette rubrique, vous pouvez configurer les réactions de Dr.Web à des actions d'autres applications qui pourraient compromettre la sécurité de votre ordinateur et choisir le niveau de la protection contre les exploits.

Dans ce cas, vous pouvez spécifier le mode de protection à part pour les applications concrètes et le mode général, dont les paramètres seront appliqués à tous les autres processus.

Pour spécifier le mode général de la protection préventive, sélectionnez-le dans la liste **Mode de fonctionnement** et cliquez sur l'option **Modifier le niveau de blocage des activités suspectes**. Dans le dernier cas, une fenêtre va s'afficher dans laquelle vous pouvez consulter les paramètres de chaque mode et les modifier. Toutes les modifications des paramètres sont enregistrées en mode **Utilisateur**. Dans cette fenêtre vous pouvez également créer un nouveau profil pour enregistrer les paramètres nécessaires.

Création d'un nouveau profil

1. Cliquez sur .
2. Dans la fenêtre qui s'affiche, indiquez le nom du nouveau profil.
3. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.

Pour configurer les paramètres de la protection préventive pour les applications concrètes, cliquez sur l'option **Modifier les paramètres d'accès pour les applications**. Dans la fenêtre qui s'affiche, vous pouvez ajouter une nouvelle règle pour l'application, modifier une règle déjà créée ou supprimer une règle inutile.

Ajouter une règle

1. Cliquez sur .
2. Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et spécifiez le chemin vers le fichier exécutable de l'application.
3. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.

Pour modifier une règle déjà créée, sélectionnez-la dans la liste et cliquez sur .

Pour supprimer une règle de la liste, sélectionnez-le et cliquez sur .

Pour en savoir plus sur chaque mode de fonctionnement, consultez la rubrique Niveau de la Protection préventive ci-dessous.

Niveau de la Protection préventive

Dans le mode **Optimal** par défaut, Dr.Web interdit automatiquement les modifications des objets système, modification qui indiquerait clairement une tentative malveillante d'endommager le système d'exploitation. Il bloque également l'accès bas niveau au disque et protège le fichier HOSTS de toute modification.

S'il existe un risque élevé d'infection de votre ordinateur, vous pouvez augmenter la protection en choisissant le mode **Moyen**. Dans ce mode, l'accès aux objets critiques, qui peuvent être potentiellement utilisés par des programmes malveillants, est bloqué.

> L'utilisation de ce mode peut entraîner des problèmes de compatibilité avec des logiciels légitimes qui utilisent les branches du registre protégées.

Lorsqu'il est nécessaire d'avoir un contrôle total de l'accès aux objets Windows critiques, vous pouvez choisir le mode **Paranoïde**. Dans ce mode, Dr.Web fournit également un contrôle interactif sur le chargement de drivers et le démarrage automatique de programmes.

Dans le mode **Définis par l'utilisateur** vous pouvez choisir vous-même le niveau de la protection pour chaque objet.

Objet protégé	Description
Intégrité des applications en cours d'exécution	Cette option permet la détection des processus qui injectent leur code dans les applications en cours d'exécution. Elle indique que le processus peut compromettre la sécurité de l'ordinateur. Les processus qui sont ajoutés à la liste d'exclusions ne sont pas gérés.
Intégrité des fichiers des utilisateurs	Cette option permet de détecter des processus qui modifient des fichiers utilisateur avec un algorithme connu qui indique que le processus peut compromettre la sécurité de l'ordinateur. Les processus qui sont ajoutés aux exclusions ne sont pas suivis. Pour protéger vos données contre leur modification, vous pouvez activer la création de copies protégées pour les données importantes.
Fichier HOSTS	Le système d'exploitation utilise le fichier HOSTS lors de sa connexion à Internet. Des modifications de ce fichier peuvent indiquer une infection virale.
Accès bas niveau au disque	Empêche les applications d'écrire sur les disques par secteurs évitant le système de fichiers.
Téléchargement de pilotes	Empêche les applications de charger des drivers nouveaux ou inconnus.
Objets critiques Windows	D'autres options permettent la protection des branches de registre suivantes contre la modification (dans le profil système ainsi que dans les profils de tous les utilisateurs). Accès à Image File Execution Options : • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Accès à User Drivers : • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Paramètres de Winlogon : • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Notificateurs Winlogon : • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Autodémarrage de Windows : • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Assosiations de fichiers exécutables : • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (clés)

Objet protégé	Description
	• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (clés) Politiques de restriction du démarrage des programmes (SRP) : • Software\Policies\Microsoft\Windows\Safer Plugin Internet Explorer (objet application d'assistance du navigateur) : • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Autodémarrage de programmes : • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Autodémarrage de politiques : • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Configuration du mode sans échec : • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Paramètres de Session Manager : • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Services système : • System\CurrentControlXXX\Services

Si un problème survient durant l'installation d'une mise à jour Microsoft importante ou durant l'installation et le fonctionnement de programmes (y compris des programmes de défragmentation), désactivez la protection préventive.

Vous pouvez configurer les notifications sur les actions de la protection préventive s'affichant sur le bureau et l'envoi de telles notifications par e-mail.

Protection contre les exploits

Cette option permet de bloquer les objets malveillants qui utilisent les vulnérabilités des applications connues. Sélectionnez le niveau nécessaire de la protection contre les exploits dans la liste déroulante.

Niveau de protection	Description
Bloquer l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera bloquée automatiquement.
Mode interactif	En cas de tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation, Dr.Web affichera le message correspondant. Lisez les informations et sélectionnez une action nécessaire.
Autoriser l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera autorisée automatiquement.

13. Statistiques

Pour consulter les informations sur le fonctionnement des composants, ouvrez le menu de SpIDer Agent en mode administrateur et passez à la rubrique **Statistiques**. Sur la page **Statistiques**, les rapports pour les groupes suivants sont disponibles :

- Menaces
- Mise à jour

Le rapport détaillé est disponible pour les entrées des groupes **Menaces** et **Mise à jour**. Vous pouvez appliquer les filtres pour les entrées du rapport.

Rapport détaillé

Pour consulter le rapport détaillé sur les événements du fonctionnement de Dr.Web, sélectionnez l'événement nécessaire et cliquez sur . Si vous cliquez sur ce bouton encore une fois, les données détaillées seront masquées.

Avec le bouton , vous pouvez supprimer, copier ou exporter les événements particuliers ou le rapport entier et vider le rapport.

Vous pouvez utiliser les filtres pour sélectionner des événements.

Filtres

Pour voir dans la liste uniquement les événements qui correspondent aux paramètres déterminés utilisez les filtres. Pour tous les rapports il existe des filtres préinstallés qui sont disponibles dans la liste déroulante en haut de la page de chaque groupe.

Vous pouvez créer vos propres filtres d'événements. Pour créer un nouveau filtre, cliquez sur et sélectionnez l'élément **Créer** dans la liste déroulante. Dans la fenêtre qui s'affiche, spécifiez les critères nécessaires de filtrage. Notez que vous pouvez spécifier plusieurs composants en même temps dans le champ **Composants**.

Vous pouvez trier les événements par codes. Pour ce faire, indiquez-les dans le champ **Code** en respectant les règles suivants :

- séparez les codes par une virgule ;
- vous pouvez indiquer une plage de codes (par exemple, 100-1010) ;
- le symbole « - » devant le code l'exclut de la plage.

Ainsi, une ligne du type suivant «`100-1010,-1000,1002`» signifie qu'il faut afficher les événements «1002», tous les événements de «100» à «1010» et exclure du filtre le code «-1000».

Les filtres créés par l'utilisateur peuvent être modifiés ou supprimés.

Applications

Annexe A. Paramètres de ligne de commande

Des clés en ligne de commande sont utilisées pour définir les paramètres des programmes lancés par l'ouverture d'un fichier exécutable. Ils se rapportent au Scanner Dr.Web, au Scanner en ligne de commande et à l'Updater Dr.Web. Les clés peuvent définir les paramètres qui ne sont pas présents dans le fichier de configuration ou possèdent une priorité supérieure à ceux indiqués dans le fichier.

Les clés commencent par le signe « / » et sont séparées par des espaces comme les autres paramètres en ligne de commande.

Les clés sont rangées dans l'ordre alphabétique.

Paramètres du Scanner et du Scanner en ligne de commande

`/AA` – appliquer automatiquement les actions aux menaces détectées (uniquement pour le Scanner).

`/AC` – scanner les packages d'installation. L'option est activée par défaut.

`/AFS` – utiliser un slash droit pour spécifier l'emboîtement dans l'archive. L'option est désactivée par défaut.

`/AR` – scanner les archives. L'option est activée par défaut.

`/ARC:`<*ratio_de_compression*> – ratio maximum de compression. Si le scanner détecte que le ratio dépasse le maximum spécifié, l'extraction depuis l'archive ne se fait pas et le scan d'une telle archive ne sera pas effectué. Par défaut – illimité.

`/ARL:`<*niveau_d'emboîtement*> – niveau maximum d'emboîtement de l'archive scannée. Par défaut - illimité.

`/ARS:`<*taille*> – taille maximum de l'archive scannée, en Ko. Par défaut - illimité.

`/ART:`<*taille*> – seuil de vérification du ratio de compression (la taille minimum du fichier dans l'archive à partir de laquelle s'effectue la vérification du ratio de compression), en Ko. Par défaut – illimité.

`/ARX:`<*taille*> – taille maximum des objets archivés à scanner, en Ko. Par défaut – illimité.

`/CUSTOM` – lancer le Scanner sur la page pour le scan personnalisé. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets pour le scan ou les paramètres /TM, /TB), le scan personnalisé des objets spécifiés sera lancé. (Uniquement pour le Scanner).

`/BI` – afficher les informations sur les bases de données virales. L'option est activée par défaut.

/DR – scanner les dossiers de manière récursive (vérifier les sous-dossiers). L'option est activée par défaut.

/E:<*nombre_de_flux*> – effectuer une analyse à un nombre spécifié de flux.

/FAST – lancer l'analyse rapide du système. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets pour le scan ou les paramètres /TM, /TB), les objets spécifiés seront également scannés. (Uniquement pour le Scanner).

/FL:<*nom_du_fichier*> – scanner les chemins spécifiés dans le fichier.

/FM:<*masque*> – scanner les fichiers par masque. Par défaut, tous les fichiers seront analysés.

/FR:<*expression_régulière*> – scanner les fichiers selon une expression régulière. Par défaut, tous les fichiers sont scannés.

/FULL – lancer l'analyse complète de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage). Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets pour le scan ou les paramètres /TM, /TB), le scan rapide et le scan des objets spécifiés seront lancés. (Uniquement pour le Scanner).

/FX:<*masque*> – exclure du scan les fichiers qui correspondent au masque. (Uniquement pour le Scanner en ligne de commande).

/H ou /? – afficher la rubrique d'aide sur le fonctionnement du programme. (Uniquement pour le Scanner en ligne de commande).

/HA – réaliser une analyse heuristique des fichiers afin d'y rechercher de menaces inconnues. L'option est activée par défaut.

/KEY:<*fichier_clé*> – spécifier le chemin vers le fichier clé. Le paramètre est nécessaire si le fichier clé se trouve dans un dossier autre que le dossier dans lequel se trouve le scanner. Par défaut, drweb32.key ou une autre clé appropriée depuis le dossier C:\Program Files\DrWeb\ sera utilisée.

/LITE – réaliser un scan du système en analysant la mémoire vive, les secteurs d'amorçage de tous les disques, effectuer une recherche des rootkit. (Uniquement pour le Scanner).

/LN – scanner les fichiers par raccourcis associés. L'option est désactivée par défaut.

/LS – scanner sous le compte LocalSystem. L'option est désactivée par défaut.

/MA – scanner les fichiers d'e-mail. L'option est active par défaut.

/MC:<*nombre_de_tentatives* > – spécifier un nombre maximum de tentatives de désinfecter le fichier. Par défaut – illimité.

/NB – ne pas créer les copies de sauvegardes des fichiers désinfectés/supprimés. L'option est désactivée par défaut.

`/NI[:X]` – niveau de l'utilisation des ressources système, en pourcentage. Ce paramètre détermine le volume de la mémoire utilisée pour le processus de scan et la priorité système de la tâche de scan. Par défaut – illimité.

`/NOREBOOT` – annule le redémarrage et l'extinction après le scan. (Uniquement pour le Scanner).

`/NT` – scanner les flux NTFS. L'option est activée par défaut.

`/OK` – afficher la liste complète des objets scannés et accompagner les objets sains par une note `Ok`. L'option est désactivée par défaut.

`/P:`<*priorité*> – priorité de la tâche de scan en cours dans la file des tâches de scan :

0 – inférieure.

L – basse.

N – normale. Priorité par défaut.

H – supérieure.

M – maximum.

`/PAL:`<*niveau_d'emboîtement*> – niveau d'emboîtement maximum des outils de compression d'un fichier exécutable. Si le niveau d'emboîtement dépasse la valeur spécifiée, l'analyse va uniquement jusqu'au niveau d'emboîtement spécifié. Par défaut – 1000.

`/QL` – afficher la liste de tous les fichiers mis en quarantaine sur tous les disques. (Uniquement pour le Scanner en ligne de commande).

`/QL:`<*nom_du_disque_logique*> – afficher la liste de tous les fichiers mis en quarantaine sur le disque logique spécifié. (Uniquement pour le Scanner en ligne de commande).

`/QNA` – afficher les chemins entre guillemets doubles.

`/QR[:[d][:p]]` – supprimer du disque spécifié <*d*> *(nom_du_disque_logique)* les fichiers se trouvant dans la quarantaine pendant plus de <*p*> jours. Si les valeurs <*d*> et <*p*> ne sont pas spécifiées, tous les fichiers se trouvant dans la quarantaine seront supprimés de tous les disques logiques (uniquement pour le Scanner en ligne de commande).

`/QUIT` – fermer le Scanner après le scan (indépendamment de l'application/non application des actions aux menaces détectées). (Uniquement pour le Scanner).

`/RA:`<*nom_du_fichier*> – ajouter le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut – ne pas créer un journal.

`/REP` – scanner selon les liens symboliques. L'option est désactivée par défaut.

`/RP:`<*nom_du_fichier*> – écrire le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut – ne pas créer un journal.

/RPC:<*secondes*> – délai de connexion à Scanning Engine, en secondes. Par défaut – 30 s. (Uniquement pour le Scanner en ligne de commande).

/RPCD – utiliser l'identificateur dynamique RPC. (Uniquement pour le Scanner en ligne de commande).

/RPCE – utiliser l'adresse cible dynamique RPC. (Uniquement pour le Scanner en ligne de commande).

/RPCE:<*adresse_cible*> – utiliser l'adresse cible RPC spécifiée. (Uniquement pour le Scanner en ligne de commande).

/RPCH:<*nom_d'hôte*> – utiliser le nom d'hôte spécifié pour les appels RPC. (Uniquement pour le Scanner en ligne de commande).

/RPCP:<*protocole*> – utiliser le protocole spécifié RPC. Il est possible d'utiliser les protocoles : lpc, np, tcp. (Uniquement pour le Scanner en ligne de commande).

/SCC – afficher le contenu des objets complexes. L'option est désactivée par défaut.

/SCN – afficher le nom du package d'installation. L'option est désactivée par défaut.

/SLS – afficher les logs sur l'écran. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).

/SPN – afficher le nom de l'outil de compression. L'option est désactivée par défaut.

/SPS – afficher la progression du processus de scan. L'option est activée par défaut (uniquement pour le Scanner en ligne de commande).

/SST – afficher la durée du scan. L'option est désactivée par défaut.

/TB – scanner les secteurs de boot et les secteurs MBR du disque dur.

/TM – détecter les menaces dans la mémoire vive (y compris la partie système Windows).

/TR – scanner les points de restauration système.

/W:<*secondes*> – durée maximum de scan, en secondes. Par défaut – illimité.

/WCL – afficher dans la console drwebwcl. (Uniquement pour le Scanner en ligne de commande).

/X:S[:R] – à la fin du scan, basculer la machine vers un mode de fonctionnement spécifié : arrêt/redémarrage/mode veille/mode veille prolongée.

Vous pouvez configurer les actions à appliquer aux les objets divers (C – désinfecter, Q – déplacer vers la quarantaine, D – supprimer, I – ignorer, R – informer. L'action R est applicable uniquement au Scanner en ligne de commande. Par défaut, pour tous les objets – notifier (uniquement pour le Scanner en ligne de commande)) :

- /AAD:<*action*> – actions sur les adwares (actions possibles : DQIR)
- /AAR:<*action*> – actions sur les archives infectées (actions possibles : DQIR)
- /ACN:<*action*> – actions sur les packages d'installation infectés (actions possibles : DQIR)
- /ADL:<*action*> – actions sur les dialers (actions possibles : DQIR)
- /AHT:<*action*> – actions sur les hacktools (actions possibles : DQIR)
- /AIC:<*action*> – actions sur les fichiers incurables (actions possibles : DQR)
- /AIN:<*action*> – actions sur les fichiers infectés (actions possibles : CDQR)
- /AJK:<*action*> – actions sur les canulars (actions possibles : DQIR)
- /AML:<*action*> – actions sur les fichiers d'e-mail infectés (actions possibles : QIR)
- /ARW:<*action*> – actions sur les riskwares (actions possibles : DQIR)
- /ASU:<*action*> – actions sur les fichiers suspects (actions possibles : DQIR)

Certaines clés peuvent avoir des modificateurs activant ou désactivant le mode de fonctionnement de manière explicite. Par exemple :

/AC –le mode est explicitement désactivé,

/AC, /AC+ –le mode est explicitement activé.

Cette option peut être utile dans le cas où le mode est activé/désactivé par défaut ou selon le paramétrage du fichier de configuration. Les clés pouvant être utilisées avec des modificateurs sont les suivantes :

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.

En cas de clé /FL, le modificateur « – » signifie : scanner les chemins listés dans le fichier spécifié et supprimer ce fichier.

En cas de clés /ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W, la valeur « 0 » enlève toute limitation.

Exemple d'utilisation des clés lors du démarrage du Scanner en ligne de commande :

[<*chemin_vers_le_programme*>]dwscancl /AR- /AIN:C /AIC:Q C:\

scanner tous les fichiers se trouvant sur le disque C, excepté les archives ; désinfecter les fichiers infectés ; placer dans la quarantaine les fichiers incurables. Pour lancer le Scanner pour Windows de manière analogique, à la place de dwscancl, saisissez la commande dwscanner.

Paramètres de l'Updater Dr.Web

Paramètres généraux :

Paramètre	Description
-h [--help]	Afficher sur l'écran la rubrique d'aide abrégée sur le programme.
-v [--verbosity] arg	Niveau de détail du rapport : error (standard), info (élevé), debug (débogage).
-d [--data-dir] arg	Répertoire dans lequel sont conservés le dépôt des produits et les paramètres.
--log-dir arg	Répertoire dans lequel le rapport sera sauvegardé.
--log-file arg (=dwupdater.log)	Nom du fichier de rapport.
-r [--repo-dir] arg	Répertoire du dépôt des produits, (par défaut <data_dir>/repo).
-t [--trace]	Activer le traçage.
-c [--command] arg (=update)	Commande à exécuter : getversions – obtenir les versions, getcomponents – obtenir les composants, init – initialisation, update – mise à jour, uninstall – supprimer, exec – exécuter, keyupdate – mettre à jour la clé, download – télécharger.
-z [--zone] arg	Liste des zones à utiliser à la place des zones spécifiées dans le fichier de configuration.

Paramètres de la commande d'initialisation (init) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-p [--product] arg	Nom du produit.
-a [--path] arg	Chemin d'installation du produit. Ce répertoire sera utilisé par défaut comme répertoire pour tous les composants inclus dans le produit. L'Updater va vérifier la présence du fichier clé dans ce répertoire.
-n [--component] arg	Nom du composant et le répertoire d'installation au format <*name*>, <*install path*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.

Paramètre	Description
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>:<*port*>.
-e [--exclude] arg	Nom du composant à enlever du produit lors de l'installation.

Paramètres de la commande de mise à jour (update) :

Paramètre	Description
-p [--product] arg	Le nom du produit. Si un nom est spécifié, seul le produit correspondant sera mis à jour. Si aucun produit n'est spécifié, ni aucun composant, alors tous les produits seront mis à jour. S'il y a des composants spécifiés, ces composants seront mis à jour.
-n [--component] arg	Liste des composant à mettre à niveau vers une révision spécifiée. Syntaxe : <*name*>, <*target revision*>.
.-x [--selfrestart] arg (=yes)	Redémarrage après la mise à jour de l'Updater. La valeur par défaut – `yes`. En cas de valeur `no`, une notification sur la nécessité de redémarrer sera affichée.
--geo-update	Obtenir une liste des adresses IP d'update.drweb.com avant la mise à jour.
--type arg (=normal)	Peut prendre l'une des valeurs suviantes : • reset-all – forcer la mise à jour de tous les composants ; • reset-failed – annuler toutes les modifications pour les composants corrompus ; • normal-failed – essayer de mettre à niveau les composants y compris ceux qui sont corrompus, vers la dernière version ou vers une version spécifiée ; • update-revision – mettre à jour les composant au sein de la révision courante ; • normal – mettre à jour tous les composants.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>:<*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <*nom*> : <*valeur*>.
-l [--progress-to-console]	Afficher sur la console des informations sur le chargement et l'exécution du script.

Paramètres spécifiques de la commande d'exécution (exec) :

Paramètre	Description
-s [--script] arg	Exécuter le script spécifié.
-f [--func] arg	Exécuter la fonction du script.
-p [--param] arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <*nom*> *:* <*valeur*>.
-l [--progress-to-console]	Afficher sur la console des informations sur la progression de l'exécution du script.

Paramètres de la commande d'obtention des composants (getcomponents) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-p [--product] arg	Spécifiez le nom du produit pour consulter les composants inclus. Si aucun produit n'est spécifié, tous les composants correspondant à la version courante seront affichés.

Paramètres de la commande d'obtention des révisons (getrevisions) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-n [--component] arg	Nom du composant.

Paramètres de la commande de suppression (uninstall) :

Paramètre	Description
-n [--component] arg	Nom du composant à supprimer.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <*nom*> *:* <*valeur*>.
-e [--add-to-exclude]	Composants qui seront supprimés, leur mise à jour ne sera pas réalisée.

Paramètres de la commande de mise à jour automatique de la clé (keyupdate) :

Paramètre	Description
-m [--md5] arg	Somme de contrôle md5 de l'ancien fichier clé.
-o [--output] arg	Nom du fichier.
-b [--backup]	Copie de sauvegarde de l'ancien fichier clé s'il existe.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>:<*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-l [--progress-to-console]	Afficher sur la console des informations sur le téléchargement du fichier clé.

Paramètres de la commande de téléchargement (download) :

Paramètre	Description
--zones arg	Fichier contenant une liste des zones.
--key-dir arg	Répertoire dans lequel se trouve le fichier clé.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>:<*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-s [--version] arg	Nom de la version
-p [--product] arg	Nom du produit à télécharger.

Codes de retour

Les valeurs possibles du code de retour et les événements y correspondant sont les suivants :

Code de retour	Événement
0	Aucun virus ou soupçon de virus n'est détecté.
1	Les virus connus sont détectés.
2	Les modifications de virus connus sont détectées.
4	Les objets suspects sont détectés.
8	Les virus connus sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
16	Les modifications de virus connus sont détectées dans une archive, un conteneur ou dans une boîte e-mail.
32	Les objets suspects sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
64	Au moins un objet infecté a été désinfecté avec succès.
128	La désinfection/la renomination/le déplacement d'au moins un fichier infecté est effectué.

Le code de retour final, formé à la fin du scan, est égal à la somme des codes des événements survenus lors du scan (les termes peuvent être reconstitués d'après le code final).

Par exemple, le code de retour 9 = 1 + 8 signifie que des virus connus (un virus) ont été détectés lors du scan, y compris dans les archives ; la désinfection n'a pas été effectuée ; il n'y avait plus aucun événement « viral ».

Annexe B. Menaces et méthodes de neutralisation

Avec le développement des technologies IT et des solutions réseau, les programmes malveillants de différents types, conçus pour attaquer les utilisateurs, deviennent de plus en plus répandus. Leur développement est apparu en même temps que la science des ordinateurs et les outils de protection contre eux ont progressé en même temps. Néanmoins, il n'existe toujours pas de classification commune pour toutes les menaces potentielles en raison du caractère imprévisible de leur développement et de leur constante amélioration.

Les programmes malveillants peuvent être diffusés via Internet, les réseaux locaux, les e-mails et les supports amovibles. Certains d'entre eux comptent sur l'imprudence des utilisateurs et leur manque d'expérience et peuvent fonctionner en mode complètement automatique. D'autres sont des outils contrôlés par un ordinateur qui peuvent endommager même le système le plus sécurisé.

Ce chapitre décrit les types de programmes malveillants les plus connus et les plus répandus, contre lesquels luttent les produits de Doctor Web.

Classification de menaces

Sous le terme « menace », ce classement comprend tout logiciel pouvant endommager directement ou indirectement l'ordinateur, le réseau, l'information ou porter atteinte aux droits de l'utilisateur (programmes malicieux ou indésirables). Dans le sens plus large du terme, « menace » peut signifier un danger potentiel pour l'ordinateur ou pour le réseau (une vulnérabilité pouvant être utilisée pour des attaques de pirates).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour son droit à la confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels pour diffusion du spam ou analyseurs du trafic), normalement ne sont pas classés comme menaces, mais sous certaines conditions, ils peuvent causer des dommages à l'utilisateur.

Dans les produits et la documentation de Doctor Web, les menaces sont divisées en deux types, selon le niveau de danger qu'elles représentent :

- **menaces graves** – ce sont des menaces classiques qui sont capables de mener des actions destructives et illégales au sein du système (suppression et vol de l'information, défaillance du réseau etc.). Ce type de menace regroupe les logiciels appelés malveillants (virus, vers, programmes de Troie) ;
- **menaces insignifiantes** – ce sont des menaces considérées comme moins dangereuses que des menaces graves, mais qui sont à éviter elles aussi, car de tierces personnes peuvent s'en servir pour effectuer des actions nocives. De plus, toute présence de menaces, même insignifiantes, dans le système, témoigne de sa vulnérabilité. Les spécialistes de la protection informatique qualifient ce type de menaces de logiciels « gris » ou « logiciels potentiellement non désirés ». Les menaces insignifiantes sont représentées par des adwares, des dialers, des canulars, des riskwares et des hacktools.

Menaces graves

Virus informatiques

Ce type de menaces informatiques est capable d'introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'*infection*. Dans la plupart des cas, le fichier infecté devient lui-même porteur de virus et le code introduit n'est plus conforme à l'original. La majeure partie des virus est conçue pour endommager ou exterminer les données.

En fonction du type d'objet infecté, Doctor Web classifie les virus selon les types suivants :

- **virus de fichier** infectent les fichiers de système d'exploitation (fichiers exécutables, fichiers dll). Ces virus sont activés lors de l'accès au fichier infecté ;
- **macrovirus** infectent les fichiers de documents utilisés par les applications Microsoft® Office et d'autres programmes utilisant des commandes macros généralement écrits en Visual Basic. Macros - ce sont des logiciels internes, écrits en langage de programmation totalement fonctionnel, qui sont automatiquement lancés sous des conditions déterminées (par exemple, dans Microsoft® Word, quand vous ouvrez, fermez, sauvegardez ou créez un document) ;
- **virus Script** sont écrits en langages des scénarios (langages de script). Ils infectent dans la plupart des cas d'autres fichiers script (par exemple, les fichiers du système d'exploitation). Ils peuvent infecter aussi d'autres types de fichiers qui supportent l'exécution des scénarios script, tout en se servant des scénarios vulnérables des applications Web ;
- **virus de téléchargement** infectent les secteurs boot des disques et des partitions aussi bien que les principaux secteurs boot des disques durs. Ils occupent peu de mémoire et restent prêts à remplir leurs fonctions jusqu'à ce qu'un déchargement, un redémarrage ou un arrêt du système ne soient effectués.

La plupart des virus possèdent des mécanismes spécifiques pour se dissimuler dans le système. Leurs méthodes de protection contre la détection s'améliorent sans cesse. Cependant, dans le même temps, de nouveaux moyens d'élimination de cette protection apparaissent. On peut également diviser les virus selon les principes de protection contre la détection :

- **les virus cryptés** chiffrent leur code à chaque infection pour éviter leur détection dans un fichier, un secteur boot ou un secteur de mémoire. Toutes les copies de tels virus contiennent seulement un petit fragment de code commun (procédure de décryptage), qui peut être utilisé comme une signature de virus ;
- **les virus polymorphes** cryptent également leur code, mais ils génèrent en plus une procédure de décryptage spéciale différente dans chaque copie de virus. Ceci signifie que de tels virus n'ont pas de signatures.

Les virus peuvent également être classifiés selon le langage de programmation dans lequel ils sont écrits (dans la plupart des cas c'est en assembleur, des langages de programmation de haut niveau, des langages script, etc.) ou selon les systèmes d'exploitation qu'ils ciblent.

Vers d'ordinateurs

Les vers sont récemment devenus beaucoup plus répandus que les virus et les autres programmes malveillants. Comme les virus, ils sont capables de créer leurs copies. Un ver infiltre un ordinateur via le réseau (généralement sous forme d'une pièce jointe dans les messages e-mail) et distribue ses copies fonctionnelles à d'autres ordinateurs. Pour se propager, les vers peuvent profiter des actions de l'utilisateur ou choisir le poste à attaquer de manière automatique.

Les vers ne consistent pas forcément en un seul fichier (le corps du ver). La plupart d'entre eux comportent une partie infectieuse (le shellcode) qui se charge dans la mémoire vive de l'ordinateur, puis télécharge le corps du ver via le réseau sous forme d'un fichier exécutable. Tant que le système n'est pas encore infecté par le corps du ver, vous pouvez régler le problème en redémarrant l'ordinateur (et la mémoire vive est déchargée et remise à zéro). Mais aussitôt que le corps du ver entre dans le système, seul l'antivirus peut le désinfecter.

A cause de leur propagation intense, les vers peuvent mettre hors service des réseaux entiers, même s'ils n'endommagent pas directement le système.

Doctor Web divise les vers d'après leur mode de propagation :

- **vers de réseau** se propagent à l'aide de différents protocoles réseau ou protocoles d'échanges de fichiers ;
- **vers de courrier** se propagent via les protocoles de courrier (POP3, SMTP, etc.).

Chevaux de Troie

Ce type de programmes malveillants ne peuvent se reproduire. Un Trojan effectue des actions malveillantes (endommage ou supprime des données, envoie des informations confidentielles, etc.) ou rend l'accès de l'ordinateur possible à un tiers, sans autorisation, afin de nuire à l'utilisateur.

Le masquage de Trojan et les fonctions malveillantes sont similaires à ceux d'un virus et peuvent même être un composant de virus. Cependant, la plupart des Trojans sont diffusés comme des fichiers exécutables séparés (via des serveurs d'échanges de fichiers, des supports amovibles ou des pièces jointes), qui sont lancés par l'utilisateur ou par une tâche système.

Vous trouverez ci-dessous la liste de certains types de trojans qui sont classés par les spécialistes de Doctor Web :

- **backdoors** – ce sont des programmes de Troie qui offrent un accès privilégié au système, contournant le mécanisme existant d'accès et de protection. Les backdoors n'infectent pas les fichiers, mais ils s'inscrivent dans le registre, modifiant les clés ;
- **droppers** – ce sont les fichiers qui contiennent dans leur corps les programmes malveillants. Une fois le dropper est lancé, il copie sur le disque de l'utilisateur les fichiers malveillants sans avertir l'utilisateur et puis, il les lance ;

- **enregistreurs de frappe (keyloggers)** – ils sont utilisés pour collecter les données que l'utilisateur entre avec son clavier. Le but de ces actions est le vol de toute information personnelle (mots de passe, logins, numéros de cartes bancaires etc.) ;
- **clickers** – ils redirigent les liens quand on clique dessus. D'ordinaire, l'utilisateur est redirigé vers des sites déterminés (probablement malveillants) avec le but d'augmenter le trafic publicitaire des sites web ou pour organiser des attaques par déni de service (attaques DoS) ;
- **trojans proxy** – ils offrent au malfaiteur l'accès anonyme à Internet via l'ordinateur de la victime ;
- **rootkits** – ils sont destinés à intercepter les fonctions du système d'exploitation pour dissimuler leur présence dans le système. En outre, le rootkit peut masquer les processus des autres logiciels, les clés de registre, des fichiers et des dossiers. Le rootkit se propage comme un logiciel indépendant ou comme un composant supplémentaire d'un autre logiciel malicieux. Selon le principe de leur fonctionnement, les rootkits sont divisés en deux groupes : les rootkits qui fonctionnent dans le mode utilisateur (interception des fonctions des bibliothèques du mode utilisateur) (User Mode Rootkits (UMR)), et les rootkits qui fonctionnent dans le mode noyau (interception des fonctions au niveau du noyau système, ce qui rend toute détection et toute désinfection très difficile) (Kernel Mode Rootkits (KMR)).

Outre les actions listées ci-dessus, les programmes de Troie peuvent exécuter d'autres actions malveillantes, par exemple, changer la page d'accueil dans le navigateur web ou bien supprimer certains fichiers. Mais ces actions peuvent être aussi exécutées par les menaces d'autres types (par exemple, virus et vers).

Menaces insignifiantes

Hacktools

Les hacktools sont créés pour aider les hackers. Les logiciels de ce type les plus répandus sont des scanners de ports qui permettent de détecter les vulnérabilités des pare-feux (firewalls) et des autres composants qui assurent la sécurité informatique de l'ordinateur. Ces instruments peuvent également être utilisés par les administrateurs pour vérifier la solidité de leurs réseaux. Parfois, les logiciels utilisant les méthodes de l'ingénierie sociale sont aussi considérés comme hacktools.

Adwares

Sous ce terme, on désigne le plus souvent un code intégré dans des logiciels gratuits qui impose l'affichage d'une publicité sur l'ordinateur de l'utilisateur. Mais parfois, ce code peut être diffusé par d'autres logiciels malicieux et afficher la publicité, par exemple, sur des navigateurs Internet. Très souvent, ces logiciels publicitaires fonctionnent en utilisant la base de données collectées par des logiciels espions.

Canulars

Comme les adwares, ce type de programme malveillant ne provoque pas de dommage direct au système. Habituellement, les canulars génèrent des alertes sur des erreurs qui n'ont jamais eu lieu et effraient l'utilisateur afin qu'il effectue des actions qui conduiront à la perte de données. Leur objectif est d'effrayer ou de déranger l'utilisateur.

Dialers

Ce sont les logiciels spécifiques utilisant l'accès à Internet avec l'autorisation de l'utilisateur pour accéder aux sites déterminés. D'habitude, il possèdent un certificat signé et notifient toutes leurs actions à l'utilisateur.

Riskwares

Ces logiciels ne sont pas créés pour endommager le système, mais à cause de leurs particularités, ils peuvent présenter une menace pour la sécurité du système. Ces logiciels peuvent non seulement endommager les données ou les supprimer par hasard, mais ils peuvent également être utilisés par des hackers ou par d'autres logiciels pirates pour nuire au système. Les logiciels utilisés à distance, d'administration à distance, les serveurs FTP etc. peuvent être considérés comme potentiellement dangereux.

Objets suspects

Ce sont des menaces potentielles détectées à l'aide de l'analyse heuristique. Ces objets peuvent appartenir à un des types de menaces informatiques (même inconnues pour les spécialistes de la sécurité informatique) ou être absolument inoffensifs, en cas de faux positif. En tous cas, il est recommandé de placer les fichiers contenant des objets suspects en quarantaine et envoyer pour analyse aux spécialistes du laboratoire antivirus de Doctor Web.

Actions appliquées aux menaces détectées

Il existe plusieurs méthodes de neutralisation des menaces. Les produits de Doctor Web combinent ces méthodes pour la protection la plus fiable des ordinateurs et des réseaux en utilisant une configuration conviviale et flexible. Les principales actions de neutralisation des programmes malveillants sont les suivantes :

1. **Désinfecter** – l'action appliquée aux virus, vers et trojans. Ceci implique la suppression du code malveillant des fichiers infectés ou la suppression d'une copie d'un programme malveillant, ainsi que la restauration des objets infectés (c'est-à-dire la restauration de la structure et du fonctionnement de l'objet tels qu'ils étaient avant son infection) si possible. Tous les programmes malveillants ne peuvent être désinfectés. Cependant, les produits de Doctor Web sont basés sur les plus efficaces algorithmes de désinfection et de restauration de fichiers infectés.
2. **Déplacer en quarantaine** – il s'agit de déplacer l'objet malveillant vers un dossier spécial et de l'isoler du reste du système. Cette action est préférable en cas d'impossibilité de désinfecter et pour tous les objets suspects. Il est recommandé d'envoyer des copies de ces fichiers au laboratoire antivirus de Doctor Web afin qu'elles soient analysées.
3. **Supprimer** – l'action efficace de neutralisation des menaces. Elle peut s'appliquer à n'importe quel type d'objet malveillant. Notez que la suppression sera parfois appliquée aux objets pour lesquels la désinfection était sélectionnée. Ceci arrive si l'objet contient uniquement le code malveillant et ne contient pas d'information utile. Dans le cas de vers d'ordinateurs, par exemple, leur élimination implique la destruction de toutes leurs copies opérationnelles.
4. **Bloquer, renommer** – ces actions peuvent également être utilisées pour neutraliser des programmes malveillants. Cependant, des copies totalement fonctionnelles de ces programmes demeurent dans le système. En utilisant l'action Bloquer, toutes les tentatives d'accès vers ou depuis le fichier sont bloquées. Le renommage signifie que l'extension du fichier est renommée, ce qui le rend inopérant.

Annexe C. Principes de nomination des menaces

En cas de détection d'un code viral les composants Dr.Web le signalent à l'utilisateur à l'aide des outils de l'interface et inscrivent le nom du virus, attribué par les spécialistes Doctor Web, dans le fichier du rapport. Ces noms sont créés en fonction de certains principes et reflètent un modèle de menace, des catégories d'objets vulnérables, l'environnement de diffusion (OS et applications) et d'autres caractéristiques. Le fait de savoir ces principes peut être utile pour la compréhension du logiciel et les vulnérabilités organisationnelles du système protégé. Vous trouverez ci-dessous le bref exposé de ces principes, la version complète de cette classification qui est mise à jour constamment se trouve sur http://vms.drweb.com/classification/.

Dans certains cas, cette classification est conventionnelle, car certains virus possèdent plusieurs caractéristiques en même temps. De plus, elle ne devrait pas être considérée comme exhaustive car de nouveaux types de virus apparaissent constamment et la classification devient de plus en plus précise.

Le nom complet d'un virus se compose de plusieurs éléments, séparés par des points. Certains éléments au début du nom (préfixes) et à la fin du nom (suffixes) sont standards dans la classification.

Préfixes généraux

Préfixes du système d'exploitation

Les préfixes listés ci-dessous sont utilisés pour nommer les virus infectant les fichiers exécutables de certains OS :

- `Win` – programmes 16-bit Windows 3.1 ;
- `Win95` – programmes 32-bit Windows 95, Windows 98, Windows Me ;
- `WinNT` – programmes 32-bit Windows NT, Windows 2000, Windows XP, Windows Vista ;
- `Win32` – programmes 32-bit OS Windows 95, Windows 98, Windows Me et Windows NT, Windows 2000, Windows XP, OS Windows Vista ;
- `Win32.NET` –programmes Microsoft .NET Framework ;
- `OS2` – programmes OS/2 ;
- `Unix` – programmes dans différents systèmes basés sur UNIX ;
- `Linux` – programmes Linux ;
- `FreeBSD` – programmes FreeBSD ;
- `SunOS` – programmes SunOS (Solaris) ;
- `Symbian` - programmes Symbian OS (OS mobile).

Notez que certains virus peuvent infecter les programmes d'un système même s'ils sont créés pour fonctionner dans un autre système.

Virus infectant les fichiers MS Office

La liste des préfixes pour les virus qui infectent les objets MS Office (le langage des macros infectées par de tels virus est spécifié) :

- `WM` – Word Basic (MS Word 6.0-7.0) ;
- `XM` – VBA3 (MS Excel 5.0-7.0) ;
- `W97M` – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- `X97M` – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- `A97M` – bases de données de MS Access'97/2000 ;
- `PP97M` – présentations MS PowerPoint ;
- `O97M` –VBA5 (MS Office'97), VBA6 (MS Office 2000) ; ce virus infecte les fichiers de plus d'un composant de MS Office.

Prefixes de langage de programmation

Le groupe de préfixes `HLL` est utilisé pour nommer les virus écrits en langages de programmation de haut niveau comme C, C++, Pascal, Basic et d'autres. On utilise des modificateurs, indiquant l' algorithme de fonctionnement de base, notamment :

- `HLLW` – vers;
- `HLLM` – vers de mail ;
- `HLLO` – virus qui réécrivent le code du programme victime ;
- `HLLP` – virus parasites ;
- `HLLC` – virus compagnon.

Le préfixe suivant se réfère également à un langage de développement :

- `Java` – virus destinés à la machine virtuelle Java.

Chevaux de Troie

`Cheval de Troie` – nom général pour désigner différents programmes de Troie (Trojans). Dans de nombreux cas, les préfixes de ce groupe sont utilisés avec le préfixe Trojan.

- `PWS` – Trojan voleur de mots de passe ;
- `Backdoor` – Trojan avec des fonctions de RAT (Remote Administration Tool – utilitaire d'administration à distance) ;
- `IRC` – Trojan qui utilise des canaux Internet Relay Chat ;
- `DownLoader` – Trojan qui télécharge secrètement différents programmes malveillants depuis Internet ;
- `MulDrop` – Trojan qui télécharge secrètement des virus contenus dans son corps ;

- `Proxy` – Trojan qui autorise une tierce personne à travailler anonymement sur Internet via l'ordinateur infecté ;
- `StartPage` (synonyme : `Seeker`) – Trojan qui remplace sans autorisation la page d'accueil du navigateur (page de démarrage) ;
- `Click` – Trojan qui redirige un utilisateur vers un site spécial (ou des sites) ;
- `KeyLogger` – Trojan spyware qui connecte des touches ; il peut envoyer des données collectées à un malfaiteur ;
- `AVKill` – stoppe ou supprime les programmes antivirus, pare-feu, etc. ;
- `KillFiles`, `KillDisk`, `DiskEraser` – supprime certains fichiers (des fichiers dans certains répertoires, des fichiers selon certains masques, tous les fichiers sur les disques etc.) ;
- `DelWin` – supprime les fichiers vitaux pour le fonctionnement de l'OS Windows ;
- `FormatC` – formate le disque C : (synonyme : `FormatAll` – formate certains disques ou tous les disques) ;
- `KillMBR` – corrompt ou supprime le contenu du secteur principal d'amorçage (MBR) ;
- `KillCMOS` – corrompt ou supprime la mémoire CMOS.

Outil exploitant les vulnérabilités

- `Exploit` – un outil exploitant les vulnérabilités connues d'un OS ou d'une application pour introduire un code malveillant ou effectuer des actions non autorisées.

Outils d'attaques réseaux

- `Nuke` – outils pour attaquer certaines vulnérabilités connues des systèmes d'exploitation conduisant à la chute des systèmes attaqués ;
- `DDoS` – programme-agent destiné à provoquer une attaque par déni de service (Distributed Denial of Service) ;
- `FDoS` (synonyme : Flooder) – Flooder Denial Of Service – programmes destinés à effectuer des actions malveillantes sur Internet reposant sur l'idée des attaques par déni de service ; contrairement aux DDoS, lorsque plusieurs agents sur différents ordinateurs sont utilisés simultanément pour attaquer un système, un programme FDoS opère comme un programme indépendant « autosuffisant ».

Virus-script

Préfixes des virus écrits en différents langages de script :

- `VBS` – Visual Basic Script ;
- `JS` – Java Script ;
- `Wscript` – Visual Basic Script et/ou Java Script ;
- `Perl` – Perl ;
- `PHP` – PHP ;

- `BAT` – langage d'nterprète de commande de l'OS MS-DOS.

Programmes malveillants

Préfixes des objets qui ne sont pas des virus, mais des programmes malveillants :

- `Adware` – publicité ;
- `Dialer` – programme dialer (il redirige les appels du modem vers des numéros payants) ;
- `Joke` – canular ;
- `Program` – un programme potentiellement dangereux (riskware) ;
- `Tool` – programme utilisé pour faire du piratage (hacktool).

Divers

Le préfixe `generic` est utilisé, après un autre préfixe décrivant l'environnement ou la méthode de développement, pour nommer un représentant typique de ce type de virus. Un tel virus ne possède aucune caractéristique (comme des séries de texte, des effets spécifiques etc.) qui permettrait de lui donner un nom particulier.

Auparavant le préfixe `Silly` était utilisé avec les modificateurs différents pour nommer les virus simples, sans signe particulier.

Suffixes

Les suffixes sont utilisés pour nommer des objets viraux particuliers :

- `generator` – un objet qui n'est pas un virus, mais un générateur de virus ;
- `based` – un virus développé à l'aide d'un générateur spécifique ou d'un virus modifié. Dans les deux cas, les noms de virus de ce type sont génériques et peuvent définir des centaines voire des milliers de virus ;
- `dropper` – un objet qui n'est pas un virus mais l'installateur du virus indiqué.