Dr.WEB

Agent pour Windows

Manuel Utilisateur

Agent Dr.Web pour Windows
Version 11.5
Manuel Utilisateur
21/04/2020

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125040 Moscou, Russie

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

Téléphone : +7 (495) 789-45-87

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

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

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

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

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

Nous remercions tous nos clients pour leur soutien !

Contenu

1. Introduction

Agent pour Windows est destiné à protéger la mémoire système, les disques durs et les supports amovibles tournant sous les OS de la famille Microsoft® Windows® contre menaces de tout types : virus, rootkits, trojans, spywares, adwares, hacktools et d'autres objets malveillants provenant de sources externes.

Du point de vue de l'architecture, Agent pour Windows est composé de plusieurs modules responsables des fonctions différentes. Le moteur antivirus et les bases virales sont communs pour tous les composants et les plateformes différentes.

Les composants du produit sont constamment mis à jour, les bases virales, les bases des catégories de ressources web et les bases des règles de filtrage antispam de messages e-mail sont régulièrement complétées par les signatures de virus. La mise à jour permanente assure un niveau actuel de la protection des appareil de l'utilisateur, ainsi que des applications et des données. Pour une protection supplémentaires contre des logiciels malveillants, on utilise les méthodes de l'analyse heuristiques réalisées dans le moteur antivirus.

Agent pour Windows 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 sur demande de l'utilisateur. Il analyse votre ordinateur à la recherche de virus et autres logiciels malveillants.

Scanner en ligne de commande Dr.Web : version du Scanner Dr.Web avec l'interface de la ligne de commande.

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

SpIDer Mail : moniteur antivirus de messagerie pour les postes de travail qui intercepte toutes les requêtes de clients de messagerie fonctionnant sur l'ordinateur aux serveurs de messagerie via les protocoles POP3/SMTP/IMAP4/NNTP (sous IMAP4 on comprend le protocole IMAPv4rev1). Il détecte et neutralise les menaces avant que les messages soient reçus du serveur (ou envoyés sur le serveur de messagerie) par le client de messagerie. Le moniteur de messagerie peut également analyser les e-mails pour la présence du spam avec l'Antispam Dr.Web.

Dr.Web pour Outlook : plug-in qui analyse les boîtes mail Microsoft Outlook pour la présence de menaces et de spam.

SpIDer Gate : module de l'analyse antivirus du trafic HTTP. Configuré par défaut, l'antivirus web SpIDer Gate analyse automatiquement le trafic HTTP entrant et bloque le transfert des objets

contenant des virus et d'autres programmes malveillants. Le filtrage des URL de sites non recommandés et de sites connus comme sources de virus est également activé par défaut.

Office Control : composant qui restreint l'accès aux sites, aux fichiers et dossiers, et permet de limiter le temps d'utilisation de l'ordinateur et d'Internet pour les différents comptes Windows.

Pare-feu Dr.Web : pare-feu personnel qui protège votre ordinateur d'un accès non autorisé et prévient la perte de données vitales via le réseau.

Agent Dr.Web : module qui vous aide à configurer et à gérer les composants du produit antivirus.

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, pour les utilisateurs expérimentés.

> ⚠ Etant en développement constant, l'interface du logiciel peut afficher d'autres images que celles contenues dans le présent Manuel. Vous pouvez trouver les informations toujours à jour sur https://download.drweb.com/doc.

1.2. Conventions et abréviations

Les styles de texte utilisées dans ce manuel :

Styles	Utilisés
⚠	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
Réseau antivirus	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.

Styles	Utilisés
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
`C:\Windows\`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

1.3. Méthode de détection des menaces

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

Analyse de signature

Cette méthode de détection est appliquée en premier lieu. Elle est mise en oeuvre en examinant le 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 somme de contrôle ce qui permet de réduire considérablement la taille des entrées dans les bases de données 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.

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.L'analyseur heuristique utilise également la technologie FLY-CODE — un algorithme universel pour l'extraction des fichiers.

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 ».

Analyse de comportement

Les techniques de l'analyse de comportement permettent d'analyser la cohérence des actions de tous les processus du système. Si une application se comporte comme un programme malveillant, ses actions seront bloquées.

Dr.Web Process Heuristic

La technologie de l'analyse de comportement Dr.Web Process Heuristic protège contre les nouveaux programmes les plus dangereux qui sont capables d'éviter la détection par les moyens traditionnels : le mécanisme de signatures et le mécanisme heuristique.

Dr.Web Process Heuristic analyse le comportement de chaque programme lancé. Dr.Web Process Heuristic se base sur les connaissances actuelles sur le comportement des programmes malveillants, il évalue le niveau de danger et prend les mesures nécessaires afin de neutraliser la menace.

Cette technologie permet de minimiser les pertes dues à l'action d'un virus inconnu — en cas de consommation minimum des ressources du système à protéger.

Dr.Web Process Heuristic contrôle toutes les tentatives de modifier le système :

- il identifie les processus de programmes malveillants qui modifient des fichiers utilisateur d'une manière indésirable (par exemple, les tentatives de chiffrements de la part des trojans-encodeurs), y compris les fichiers se trouvant dans des répertoires accessibles par le réseau ;
- il empêche les tentatives de programmes malveillants de s'infiltrer dans des processus d'autres applications ;
- il protège les zones critiques du système contre les modifications par les programmes malveillants ;
- il détecte et arrête des scripts et des processus malveillants, suspects et peu fiables ;
- il bloque la possibilité de modifier les zones d'amorçage du disque par les programmes malveillants afin d'éviter le lancement (par exemple, d'un bootkit) sur l'ordinateur ;
- il prévient la désactivation de la mode sécurisée Windows en bloquant les modification du registre ;
- il n'autorise pas aux programmes malveillants de modifier les règles de lancement de programmes ;
- il bloque les téléchargements de nouveaux pilotes ou de pilotes inconnus qui sont lancés sans avertissement de l'utilisateur ;
- il bloque l'autodémarrage de programmes malveillants et des applications particulières, par exemple des anti-antivirus en les empêchant de s'enregistrer dans le registre pour le lancement ultérieur ;
- il bloque les branches du registre qui sont responsables des pilotes des dispositifs virtuels ce qui rend impossible l'installation du cheval de Troie sous forme d'un nouveau dispositif virtuel ;
- il ne permet pas au logiciel malveillant de perturber le fonctionnement normal des services système.

Dr.Web Process Dumper

L'analyseur complexe des menaces compressées Dr.Web Process Dumper augmente considérablement le niveau de détection des menaces supposées « nouvelles » (ce sont des menaces connues dans la base virale de Dr.Web, mais elle sont masquées sous de nouveaux packers) et exclut la nécessité d'ajouter dans les bases de nouvelles entrées portant sur les menaces. Vu que les bases virales Dr.Web gardent leur taille réduite, les pré-requis système n'augmentent pas et les mises à jour restent légères pendant que la détection et la désinfection de menaces est de haut niveau.

Dr.Web ShellGuard

La technologie Dr.Web ShellGuard protège l'ordinateur contre les *exploits* — les objets malveillants qui essaient d'exploiter les vulnérabilités afin d'obtenir le contrôle sur les applications attaquées et sur le système entier.

Dr.Web ShellGuard protège les applications les plus utilisées installées sur les ordinateurs tournant sous Windows :

- les navigateurs web (Internet Explorer, Mozilla Firefox, Yandex.Browser, Google Chrome, Vivaldi Browser, etc.) ;
- les applications MS Office, y compris MS Office 2016 ;
- les applications système ;
- les applications utilisant les technologies java, flash et pdf ;
- les lecteurs média.

Méthode de l'apprentissage machine

Elle est utilisée pour rechercher et neutraliser les objets malveillant qui ne sont pas encore inclus dans les bases virales. L'avantage de cette méthode est que le code malveillant est détecté en fonction de ses caractéristiques, sans être exécuté.

La détection de menaces est basée sur la classification des objets malveillants par les caractéristiques particulières. La technologie de l'apprentissage machine est basée sur les machines à vecteurs de support et elle permet d'effectuer la classification et l'enregistrement des fragments du code de langages de script dans la base. Ensuite, les objets détectés sont analysés pour leur conformité aux caractéristiques du code malveillant. La technologie de l'apprentissage machine met à jour automatiquement la liste des caractéristiques et les bases virales. De plus, la technologie peut fonctionner sans la connexion permanente au cloud.

La méthode de l'apprentissage machine économise les ressources du système d'exploitation car elle ne nécessite pas l'exécution du code pour détecter des menaces et l'apprentissage machine dynamique peut s'effectuer sans la mise à jour permanente de bases virales comme c'est le cas de l'analyse de signatures.

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 ;
- si Pare-feu Dr.Web est installé, vous devrez supprimer tout autre pare-feu installé sur votre ordinateur ;
- 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 XP avec Service Pack 2 ou supérieur ; • Windows Vista avec Service Pack 2 ou supérieur ; • Windows 7 ; • Windows 8 ; • Windows 8.1 ; • Windows 10 19H1 ou une version antérieure; • Windows Server 2003 avec Service Pack 1 ; • Windows Server 2008 avec Service Pack 2 ou supérieur. Pour les plateformes 64-bits : • Windows Vista avec Service Pack 2 ou supérieur ; • Windows 7 ; • Windows 8 ; • Windows 8.1 ; • Windows 19H1 Redstone 6 ou une version antérieure ; • Windows Server 2008 avec Service Pack 2 ou supérieur ; • Windows Server 2008 R2 ; • Windows Server 2012 ; • Windows Server 2012 R2 ;

Composant	Pré-requis
	• Windows Server 2016.
RAM disponible	512 Mo et plus.
Résolution	Résolution d'écran recommandée est au minimum de 800x600.
Support d'environnements virtuels et cloud	Le programme fonctionne dans les environnement suivants : • VMware ; • Hyper-V ; • Xen ; • KVM.
Autre	Une connexion au serveur de la protection centralisée ou Internet dans le mode mobile est requise pour mettre à jour les bases virales Dr.Web et les composants de Dr.Web. Le plug-in Dr.Web pour Outlook nécessite l'installation du client Microsoft Outlook intégré dans Microsoft Office : • Outlook 2000 ; • Outlook 2002 ; • Outlook 2003 ; • Outlook 2007 ; • Outlook 2010 avec Service Pack 2 ; • Outlook 2013 ; • Outlook 2016.

Agent Dr.Web 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 d'autres pré-requis, se référer au système d'exploitation correspondant.

3. Installation, modification et suppression du programme

Avant d'installer Agent pour Windows, consultez les pré-requis système et effectuez les actions suivantes :

- 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 : https://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 et les pare-feu afin d'éviter une éventuelle incompatibilité de leurs composants résidents.

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

L'installation, la modification et la suppression de Dr.Web peuvent être réalisées d'une de deux manières :

1. A distance : depuis le serveur de la protection centralisée via le réseau. Effectué par l'administrateur du réseau antivirus sans aucune intervention de l'utilisateur.
2. Localement : sur la machine de l'utilisateur directement. Dans ce cas, pour installer Dr.Web, l'installateur complet ou le package d'installation personnel peuvent être utilisés.

L'installation de Dr.Web se fait dans l'un des modes suivants :

- en mode de la ligne de commande ;
- en mode de l'assistant d'installation.

3.1. Installation avec le package d'installation complet

Installation en mode de la ligne de commande

Pour lancer l'installation de Dr.Web en mode de la ligne de commande, ouvrez le dossier où se trouve la distribution, et ensuite, entrez le nom du fichier exécutable de l'installation (`drweb-11.05.0-xxxxxxx-esuite-agent-full-windows.exe`) avec les paramètres nécessaires.

La liste complète des paramètres en ligne de commande se trouve dans l'Annexe A.

Installation en mode de l'assistant d'installation

1. Lancez le package d'installation fourni par l'administrateur. La fenêtre de l'Assistant d'installation de Dr.Web va s'ouvrir.

   S'il y a des programmes antivirus installés sur le poste, l'Assistant d'installation va essayer de les supprimer. Si cette tentative échoue, vous devez supprimer manuellement le logiciel antivirus installé sur le poste.

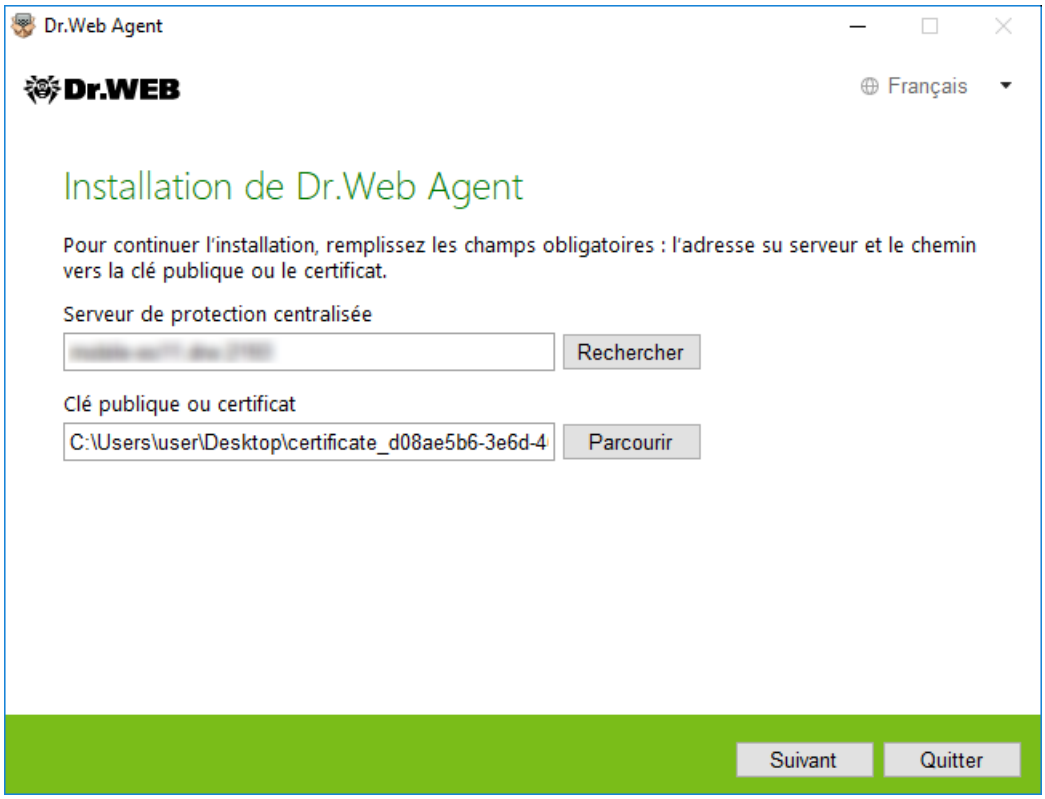

Figure 1. Assistant d'installation

2. Dans le champ **Serveur de protection centralisée**, entrez l'adresse réseau du serveur depuis laquelle l'installation de Dr.Web sera réalisée, et dans le champ **Clé publique ou certificat**, indiquez le chemin complet vers la clé publique de chiffrement (**drwcsd.pub**) ou le certificat avec l'extension **.pem** se trouvant sur votre ordinateur.

   Cliquez sur **Suivant**.

3. l'Assistant d'installation vous informe sur l'état prêt à l'installation. Vous pouvez lancez l'installation avec les paramètres par défaut en cliquant sur**Installer.**

   Afin de choisir des composant à installer, spécifier un chemin d'installation et certains paramètres supplémentaires, cliquez sur **Paramètres d'installation**. Cette option est destinée aux utilisateurs expérimentés.

4. Cliquez sur **Suivant**.

5. Si à l'étape précédente, vous avez cliqué sur **Installer**, passez à l'étape 8. Dans le cas contraire, la fenêtre **Paramètres d'installation** sera ouverte.

L'onglet **Composants** contient les composants à installer de Dr.Web.

Activez les cases contre les composants que vous souhaitez installer sur votre ordinateur. Par défaut, tous les composants sont sélectionnés, sauf le Pare-feu Dr.Web.

6. L'onglet **Chemin d'installation** vous permet de spécifier le dossier dans lequel Agent pour Windows sera installé.

   Par défaut, c'est le dossier DrWeb se trouvant dans le répertoire Program Files sur le disque système. Pour modifier le chemin d'installation, cliquez sur **Parcourir** et spécifiez le chemin souhaité.

7. Dans l'onglet **Options avancées** vous pouvez spécifier les paramètres avancés.

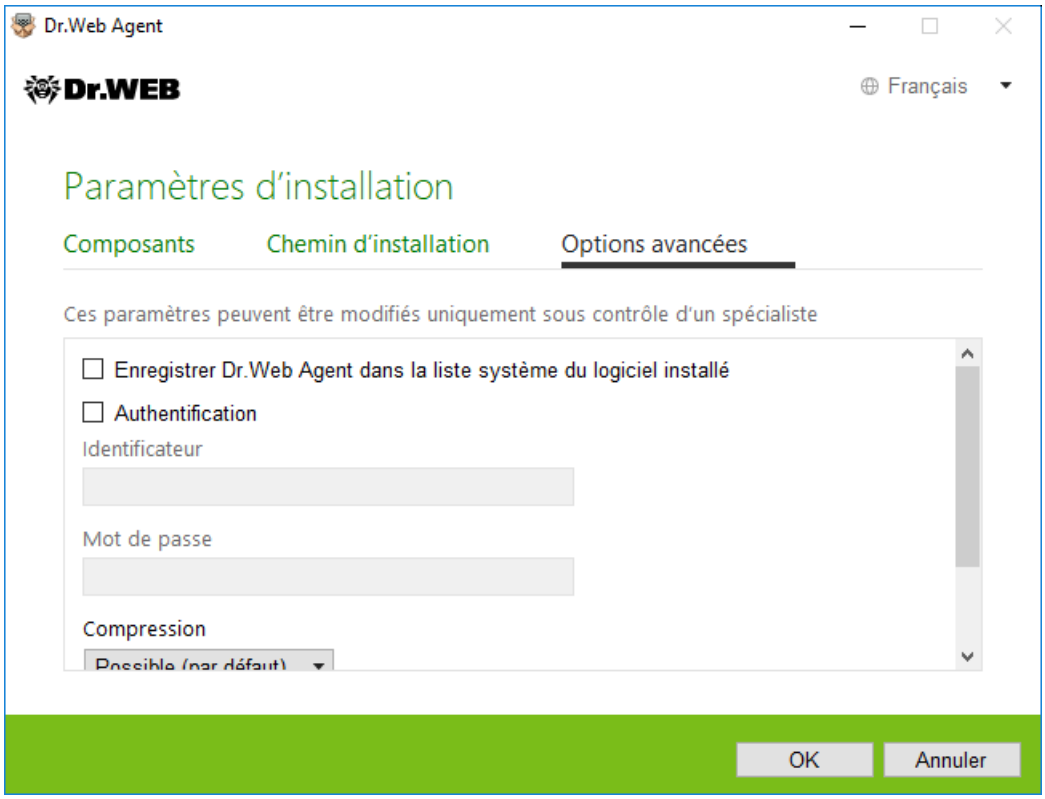

Figure 2. Assistant d'installation, paramètres avancés

Si cela est nécessaire, cochez la case **Enregistrer Dr.Web Agent dans la liste système du logiciel installé**. Entre autres, cette option permet de supprimer le logiciel Dr.Web en utilisant le Panneau de gestion de Windows.

Pour vous authentifier sur le serveur de protection centralisée, activez manuellement la case appropriée **Authentification**. Spécifiez ensuite les paramètres d'authentification du poste :

- **Identificateur** du poste sur le serveur ;
- **Mot de passe** pour l'accès au serveur.

Dans ce cas, le poste sera accessible sans approbation manuelle de l'administrateur sur le serveur.

Dans les listes déroulantes **Compression** et **Chiffrement**, spécifiez les modes correspondants pour le trafic entre le serveur et Dr.Web.

Pour enregistrer les modifications apportées, cliquez sur **OK**, puis, cliquez sur **Installer**.

8. L'installation de Dr.Web va commencer. Aucune intervention de l'utilisateur n'est requise.
9. Après la fin de l'installation, le programme va vous informer sur la nécessité de redémarrer votre ordinateur. Cliquez sur **Redémarrer maintenant**.

3.2. Installation avec le package d'installation personnel

Installation en mode de la ligne de commande

Pour lancer l'installation de Dr.Web en mode de la ligne de commande, ouvrez le dossier où se trouve la distribution, et ensuite, entrez le nom du fichier exécutable de l'installation (`drweb_ess_windows_<Station_name>.exe`) avec les paramètres nécessaires.

La liste complète des paramètres en ligne de commande se trouve dans l'Annexe A.

Installation en mode de l'assistant d'installation

1. Lancez le package d'installation fourni par l'administrateur. L'Assistant d'installation de Dr.Web va s'ouvrir.

> S'il y a des programmes antivirus installés sur le poste, l'Assistant d'installation va essayer de les supprimer. Si cette tentative échoue, vous devez supprimer manuellement le logiciel antivirus installé sur le poste.

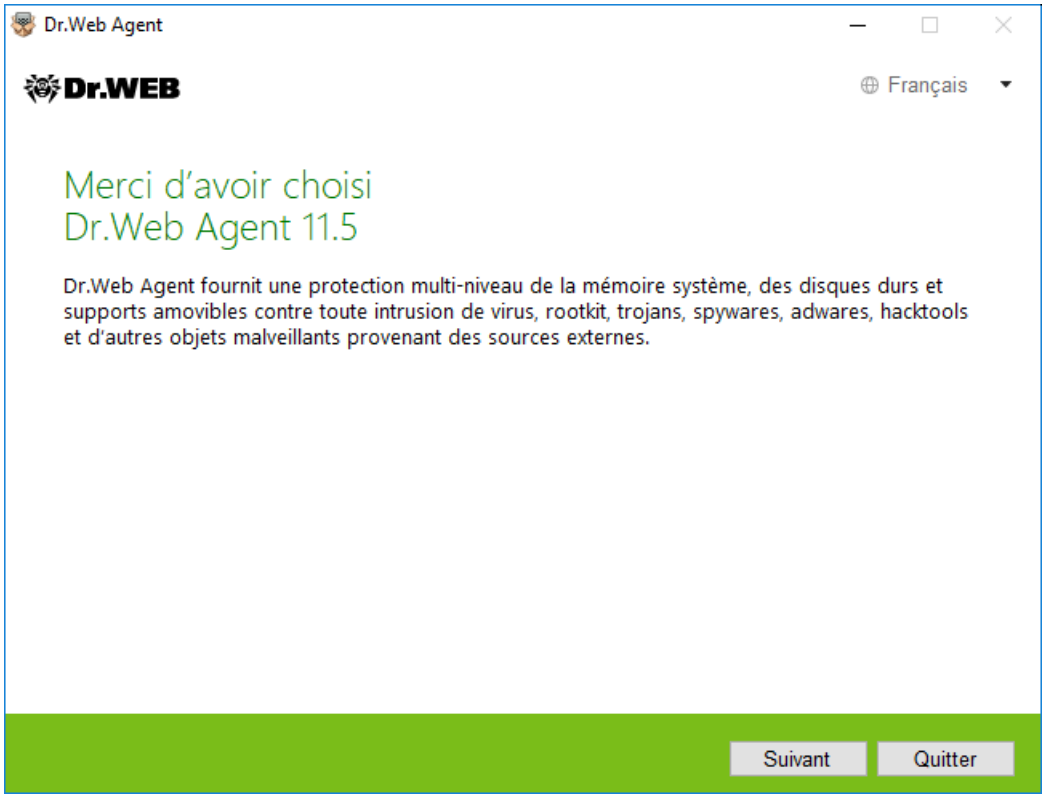

Figure 3. Assistant d'installation

2. Cliquez sur **Suivant**.
3. A l'étape suivante de l'assistant, spécifiez le chemin vers la clé de chiffrement publique (**drwcsd.pub**) ou le certificat avec l'extension **.pem** se trouvant sur votre ordinateur.
4. Vous pouvez modifier les paramètres de connexion au serveur de protection centralisée. Pour ce faire, suivez le lien approprié, la fenêtre **Paramètres de connexion** sera ouverte.

> Il est fortement recommandé de n'apporter aucune modification sans approbation de l'administrateur de votre réseau antivirus.

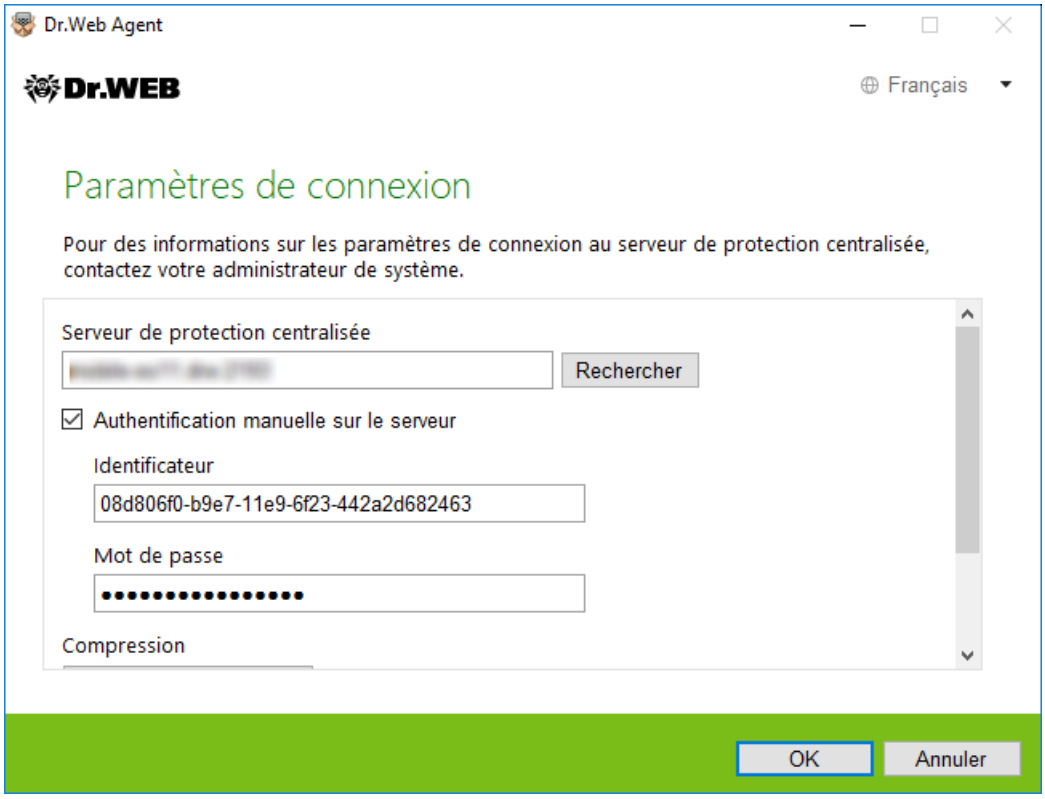

Figure 4. Spécification des paramètres de connexion au serveur de protection centralisée

> Pour des informations sur les paramètres de connexion au serveur de protection centralisée, contactez l'administrateur.

Dans le champ **Serveur de protection centralisée**, spécifiez l'adresse réseau du serveur depuis lequel sera installé Dr.Web. Ce champ est rempli automatiquement, les données correspondent au serveur sur lequel a été créé le fichier d'installation.

Cochez la case appropriée pour l'authentification manuelle sur le serveur. Puis spécifiez les paramètres d'authentification du poste :

- **Identificateur** du poste sur le serveur ;
- **Mot de passe** pour l'accès au serveur.

Dans ce cas, le poste sera accessible sans approbation manuelle de l'administrateur sur le serveur.

Dans le cas où vous installez Dr.Web avec un fichier d'installation créé dans le Centre de gestion Dr.Web, les champs **Identificateur** et **Mot de passe** pour l'authentification manuelle sont remplis automatiquement.

Dans les listes déroulantes **Compression** et **Chiffrement**, spécifiez les modes correspondants pour le trafic entre le serveur et Dr.Web.

Pour enregistrer les modifications apportées, cliquez sur **OK**, puis, cliquez sur **Suivant**.

Si la connexion n'est pas établie, utiliser le lien pour vérifier les paramètres réseau ou/et réessayez en cliquant sur le bouton approprié.

5. En cas de connexion réussie au serveur de protection centralisée, une fenêtre s'ouvre et affiche le message sur l'état prêt à l'installation. Vous pouvez lancez l'installation avec les paramètres par défaut en cliquant sur**Installer**.

   Afin de choisir des composant à installer, spécifier un chemin d'installation et certains paramètres supplémentaires, cliquez sur **Paramètres d'installation**. Cette option est destinée aux utilisateurs expérimentés.

6. Si à l'étape précédente, vous avez cliqué sur **Installer**, passez à l'étape 8. Dans le cas contraire, la fenêtre **Paramètres d'installation** sera ouverte.

   L'onglet **Composants** contient les composants à installer de Dr.Web.

   Activez les cases contre les composants que vous souhaitez installer sur votre ordinateur. Par défaut, tous les composants sont sélectionnés, sauf le Pare-feu Dr.Web.

7. L'onglet **Chemin d'installation** vous permet de spécifier le dossier dans lequel **Agent pour Windows** sera installé. Par défaut, c'est le dossier DrWeb se trouvant dans le répertoire Program Files sur le disque système. Pour modifier le chemin d'installation, cliquez sur **Parcourir** et spécifiez le chemin souhaité.

8. Dans l'onglet **Options avancées**, vous pouvez spécifier les paramètres avancés de Dr.Web.

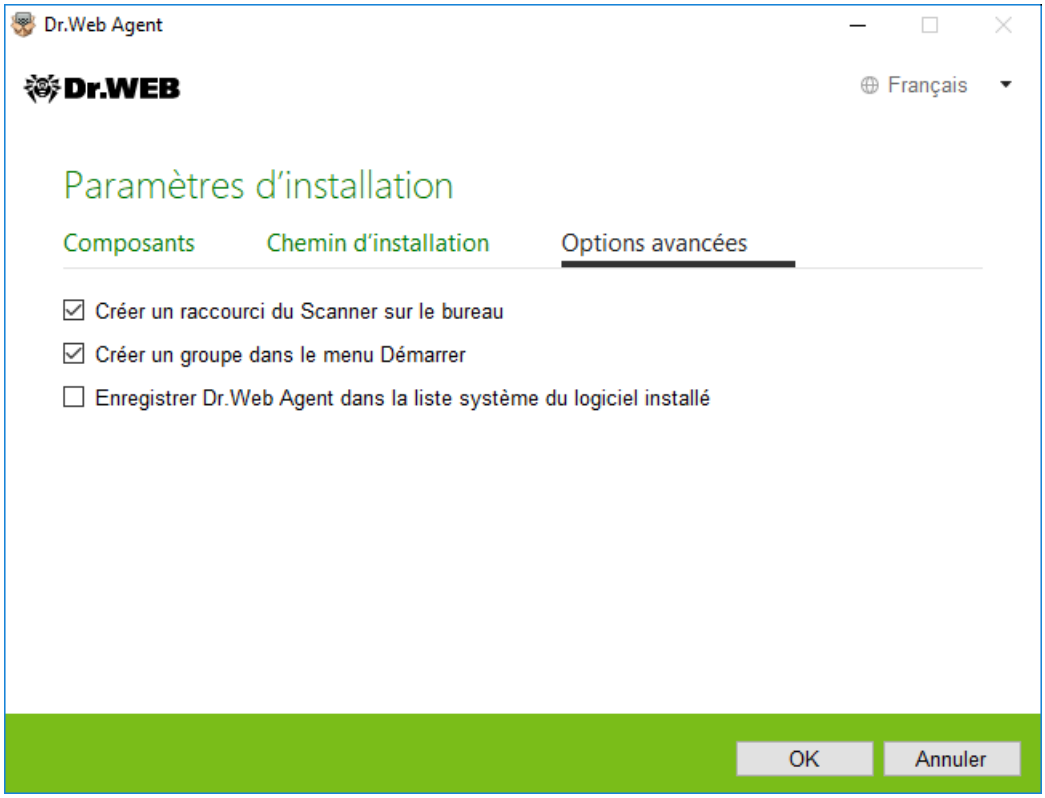

Figure 5. Assistant d'installation, paramètres avancés

Si cela est nécessaire, activez la case **Enregistrer Dr.Web Agent dans la liste système du logiciel installé**. Entre autres, cette option permet de supprimer le logiciel Dr.Web en utilisant le Panneau de gestion de Windows.

Pour enregistrer les modifications apportées, cliquez sur **OK**, puis, cliquez sur **Installer**.

9. L'installation de Dr.Web va commencer. Aucune intervention de l'utilisateur n'est requise.
10. Après la fin de l'installation, l'assistant va vous informer sur la nécessité de redémarrer votre ordinateur. Cliquez sur **Redémarrer maintenant**.

Erreur du service BFE lors de l'installation du logiciel Dr.Web

Pour le fonctionnement de certains composants de Dr.Web, il faut que le service du moteur de filtrage de base (BFE) soit lancé. Si ce service est manquant ou endommagé, l'installation de Dr.Web est impossible. L'endommagement ou l'absence du service BFE peut signaler la présence des menaces de sécurité sur votre ordinateur.

Si la tentative d'installer Dr.Web a échoué avec l'erreur du service BFE, faites le suivant :

1. Scannez le système avec l'utilitaire de désinfection CureNet! de Doctor Web. Vous pouvez demander la version de démonstration de l'utilitaire (diagnostic sans fonctionnalité de désinfection) à l'adresse : https://download.drweb.com/curenet/.

   Vous pouvez consulter les conditions d'utilisation et le prix de la version complète de l'utilitaire à l'adresse : https://estore.drweb.com/utilities/.

2. Restaurez le service BFE. Pour cela, vous pouvez utilisez l'utilitaire de résolution de problèmes du Pare-feu créé par Microsoft (pour les systèmes d'exploitation Windows 7 ou les versions supérieures). Vous pouvez télécharger l'utilitaire sur le site : https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall.
3. Lancez l'Assistant d'installation Dr.Web et effectuez l'installation selon la procédure standard décrite ci-dessus.

Si le problème persiste, contactez le support technique de Doctor Web.

3.3. Modification des composants du programme

1. Pour supprimer ou modifier les composants de Dr.Web, allez dans la section consacrée à l'installation et la suppression de programmes du Panneau de gestion Windows.
2. Dans la liste des programmes installés, sélectionnez la ligne portant le nom du programme.
3. Cliquez sur **Modifier**. Dans ce cas, l'Assistant de suppression/modification des composants du programme va s'afficher.

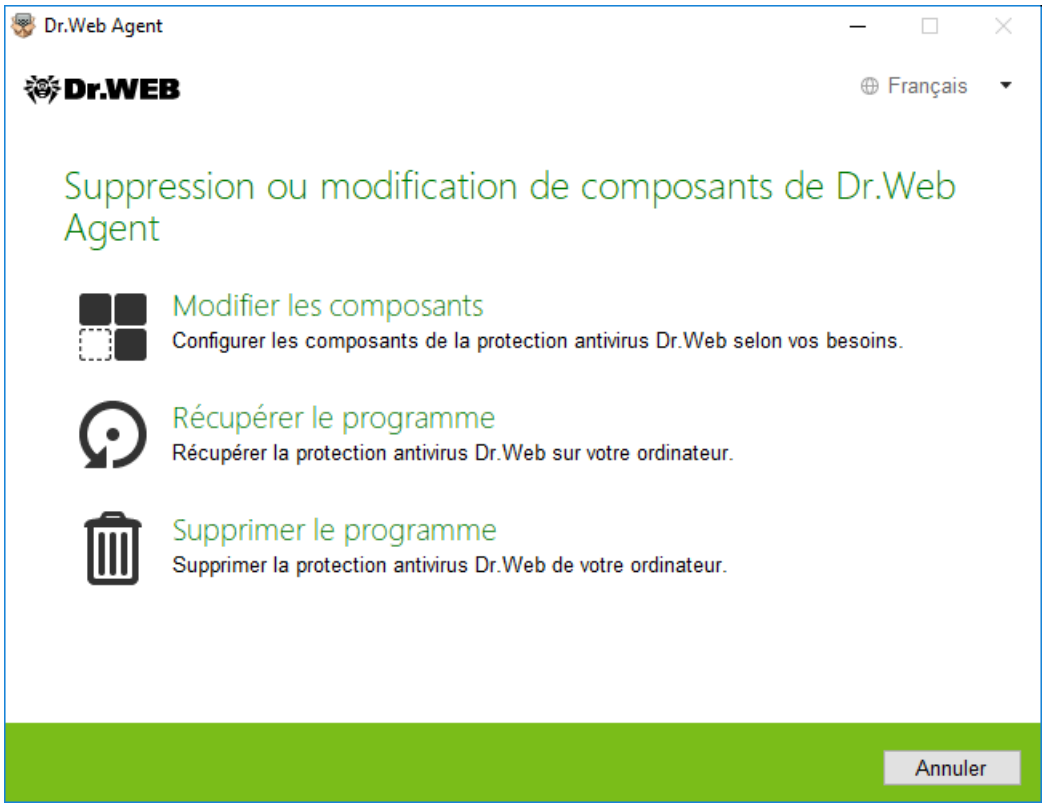

Figure 6. Assistant de suppression/modification des composants

4. Sélectionnez l'une des options :
   - **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**.
   - **Récupérer le programme**, s'il faut restaurer la protection antivirus sur votre ordinateur. Cette fonction est appliquée au cas où certains composants de Dr.Web seraient endommagés.

- **Supprimer le programme**, pour supprimer tous les composants installés.

3.4. Suppression du logiciel

Pour supprimer Dr.Web de manière locale, cette option doit être autorisée par l'administrateur sur le serveur de protection centralisée.

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

Suppression de Dr.Web du Panneau de gestion de Windows

Cette méthode de suppression n'est disponible que dans le cas où dans l'Assistant d'installation, vous avez activé la case **Enregistrer Dr.Web Agent dans la liste système du logiciel installé**.

Si Dr.Web a été installé en mode de tâche de fond, la suppression de Dr.Web avec des outils système standard est possible à condition que lors de l'installation, la clé `–regagent` ait été utilisée.

1. Pour supprimer Agent pour Windows lancez le composant de suppression des programmes Windows.
2. Dans la liste qui apparaît, sélectionnez la ligne affichant le nom du programme.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre **Paramètres sauvegardés**, cochez les cases contre les éléments à conserver après la suppression du logiciel. Les objets et les paramètres conservés peuvent être utilisés par le logiciel en cas de réinstallation. Par défaut, toutes les options sont activées : **Quarantaine**, **Configuration de Dr.Web Agent** et **Copies de fichiers protégées**. Cliquez sur **Installer**.
5. Dans la fenêtre suivante, pour confirmer la désinstallation de Dr.Web, cliquez sur **Supprimer**.
6. Les modifications entrent en vigueur après le redémarrage de l'ordinateur. Vous pouvez reporter le redémarrage en cliquant sur **Ultérieurement**. Cliquez sur **Redémarrer maintenant** pour terminer la désinstallation et modifier l'ensemble des composants Dr.Web tout de suite.

Suppression en mode de la ligne de commande

Pour supprimer Dr.Web en mode de la ligne de commande, entrez le nom du fichier (`win-es-agent-setup.exe`) accompagné des paramètres nécessaires.

Le fichier win-es-agent-setup.exe se trouve dans le dossier C:\ProgramData\Doctor Web\Setup\.

Par exemple, la commande suivante supprime Dr.Web en tâche de fond et réalise un redémarrage :

```
win-es-agent-setup.exe /instMode remove /silent yes
```

4. Mise en route

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

> L'icône de Dr.Web n'est pas affichée dans la zone de notification si l'administrateur de votre réseau antivirus a activé l'option appropriée sur le serveur de protection centralisée.
>
> Si le programme n'est pas lancé, ouvrez le groupe **Dr.Web** et sélectionnez **SpIDer Agent** dans le menu **Démarrer**.

L'icône Dr.Web indique l'état actuel du logiciel :

- : tous les composants nécessaires sont activés et fonctionnent correctement, la connexion au serveur de protection centralisée est établie ;
- : l'Autoprotection Dr.Web ou un des composants est désactivé, ce qui compromet la sécurité de l'antivirus et de votre ordinateur ; ou bien la connexion au serveur est attendue mais pas encore établie. Il se peut que le serveur ait rejeté la connexion du poste ou l'accès à ses ressources. Activez l'autoprotection ou le composant désactivé, attendez une connexion au serveur ou contactez l'administrateur de votre réseau antivirus si la connexion n'est pas établie ;
- : 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. Si l'icône ne change pas, contactez l'administrateur de votre réseau antivirus.

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

Pour accéder au menu de Dr.Webt, cliquez sur l'icône dans la zone de notification Windows.

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

Le menu Dr.Web vous offre les outils principaux de gestion et de configuration du logiciel.

Outils. Ouvre un menu donnant accès aux sections suivantes :

- Gestionnaire de quarantaine ;
- Support.

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

Scanner. Accès rapide au lancement de trois modes différents.

Messages du serveur. Ouvre la fenêtre de consultation de messages du serveur.

Mode de fonctionnement . Permet de passer du mode utilisateur au mode administrateur. Par défaut, Dr.Web démarre en mode utilisateur restreint, qui ne donne pas accès à 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 demandera un accès aux privilèges administrateur. De plus, vous devez également entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la fenêtre Configuration. Veuillez noter que vous serez de nouveau en mode utilisateur 15 minutes après être passé en mode administrateur. Si vous êtes toujours en train de configurer les paramètres lorsque ce délai expire, vous reviendrez en mode utilisateur après la fermeture de la fenêtre de configuration.

Statistiques . 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, etc.

Configuration . Ouvre la fenêtre des paramètres généraux, des paramètres des composants de protection, ainsi que le module Office Control et des exclusions.

Il est impossible de modifier des paramètres ou de désactiver des composants sans que l'administrateur du serveur de protection centralisée auquel est connecté Dr.Web n'autorise ces actions.

Pour accéder aux paramètres des composants, vous devez également entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de 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 l'administrateur de votre réseau antivirus.

Aide . Ouvre le manuel.

4.1. Tester l'antivirus

Test avec le fichier EICAR

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.

Dans ce but, 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 un virus, il est traité par la plupart des antivirus comme tel. Sur la détection de ce « virus », la solution antivirus Dr.Web établit le rapport

suivant : `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 imprime la ligne suivante 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 programme malveillant et par défaut le déplace en Quarantaine.

5. Outils

Ouvrez le menu de Dr.Web et lancez les **Outils**. Pour rendre toutes les options accessibles passez en mode administrateur.

Pour voir la liste des fichiers isolés et restaurer les fichiers de la quarantaine, sélectionnez Gestionnaire de quarantaine.

Si vous rencontrez un problème ou que vous avez une question sur l'utilisation de Dr.Web, sélectionnez la section Support.

5.1. Gestionnaire de quarantaine

La fenêtre contient des informations sur la Quarantaine de Dr.Web qui permet d'isoler les fichiers suspectés d'être malveillants. La Quarantaine stocke également les copies de sauvegarde des fichiers traités par Dr.Web.

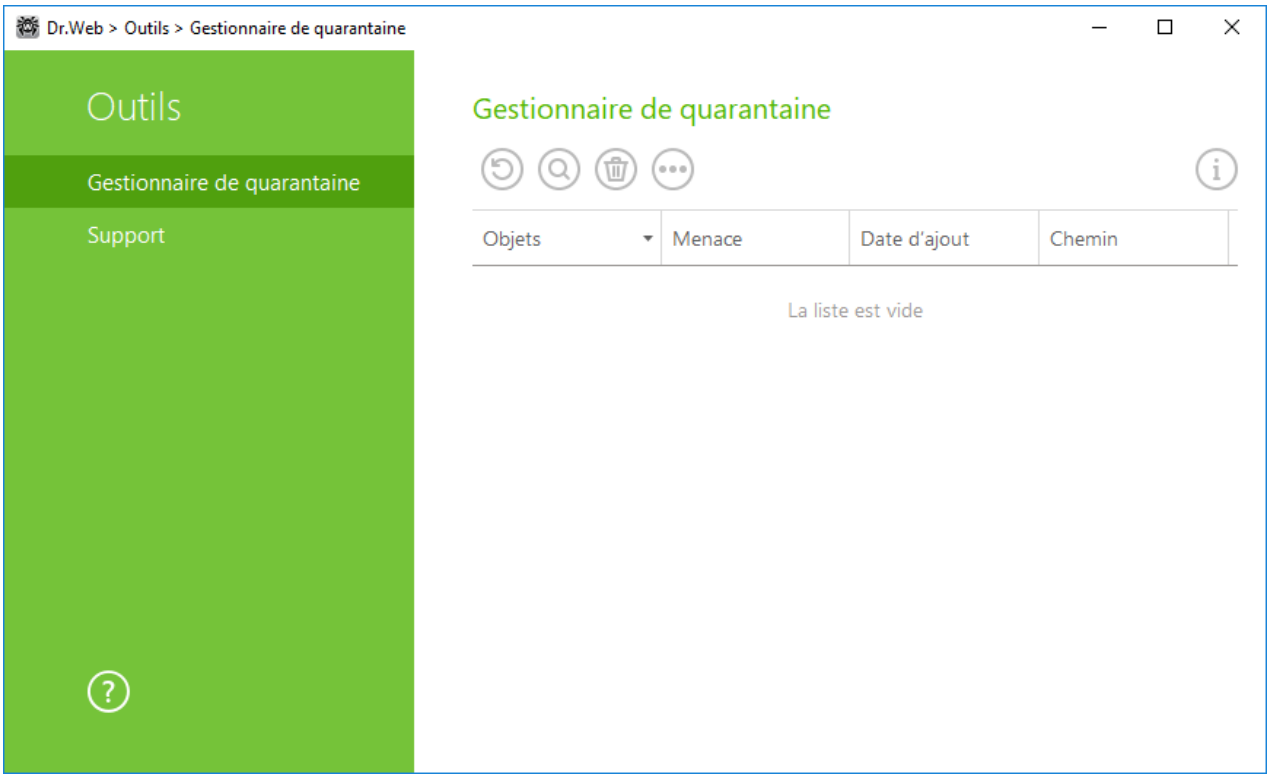

Figure 7. Objets en quarantaine

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.

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 logiciel malveillant déterminé par Dr.Web lorsque l'objet est placé en quarantaine ;
- **Date d'ajout** : 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.

Les copies de sauvegarde déplacées en quarantaine sont affichées dans le tableau par défaut. Pour les voir dans la liste des objets, cliquez sur ⋯ et dans la liste déroulante, sélectionnez l'élément **Montrer les copies de réserve**.

Gestion des objets en quarantaine

En mode administrateur, les boutons suivants sont disponibles pour chaque objet :

- **Restaurer** : déplacer un ou plusieurs objets sélectionnés sous les noms spécifiés vers le dossier nécessaire ;

> ⚠ 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 un ou plusieurs 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 en même temps, cliquez sur le bouton ⋯ et sélectionnez **Tout supprimer** dans la liste déroulante.

5.2. 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.

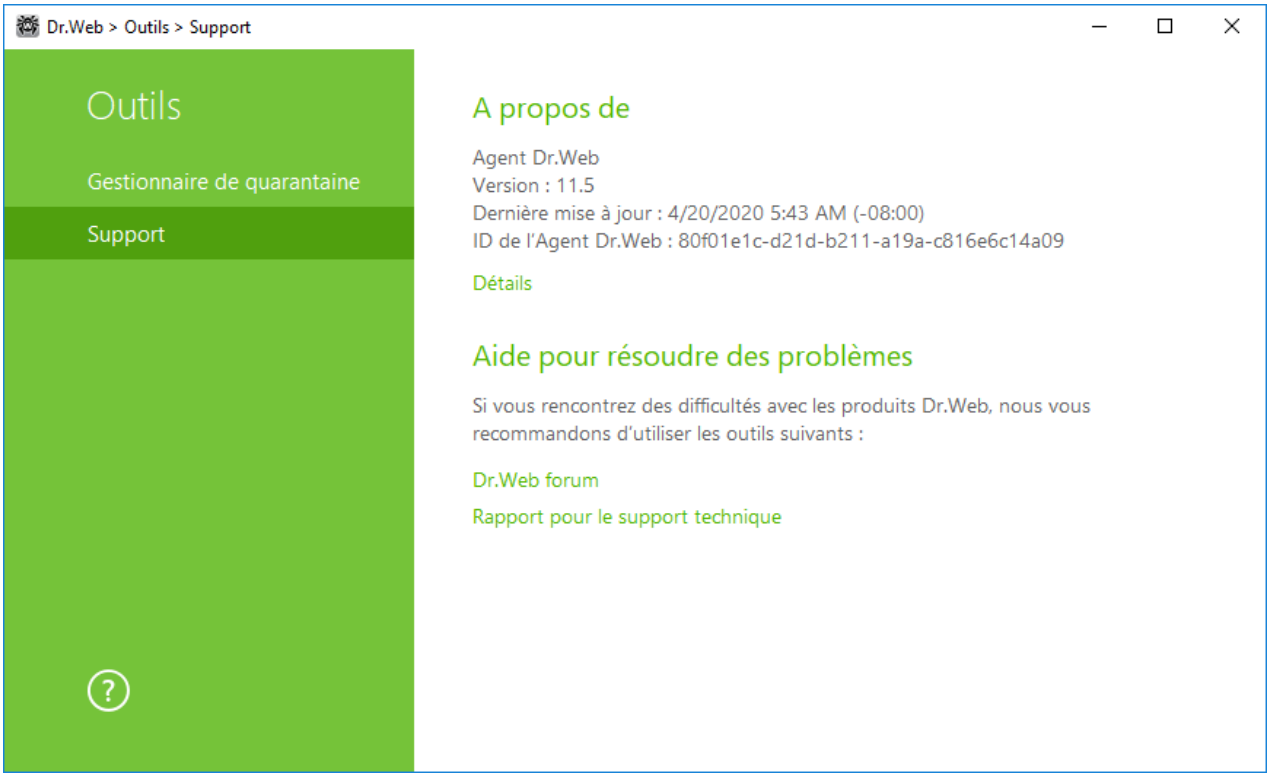

Figure 8. Informations sur la version du produit et support

Si vous avez des questions, utilisez les outils suivants.

Dr.Web forum. Ce lien ouvre le forum Dr.Web à la page https://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 la solution de votre problème, vous pouvez demander une assistance directe du support technique de Doctor Web en remplissant le formulaire dans la section du support à la page https://support.drweb.com. Vous pouvez joindre le rapport pour le service technique, des captures d'écran et d'autres informations nécessaires.

Pour trouver le bureau Doctor Web le plus proche de chez vous et tous les contacts nécessaires, visitez la page https://company.drweb.com/contacts/.

5.2.1. Créer un rapport

Pour contacter l'administrateur de votre réseau antivirus, vous pouvez générer un rapport sur votre système d'exploitation et le fonctionnement de Dr.Web.

Pour créer un rapport

1. Ouvrez le menu .
2. Passez sur la page **Outils**.

3. Sélectionnez **Support**.

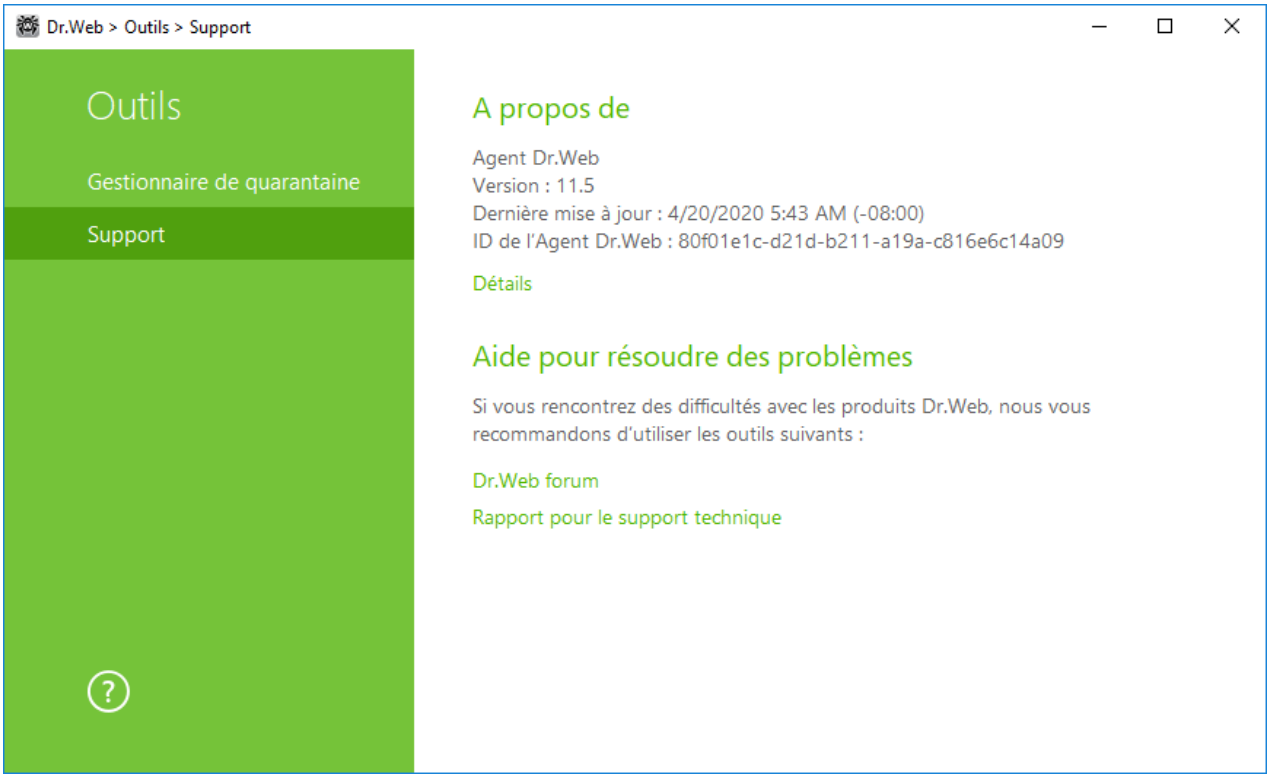

Figure 9. Support

4. Cliquez sur le lien **Rapport pour le support technique**.
5. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Créer un rapport**.

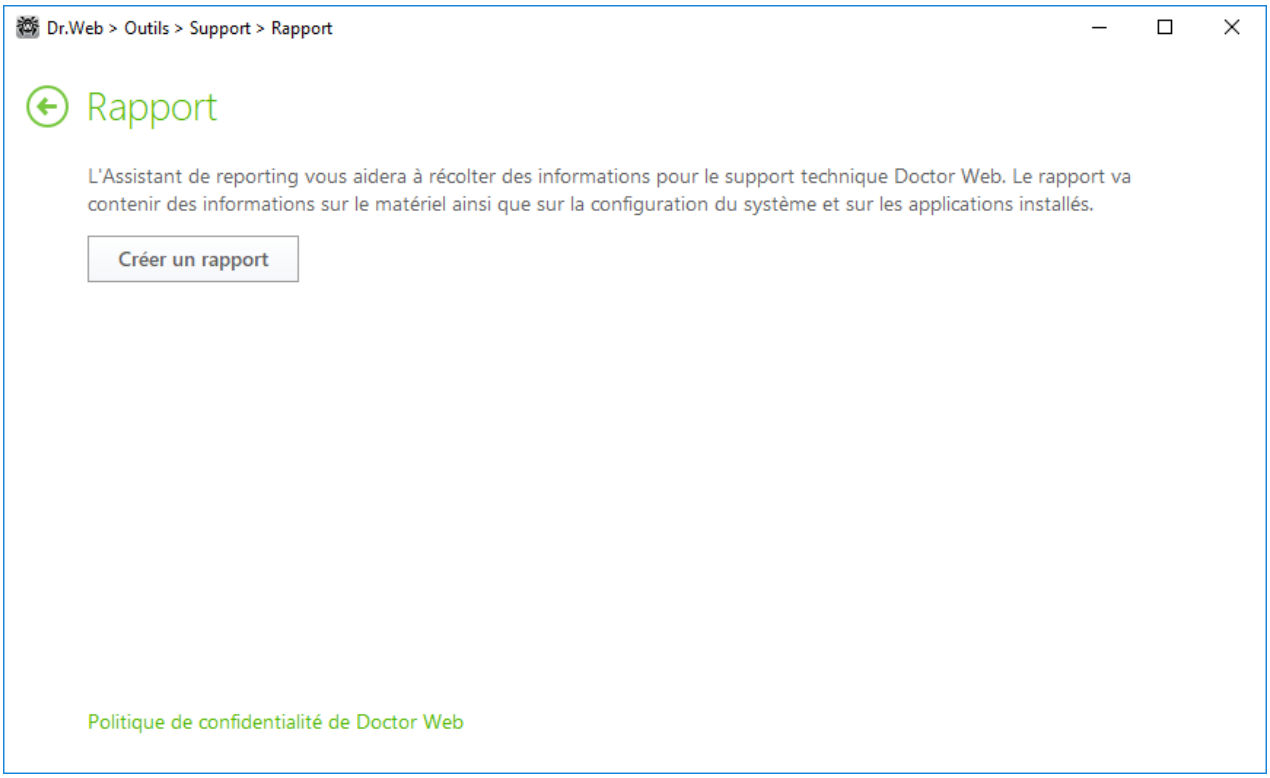

Figure 10. Création d'un rapport

Le rapport sera créé automatiquement et enregistré sous forme d'archive dans le dossier 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 plug-ins 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 enregistré sous forme d'archive dans le dossier 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 d'accès au fichier de rapport.

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

6. Scanner Dr.Web

Scanner Dr.Web pour Windows vous permet de lancer le scan 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 e-mails avec des pièces jointes. Toutes les méthodes de détection de menaces sont utilisées pour l'analyse.

Lorsqu'un objet malveillant est détecté, 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 de 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.

6.1. Lancement et modes d'analyse

Si vous utilisez Windows Vista, Windows Server 2003 ou un système d'exploitation ultérieur, il est recommandé de lancer Scanner Dr.Web avec les droits d'administrateur. Sinon, les fichiers et les dossiers auxquels l'utilisateur sans droits n'a pas accès (y compris les dossiers système) ne seront pas analysés.

Lancer le Scanner Dr.Web

1. Dans le menu  sélectionnez l'élément **Scanner**. Le menu d'accès rapide aux différents modes d'analyse va s'ouvrir.

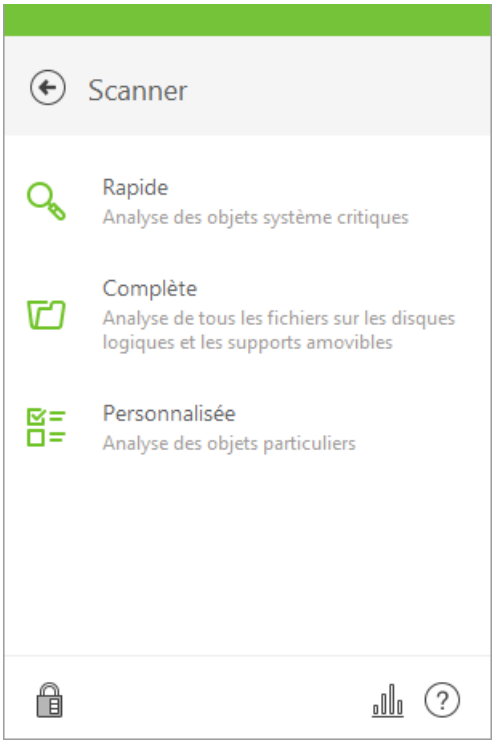

Figure 11. Sélection du mode de l'analyse effectuée par le scanner

2. Sélectionnez le mode d'analyse nécessaire :
   - l'élément **Personnalisée** pour scanner uniquement les objets que vous avez désignés. La fenêtre de sélection de fichiers pour l'analyse par le Scanner Dr.Web va s'ouvrir ;
   - l'élément **Rapide** pour analyser uniquement les zones critiques de Windows ;
   - l'élément **Complète**, pour analyser tous les fichiers.

Vous pouvez également lancer 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 **Configuration** → **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 l'analyse cliquez sur **Lancer l'analyse** Pour ajouter des objets dans la liste, cliquez sur  .

Processus de l'analyse

Dès que 'analyse commence, les bouton **Pause** et **Stop** dans la partie droite de la fenêtre deviennent disponibles. A chaque étape de l'analyse, vous pouvez faire le suivant :

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

De cette fenêtre vous pouvez retourner dans la fenêtre de sélection de mode de scan.

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

6.2. Actions en cas de détection de menaces

Après la fin d'analyse, 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, après la fin de l'analyse, sélectionnez toutes les menaces et

cliquez sur le bouton **Neutraliser**, et Scanner Dr.Web appliquera des actions définies par défaut qui sont optimales pour toutes les menaces détectées.

En cliquant sur **Neutraliser**, vous appliquez les actions aux objets sélectionnées dans le tableau. Il faut sélectionner manuellement certains objets ou groupes d'objets auxquels il faut appliquer l'action en cliquant sur **Neutraliser**. Pour ce faire, utilisez les cases contre les noms des objets ou le menu déroulant dans l'en-tête du tableau.

Sélection d'une action

1. Dans le champ **Action** de la liste déroulante, sélectionnez une action pour chaque objet (par défaut, Scanner Dr.Web suggère une action optimale).
2. Cliquez sur **Neutraliser**. 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 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 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	Cette colonne contient l'action recommandée pour la menace détectée. Cliquez sur la flèche sur ce bouton pour définir l'action pour la menace sélectionnée. Vous pouvez appliquer l'action indiquée sur le bouton séparément, sans neutraliser les menaces restantes. Pour ce faire, cliquez sur ce bouton.

Nom de colonne	Description
Chemin	Ce colonne affiche le chemin complet vers le fichier correspondant.

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

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

Vous pouvez lancer Scanner Dr.Web en mode ligne de commande. Ce mode vous permet de configurer les paramètres nécessaires pour la session courante de scan ainsi qu'une liste d'objets spécifiques à scanner avec les clés correspondantes.

Syntaxe de la commande de lancement :

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

La liste des objets à scanner peut être vide ou contenir plusieurs éléments séparés par des blancs. Si le chemin vers les objets à analyser n'est pas spécifié, la recherche sera effectuée dans le dossier d'installation Dr.Web.

Les objets les plus souvent vérifiés 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 rootkit sera également réalisée.

Paramètres : les clés de la ligne de commande déterminant la configuration du logiciel. 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 slash (`/`) et sont séparées par des espaces comme les autres paramètres de ligne de commande.

6.4. 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.

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

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

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 :

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

6.5. 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.

Si Pare-feu est installé, il bloquera le planificateur de tâches après l'installation de Dr.Web et le premier redémarrage du système. Les **tâches planifiées** seront effectuées uniquement après le second redémarrage si une nouvelle règle a déjà été créée.

7. Configuration

Pour configurer les paramètres, ouvrez le menu de Dr.Web, et lancez **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 l'administrateur de votre réseau antivirus.

8. Paramètres généraux

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

Pour accéder aux paramètres principaux de Dr.Web, ouvrez le menu, lancez **Configuration** en mode administrateur et sélectionnez la section **Général**.

> La modification des paramètres principaux est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.
>
> ---
>
> 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 Configuration.

Pour configurer l'affichage de notifications sur l'écran, sélectionnez la section Notifications.

Pour configurer les paramètres de sécurité avancés, sélectionnez la section Autoprotection.

Pour restreindre l'accès à un périphérique spécifique ou à un bus de périphériques, sélectionnez la section Périphériques.

Pour modifier la langue d'interface ou les paramètres du journal ou de la quarantaine, sélectionnez Avancé.

Pour configurer les paramètres de connexion au serveur de protection centralisée, sélectionnez Serveur.

8.1. Notifications

Dans cette section, vous pouvez configurer les paramètres de réception de notifications de fonctionnement de Agent pour Windows.

Notifications pop-up

Activez l'option correspondante pour avoir des notifications pop-up sur l'icône de Dr.Web dans la zone de notification Windows.

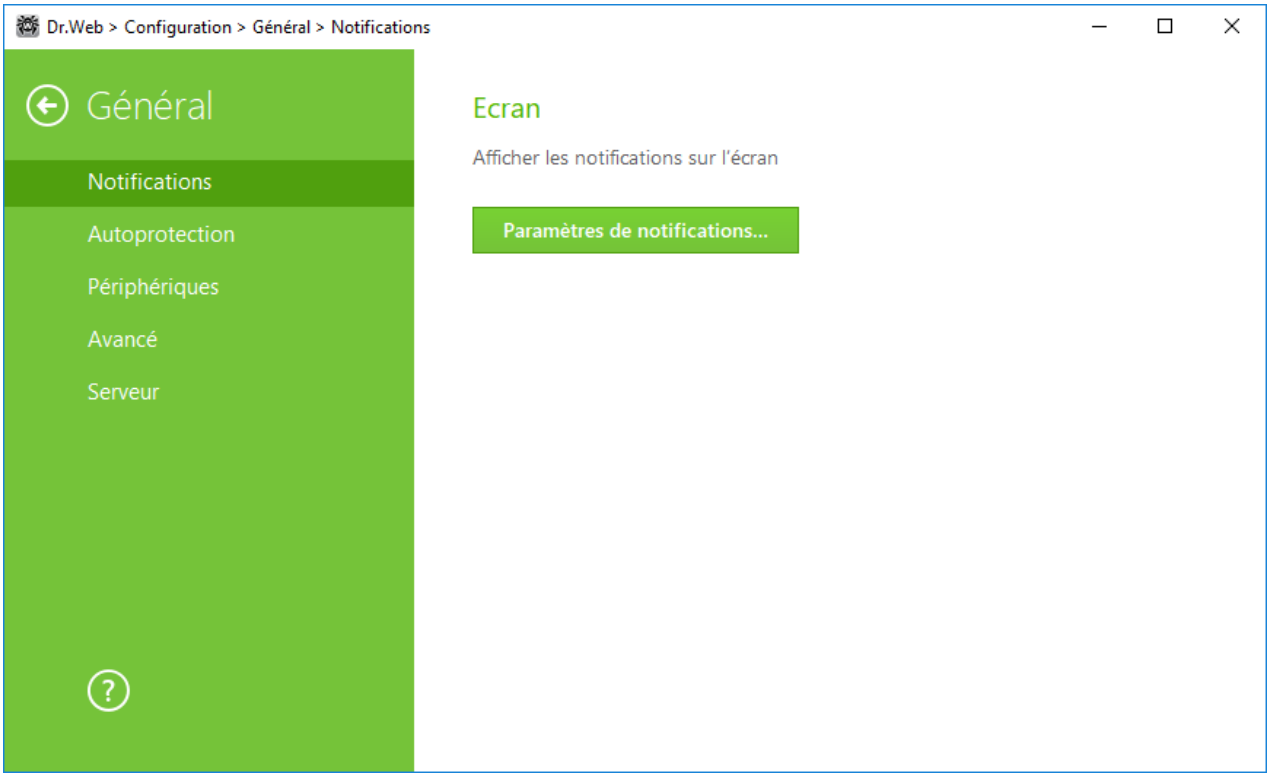

Figure 12. Paramètres de notifications

Paramètres des notifications

1. Cliquez sur **Paramètres des notifications**.
2. Choisissez les notifications que vous souhaitez recevoir. Pour afficher les notifications, cochez les cases contre les types de notifications nécessaires.Si vous ne boulez pas recevoir les notifications des événements, décochez les cases.

Type de notification	Description
Menace détectée	Notifications des menaces détectées par les composants SpIDer Guard et SpIDer Gate. Ces notifications sont activées par défaut.
Notifications critiques	Notifications critiques des événements suivants : • des connexions en attente de réponse du Pare-feu ; • votre login et mot de passe sont déjà utilisés pour la connexion au serveur de protection centralisée Ces notifications sont activées par défaut.
Notifications majeures	Notifications importantes des événements suivants : • la durée d'utilisation de l'ordinateur est écoulée ;

Type de notification	Description
	• le dispositif est bloqué ; • une tentative de changer la date et l'heure système a été bloquée ; • la tentative d'accès à l'objet protégé est bloquée par la Protection préventive ; • les bases virales Dr.Web sont périmées (dans le mode Mobile). Ces notifications sont activées par défaut.
Notifications mineurs	Notifications mineures des événements suivants : • mise à jour réussie ; • erreur de mise à jour ; • la durée d'utilisation d'Internet est écoulée ; • l'URL a été bloquée par le module Office Control ; • l'URL a été bloquée par SpIDer Gate ; • la tentative d'accès à l'objet protégé est bloquée par le module Office Control; • l'administrateur de votre réseau antivirus a lancé le scan sur votre ordinateur ; • le scan de votre ordinateur est lancé selon la planification ; • le scan de votre ordinateur s'est terminé. Les notifications sont désactivées par défaut.

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

Option	Description
Ne pas afficher les notifications en mode plein écran	Notifications s'affichant lorsque vous travaillez avec des applications en mode plein écran (affichage des filmes, graphiques etc.). Décochez la case pour recevoir toujours de telles notifications.
Afficher les notifications du Pare-feu dans une fenêtre séparée en mode plein écran	Affichage des notifications du Pare-feu sur un bureau séparée lorsque des applications tournent en mode plein écran (jeux, vidéo). Décochez la case pour afficher les notifications sur le même bureau que celui où une application est lancée en mode plein écran.

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 ;
- message envoyé par l'administrateur du serveur de protection centralisée.

8.2. Autoprotection

Dans cette section, vous pouvez configurer les paramètres de l'autoprotection de Dr.Web contre l'influence non autorisée des programmes attaquant les antivirus ou contre les dommages accidentels.

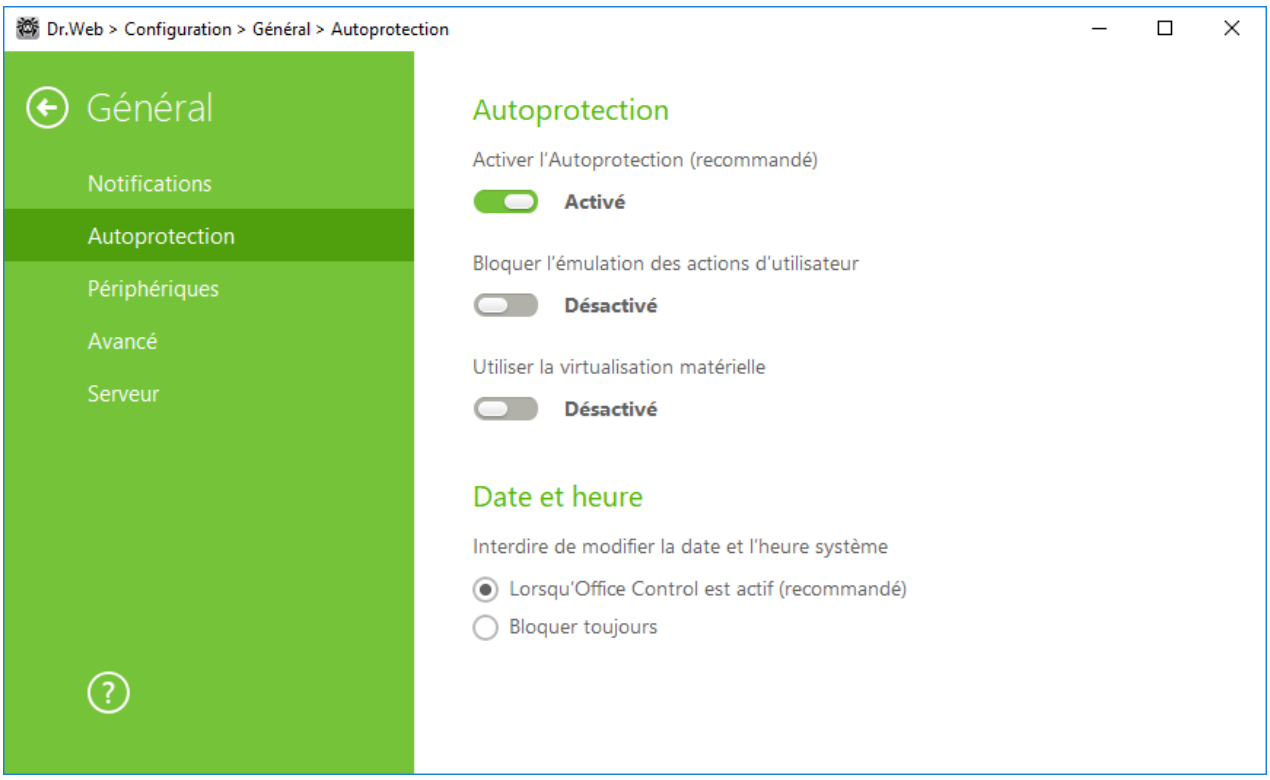

Figure 13. Paramètres de la protection Dr.Web

Autoprotection

L'option **Activer l'Autoprotection (recommandé)** 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

Certains programmes malveillants modifient la date et l'heure système. Dans ce cas, les mises à jour des bases virales ne se font pas selon la planification, la licence peut être considérée comme obsolète et les composants de la protection peuvent être désactivés.

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. L'option permet d'améliorer la fonction de limitation de durée implémentée dans Office Control. Si les limites d'utilisation d'Internet ou de l'ordinateur sont définies dans Office Control, cette option est automatiquement activée. Vous pouvez configurer les notifications afin d'être informé d'une tentative de modification de l'heure système.

8.3. Périphériques

Dans cette section, vous pouvez restreindre l'accès aux appareils particuliers et aux bus d'appareils et configurer les listes noire et blanche.

Les règles d'accès aux appareils s'appliquent pour tous les comptes Windows.

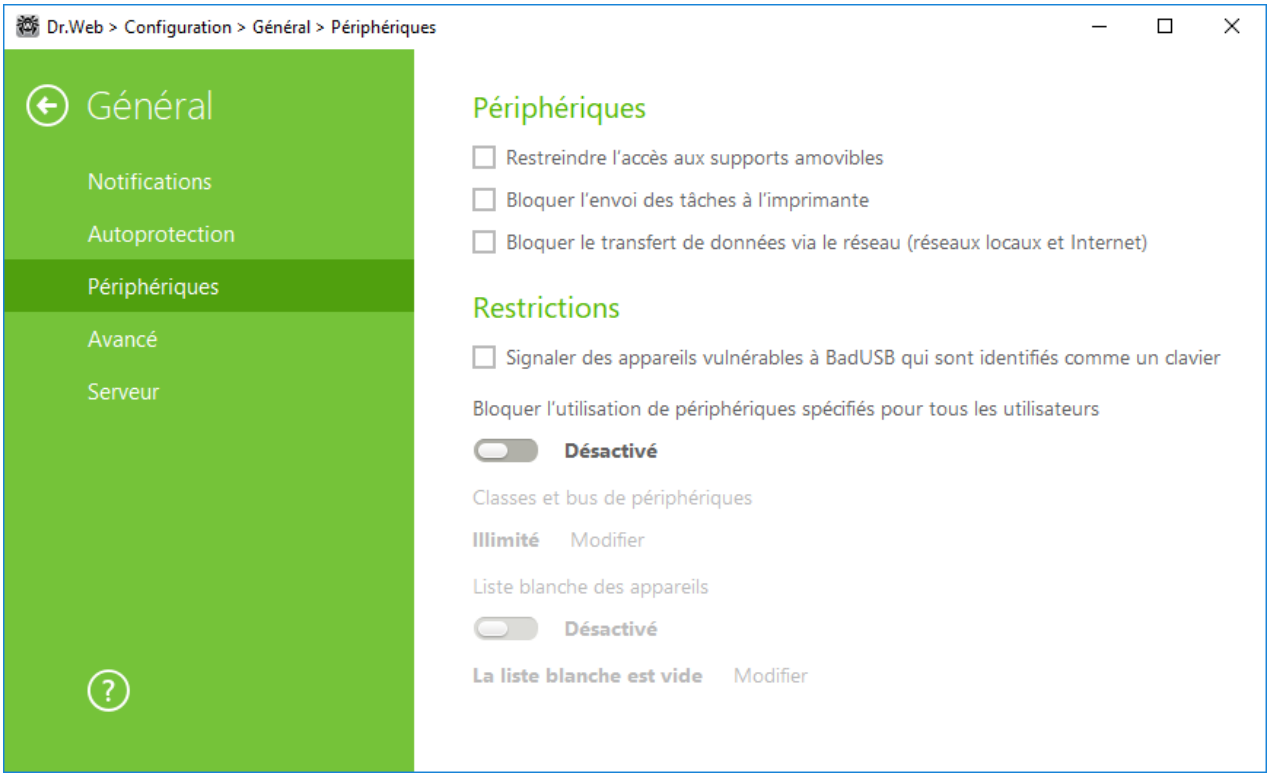

Figure 14. Paramètres du blocage des périphériques

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**.

Classes et bus de périphériques

Cette fonction permet de bloquer une ou plusieurs classes de périphériques sur tous les bus et de bloquer tous les appareils connectés à un ou plusieurs bus. Une classe de périphérique, ce sont les appareils exécutant les mêmes fonctions (par exemple, les périphériques d'impression). Les bus, ce sont les sous-systèmes de transfert de données entre les blocs fonctionnels de l'ordinateur (par exemple, le bus USB).

Pour bloquer l'accès aux classes sélectionnés et aux bus de périphériques, activez l'option correspondante. Générez la liste de tels objets, en cliquant sur le bouton **Modifier**. Dans la fenêtre qui s'ouvre, vous pouvez sélectionner les classes ou les bus de périphériques auxquels vous voulez bloquer l'accès.

Formation de la liste de classes de périphériques bloquées

1. Pour bloquer entièrement une classe de périphériques, cliquez sur le bouton  dans la colonne **Classes bloquées**.
2. Dans la liste qui s'ouvre, sélectionnez les classes nécessaires et cliquez sur **OK**. Les classes de périphériques nécessaires seront bloquées sur tous les bus. Seules les classes non bloquées sont affichées dans la liste de sélection de classes de périphériques.
3. Pour débloquer une classe de périphériques, sélectionnez la classe nécessaire dans la fenêtre **Classes et bus de périphériques** et cliquez sur le bouton  .

Formation de la liste de bus de périphériques bloqués

1. Pour bloquer le bus entier ou certains périphériques sur le bus, cliquez sur le bouton  dans la colonne **Bus bloqués**.
2. Dans la fenêtre qui s'affiche, sélectionnez les classes de périphériques nécessaires. Pour bloquer tout le bus, sélectionnez toutes les classes dans la liste. Cliquez sur **OK**.
3. Pour débloquer un bus, sélectionnez le bus nécessaire dans la fenêtre **Classes et bus de périphériques** et cliquez sur le bouton  .
4. Pour éditer la liste de classes bloquées sur un bus particulier, cliquez sur le bouton  .

Si vous activez le blocage d'un appareil déjà connecté, il faut connecter l'appareil encore une fois ou redémarrer l'ordinateur. Le blocage fonctionne uniquement pour les appareils connectés après l'activation de la fonction.

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.

Ajout d'un périphérique à la liste blanche

1. Activez l'option **Liste blanche des appareils** (l'option devient active si les limitations sont spécifiées).
2. Pour créer la liste d'appareils, cliquez sur **Modifier**.
3. Assurez-vous que le périphérique est connecté à l'ordinateur.

4. Cliquez sur . Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et sélectionnez le périphérique nécessaire. Utilisez le filtre pour afficher dans le tableau uniquement les périphériques connectés ou non connectés. Cliquez sur **OK**.
5. 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 .
6. Pour sauvegarder les modifications apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**. Vous allez revenir à la liste blanche.
7. Pour modifier l'ensemble de règles pour un périphérique, sélectionnez-le dans la liste et cliquez sur .
8. Pour supprimer l'ensemble de règles pour un périphérique, sélectionnez-le et cliquez sur .

8.4. Avancé

Dans cette section, vous pouvez spécifier la langue du logiciel, les paramètres du journal et 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.

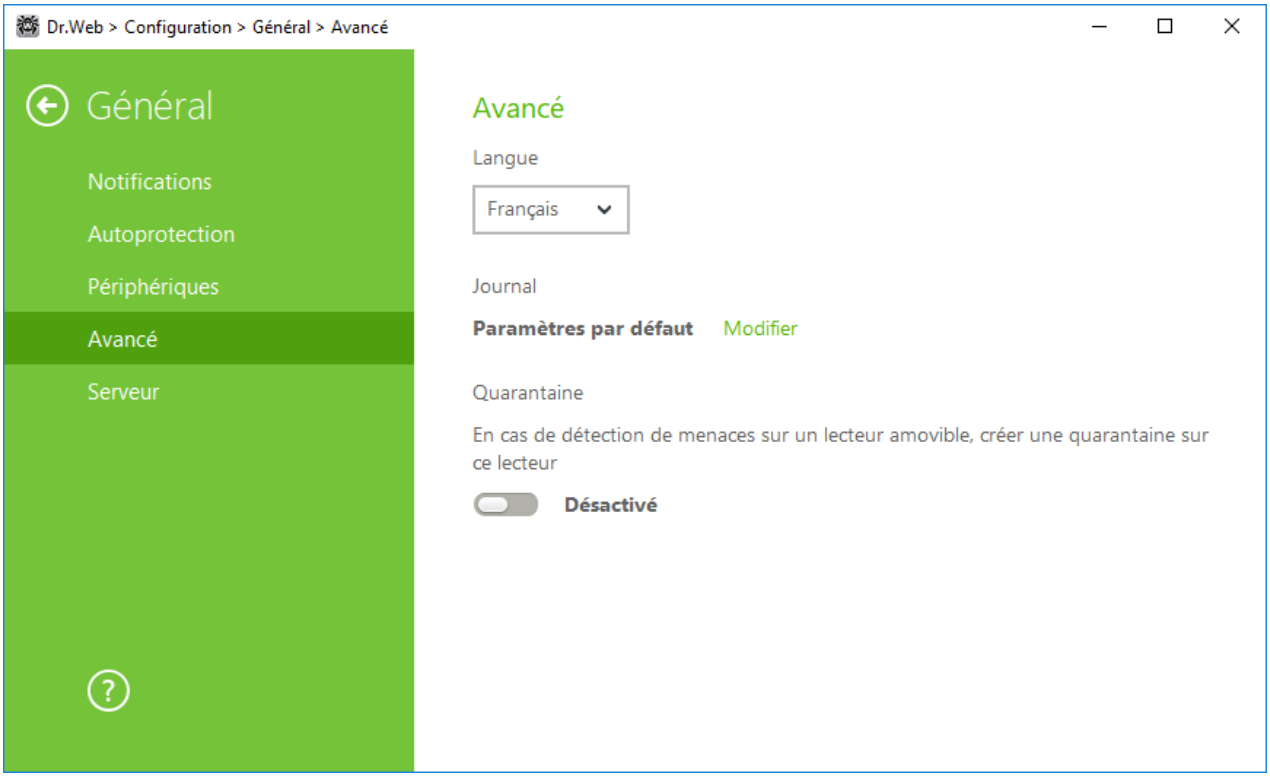

Figure 15. Paramètres avancés

Paramètres du Journal

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

La modification des paramètres de journalisation est impossible si l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web n'a pas autorisé de telles actions.

Par défaut, la taille des fichiers de journal est limitée à 10 Mo (pour le composant SpIDer Guard — 100 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 heures des mises à jour et des démarrages/arrêts de SpIDer Guard, les événements viraux, les noms des fichiers scannés, les noms des packers et le contenu des objets complexes analysés (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 des exclusions afin d'augmenter les performances de l'ordinateur.
SpIDer Mail	Les heures des mises à jour et des démarrages/arrêts de SpIDer Mail, les événements viraux, les paramètres d'interception des connexions, les informations sur les fichiers scannés, les noms des packers et le contenu des archives scannées. Il est recommandé d'utiliser ce mode lors du test des paramètres d'interception des connexions avec les serveurs de messagerie.
SpIDer Gate	Les heures des mises à jour et des démarrages/arrêts de SpIDer Gate, les événements viraux, les paramètres d'interception des connexions, les informations sur les fichiers scannés, les noms des packers et le contenu des archives scannées. Il est recommandé d'utiliser ce mode pour recevoir des informations plus détaillées sur les objets scannés et le fonctionnement de l'antivirus web.
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

	informations sur les noms des packers et sur le contenu des archives scannées.
Pare-feu	Pare-feu n'écrit pas le journal en mode standard. Si vous activez les journaux détaillés, le Pare-feu collecte des données sur les paquets réseau (pcap logs).
Mise à jour 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 serveur de protection centralisée.

Créer des dumps de mémoire

L'option **Créer des dumps de mémoire en cas d'erreurs de l'analyse** permet de sauvegarder les informations utiles sur le fonctionnement de plusieurs composants de Dr.Web. Cette option aide les spécialistes du support technique 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\ folder.

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 de l'administrateur de votre réseau antivirus.

1. Pour activer les journaux détaillés pour un composant Dr.Web, cochez la case correspondante.
2. 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.

8.5. Serveur

Dans cette rubrique, vous pouvez consulter et éditer les paramètres d'interaction de Dr.Web avec le serveur de protection centralisée ainsi que spécifier les paramètres du mode Mobile de Dr.Web. L'administrateur de votre réseau antivirus peut vous interdire de modifier les paramètres d'interaction avec le serveur. Dans ce cas, les boutons et les cases concernés seront indisponibles.

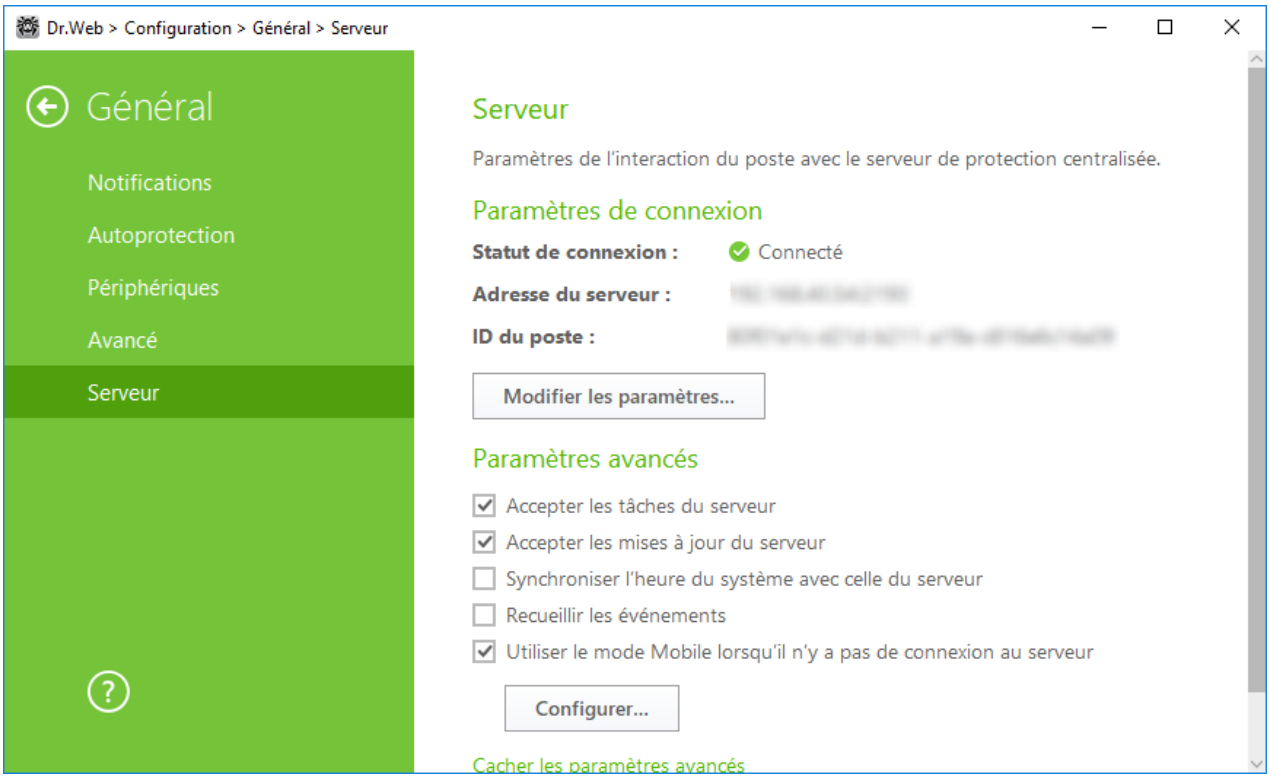

Figure 16. Paramètres de connexion au serveur

Paramètres de connexion

Dans le groupe **Paramètres de connexion** sont affichés :

- **Statut de connexion** : statut de connexion au serveur de protection centralisée ;
- **Adresse du serveur** : adresse du serveur de protection centralisée auquel le poste est connecté ;
- **ID du poste** : identificateur du poste utilisé pour la connexion au serveur.

Vous pouvez consulter et gérer les paramètres de connexion au serveur, si l'administrateur du réseau vous a accordé ces droits.

Toute modification des paramètres de connexion au serveur de protection centralisée doit être approuvée par l'administrateur de votre réseau antivirus, dans le cas contraire, votre ordinateur sera déconnecté du réseau antivirus.

Pour modifier les paramètres de connexion au serveur courant, ou afin de configurer une connexion avec un autre serveur, cliquez sur **Modifier les paramètres**. La fenêtre **Paramètres de connexion** sera ouverte.

Paramètres de connexion

Le tableau contient la liste de tous les serveurs auxquels le poste peut se connecter. Vous pouvez supprimer les serveurs du tableau et ajouter de nouveaux serveurs. Pour supprimer une ligne, cliquez sur  . Pour configurer la connexion à un autre serveur, cliquez sur  . Dans la fenêtre qui s'affiche, il faut spécifier l'adresse du serveur de protection centralisée fournie par l'administrateur.

Ajouter un certificat

La présence du certificat valide est la condition obligatoire de la connexion du poste au serveur de protection centralisée. Le certificat peut être unique pour chaque serveur, ou bien, il peut correspondre à plusieurs serveurs. Vous pouvez ajouter plusieurs certificats pour la connexion à plusieurs serveurs.

Par défaut, le certificat utilisé lors de l'installation du programme est indiqué s'il n'y a pas eu de remplacement planifié des clés de chiffrement. Si les clés sont remplacés, le dernier certificat généré sera affiché. Pour voir la liste des certificats disponibles ou ajouter un nouveau certificat, suivez le lien **Liste des certificats**.

Pour ajouter un nouveau certificat, cliquez sur  et, dans la fenêtre qui s'affiche, sélectionnez le fichier nécessaire.

Pour supprimer le certificat non utilisé, cliquez sur  .

Paramètres de connexion du poste

Pour modifier les paramètres de connexion du poste :

1. Dans la fenêtre **Paramètres de connexion du poste**, spécifiez l'identificateur du poste et le mot de passe pour la connexion au serveur. Ces informations sont fournies par l'administrateur du serveur.
2. Cliquez sur **OK** pour sauvegarder les modifications apportées.

Pour réinitialiser les paramètres de connexion et se connecter au serveur de protection centralisée en tant que novice :

1. Dans la fenêtre **Paramètres de connexion du poste**, cliquez sur **Réinitialiser les paramètres et se connecter en tant que novice**.
2. Dans la fenêtre qui s'ouvre, confirmez que vous voulez réinitialiser les paramètres de connexion au poste et vous connecter en tant que novice. Notez que cette action est irréversible.

3. Après la confirmation de l'enregistrement du poste sur le serveur de protection centralisée, Dr.Web recevra un nouvel identificateur de poste et le mot de passe. Ils seront utilisés pour la connexion au serveur.

Paramètres avancés

Dans le groupe **Paramètres avancés**, vous pouvez sélectionner les options suivantes :

- **Accepter les tâches du serveur** : pour recevoir périodiquement des tâches de l'administrateur.
- **Accepter les mises à jour du serveur** : pour recevoir des mises à jour régulières des composants de Dr.Web et des bases virales depuis le serveur de protection centralisée. Les mises à jour sont effectuées conformément aux paramètres spécifiés sur le serveur.
- **Synchroniser l'heure du système avec celle du serveur** : pour synchroniser l'heure système de votre ordinateur avec l'heure du serveur de protection centralisée. Dans ce mode, Dr.Web périodiquement, établie l'heure système sur votre ordinateur selon l'heure sur le serveur.
- **Recueillir les événements** : pour enregistrer les données sur les événements passés afin de les envoyer ultérieurement au serveur de protection centralisée. Une fois l'option activée, des informations ne sont pas transmises sur le serveur. Si la case n'est pas cochée et que la connexion au serveur n'est pas établie, des informations importantes (par exemple, sur les menaces détectées et des statistiques) seront perdues.
- **Utiliser le mode Mobile lorsqu'il n'y a pas de connexion au serveur** : pour les mises à jour régulières de base virales.

Si votre ordinateur n'est pas connecté au serveur de protection centralisée pendant une longue période, il est recommandé, pour recevoir les mises à jour régulières depuis les serveurs de Doctor Web, d'activer le mode mobile de fonctionnement de Dr.Web. Pour cela, cochez la case **Utiliser le mode Mobile lorsqu'il n'y a pas de connexion au serveur**.

La case **Utiliser le mode Mobile lorsqu'il n'y a pas de connexion au serveur** est disponible à condition que la **Modification de la configuration de l'Agent Dr.Web** soit autorisée sur le serveur de protection centralisée dans les droits de poste.

Dans le mode Mobile, Dr.Web tente de se connecter au serveur de protection centralisée, si les trois tentatives échouent, il réalise une mise à jour HTTP depuis les serveurs de Doctor Web. Les tentatives de détecter le serveur de protection centralisée sont permanentes avec un intervalle d'une minute.

Pour configurer les paramètres du mode Mobile, cliquez sur **Configurer**. La fenêtre **Mode mobile** apparaît.

Dans la liste déroulante **Périodicité des mises à jour**, vous pouvez sélectionner une périodicité avec laquelle la vérification des mises à jour sur les serveurs de Doctor Web sera réalisée.

Si, dans la liste **Périodicité des mises à jour**, l'option **Manuellement** est sélectionnée, les mises à jour automatiques ne seront pas effectuées. Vous pouvez lancer la mise à jour dans le menu de Dr.Web.

En cas d'utilisation d'un serveur proxy, cochez la case correspondante. Dans ce cas, les champs suivants sont activés :

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.

A la fin d'édition, cliquez sur **OK** pour enregistrer les modifications apportées ou sur **Annuler** pour quitter la fenêtre sans sauvegarder les modifications. Pour éditer les paramètres de connexion au serveur proxy, cliquez sur **Modifier** encore une fois.

Dans le mode mobile, uniquement les bases virales sont mis à jour.

Si vous décochez la case **Utiliser le mode Mobile lorsqu'il n'y a pas de connexion au serveur** n'est pas établie jusqu'à la reprise de la connexion au serveur de protection centralisée, les bases virales ne seront pas mises à jour, mais la recherche du serveur va continuer.

Toutes les modifications spécifiées pour le poste sur le serveur de protection centralisée seront prises en charge dès que la connexion de Dr.Web au serveur sera rétablie.

8.6. Messages du serveur

Pour plus de commodité de gestion des notifications sur le serveur de protection centralisée, l'administrateur du réseau a la possibilité d'activer l'envoi de messages sur le poste. Dans ce cas, la section **Messages du serveur** apparaîtra dans la fenêtre **Général**.

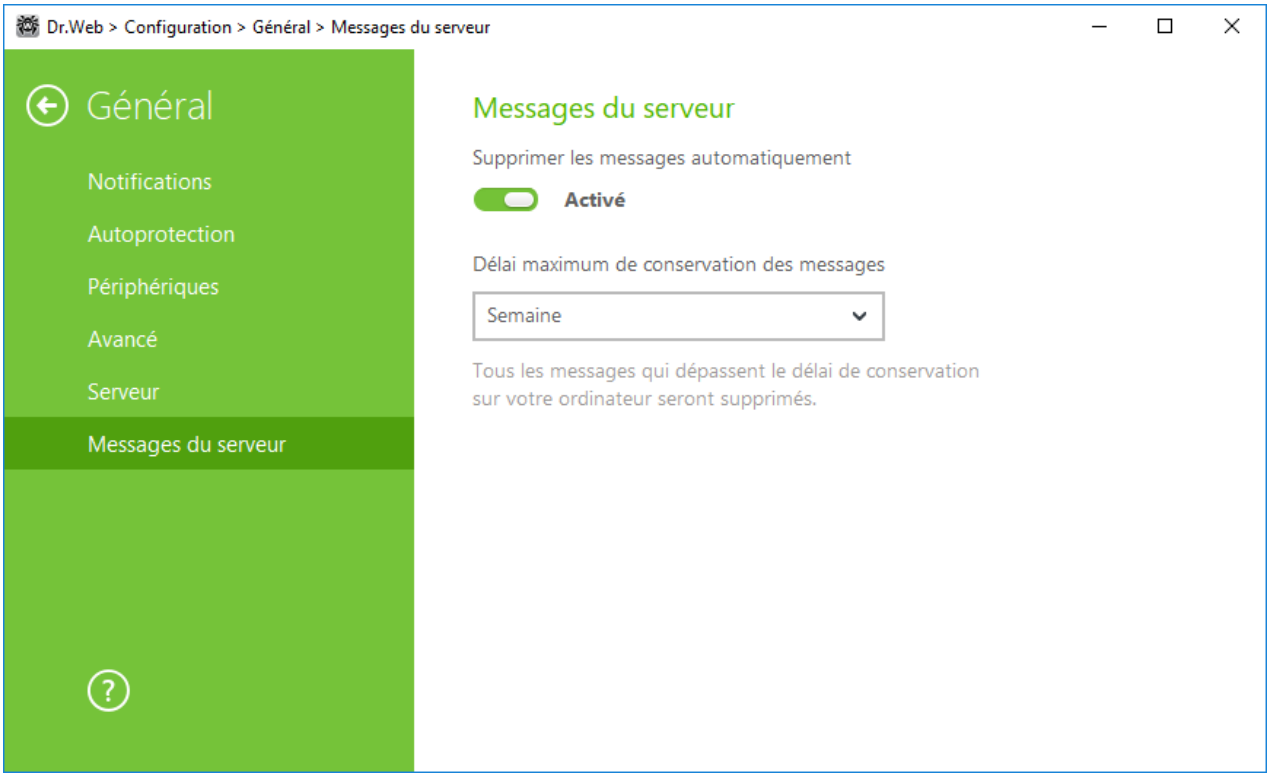

Figure 17. Paramètres de suppression automatique des messages du serveur

Vous pouvez spécifier les paramètres de suppression automatique des messages. Pour ce faire, activez l'option **Supprimer les messages automatiquement** et, dans l'élément **Délai maximum de conservation des messages**, dans la liste déroulante, sélectionnez le délai nécessaire. Les messages seront supprimés à l'expiration de ce délai.

9. Office Control

Le composant Office Control permet de gérer l'accès aux sites et aux fichiers et dossiers. Vous pouvez également programmer des limitations de durée d'utilisation d'Internet et de l'ordinateur pour différents comptes Windows.

Pour configurer Office Control, ouvrez le menu Dr.Web, lancez **Configuration** en mode administrateur et sélectionnez la section **Office Control**.

En restreignant l'accès au système de fichiers local, vous pouvez garantir l'intégrité de fichiers importants, les protéger contre les virus et préserver la confidentialité des données stockées. Il existe également la possibilité de protéger des fichiers séparés ou des dossiers entiers sur des disques locaux et sur des supports amovibles.

En contrôlant l'accès aux ressources web, vous pouvez empêcher les utilisateurs d'accéder à des sites indésirables (sites consacrés à la violence, jeux d'argent, etc.) ou autoriser l'accès à certains sites spécifiés dans les paramètres du module Office Control.

9.1. Configurer le module Office Control

La modification des paramètres du composant est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.

Pour accéder aux paramètres du module Office Control, 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 section Configuration.

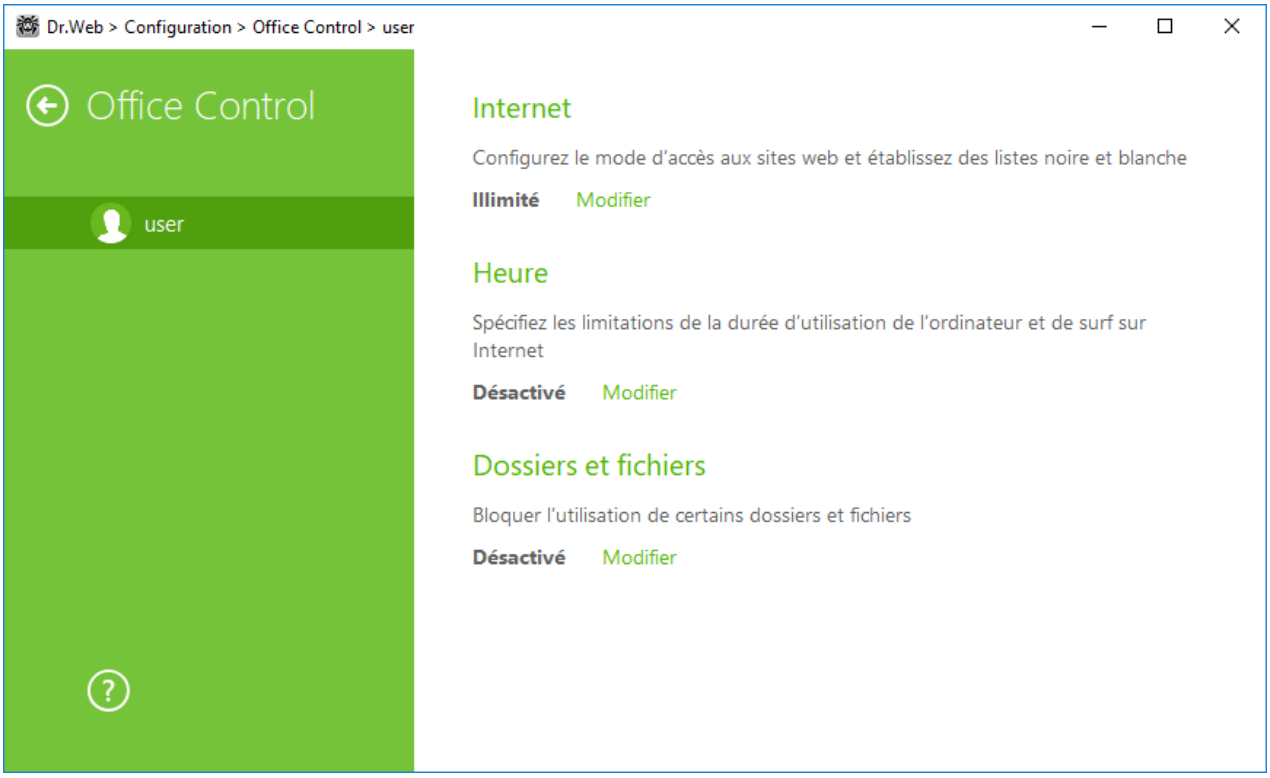

Figure 18. Paramètres du module Office Control

Configurer les paramètres du module Office Control pour les différents utilisateurs

Pour configurer une restriction d'accès pour un utilisateur, sélectionnez son nom dans le panneau de gauche. Dans la partie principale de la fenêtre, vous pouvez voir les paramètres configurés pour cet utilisateur. Par défaut, l'accès à Internet et aux ressources locales n'est restreint pour aucun utilisateur de l'ordinateur et aucune limitation de temps n'est spécifiée. Pour modifier ces paramètres, cliquez sur **Modifier** contre l'option choisie.

Les nouveaux utilisateurs sont affichés dans la liste uniquement après leur première connexion au compte.

Vous pouvez configurer les notifications sur les actions du module Office Control s'affichant sur le bureau.

9.1.1. Internet

Par défaut, le mode Illimité est défini pour chaque utilisateur. Par défaut, le mode **Sans restrictions** est défini pour tous les utilisateurs. Pour modifier ces paramètres, choisissez un autre mode dans le menu déroulant.

Bloquer par catégories

Le même site peut être inclus dans plusieurs catégories en même temps. Dans ce cas, le module Office Control bloque l'accès au site s'il est inclus au moins dans une catégorie pour bloquer l'accès.

Dans ce mode, vous pouvez sélectionner des sites web à bloquer par catégorie ou en fonction des listes blanche et noire complétées manuellement :

Catégorie	Description
Sites pour adultes	Sites au contenu pornographique ou érotique, sites de rencontres, etc.
Violence	Sites appelant à la violence, sites contenant les informations sur les accidents avec des victimes humaines, etc.
Armes	Sites consacrés aux armes et aux explosifs, sites contenant la description de fabrication d'explosifs, etc.
Jeux d'argent	Sites de jeux en ligne, casinos en ligne, sites d'enchères en ligne, sites de paris, etc.
Drogues	Sites faisant l'apologie de la production, distribution et consommation de drogues, etc.
Jeux en ligne	Sites de jeux nécessitant la connexion Internet permanente.
Terrorisme	Sites contenant de la propagande agressive, sites contenant les descriptions des attentats, etc.
Langage obscène	Sites contenant du langage obscène (dans des titres de sections, articles, etc.).
Tchats	Sites d'échange de messages en temps réel.
E-mail	Sites permettant de créer gratuitement une boîte e-mail.
Réseaux sociaux	Réseaux sociaux d'ordre général, réseaux d'entreprise, réseaux sociaux thématiques et des sites de rencontres thématiques.
Anonymiseurs	Sites permettant aux utilisateurs de masquer leurs informations personnelles et donnant accès à des sites bloqués.
Pools de minage de cryptomonnaies	Sites donnant accès aux services rassemblant les utilisateurs pour le minage de cryptomonnaies.

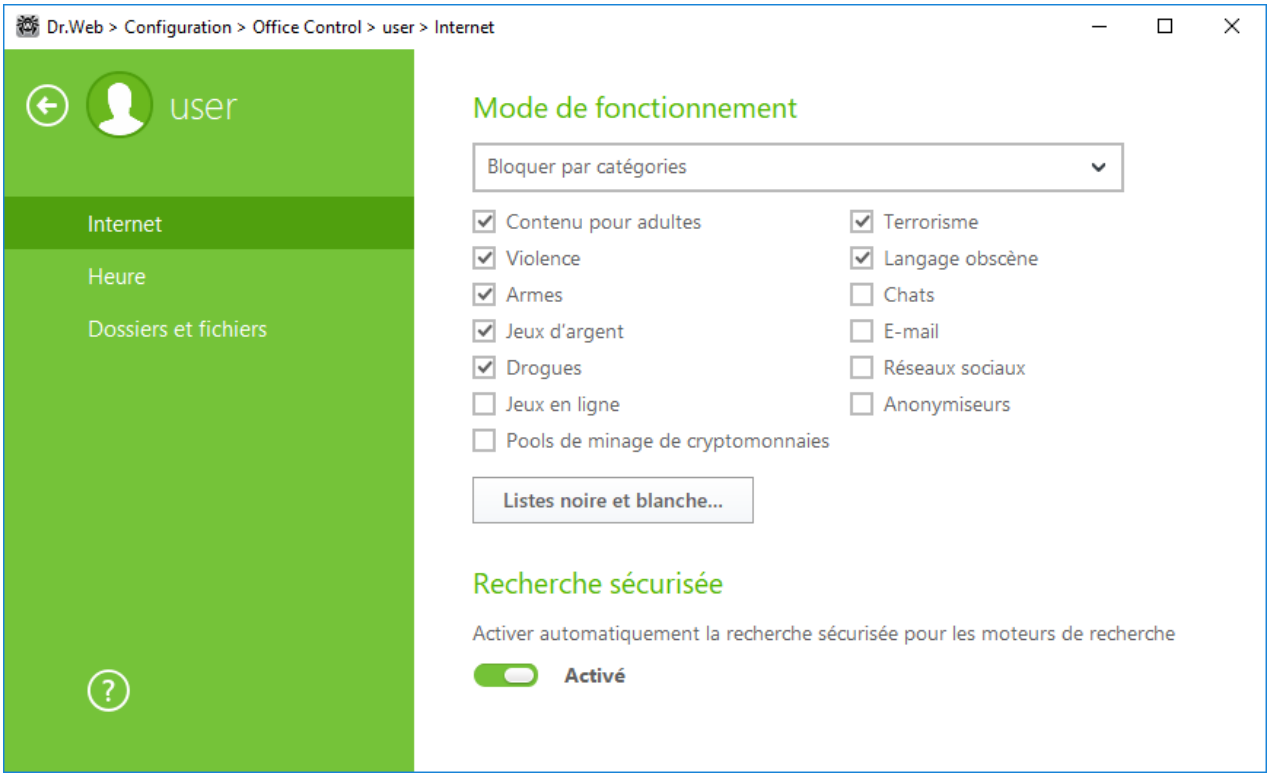

Figure 19. Configuration de l'accès à Internet par les catégories de sites

Pour interdire l'accès aux ressources de la catégorie nécessaire, cochez la case correspondante.

Dans ce mode, vous pouvez indiquer les sites auxquels l'accès sera autorisé ou interdit en fonction des autres limitations :

- Pour bloquer l'accès au site qui n'est inclus dans aucune catégorie mentionnée, ajoutez-le dans la liste noire.
- Pour forcer l'accès à un site, même s'il est inclus dans une des catégories indésirables, ajoutez-le dans la liste blanche.

Bloquer tout sauf les sites Web figurant sur la liste blanche

Dans ce mode, vous autorisez l'accès uniquement aux sites indiqués dans la liste blanche.

Recherche sécurisée

Dans tout les modes, sauf le mode **Illimité**, vous pouvez activer l'option **Recherche sécurisée** pour contrôler les résultat du moteur de recherche. Cette option permet d'exclure les pages web non sollicitées des résultats de recherche.

Pour activer la fonction **Recherche sécurisée**, faites basculer l'interrupteur dans la position **Activé**

Listes noire et blanche de sites

Dans cette fenêtre, vous pouvez établir la liste des sites auxquels l'accès sera autorisé ou bloqué quelles que soient les valeurs des autres paramètres du Office Control.

Pour gérer la liste blanche ou la liste noire, cliquez sur le bouton **Listes noire et blanche**.

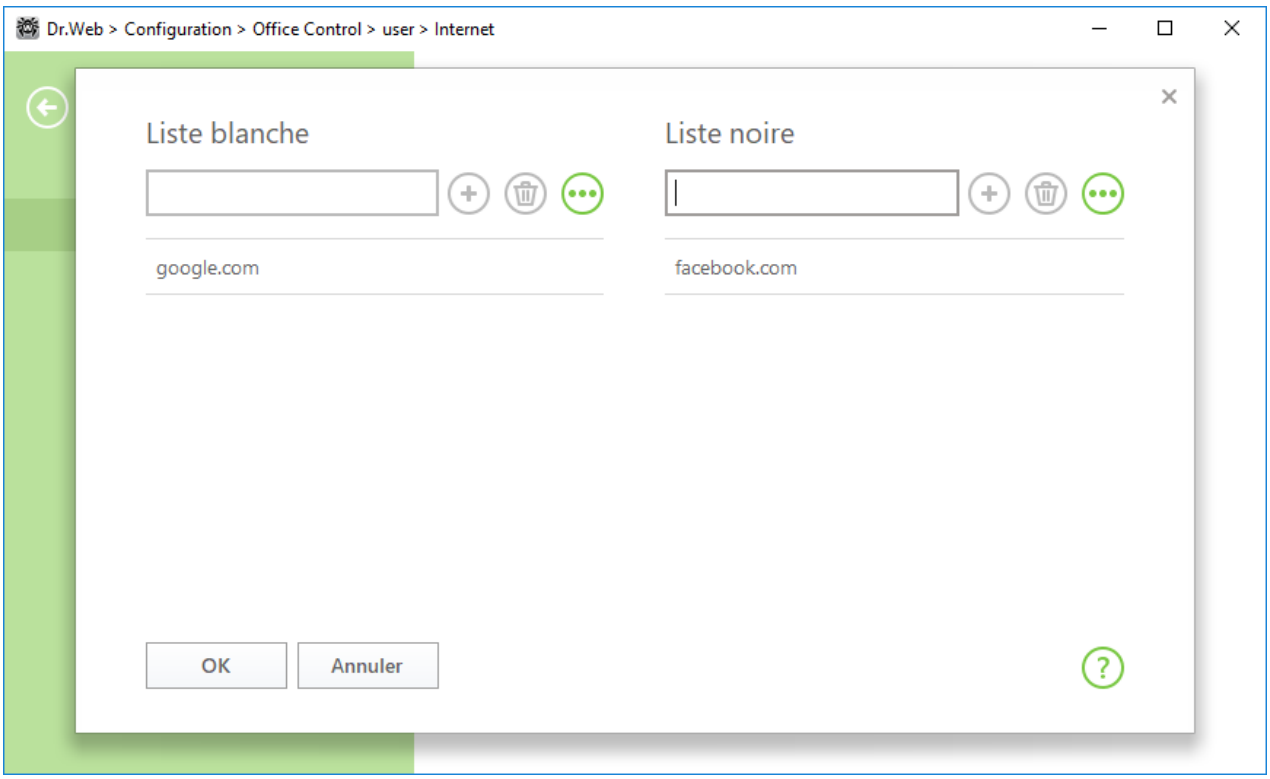

Figure 20. Formation de la liste blanche et la liste noire

Par défaut, les deux listes sont vides. Si cela est nécessaire, vous pouvez ajouter des adresses de sites à la liste blanche ou noire.

Configuration de la liste des adresses de domaines

1. Saisissez le nom de domaine ou une partie du nom de domaine du site dans le champ **Liste blanche** si vous voulez autoriser l'accès à ce site ou dans le champ **Liste noire** si vous voulez bloquer l'accès :
   - pour ajouter un site spécifique dans la liste, entrez son adresse (par exemple, `www.example.com`). Ceci configure l'accès à toutes les pages localisées sur ce site ;
   - pour autoriser l'accès aux sites dont les adresses comporte un certain texte, entrez ce texte dans le champ. Par exemple, si vous entrez `example`, ceci autorisera l'accès aux sites tels que example.com, example.test.com, test.com/example, test.example222.com etc ;
   - pour autoriser l'accès au domaine particulier, entrez le nom de domaine avec le caractère « . ». Cela autorisera l'accès à toutes les ressources se trouvant sur le domaine. Si le nom de domaine comporte le caractère « / », le substring avant le caractère « / » est considéré comme le nom de domaine alors que le substring après le caractère « / » est considéré comme une

partie de l'adresse autorisée sur ce domaine. Par exemple, si vous entrez `example.com/test`, les adresses example.com/test11, template.example.com/test22 etc. seront traités ;

- pour ajouter des sites particuliers aux exclusions, entrez dans le champ de saisie le masque les déterminant. Les masques sont ajoutés au format : `mask://...`

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

  - le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
  - le caractère « ? » remplace n'importe quel caractère (un seul caractère), y compris un caractère vide.

  Exemples :

  - `mask://*.com/` ou `.com` : tous les sites en zone .com ouvriront ;
  - `mask://mail` : tous les sites contenant le mot « mail » ouvriront ;
  - `mask://???.com` ou `.com` : tous les sites en zone .com dont les noms comprennent 3 caractères ou moins ouvriront.

La ligne entrée peut être simplifiée. Par exemple : l'adresse http://www.example.com sera convertie au format www.example.com.

2. Pour ajouter l'adresse dans la liste, cliquez sur  .
3. Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur  .
4. Pour ajouter d'autres sites web, répétez les étapes 1 et 2.

9.1.2. Heure

Sur cette page, vous pouvez configurer les restrictions de la durée de l'utilisation de l'ordinateur et du surf sur Internet.

Par défaut, les utilisateurs sont autorisés à utiliser l'ordinateur et Internet de manière illimitée.

Vous pouvez spécifier la restriction de la durée de l'utilisation de l'ordinateuren utilisant le tableau aux carrés temporaires.

Pour configurer les limitations de temps en mode de tableau

1. Sélectionnez les jours de la semaine et les heures durant lesquelles vous souhaitez interdire le surf sur Internet, et marquez les carrés temporaires nécessaires par le bleu. :
   - pour marquer un intervalle de temps, cliquez une fois dessus avec le bouton gauche de la souris ;
   - pour marquer plusieurs intervalles de temps, cliquez une fois sur le premier et sélectionnez le reste des cases en maintenant le bouton gauche de la souris appuyé.
2. Choisissez les jours de la semaine et les heures durant lesquels l'utilisateur ne pourra pas utiliser l'ordinateur et marquez les carrés correspondants par le rouge :
   - pour marquer un intervalle de temps, double-cliquez dessus ;

- pour marquer plusieurs intervalles, double-cliquez sur le premier carré, puis sélectionnez les autres en maintenant le bouton gauche de la souris appuyé.

Vous pouvez également créer des configurations différentes pour un utilisateur en les sauvegardant dans des profils. Cette option sera utilise, si vous avez besoin de changer des paramètres de temps en temps (par exemple, spécifier les restrictions pendant l'année scolaires et pendant les vacances).

Création et modification du profil de paramètres

Vous pouvez modifier le profil de paramètres utilisateur ou créer un nouveau profil.

1. Pour créer un nouveau profil, cliquez sur ⊕ et spécifiez le nom de profil. Cliquez sur **OK**.
2. Pour modifier le profil utilisateur, sélectionnez-le dans la liste.
3. Ensuite, apportez les modifications nécessaires dans le tableau.

Si vous sélectionnez le profil **Illimité** et que vous apportez les modifications dans le tableau, le profil sera automatiquement remplacé par le profil utilisateur.

9.1.3. Dossiers et fichiers

Par défaut, il n'y a aucune limitation d'accès aux fichiers et dossiers. Pour configurer les limitations, activez l'option correspondante et cliquez sur **Objets**.

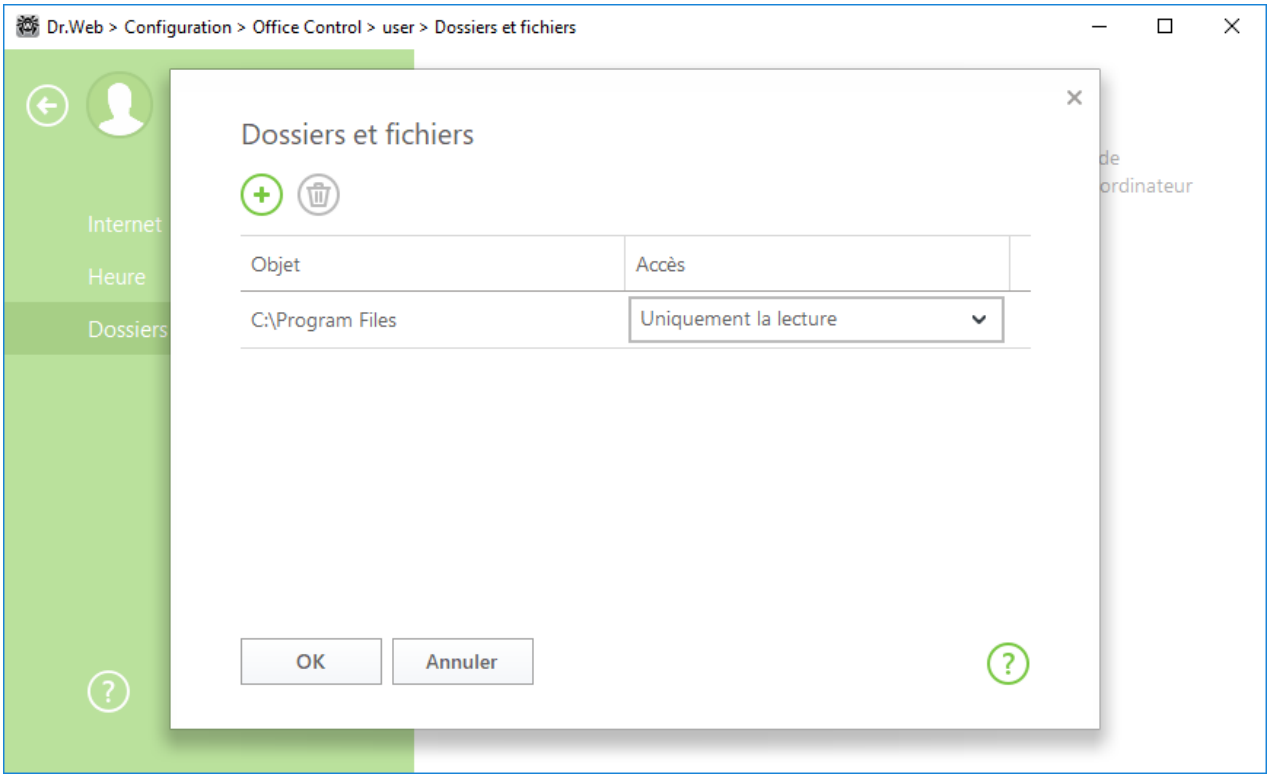

Figure 21. Gestion de l'accès aux fichiers et dossiers

Pour ajouter un objet dans la liste, cliquez sur ⊕ et sélectionnez le fichier ou le dossier nécessaire. Par défaut, l'objet ajouté sera accessible seulement pour la lecture.

Pour bloquer complètement l'accès à l'objet sélectionnée, cliquez sur la limitation spécifiée et sélectionnez **Bloqué** dans la liste déroulante.

Pour supprimer l'objet, sélectionnez-le dans la liste et cliquez sur  .

Veuillez noter que le blocage d'accès n'est pas garanti lors du chargement de l'ordinateur depuis les supporta amovibles ou lors de l'appel aux objets spécifiés depuis un autre système d'exploitation installé sur l'ordinateur.

10. Exclusions

Dans cette section, vous pouvez configurer les exclusions des analyses par les composants SpIDer Guard, SpIDer Gate, SpIDer Mail et Scanner et ajouter des adresses d'expéditeurs dans la liste noire ou blanche pour que les messages qu'ils envoient ne soient pas analysé pour la présence de spam.

Pour configurer les exclusions, ouvrez le menu, lancez **Configuration** en mode administrateur et sélectionnez la section **Exclusions**.

> Veuillez noter que l'administrateur de votre réseau antivirus peut empêcher la modification de ces paramètres.

Pour configurer l'accès aux sites qui ne sont pas recommandés par Doctor Web, sélectionnez la section Sites Web.

Pour exclure certains fichiers ou dossiers du scan, sélectionnez la rubrique Dossiers et fichiers.

Pour exclure certains processus du scan de composants de Dr.Web sélectionnez la rubrique Applications.

Pour configurer l'analyse antispam par SpIDer Mail sélectionnez la rubrique Antispam.

10.1. Sites

Si vous souhaitez accéder aux sites web qui ne sont pas recommandés par Doctor Web, ajoutez-les aux exclusions. L'accès aux sites web listés sera autorisé, mais les sites seront tout de même vérifiés. Par défaut, la liste est vide. Si vous ajoutez un site à la liste blanche, les utilisateurs pourront y accéder quels que soient les paramètres de SpIDer Gate. Veuillez noter que si le site est ajouté à la liste blanche et à la liste noire du Office Control ainsi qu'aux exclusions, l'accès sera bloqué.

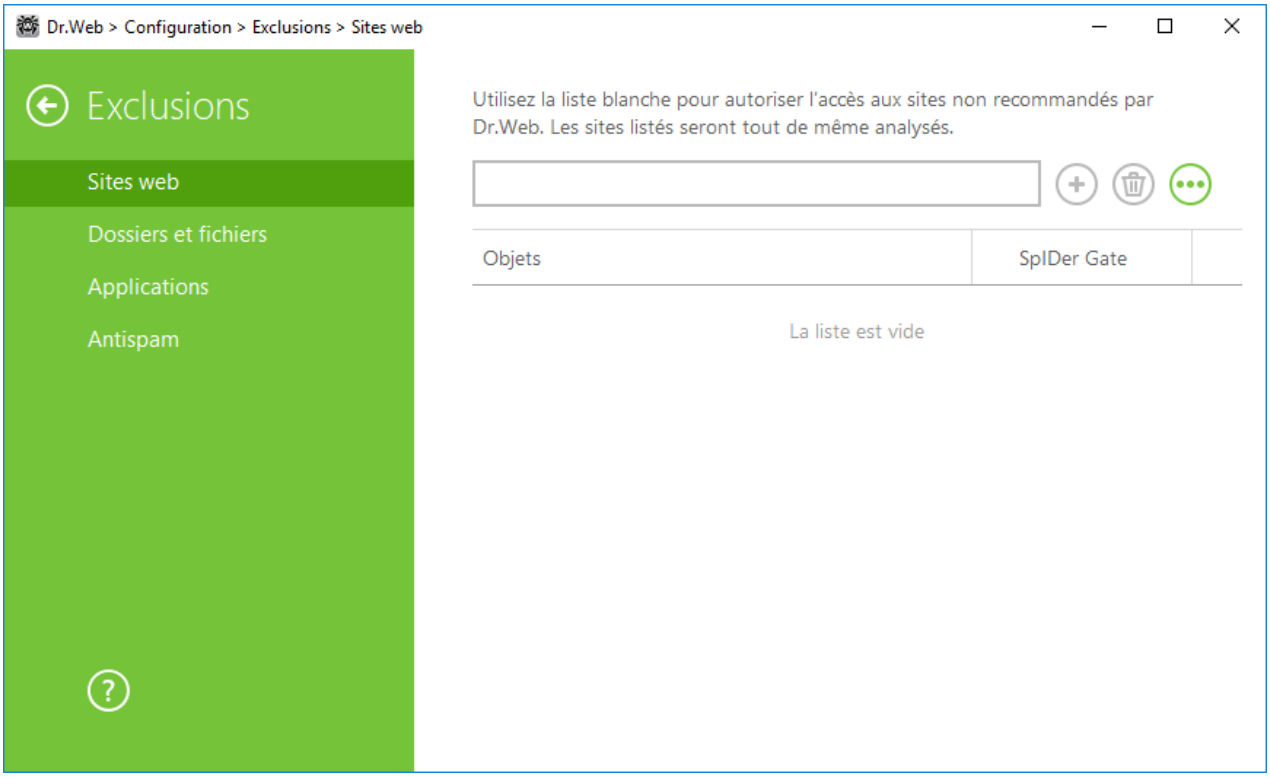

Figure 22. Exclusion de sites

Configuration de la liste des adresses de domaines

1. Entrez le nom de domaine ou une partie du nom de domaine du site auquel vous voulez autoriser l'accès sans tenir compte des autres restrictions :
   - pour ajouter un site spécifique, entrez son nom complet (par exemple, `www.example.com`). Ceci autorise l'accès à toutes les pages de ce site ;
   - pour autoriser l'accès aux sites dont l'adresse contient un texte spécifique, entrez ce texte dans le champ. Par exemple, si vous entrez `example`, ceci autorisera l'accès aux sites tels que `example.com`, `example.test.com`, `test.com/example`, `test.example222.com` etc. ;
   - pour autoriser l'accès aux sites d'un domaine particulier, entrez le nom de domaine avec un point (« . »). Si le nom de domaine comporte un symbole (« / »), le substring avant le symbole « / » est considéré comme un nom de domaine alors que le substring après le symbole « / » est considéré comme une partie de l'adresse des sites que vous souhaitez autoriser dans ce domaine. Par exemple, si vous entrez `example.com/test`, ceci autorisera l'accès aux sites tels que `example.com/test11`, `template.example.com/test22` etc. ;
   - pour ajouter des sites particuliers aux exclusions, entrez dans le champ de saisie le masque les déterminant. Les masques sont ajoutés au format : `mask://...`

     Un masque désigne les éléments communs aux noms des objets, ainsi :
     - le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
     - le caractère « ? » remplace n'importe quel caractère (un seul caractère), y compris un caractère vide.

Exemples :

- `mask://*.com` : tous les sites en zone .com ouvriront ;
- `mask://mail` : tous les sites contenant le mot « mail » ouvriront ;
- `mask://???.com` : tous les sites en zone .com dont les noms comprennent 3 caractères ou moins ouvriront.

La ligne entrée peut être simplifiée. Par exemple : l'adresse http://www.example.com sera convertie au format www.example.com.

2. Cliquez sur . L'adresse apparaîtra dans la liste.
3. Pour ajouter d'autres adresses, répétez les étapes 1 puis 2. Pour supprimer une adresse de la liste blanche, sélectionnez l'élément nécessaire dans la liste et cliquez sur .

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.
- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

10.2. Dossiers et fichiers

Dans cette section, vous pouvez spécifier la liste des fichiers et dossiers qui sont exclus du scan de SpIDer Guard et de 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.

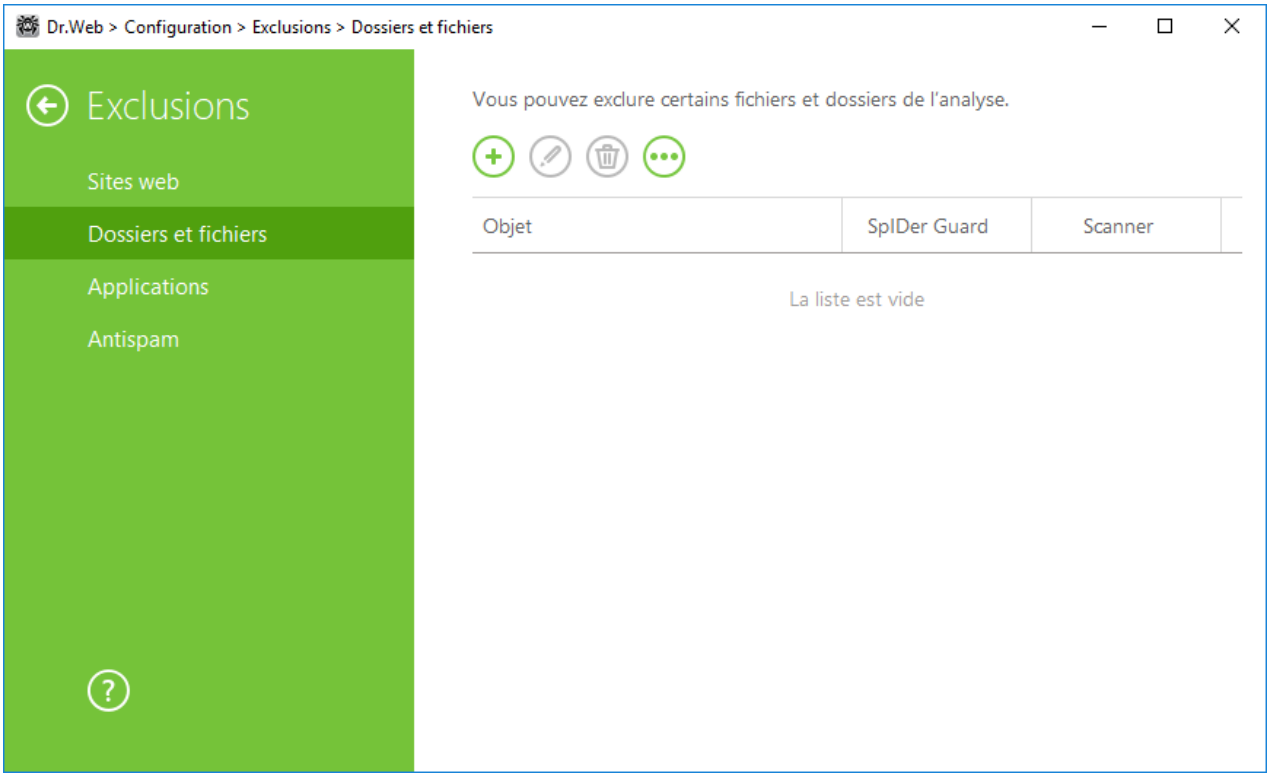

Figure 23. Exclusion des fichiers et des dossiers de l'analyse

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 le 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 . Par exemple :
     - `C:\folder\file.txt` : exclut de l'analyse le fichier file.txt se trouvant dans le dossier C:\folder.
     - `C:\folder` : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier C:\folder.
   - pour exclure de l'analyse un 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 . Par exemple :
     - `file.txt` : exclut de l'analyse tous les fichiers avec le nom file et l'extension .txt dans tous les dossiers.
     - `file` : exclut de l'analyse tous les fichiers avec le nom file sans extension dans tous les dossiers.
   - pour exclure du scan des fichiers ou des dossiers du type particulier, entrez le masque qui les détermine dans le champ de saisie.

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

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

Exemples :

- rapport*.doc : un masque qui désigne tous les documents Microsoft Word dont les noms commencent par le mot « rapport », par exemple, les fichiers rapport-fevrier.doc, rapport121209.doc etc. ;
- *.exe : un masque qui désigne tous les fichiers exécutable ayant l'extension EXE, par exemple, setup.exe, iTunes.exe etc. ;
- photo????09.jpg : un masque qui désigne tous les fichiers des images au format JPG dont le nom commence par « photo » et se termine par « 09 », dans ce cas entre ces deux fragments, dans le nom de fichier, il y a quatre n'importe quels symboles, par exemple photo121209.jpg, photopapa09.jpg ou photo----09.jpg.
- 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.
- C:\folder** : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier C:\folder. Cependant les fichiers dans les sous-dossiers seront scannés.
- 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.

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  .

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.

- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

10.3. Applications

Dans cette section, vous pouvez spécifier la liste des programmes et des processus à exclure du scan de SpIDer Guard, SpIDer Gate et SpIDer Mail.

Par défaut, la liste est vide.

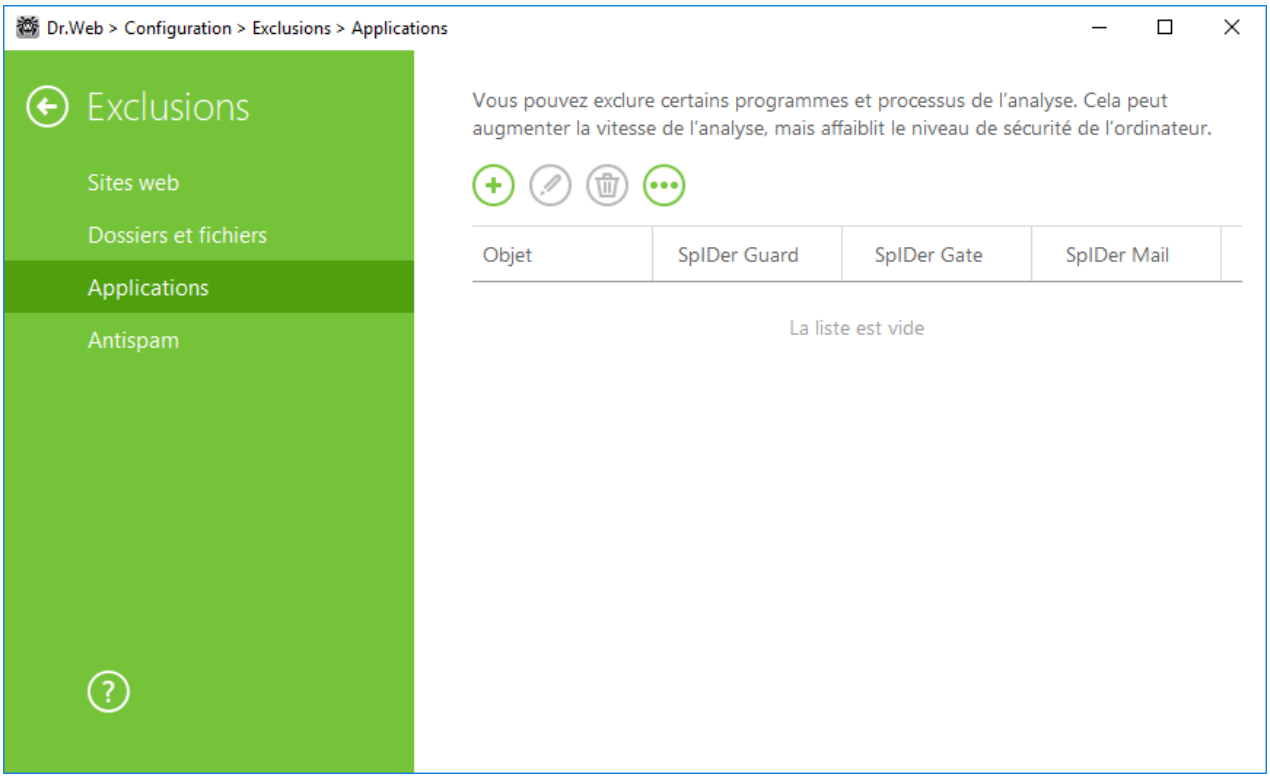

Figure 24. Liste des applications à exclure

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 de saisie . Par exemple :

     `C:\Program Files\folder\example.exe`
   - 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 des applications du type particulier, entrez le masque qui les détermine dans le champ de saisie

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

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

Exemples de configuration des exclusions :

- `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.

- 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. Par exemple :

- `%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`.

2. Dans la fenêtre de configuration, indiquez les composants qui ne doivent pas analyser l'application sélectionnée. Pour les objets exclus de l'analyse par les composants SpIDer Gate et SpIDer Mail, indiquez les conditions supplémentaires.

Paramètre	Description
Indépendamment de la présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan indépendamment de la présence de la signature numérique.

Paramètre	Description
En cas de présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan uniquement en cas de présence de la signature numérique d'application. Sinon l'application sera scannée par les composants.
Tout trafic	Sélectionnez ce paramètre pour exclure du scan le trafic chiffré et non chiffré de l'application.
Trafic chiffré	Sélectionnez ce paramètre pour exclure du scan seulement le trafic chiffré de l'application.
Via toutes les adresses IP et tous les ports	Sélectionnez ce paramètre pour exclure du scan le trafic acheminé vers toutes les adresses IP et tous les ports.
Via les adresses IP et les ports indiqués	Sélectionnez ce paramètre pour indiquer les adresses IP et les ports dont le trafic sera exclu du scan. Le trafic acheminé des autres adresses IP et des ports sera scanné (s'il n'est pas exclu par un autre paramètre).
Spécifier des adresses et des ports	Pour configurer les exclusions de manière précise, utilisez les recommandations suivantes : • pour exclure de l'analyse un domaine particulier par un port particulier, indiquez, par exemple, `site.com:80` ; • pour exclure de l'analyse le trafic par un port non standard (par exemple, 1111) il faut indiquer : `*:1111` ; • pour exclure de l'analyse le trafic du domaine par n'importe quel port, indiquez : `site:*`

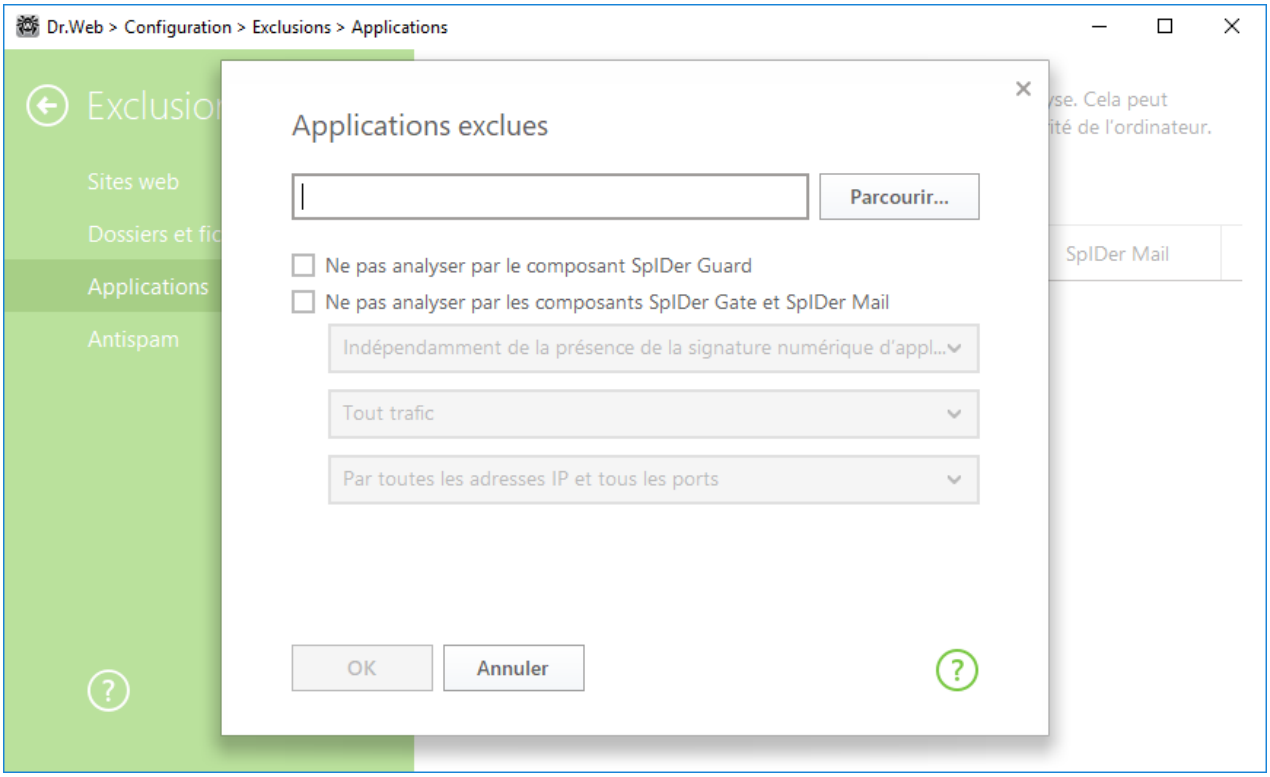

Figure 25. Exclusion d'applications

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.

Gestion des objets dans la liste

Pour éditer une exclusion, sélectionnez l'élément nécessaire dans la liste et cliquez sur . Pour supprimer une application de la liste des exclusions, sélectionnez l'élément nécessaire dans la liste et cliquez sur .

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.
- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

10.4. Antispam

Dans cette fenêtre vous pouvez spécifier les listes d'expéditeurs dont les messages seront exclus de l'analyse pour la présence de spam. Le composant SpIDer Mail saute ces messages ou les considère comme spam sans analyse.

Si vous ajoutez une adresse à la blanche liste, les messages de l'expéditeur seront toujours délivrés à la messagerie. Si l'adresse de l'expéditeur figure dans la noire liste, les messages provenant de cette adresse seront classés comme spam sans aucune analyse complémentaire. Les deux listes sont vides par défaut.

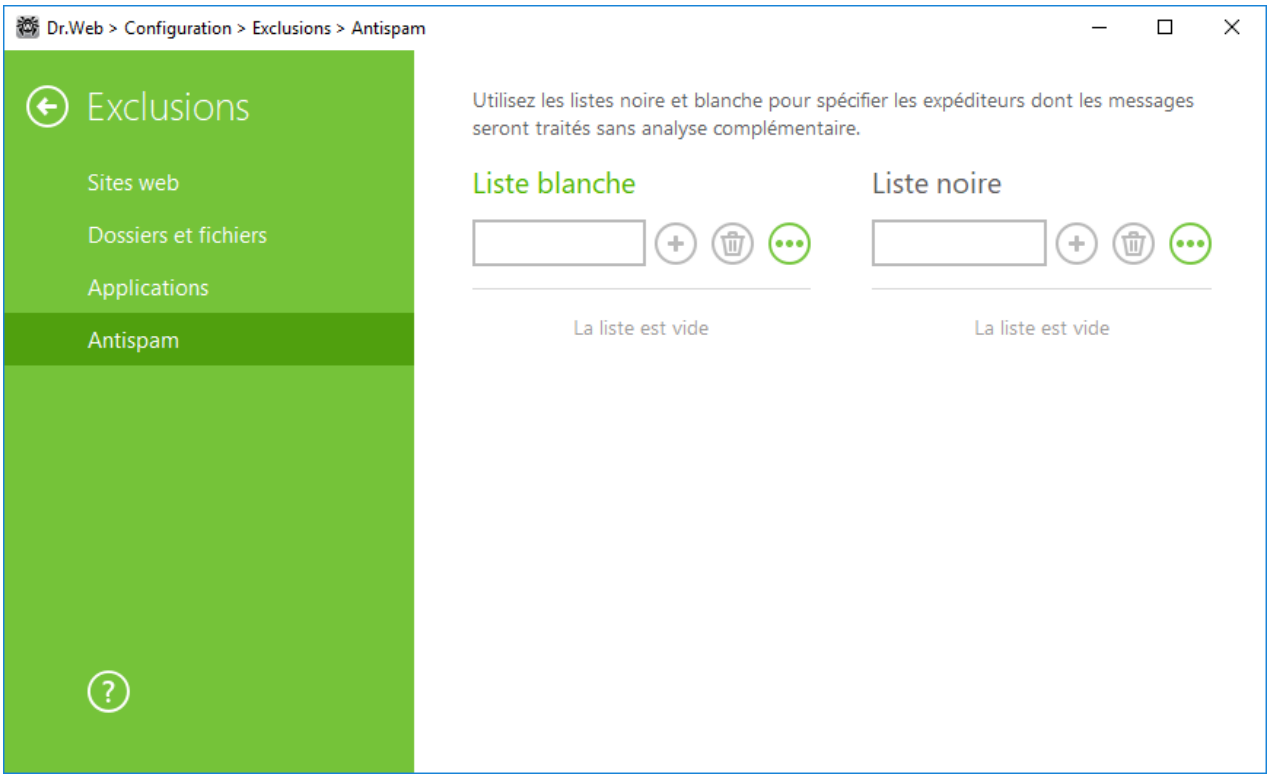

Figure 26. Exclusion d'adresses e-mail

Pour configurer les listes antispam, procédez comme suit

1. Entrez un e-mail ou un masque pour les adresses des expéditeurs dont vous souhaitez recevoir les messages sans qu'ils soient analysés. Méthodes d'entrée :
   - pour ajouter un expéditeur spécifique, entrez l'adresse e-mail complète (par exemple, `ami@mail.com`). Ceci assure la délivrance automatique de tous les messages de cet expéditeur sans analyse ;
   - pour ajouter des expéditeurs ayant un nom similaire, remplacez les éléments qui diffèrent dans leur adresse par les caractères « `*` » et « `?` ». Utilisez le symbole « `*` » pour substituer n'importe quel ensemble de symboles ou bien le symbole « `?` » pour substituer un symbole unique. Par exemple, si vous entrez `ami*@mail.com`, SpIDer Mail délivrera sans les scanner les messages des expéditeurs comme ami@mail.com, ami1@mail.com, ami_à_moi@mail.com et ceux des expéditeurs ayant le même type de noms ;
   - pour assurer la délivrance ou bloquer des messages envoyés depuis n'importe quelle adresse e-mail contenue dans un domaine concret, utilisez le signe « `*` » à la place du nom de l'utilisateur. Par exemple, pour spécifier tous les messages provenant du domaine mail.com entrez `*@mail.com`.
2. Pour ajouter l'adresse saisie à la liste, cliquez sur  .

3. Pour ajouter d'autres adresses, répétez les étapes 1 et 2. Pour supprimer une adresse de la liste, sélectionnez l'élément correspondant dans la liste et cliquez sur  .

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.
- **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

11. Composants de protection

Les composant de protection assure le scan du système, l'analyse des messages pour la présence de menaces et du spam, le contrôle des connexions réseau et du trafic HTTP.

Pour configurer les composants de protection, ouvrez le menu , lancez **Configuration** en mode administrateur et sélectionnez la section **Composants de protection**.

> La configuration des composants est possible uniquement avec les privilèges d'administrateurs.

Pour configurer le scan des fichiers ou des processus en cours, allez à l'onglet SpIDer Guard.

Pour configurer l'analyse du trafic HTTP, sélectionnez SpIDer Gate.

Pour configurer l'analyse du courrier, sélectionnez SpIDer Mail.

Pour contrôler les connexions et le transfert de données via Internet et pour bloquer les connexions suspectes au niveau des paquets et des applications, allez à l'onglet Pare-feu.

Pour configurer les paramètres généraux de scan de fichiers et d'objets différents et les réactions à la détection des fichiers infectés, suspects ou des programmes malveillants, sélectionnez Scanner.

Pour contrôler les applications tierces, sélectionnez la section Protection préventive.

11.1. 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 analyse 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. Pour prévenir la pénétration des objets malveillants diffusés via le courrier électronique sur votre ordinateur, utilisez SpIDer Mail.

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.

Une incompatibilité de Dr.Web avec MS Exchange Server peut avoir lieu. En cas de problème d'incompatibilité, ajoutez les bases de données et le journal des transactions de MS Exchange Server dans la liste des exclusions de SpIDer Guard.

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

11.1.1. Configurer SpIDer Guard

La modification des paramètres du composant est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.

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 section Configuration.

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

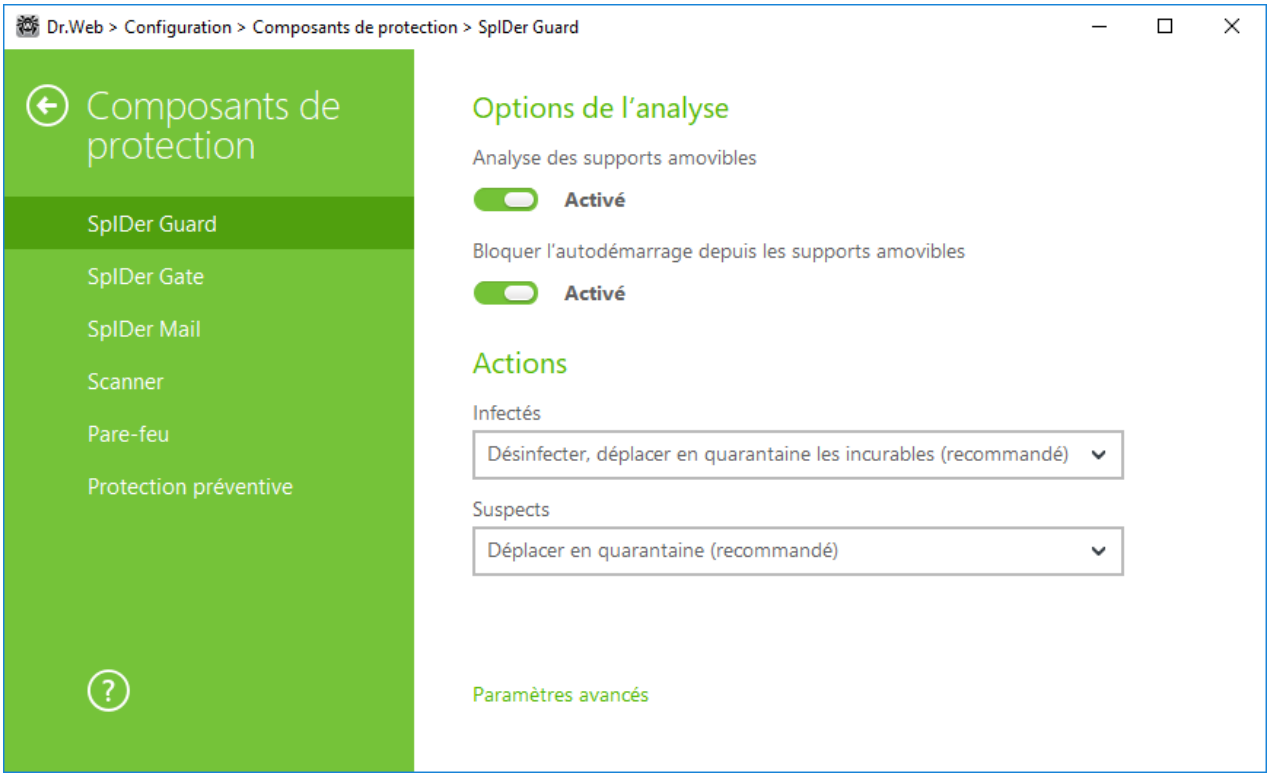

Figure 27. Configuration de SpIDer Guard

Options de l'analyse

SpIDer Guard analyse par défaut les fichiers ouverts, modifiés et lancés sur les supports amovibles (disques CD/DVD, clés USB, 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. Si ces options sont désactivées, les objets sur les supports amovibles ne seront pas analysés.

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'autodémarrage 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 :

- **Infectés** : objets infectés par un virus connu et (supposé) curable ;
- **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**.

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

Par défaut, SpIDer Guard essaie de désinfecter les fichiers qui sont infectés par un virus connu et considéré comme curable, tandis que les autres objets qui sont considérés comme les plus dangereux sont placés en Quarantaine. Les canulars, les hacktools et les riskwares sont ignorées par défaut. Les réaction de SpIDer Guard sont similaires aux réactions correspondantes 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 uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).

Action	Description
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 uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
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.
Notifier	Afficher une notification et laisser passer l'objet sans appliquer aucune action. Cette réaction est disponible uniquement pour les objets suspects et les programmes malveillants.

⚠ SpIDer Guard n'analyse pas les objets complexescomme les archives, les boîtes e-mails ou les conteneurs de fichiers. 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 ;

Paramètre	Description
	• 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 programme malveillant et par défaut le déplace en Quarantaine.

Détails et recommandations

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 le groupe de paramètres **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.

Paramètres avancés

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) ;
- l'analyse des scripts exécutés par Windows Script Host et PowerShell (pour Windows 10).

Analyse heuristique

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

Scan Anti-rootkit en tâche de fond

Le composant Anti-rootkit intégré à Dr.Web offre des fonctions de scan en tâche de fond du système d'exploitation à la recherche de menaces complexes ainsi que des fonctionnalités de traitement des infections actives lorsque c'est nécessaire.

Si cette option est activée, Antirootkit Dr.Web réside de manière permanente en mémoire. A la différence du scan à la volée des fichiers effectué par SpIDer Guard, le scan des rootkits (programmes malveillant utilisés pour dissimuler les modifications apportés dans l'OS telles que le fonctionnement de certains processus, la modification des clés de la base de registre, des dossiers et fichiers) inclut la vérification des objets autorun, des processus et des modules en cours, de la mémoire vive (RAM), des disques MBR/VBR, du BIOS de l'ordinateur et d'autres objets système.

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 Antirootkit Dr.Web détecte une menace, il notifie l'utilisateur et neutralise l'activité malveillante.

⚠ Durant l'analyse en tâche de fond pour la présence 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.

11.2. SpIDer Gate

SpIDer Gate est un moniteur antivirus HTTP. Par défaut, SpIDer Gate analyse automatiquement le trafic HTTP entrant et bloque tous les objets malveillant. L'HTTP est utilisé par les navigateurs, les

gestionnaires de téléchargement et d'autres applications qui échangent des données avec des serveurs web, c'est-à-dire qui travaillent avec Internet.

Vous pouvez configurer les paramètres de SpIDer Gate pour désactiver l'analyse du trafic entrant, ajouter à l'analyse le trafic sortant ou dresser une liste des applications pour lesquelles le trafic HTTP sera toujours analysé. Il existe également la possibilité d'exclure certaines applications de l'analyse.

Par défaut, SpIDer Gate bloque tous les objets malveillants transmis par le réseau. Le filtrage d'URL des sites non recommandés et des sites connus comme sources des virus est également activé par défaut.

SpIDer Gate ne supporte pas l'analyse des connexions sécurisées, ça veut dire qu'il n'analyse pas les données transmises via les protocoles cryptographiques.

SpIDer Gate se lance automatiquement au démarrage de Windows et réside en mémoire.

11.2.1. Configurer SpIDer Gate

La modification des paramètres du composant est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.

Pour accéder aux paramètres de SpIDer Gate, 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 Configuration.

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

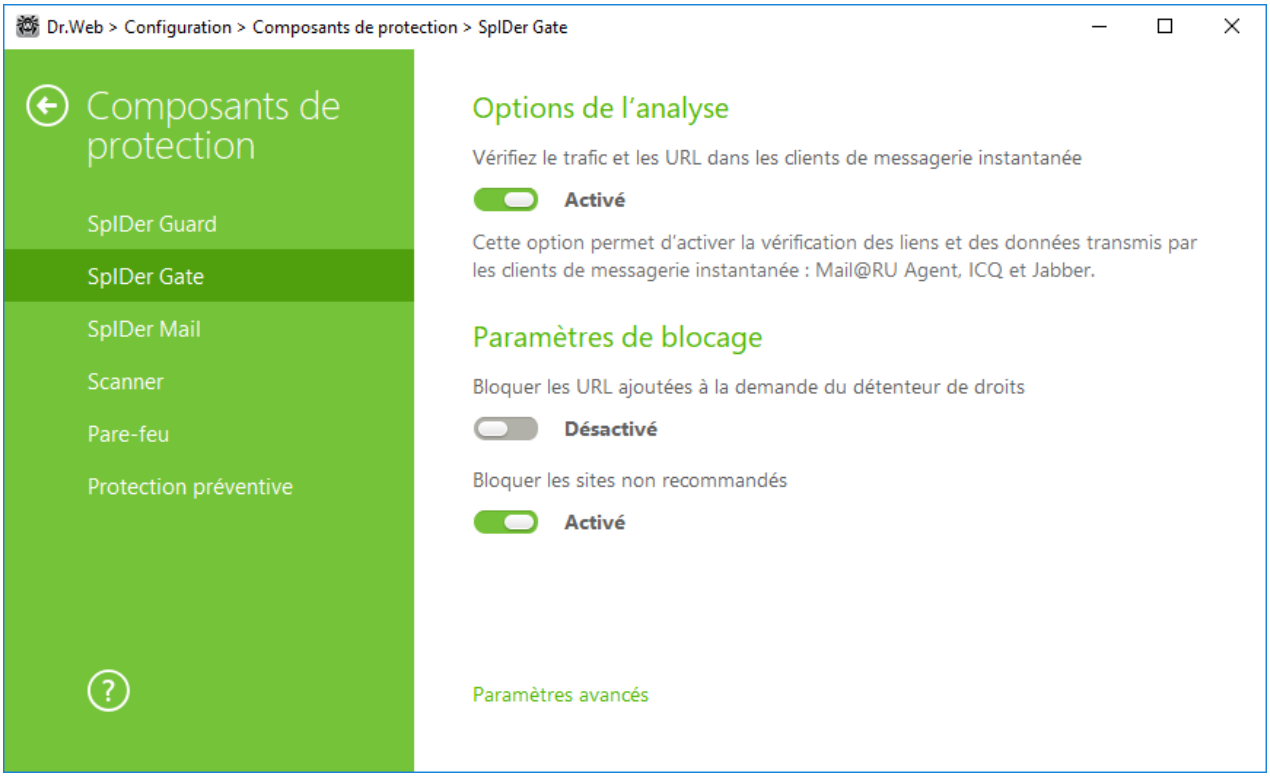

Figure 28. Configuration de SplDer Gate

Analyse du trafic des clients IM

Dans le groupe **Options de l'analyse**, vous pouvez activer l'analyse des liens et des données transmis par les clients de messagerie instantanée (Mail.ru Agent, ICQ et les clients utilisant le protocole Jabber). C'est uniquement le trafic entrant qui est analysé. L'option est activée par défaut.

Les liens transmis dans les messages sont analysés selon les paramètres de SplDer Gate : les liens vers les sites connus comme sources de virus sont automatiquement bloqués, les liens vers les sites non recommandés et les URL ajoutées selon la demande du détenteur de droits sont bloqués si les options correspondantes sont activées dans la rubrique **Paramètres de blocage**. Dans ce cas, la liste blanche des sites et les applications exclues de l'analyse sont pris en compte.

Les fichiers transmis par les messageries instantanées sont également vérifiés. Lorsqu'une menace est détectée, la transmission de fichiers est bloquée si l'option correspondante est activée dans la section **Bloquer les programmes**. Les virus sont bloqués automatiquement si l'option **Vérifiez le trafic et les URL dans les clients de messagerie instantanée** est activée.

Paramètres de blocage

Dans le groupe **Paramètres de blocage**, vous pouvez établir le blocage automatique d'accès aux URL ajoutées sur la demande du détenteur de droits (pour cela, activez l'option correspondante), ainsi que de bloquer l'accès aux sites non recommandés, connus comme suspects (afin de bloquer l'accès à ces sites, activez l'option **Bloquer les sites non recommandés**). Dans la rubrique

Exclusions vous pouvez spécifier les sites auxquels vous pouvez accéder sans prendre en compte d'autres restrictions configurées.

Par défaut, SpIDer Gate bloque l'accès aux sites connus comme sources de virus ou d'autres types de programmes malveillants. Dans ce cas, la listes des applications exclues de l'analyse est prise en compte.

Bloquer les programmes

SpIDer Gate peut également bloquer les objets suivants :

- suspects ;
- riskware ;
- dialers ;
- hacktools ;
- adwares ;
- canulars.

Les suspects, les adwares est les dialers sont bloqués par défaut.

Bloquer les objets

SpIDer Gate peut bloquer des objets endommagés ou non vérifiés. Cette option est désactivée par défaut.

Paramètres avancés

Vous pouvez configurer le scan des archives et des packages d'installation. Le scan des archives et des packages d'installation est désactivé par défaut.

Vous pouvez également paramétrer **Priorité de l'analyse** qui définit la distribution des ressources en fonction de la priorité de scan du trafic. La vitesse de la connexion Internet décroît lorsque SpIDer Gate fonctionne en priorité basse, car le moniteur doit attendre longtemps pour télécharger et scanner de gros volumes de données. Lorsque vous augmentez la priorité, SpIDer Gate scanne les données plus souvent, ce qui accroît la vitesse de la connexion Internet. Cependant, des scans fréquents augmentent la charge sur le processeur.

Vous pouvez choisir le type de trafic HTTP à analyser. Par défaut, seul le trafic entrant est contrôlé. Les actions spécifiées, la liste blanche de sites et les applications exclues de l'analyse sont prises en considération.

11.3. SpIDer Mail

SpIDer Mail est un moniteur de courrier qui s'installe par défaut avec les autres composants et reste en permanence en mémoire. Il se lance au démarrage du système de manière automatique.

SpIDer Mail ne supporte pas l'analyse du trafic chiffré de messagerie.

Traitement des e-mails

Tous les messages entrants sont interceptés par SpIDer Mail avant d'être réceptionnés par les clients messagerie. Les messages sont analysés à la recherche de virus avec le niveau de détail le plus élevé possible. S'ils ne comportent aucun virus ou objet suspect, les messages sont acheminés dans la boîte de réception en mode « transparent », comme s'ils venaient immédiatement du serveur. La même procédure est appliquée aux messages sortants avant leur envoi au serveur.

Par défaut, SpIDer Mail réagit aux messages infectés aussi bien qu'aux messages qui n'ont pas été analysés (à cause de leur structure compliquée par exemple) de cette façon :

- les codes malicieux sont supprimés des messages infectés puis les messages sont délivrés. Cette action est appelée *désinfection* du message ;
- les messages comportant des objets suspects sont déplacés en Quarantaine dans des fichiers à part ; le client de messagerie reçoit alors une alerte. Cette action est appelée *déplacement* du message. Les messages supprimés ou déplacés sont également supprimés du serveur POP3 ou IMAP4 ;
- les messages qui n'ont pas été analysés et les messages sains sont transmis sans modifications (*sautés*).

Les messages sortants infectés ou suspects ne sont pas envoyés au serveur, l'utilisateur est alerté que le message ne sera pas envoyé (généralement, le client messagerie sauvegarde les messages).

Les paramètres par défaut de SpIDer Mail sont optimaux pour les utilisateurs novices, fournissant une protection maximum tout en sollicitant au minimum l'intervention de l'utilisateur. Cependant, SpIDer Mail peut bloquer par défaut certaines options des outils de messagerie (par exemple, l'envoi d'un message à plusieurs destinataires peut être considéré comme un envoi massif, ou bien les messages entrants ne sont pas analysés à la recherche de spam), de l'information utile contenue dans une partie saine d'un message infecté peut devenir inaccessible dans les cas de suppression automatique. Les utilisateurs avancés peuvent configurer l'analyse des e-mails et les réactions de SpIDer Mail aux différents événements.

Analyse des e-mails par d'autres composants

Scanner Dr.Web peut également détecter des virus dans les messageries de différents formats, mais SpIDer Mail comporte plusieurs avantages :

- tous les formats de messageries ne sont pas supportés par le Scanner Dr.Web. En utilisant SpIDer Mail, les messages infectés ne sont même pas délivrés dans la boîte de réception ;

- Scanner Dr.Web n'analyse pas les boîtes de réception au moment de la réception des e-mails, mais à la demande de l'utilisateur. De plus, cette action consomme des ressources et prend beaucoup de temps.

Ainsi, parmi tous les composants de Dr.Web avec leurs paramètres par défaut, SpIDer Mail détecte les virus et les objets suspects contenus dans les e-mails en premier et les empêche de pénétrer dans votre ordinateur. L'action de SpIDer Mail est plutôt économe en ressources système ; l'analyse des e-mails peut être effectuée sans les autres composants.

11.3.1. Configurer SpIDer Mail

La modification des paramètres du composant est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.

Pour accéder aux paramètres du pare-feu, SpIDer Mail demande le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par mot de passe** dans la section Configuration.

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

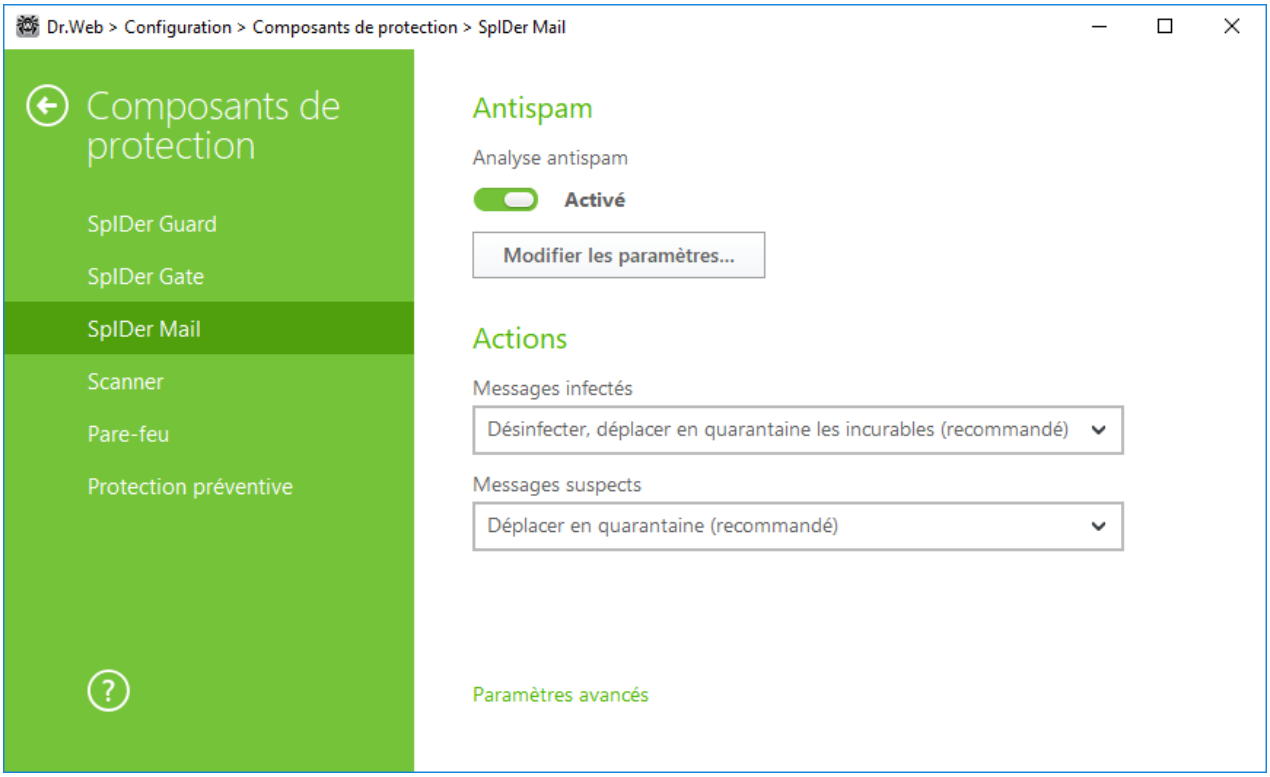

Figure 29. Configuration de SpIDer Mail

Antispam

Par défaut, SpIDer Mail cherche le spam dans des messages. Vous pouvez désactiver cette option à l'aide du bouton correspondant ou modifier les paramètres de scan en cliquant sur le bouton **Modifier les paramètres**. Pour en savoir plus sur les technologies du filtre-antispam et les paramètres configurés, consultez la rubrique Antispam.

Actions

Par défaut,SpIDer Mail tente de désinfecter les messages infectés par un virus connu et (supposé) curable et déplace les messages incurables et suspects, comme les dialers et les adwares, en Quarantaine tout en ignorant les menaces mineures. D'autres messages sont délivrés par le Moniteur de courrier *sans traitement*.

Les réactions de SpIDer Mail sont similaires à celles du Scanner Dr.Web.

Vous pouvez spécifier pour SpIDer Mail une des réactions suivantes :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Restaurer le message dans son état initial avant infection. Si le message est incurable, ou que la tentative de désinfection a échoué, le message est placé en quarantaine. Disponible pour les messages infectés par des virus connus et « curables » seulement, exceptés les trojans éliminés dès leur détection. Cette action n'est pas applicable aux messages contenus dans les archives, quel que soit le type de virus.
Désinfecter, supprimer les incurables	Restaurer le message dans son état initial avant infection. Si le virus est incurable, ou que la tentative de désinfection a échoué, le message est supprimé.
Supprimer	Supprimer le message. Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification de l'opération effectuée.
Déplacer en quarantaine	Déplacer le message dans la Quarantaine. Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification sur l'opération effectuée.
Ignorer	Commande d'adresser le message à la boîte de réception comme d'habitude, c'est-à-dire sans entreprendre aucune action.

Si un e-mail contient un objet malveillant, chaque réaction, exceptée **Ignorer** a pour résultat un échec de l'envoi de l'e-mail au serveur de messagerie ou à la boîte de réception.

Pour accroître la sécurité de la protection antivirus par rapport au niveau par défaut, sélectionnez l'élément **Déplacer en quarantaine** dans la liste **Non vérifiés**. Il est recommandé d'analyser les fichiers déplacés plus tard avec le Scanner Dr.Web.

Si vous souhaitez désactiver la protection contre les e-mails suspects, assurez-vous que SpIDer Guard contrôle constamment votre ordinateur.

Actions sur les messages

Dans ce groupe, vous pouvez configurer des actions additionnelles à appliquer lorsque SpIDer Mail contrôle les messages.

Paramètre	Description
Ajouter l'en-tête 'X-Antivirus' dans les messages	Activée par défaut. Commande à SpIDer Mail d'ajouter les résultats du scan et des informations sur la version de Dr.Web à l'en-tête des messages après le scan. Vous ne pouvez pas éditer le format de l'en-tête ajouté.
Supprimer les messages modifiés sur le serveur	Commande à SpIDer Mail de supprimer depuis le serveur de messagerie les messages supprimés ou déplacés en Quarantaine par SpIDer Mail quels que soient les paramètres de votre client messagerie.

Optimisation de l'analyse

Vous pouvez configurer SpIDer Mail pour qu'il reconnaisse les messages trop compliqués et dont le scan est trop consommateur de temps, comme non vérifiés. Pour cela, activez l'option **Délai d'attente lors de l'analyse de message** et indiquez la durée maximum de scan d'un message. Après l'expiration de ce délai, SpIDer Mail arrête de vérifier le message. La valeur 250 secondes est utilisée par défaut.

Scan des archives

Activez l'option **Analyse des archives** si vous souhaitez que SpIDer Mail analyse les fichiers archivés transférés par e-mail. Les paramètres suivants seront disponibles :

- **Taille maximum des fichiers à décompresser**. Si la taille des fichiers extraits excède cette limite, SpIDer Mail ne les décompresse ni ne les analyse. La valeur 30720 Ko est utilisée par défaut ;
- **Ratio maximum de compression de l'archive**. Si la compression dépasse la limite, SpIDer Mail ne décompresse ni n'analyse l'archive. La valeur 0 est utilisée par défaut ;
- **Niveau maximum d'imbrication de l'archive**. Si le nombre de fichiers archivés dépasse la limite, SpIDer Mail analyse les archives jusqu'à ce que cette limite soit atteinte. La valeur 64 est utilisée par défaut.

Pour activer des paramètres d'optimisation, cochez les cases correspondantes.

Il n'existe pas de restrictions pour un paramètre si la valeur est égale à 0.

Paramètres avancés

Dans ce groupe, vous pouvez spécifier les options supplémentaires d'analyse des e-mails :

- utilisation de l'analyse heuristique – dans ce mode, des mécanismes spécialisés sont utilisés de sorte qu'ils permettent de détecter, dans le courrier électronique, des objets suspects, avec une forte probabilité, contaminés par des virus inconnus. Pour désactiver l'analyse heuristique, décochez la case **Utiliser l'analyse heuristique (recommandé)** ;
- analyse de packages d'installation. Cette option est désactivée par défaut.

11.3.2. Antispam

Les technologies de l'Antispam Dr.Web comportent des milliers des règles qui peuvent être divisées en plusieurs groupes :

- **analyse heuristique** : une technologie de haute intelligence qui analyse de façon empirique toutes les parties d'un message : en-tête, corps du message, pièces jointes s'il y en a ;
- **techniques de détection d'évasion** : cette technologie antispam avancée permet de détecter les techniques d'évasion adoptées par les spammeurs pour passer outre les filtres antispam ;
- **analyse par signature HTML** : les messages contenant du code HTML sont comparés avec une liste de modèles connus de la bibliothèque antispam. Une telle comparaison, combinée à des données sur la taille des images typiquement utilisées par les spammeurs aide à protéger les utilisateurs contre les spam contenant les liens sur des sites ;
- **analyse sémantique** : les mots et phrases d'un message, visibles ou masqués, sont comparés aux mots et phrases typiques du spam à l'aide d'un dictionnaire spécial. Des mots, des expressions et des caractères cachés sont analysés ainsi que des mots, des expressions et des caractères visibles ;
- **anti-scamming** : le scam (tout comme le pharming) inclue les scams « Nigérian », les scams de loterie ou de casino et les faux messages de banque et organismes de crédit. Un module spécial est utilisé pour filtrer les scams ;
- **filtrage de spam technique** : les messages-bounce apparaissent comme réaction à un virus ou à la manifestation de l'activité virale. Un module spécifique considère ces messages comme indésirables.

Vous pouvez configurer les paramètres suivants de l'Antispam :

Paramètre	Description
Autoriser le texte cyrillique	Activée par défaut. Commande à SpIDer Mail d'analyser les messages encodés en cyrillique au lieu de les considérer automatiquement comme du spam. Si la case est décochée, il est très probable que les messages comportant du texte cyrillique seront automatiquement considérés comme spam.
Autoriser le texte en langues asiatiques	Activée par défaut. Commande à SpIDer Mail de ne pas considérer les messages en langues asiatiques les plus connues comme spam. Si cette option est désactivée, il est très probable que les messages de ce type seront considérés comme spam.
Ajouter le préfixe au sujet des messages contenant du spam	Cette option est activée par défaut. SpIDer Mail ajoute le préfixe [SPAM] au champ Sujet des messages spam. Ce paramètre commande à SpIDer Mail d'ajouter un préfixe spécial aux messages considérés comme spam. L'utilisation d'un préfixe vous permet de créer des règles de filtrage du spam dans les clients messagerie (par exemple, Microsoft Outlook Express) dans lesquels il n'est pas possible d'activer le filtrage par en-tête.

Traitement des e-mails par le filtre antispam

SpIDer Mail ajoute les en-têtes suivants aux messages traités :

- `X-DrWeb-SpamState:` <*valeur*>, où <*valeur*> indique si le message est un spam (`Yes`) selon SpIDer Mail ou pas (`No`) ;
- `X-DrWeb-SpamVersion:` <*version*>, où <*version*> indique la version de la bibliothèque de l'Antispam Dr.Web ;
- `X-DrWeb-SpamReason:` <*score de spam*>, où <*score de spam*> est la liste des scores selon les critères de spam.

Vous pouvez utiliser ces en-têtes et le préfixe dans le champ Sujet, (si la case correspondante est cochée), pour configurer le filtrage des e-mails dans votre messagerie.

Si vous utilisez les protocoles IMAP/NNTP, configurez votre messagerie de telle sorte qu'elle télécharge les messages complets depuis le serveur de mails, c'est-à-dire sans prévisualiser leurs en-têtes. Ceci est requis pour un fonctionnement correct du filtre antispam.

Pour améliorer le filtre antispam, vous pouvez créer des rapports d'erreurs sur la détection des spam.

Le filtre spam traite les messages rédigés conformément au standard MIME RFC 822.

Pour créer un rapport d'erreurs de détection des spam

1. Créez un nouvel e-mail et attachez le message qui n'a pas été traité correctement par le filtre antispam. Les messages inclus dans le corps du mail ne sont pas analysés.
2. Envoyer le message avec la pièce jointe à l'administrateur de votre réseau antivirus.

11.4. Scanner

La modification des paramètres du composant est possible si c'est autorisé par l'administrateur du serveur de protection centralisée auquel se connecte Dr.Web.

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 Configuration.

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

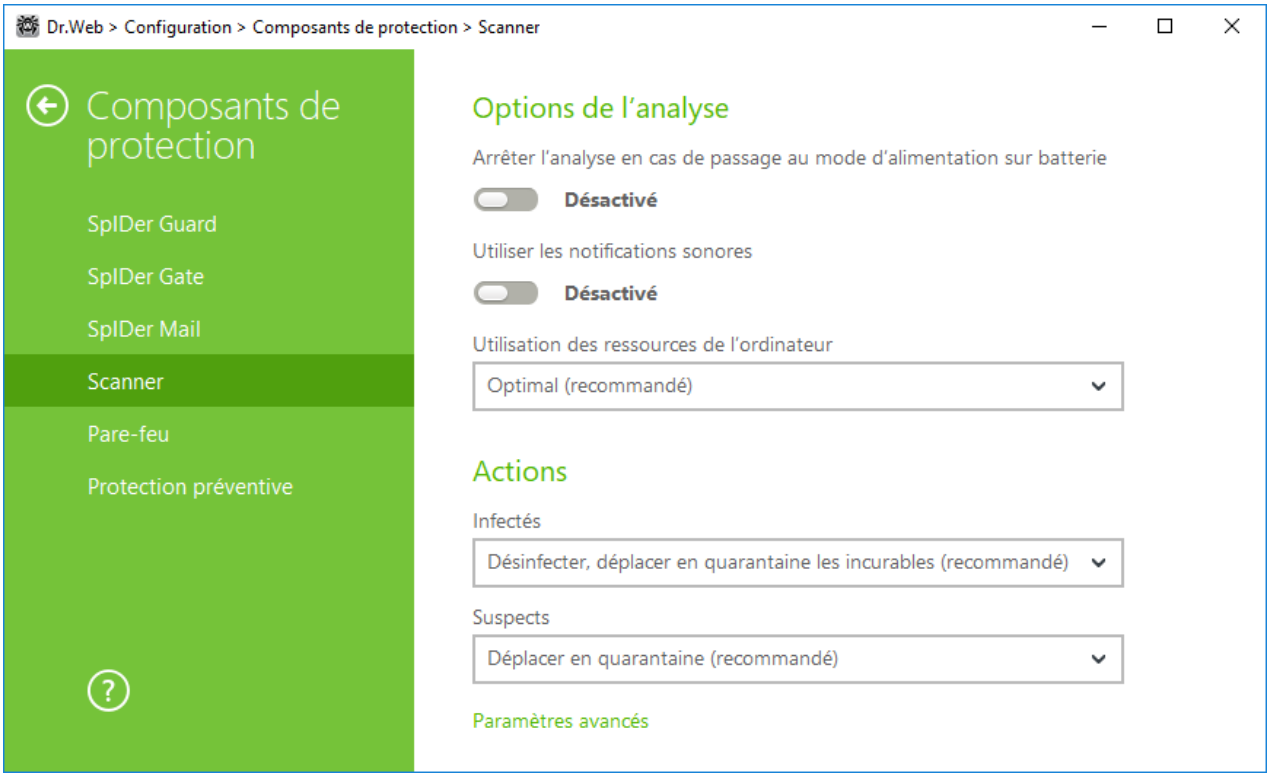

Figure 30. Configuration du Scanner

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**. Activez cette option pour arrêter l'analyse en cas de passage en mode d'alimentation sur la batterie. Cette option est désactivée par défaut.
- **Utiliser les notifications sonores**. Activez cette option pour commander au Scanner Dr.Web d'accompagner chaque événement d'un signal sonore. Cette option est désactivée par défaut.
- **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 :

- **Infectés** : objets infectés par un virus connu et (supposé) curable ;
- **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 qui sont considérés comme curables, tandis que les autres objets qui sont considérés comme les plus dangereux sont placés 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 uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
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 uniquement pour les virus connus, sauf les Trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
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.
Rapport	Afficher une notification et laisser passer l'objet sans appliquer aucune action. Cette réaction est disponible uniquement pour les objets suspects et les programmes malveillants.

⚠ Si un virus ou un code suspect est détecté au sein des objets complexescomme les archives, les boîtes e-mails ou les conteneurs de fichiers, les actions sur les menaces contenues dans tels objets sont appliquées à l'objet entier et non seulement à sa partie infectée.

Paramètres avancés

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

11.5. Pare-feu

Pare-feu Dr.Web protège votre ordinateur des accès non autorisés et prévient les fuites de données vitales via les réseaux. Il gère les tentatives de connexion et les transferts de données et vous aide à bloquer les connexions non désirées ou suspectes au niveau des applications et du réseau.

Pare-feu fournit les fonctionnalités suivantes :

- contrôle et filtrage de tout le trafic entrant et sortant ;
- contrôle d'accès au niveau des applications ;
- filtrage des paquets au niveau du réseau ;
- sélection rapide des règles ;
- journal des événements.

11.5.1. Apprentissage du Pare-feu

Après l'installation du Pare-feu, il faudra un certain temps pour apprendre le logiciel lors de votre travail sur l'ordinateur. Le mode d'apprentissage concerne les modes suivants du Pare-feu (pour en savoir plus sur les modes du Pare-feu, consultez la rubrique Configuration du pare-feu) :

- **Créer automatiquement des règles pour les applications connues** (spécifié par défaut) ;
- **Mode interactif**.

En mode **Créer automatiquement des règles pour les applications connues**, si le système ou les application tentent de se connecter au réseau, le Pare-feu vérifie si ces applications sont de confiance et si les règles de filtrage sont spécifiés. S'il n'y a pas de règles, Dr.Web affiche une alerte où vous pouvez spécifier la règle. Les règles ne sont pas spécifiées pour les application de confiance. La connexion au réseau est autorisée à ces applications.

Les applications de confiance comprennent les applications système, les applications ayant le certificat Microsoft et les applications figurant dans la liste des applications de confiance de Dr.Web.

En mode **Mode interactif**, si le système ou les applications tentent de se connecter au réseau, le Pare-feu vérifie si les règles de filtrage sont spécifiées pour ces programmes. S'il n'y en a pas, une alerte s'affiche et vous invite à créer une règle qui sera appliquée chaque fois lors du traitement des connexions pareilles.

Lors du fonctionnement sous un compte limité (Invité), Pare-feu Dr.Web n'affiche pas d'alertes à l'utilisateur sur les tentatives d'accéder au réseau. Les alertes de ce type seront affichées en mode administrateur seulement si cette session est active en même temps que la session de l'invité.

Règles pour les applications

1. En cas de détection d'une tentative de se connecter au réseau, pour prendre une décision, prenez connaissance des informations qui s'affichent lors d'une alerte :

Champ	Description
Application	Le nom de l'application concernée. Assurez-vous que le chemin vers le fichier exécutable spécifié dans le champ **Chemin vers l'application** correspond à sa localisation habituelle.
Chemin vers l'application	Le chemin complet vers le fichier exécutable de l'application et son nom.
Signature numérique	Signature numérique de l'application.
Adresse	Protocole et adresse de l'hôte auquel on tente de se connecter.
Port	Le port utilisé lors de la tentative de connexion.
Direction	Direction de connexion.

2. Après avoir pris une décision, sélectionnez l'action appropriée en bas de la fenêtre :
   - pour bloquer la connexion une fois, sélectionnez l'action **Bloquer pour une fois** ;
   - pour autoriser l'application à se connecter une seule fois, sélectionnez **Autoriser pour une fois** ;
   - pour ouvrir une fenêtre où vous pouvez créer une nouvelle règle de filtrage, sélectionnez **Créer une règle**. Dans la fenêtre ouverte, vous pouvez soit choisir une des règles prédéfinies, soit créer une règle pour cette application.
3. Cliquez sur **OK**. Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.

Dans certains cas, le système d'exploitation Windows ne permet pas l'identification explicite d'un service qui est lancé comme un processus système. Lorsqu'une tentative

de connexion d'un service système est détectée, notez le port utilisé pour la connexion. Si vous utilisez l'application qui peut s'adresser à ce port, autorisez la connexion.

Lorsque la connexion a été initiée par une application connue par le Pare-feu (possédant déjà des règles) mais que cette application a été lancée par un processus parent inconnu, une notification sera affichée par le Pare-feu.

Pour définir les règles de processus parents

1. En cas de détection d'une tentative de se connecter au réseau depuis une application lancée par un programme inconnu pour le Pare-feu, prenez connaissance des informations sur le fichier exécutable du programme parent.
2. Dès que vous avez pris une décision concernant l'opération à réaliser, sélectionnez l'une des actions suivantes :
   - pour bloquer la connexion de l'application au réseau une fois, cliquez sur **Bloquer** ;
   - pour autoriser l'application à se connecter au réseau une fois, cliquez sur **Autoriser** ;
   - pour créer une nouvelle règle de filtrage d'application, sélectionnez **Créer une règle**. Dans la fenêtre ouverte, configurez les paramètres du processus parent.
3. Cliquez sur **OK**. Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.

Lorsqu'une application inconnue a été lancée par une autre application inconnue, une notification s'affiche avec les détails. Si vous cliquez sur **Créer une règle**, une nouvelle fenêtre s'ouvrira, vous permettant de créer de nouvelles règles pour cette application et ses processus parents.

11.5.2. Configuration du Pare-feu

Dans cette section, vous pouvez configurer les paramètres suivants du Pare-feu :

- sélectionnez le mode opératoire ;
- configurer la liste des applications autorisées ;
- configurer les paramètres des réseaux connus.

Pour accéder aux paramètres du pare-feu, 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 section Configuration.

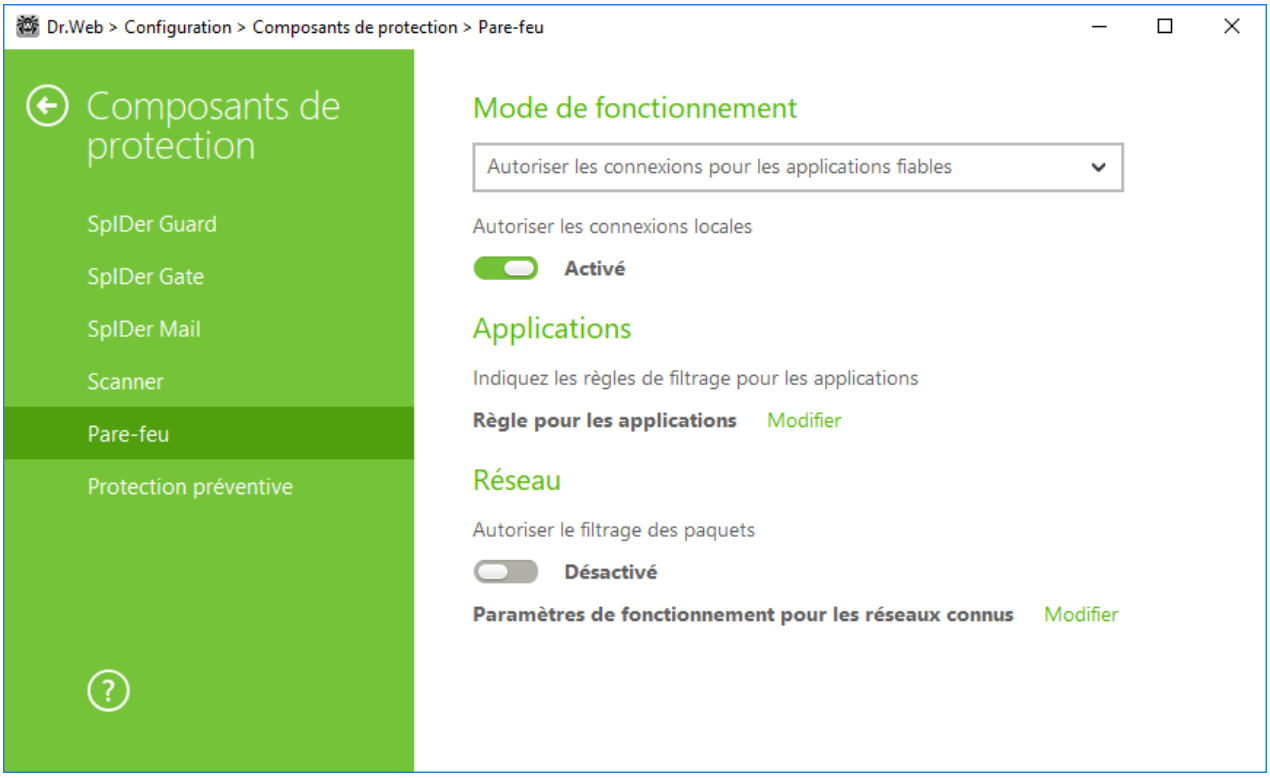

Figure 31. Paramètres principaux du Pare-feu

Par défaut, Pare-feu ne crée pas de règles pour les applications connues. Quel que soit le mode opératoire, les événements sont journalisés.

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

Le paramètre **Autoriser les connexions locales** permet à toutes les applications d'établir des connexions locales sur votre ordinateur (depuis l'interface ou à l'interface 127.0.0.1 (localhost)). Cette option s'applique après la vérification de conformité des connexions aux règles spécifiées. Désactivez cette option pour appliquer des règles de filtrage indépendamment du fait que la connexion se fait via le réseau ou au sein de votre ordinateur.

Sélection du mode opératoire

Sélectionnez un des modes suivants :

- **Créer automatiquement des règles pour les applications connues** : mode dans lequel toutes les applications de confiance sont autorisées à accéder aux ressources réseau (utilisé par défaut). Pour les autres applications, un avertissement s'affiche où vous pouvez spécifier une règle (voir la rubrique Apprentissage du Pare-feu) ;
- **Autoriser les connexions inconnues** : mode d'accès libre, lorsque toutes les applications inconnues sont autorisées à accéder au réseau ;
- **Mode interactif** : mode d'apprentissage dans lequel l'utilisateur possède un contrôle total sur les réactions du Pare-feu ;

- **Bloquer les connexions inconnues** : mode d'accès restreint, lorsque toutes les connexions inconnues sont bloquées. Pour les connexions connues, le Pare-feu applique les règles appropriées.

Autoriser les connexions pour les applications de confiances

Ce mode est utilisé par défaut.

Dans ce mode, toutes les applications de confiance sont autorisées à accéder aux ressources réseau, y compris Internet. Les applications de confiance comprennent les applications système, les applications ayant le certificat Microsoft et les applications figurant dans la liste des applications de confiance de Dr.Web. Les règles pour ces applications ne sont pas affichées dans la liste de règles. Pour d'autres applications, Pare-feu offre une possibilité de bloquer ou d'autoriser une connexion inconnue ainsi que de créer une règle pour cette connexion.

Lorsqu'une application lancée par l'utilisateur ou que le système d'exploitation tentent de se connecter au réseau, Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour l'application. S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.

Autoriser les connexions inconnues

Dans ce mode, l'accès aux ressources réseau, y compris Internet, est fourni à toutes les applications inconnues pour lesquelles les règles de filtrage ne sont pas spécifiées. Aucune notification sur les tentatives d'accès ne sont affichées par Pare-feu.

Mode interactif

Dans ce mode, vous avez un contrôle total sur les réactions du Pare-feu lors de la détection de connexions inconnues, ce qui forme le programme pendant que vous travaillez sur votre ordinateur.

Lorsqu'une application lancée par l'utilisateur ou que le système d'exploitation tentent de se connecter au réseau, Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour l'application. S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.

Bloquer les connexions inconnues

Dans ce mode, toutes les connexions inconnues aux ressources réseau y compris la connexion à Internet sont bloquées de manière automatique.

Lorsqu'une application lancée par l'utilisateur ou le système d'exploitation tente de se connecter au réseau, Pare-feu vérifie s'il existe des règles de filtrage pour ces programmes. S'il n'y en a pas, Pare-feu bloque automatiquement l'accès au réseau sans afficher aucune notification. S'il y a des règles de filtrage spécifiées pour la connexion en question, les actions déterminées seront effectuées.

Page Applications

> Vous ne pouvez pas créer plus d'un ensemble de règles par application.

Le filtrage au niveau des applications vous aide à contrôler l'accès de diverses applications et processus aux ressources réseaux, et vous permet d'interdire ou d'autoriser aux applications de lancer d'autres processus. Vous pouvez créer des règles pour les applications système et utilisateur.

Dans cette rubrique, vous pouvez établir des ensembles de règles de filtrage. Pour cela, vous pouvez créer de nouvelles règles, éditer les règles existantes ou supprimer les règles dont vous n'avez plus besoin. Chaque application est explicitement identifiée par le chemin vers son fichier exécutable. Le Pare-feu utilise le nom `SYSTEM` pour indiquer le noyau du système d'exploitation (le processus system pour lequel il n'y a pas de fichier exécutable correspondant).

> Si vous avez créé une règle bloquant pour un processus ou que vous avez installé le mode Bloquer les connexions inconnues, et après, vous avez désactivé la règle bloquant ou modifié le mode de fonctionnement, le blocage reste activé jusqu'à la deuxième tentative d'établir une connexion après le redémarrage du processus.

Les règles pour les applications supprimées de votre ordinateur ne sont pas supprimées automatiquement. Pour supprimer de telles règles, sélectionnez l'élément **Suppression de règles non utilisées** dans le menu contextuel de la liste.

Règles pour les applications

Dans la fenêtre **Création d'un nouvel ensemble de règles pour l'application** (ou **Edition de l'ensemble de règles pour**), vous pouvez configurer l'accès de l'application aux ressources réseau ainsi qu'interdire ou autoriser le lancement d'autres applications.

Pour accéder à cette fenêtre, cliquez sur le bouton **Modifier** de l'élément **Règles pour les applications** dans les paramètres du Pare-feu, ensuite cliquez sur dans la fenêtre qui s'affiche ou sélectionnez une application et cliquez sur .

Lors de fonctionnement du Pare-feu en mode d'apprentissage, vous pouvez créer une règle depuis la fenêtre de notification de tentative de connexion non autorisée.

Lancer d'autres applications

Pour interdire ou autoriser à une application de lancer d'autres application, dans la liste déroulante **Lancement des application réseau,** sélectionnez :

- **Autoriser**, pour autoriser l'application à lancer des processus ;
- **Bloquer**, pour interdire à l'application de lancer des processus ;

- **Non spécifié**. Dans ce cas, l'application va fonctionner avec les paramètres spécifiés correspondant au mode de fonctionnement du Pare-feu.

Accès aux ressources réseau

1. Spécifiez le type d'accès aux ressources réseau :
   - **Autoriser tout** : toutes les connexions seront autorisées ;
   - **Bloquer tout** : toutes les connexions seront bloquées ;
   - **Non spécifié**. Dans ce cas, l'application va fonctionner avec les paramètres spécifiés correspondant au mode de fonctionnement du Pare-feu.
   - **Défini par l'utilisateur** : dans ce mode, vous pouvez créer un ensemble de règles qui autorisera ou bloquera différentes connexions.
2. Si vous avez sélectionné le mode **Défini par l'utilisateur** de l'accès aux ressources réseau, un tableau contenant les informations sur l'ensemble de règles pour l'application correspondante sera affiché ci-dessous.

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : • **Bloquer les paquets** : bloquer la tentative de connexion ; • **Autoriser les paquets** : autoriser la connexion.
Nom de règle	Nom de la règle.
Type de connexion	Direction de la connexion : • **Entrant** : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ; • **Sortant** : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.
Description	Description de la règle.

3. Si nécessaire, éditez l'ensemble de règle pré-installé ou créez un nouvel ensemble de règles pour l'application.
4. Si vous avez choisi de créer ou d'éditer une règle, configurez les paramètres de la règle dans la fenêtre ouverte.
5. Après avoir édité l'ensemble de règles, cliquez sur **OK** pour enregistrer les modifications apportées ou sur **Annuler** pour annuler les modifications. Les modifications apportées dans l'ensemble de règles sont conservées en cas de passage en autre mode.

Cochez la case **Demander confirmation en cas de changement d'objet (recommandé)** si vous voulez que l'application demande l'accès aux ressources réseau en cas de modification ou mise à jour des applications.

Configuration des paramètres de règles

Les règles de filtrage des applications contrôlent l'interaction entre une application en particulier et un certain hôte réseau.

Création et édition de la règle

Pour ajouter une nouvelle règle, cliquez sur le bouton dans la fenêtre **Edition de l'ensemble de règles pour**. Pour éditer une règle existante, sélectionnez la règle nécessaire et cliquez sur . Dans ce cas, le mode **Défini par l'utilisateur** doit être sélectionné dans l'élément **Accès aux ressources réseau**.

Configurez les paramètres suivants :

Paramètre	Description
Général	
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : • **Bloquer les paquets** : bloquer la tentative de connexion ; • **Autoriser les paquets** : autoriser la connexion.
Statut	État de la règle : • **Activé** : la règle est appliquée ; • **Désactivé** : la règle n'est pas appliquée temporairement.
Type de connexion	Direction de la connexion : • **Entrant** : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ; • **Sortant** : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.

Paramètre	Description
Journalisation	Mode de journalisation : • **Activé** : enregistrer les événements ; • **Désactivé** : aucune information sur la règle n'est enregistrée.
Configuration de la règle	
Protocole	Les protocoles réseaux et transport utilisés lors de la tentative de connexion. Les protocoles réseaux suivants sont supportés : • IPv4 ; • IPv6 ; • IP all : toute version de protocole IP. Les protocoles de transport suivants sont supportés : • TCP ; • UDP ; • TCP & UDP – protocole TCP et UDP ; • RAW.
Adresse locale/Adresse distante	L'adresse IP du hôte distant pour la connexion. Vous pouvez spécifier soit une adresse spécifique (**Égal**), soit plusieurs adresses IP en utilisant une plage (**Dans la plage**), vous pouvez également utiliser le masque du sous-réseau (**Masque**) ou les masques de tous les sous-réseaux dans lesquels votre ordinateur à l'adresse réseau (**MY_NETWORK**). Pour appliquer la règle à tous les hôtes distants, sélectionnez **Toute**.
Port local/Port distant	Le port utilisé pour la connexion. Vous pouvez spécifier soit un port spécifique (**Égal**) ou une plage de port (**Dans la plage**). Pour appliquer la règle à tous les ports, cliquez sur **Toute**.

Paramètres des réseaux

Le filtrage des paquets vous permet de contrôler l'accès au réseau quel que soit le programme qui initie la connexion. Pare-feu applique ces règles aux paquets réseaux d'un certain type transmis via les interfaces réseaux de votre ordinateur.

Ce type de filtrage vous fournit des mécanismes généraux de contrôle à la différence du filtrage au niveau des applications.

Filtre de paquets

Dans la fenêtre Réseau, vous pouvez configurer un ensemble de règles de filtrage des paquets transmis via une interface particulière.

Pour accéder à cette fenêtre, cliquez sur **Modifier** dans l'élément **Paramètres de fonctionnement pour les réseaux connus** de la fenêtre de paramètres du Pare-feu. Sélectionnez dans la liste l'interface de votre choix et l'ensemble de règles correspondant. Si l'ensemble de règles nécessaire n'est pas présent dans la liste, vous pouvez le créer.

Le Pare-feu est fourni avec les ensembles de règles suivants :

- **Default Rule** : cet ensemble inclut des règles décrivant les configurations systèmes les plus fréquentes et prévenant contre les attaques réseaux communes. Cet ensemble de règles est utilisé par défaut pour les nouvelles interfaces réseaux ;
- **Allow All** : laisser passer tous les paquets ;
- **Block All** : bloquer tous les paquets.

Pour passer rapidement d'un mode de filtrage à un autre, vous pouvez créer des ensembles de règles de filtrage.

Pour afficher toutes les interfaces disponibles ou ajouter une nouvelle interface dans le tableau, cliquez sur le bouton  . Dans la fenêtre qui apparaît, vous pouvez spécifier les interfaces à afficher dans le tableau. Les interfaces actives seront affichées automatiquement dans le tableau.

Vous pouvez supprimer les interfaces réseau inactives du tableau affiché en cliquant sur  .

Configuration du filtre de paquets

Pour gérer les ensembles de règles existants et ajouter de nouveaux ensembles, ouvrez la fenêtre **Configuration du filtre de paquets** en cliquant sur **Ensembles de règles**.

Sur cette page, vous pouvez :

- configurer des ensembles de règles de filtrage en ajoutant de nouvelles règles, en modifiant ou en supprimant des règles existantes ;
- configurer les paramètres avancés du filtrage.

Création d'un ensemble de règles

Pour créer un ensemble de règles, effectuez l'une des actions suivantes :

- pour créer un ensemble de règles d'une interface réseau, cliquez sur  ;
- pour éditer un ensemble de règles, sélectionnez-le dans la liste et cliquez sur  ;
- pour ajouter une copie de l'ensemble de règles existant, cliquez sur  . La copie sera ajoutée au-dessous de l'ensemble sélectionné ;

- pour supprimer un ensemble de règles, sélectionnez-le et cliquez sur  .

Paramètres avancés

Pour spécifier les paramètres avancés du filtrage de paquets, dans la fenêtre **Configuration du filtre de paquets**, activez les cases suivantes :

Option	Description
Activer le filtrage dynamique des paquets	Cochez cette case pour filtrer les paquets selon l'état des connexions TCP existantes. Le Pare-feu bloquera les paquets qui ne correspondent pas aux connexions actives selon les spécifications des protocoles TCP. Cette option protège votre ordinateur contre les attaques DoS (par déni de service), scan des ressources, vol de données et autres opérations malveillantes. Il est également recommandé d'activer le filtrage dynamique des paquets si vous utilisez des protocoles de transfert de données complexes tels que FTP, SIP, etc. Décochez cette case pour filtrer les paquets sans tenir compte des sessions TCP.
Traitement des paquets IP fragmentés	Cochez cette case pour garantir le traitement correct de larges volumes de données. La taille de MTU (Maximum Transmission Unit) peut varier en fonction des différents réseaux, ainsi les paquets IP importants peuvent arriver fragmentés. Lorsque cette option est activée, le Pare-feu applique la règle sélectionnée pour le premier fragment du paquet IP important à tous les autres fragments. Décochez cette case pour traiter tous les paquets indépendamment.

Cliquez sur **OK** pour sauvegarder les modifications apportées ou **Annuler** pour quitter sans enregistrer les modifications apportées.

La fenêtre **Pour configurer l'ensemble de règles** donne la liste des règles de filtrage de paquets pour l'ensemble sélectionné. Vous pouvez configurer la liste en ajoutant de nouvelles règles pour une application ou modifier les règles existantes et l'ordre de leur exécution. Les règles sont appliquées selon leur ordre dans la liste.

Pour chaque règle dans un ensemble, les informations suivantes s'affichent :

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : • **Bloquer les paquets** : bloquer le paquet ;

Paramètre	Description
	• **Autoriser les paquets** : transmettre le paquet.
Nom de règle	Le nom de la règle.
Direction	Direction de la connexion : • : la règle s'applique lorsque le paquet provient du réseau ; • : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ; • : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie des informations à enregistrer dans le journal : • **En-têtes seulement** : enregistrer uniquement les en-têtes de paquets ; • **Paquet entier** : enregistrer les paquets entiers ; • **Désactivé** : aucune information n'est enregistrée.
Description	La description abrégée de la règle.

Édition ou création de l'ensemble de règles

1. Si nécessaire, spécifiez le nom ou changez le nom de l'ensemble de règles.
2. Utilisez les options suivantes pour créer des règles de filtrage :
   - pour ajouter une nouvelle règle, cliquez sur . La nouvelle règle est ajoutée au début de la liste ;
   - pour modifier la règle sélectionnée, cliquez sur ;
   - pour ajouter une copie de la règle sélectionnée, cliquez sur . La copie est ajoutée devant la règle sélectionnée ;
   - pour supprimer la règle sélectionnée, cliquez sur .
3. Si vous avez choisi de créer une nouvelle règle ou d'éditer une règle existante, configurez ses paramètres.
4. Utilisez la flèche près de la liste pour changer l'ordre des règles. Les règles sont appliquées en fonction de l'ordre dans lequel elles apparaissent dans l'ensemble.
5. A la fin de l'édition, cliquez sur le bouton **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.

> ⚠ Les paquets pour lesquels il n'y a pas de règles dans l'ensemble de règles sont automatiquement bloqués, sauf les paquets autorisés dans les règles du Filtre d'applications.

Pour ajouter ou éditer une règle de filtrage

1. Dans la fenêtre de modification de l'ensemble de règles du filtre de paquets, cliquez sur  ou  . Une fenêtre de création ou de modification de règle va s'ouvrir.
2. Configurez les paramètres suivants :

Paramètre	Description
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : • **Bloquer les paquets** : bloquer le paquet ; • **Autoriser les paquets** : transmettre le paquet.
Direction	Direction de la connexion : • **Entrant** : la règle s'applique lorsque le paquet provient du réseau ; • **Sortant** : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie des informations à enregistrer dans le journal : • **Paquet entier** : enregistrer les paquets entiers ; • **En-têtes seulement** : enregistrer uniquement les en-têtes de paquets ; • **Désactivé** : aucune information n'est enregistrée.

3. Si nécessaire, ajoutez un critère de filtrage, par exemple le protocole de transport ou le protocole réseau en cliquant sur **Ajouter un critère**. La fenêtre Ajouter un critère de filtrage va s'ouvrir :

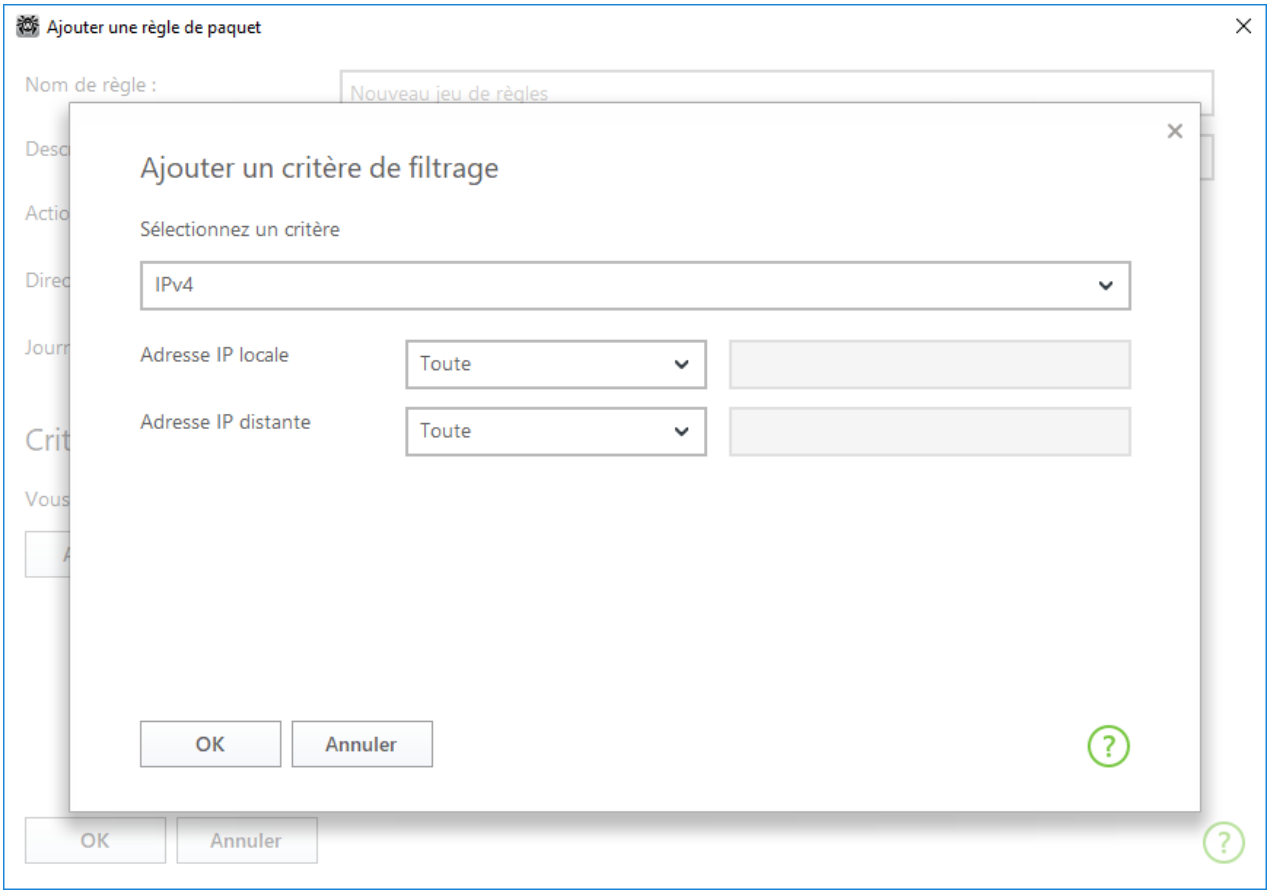

Figure 32. Ajout d'un critère de filtrage

Sélectionnez le critère nécessaire dans la liste déroulante. Dans cette fenêtre, vous pouvez configurer les paramètres pour le critère sélectionné. Vous pouvez ajouter autant de critères que vous le souhaitez. Pour que l'action de la règle soit appliquée au paquet, il faut que le paquet réponde à tous les critères de la règle.

Des critères complémentaires sont disponibles pour certains en-têtes. Tous les critères ajoutés sont affichés dans la fenêtre d'édition de la règle de paquet et ils sont disponibles pour l'édition.

4. Cliquez ensuite sur **OK** pour enregistrer les modifications ou sur **Annuler** pour les annuler.

Si vous n'ajoutez aucun critère de filtrage, alors cette règle autorisera ou bloquera tous les paquets (en fonction du champ **Action**).

Si dans cette règle, dans l'en-tête IPv4, vous sélectionnez la valeur **Toute** pour les paramètres **Adresse IP locale** et **Adresse IP distante**, la règle sera appliquée à tout paquet contenant l'en-tête IPv4 et envoyé depuis l'adresse physique d'un ordinateur local.

11.6. Dr.Web pour Outlook

Les fonctions clés du composant

Le plug-in Dr.Web pour Outlook exécute les fonctions suivantes :

- analyse antivirus des fichiers contenus dans les pièces jointes des messages entrants ;
- analyse antispam du courrier ;
- détection et neutralisation des programmes malveillants ;
- utilisation du moteur heuristique afin de renforcer la protection contre les virus inconnus.

Configuration du module Dr.Web pour Outlook

Vous pouvez configurer les paramètres et consulter les statistiques du programme dans le client de messagerie Microsoft Outlook. Pour cela, allez dans la rubrique **Outils** → **Options** → onglet **Antivirus Dr.Web** (dans Microsoft Outlook 2010 — rubrique **Fichiers** → **Options** → **Compléments** puis sélectionnez le module Dr.Web pour Outlook et cliquez sur **Options du complément**).

L'onglet **Antivirus Dr.Web** dans les paramètres de Microsoft Outlook n'est disponible que si l'utilisateur dispose des droits permettant de modifier les paramètres.

L'onglet **Antivirus Dr.Web** affiche le statut actuel de la protection (active/inactive) et permet d'accéder aux fonctions suivantes :

- Journal permet de configurer l'écriture des événements dans le fichier de journal ;
- Contrôle des pièces jointes permet de configurer le contrôle du courrier électronique et de spécifier des réactions en cas de détection d'objets malveillants ;
- Filtre antispam permet de spécifier les réactions de l'application en cas de détection de messages spam ainsi que de créer des listes noire et blanche ;
- Statistiques affiche des informations sur les objets analysés et traités par l'application.

11.6.1. Analyse antivirus

Dr.Web pour Outlook utilise les diverses méthodes de détection des virus. L'utilisateur peut spécifier les réactions à appliquer aux objets malveillants détectés : le programme peut réparer les objets infectés, ainsi que les supprimer ou les déplacer vers la Quarantaine pour les isoler et les conserver de manière sécurisée.

L'application Dr.Web pour Outlook détecte les objets malveillants suivants :

- objets infectés ;
- bombes de décompression ou bombes d'archive ;

- adwares ;
- hacktools ;
- dialers ;
- canulars ;
- riskwares ;
- spywares ;
- chevaux de Troie ;
- vers et virus.

Actions

Dr.Web pour Outlook peut être configuré pour réagir en cas de détection de fichiers infectés ou suspects et de programmes malveillants lors de l'analyse des pièces jointes du courrier électronique.

Pour configurer la vérification de la présence de virus dans les pièces jointes d'e-mail, dans l'application Microsoft Outlook, allez à **Outils** → **Options** → onglet **Antivirus Dr.Web** (dans Microsoft Outlook 2010, dans la section **Fichiers** → **Options** → **Compléments** choisissez Dr.Web pour Outlook et cliquez sur le bouton **Options du complément**) et cliquez sur **Analyse de pièces jointes**.

La fenêtre **Analyse de pièces jointes** est disponible à condition que l'utilisateur disposes des droits administrateur.

Sous l'OS Windows Vista ou supérieur, si vous cliquez sur le bouton **Analyse de pièces jointes** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits administrateur sera invité à saisir les informations d'authentification de l'administrateur système ;
- Lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

La fenêtre **Contrôle de pièces jointes** vous permet de configurer les réactions de l'application face à différentes catégories d'objets vérifiés ainsi qu'en cas d'erreurs survenues lors de l'analyse. Il existe également une possibilité de configurer l'analyse des archives.

Utilisez les paramètres listés ci-dessous pour configurer les réactions face aux objets malveillants détectés :

- la liste déroulante **Infectés** définit la réaction en cas de détection d'objets infectés par des virus connus et probablement curables ;
- la liste déroulante **Non désinfectés** définit la réaction en cas de détection d'objets infectés par un virus connu et incurable ainsi qu'en cas d'échec de la tentative de désinfection ;

- la liste déroulante **Suspects** définit la réaction face aux objets probablement infectés par un virus (réaction du moteur heuristique) ;
- la section **Programmes malveillants** définit la réaction en cas de détection des programmes malveillants suivants :
  - adwares ;
  - dialers ;
  - canulars ;
  - hacktools ;
  - riskware ;
- la liste déroulante **En cas d'échec de l'analyse** permet de configurer les réactions dans le cas où l'analyse de la pièce jointe est impossible, par exemple en cas de pièce jointe contenant un fichier endommagé ou protégé par un mot de passe ;
- la case **Analyse des archives** permet d'activer ou de désactiver l'analyse des fichiers archivés en pièce jointe. Cochez cette case pour activer l'analyse, décochez-la pour la désactiver.

Le jeu de réactions applicables est fonction de l'événement viral.

Les réactions ci-dessous sont applicables aux objets détectés :

- **Désinfecter** : l'application va tenter de réparer le fichier infecté (cette action est disponible uniquement pour les objets infectés) ;
- **Comme incurables** : la réaction sélectionnée pour les objets incurables sera appliquée à l'objet infecté (cette action est disponible uniquement pour les objets infectés) ;
- **Supprimer** : supprimer l'objet du système ;
- **Déplacer vers la quarantaine** : isoler l'objet dans le dossier de Quarantaine ;
- **Laisser passer** : laisser passer l'objet sans modifications.

11.6.2. Analyse antispam

Dr.Web pour Outlook effectue l'analyse antispam de tous les courriers avec l'Antispam Dr.Web et effectue le filtrage des messages selon les paramètres spécifiés par l'utilisateur.

Pour configurer le contrôle du spam, dans l'application de messagerie Microsoft Outlook, sélectionnez **Outils** → **Options** → l'onglet **Antivirus Dr.Web** (pour Microsoft Outlook 2010, dans la section **Fichiers** → **Options** → **Compléments** choisissez Dr.Web pour Outlook et cliquez sur le bouton **Options du complément**) et cliquez sur le bouton **Filtre antispam**. La fenêtre du Filtre antispam spam s'ouvre.

La fenêtre **Filtre antispam** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous l'OS Windows Vista ou supérieur, si vous cliquez sur le bouton **Filtre antispam** :

- lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits administrateur sera invité à saisir les informations d'authentification de l'administrateur système ;
- lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

Configuration du filtre antispam

La marche à suivre pour configurer le filtre antispam :

- Cochez la case **Contrôle antispam du courrier** pour activer le filtre antispam.
- Si vous souhaitez ajouter un texte dans les en-têtes des messages classés comme spam, cochez la case **Ajouter un préfixe au sujet des messages**. Le texte à ajouter peut être mis dans le champ de texte se trouvant à droite de la case à cocher. Le préfixe inséré par défaut est ***SPAM***.
- Les messages vérifiés peuvent être marqués comme lus dans les propriétés de message. Pour cela, cochez la case **Marquer le message comme lu**. La case **Marquer le message comme lu** est cochée par défaut.
- Vous pouvez aussi configurer les listes blanche et noire pour filtrer le courrier.

En cas d'erreur dans la reconnaissance du spam, merci de transférer les messages concernés à l'administrateur de votre réseau antivirus.

Listes noire et blanche

Les listes blanche et noire servent à filtrer les messages.

Pour afficher ou modifier les listes blanche et noire, depuis l'élément configuration du filtre antispam cliquez sur le bouton **Liste blanche** ou **Liste noire**.

Pour ajouter une adresse à la liste blanche ou noire :

1. Cliquez sur **Ajouter**.
2. Entrez l'adresse électronique dans le champ approprié.
3. Cliquez sur **OK** dans la fenêtre **Modifier la liste**.

Pour modifier des adresses dans la liste :

1. Sélectionnez une adresse à modifier, puis cliquez sur **Modifier**.
2. Apportez les modifications nécessaires.
3. Cliquez sur **OK** dans la fenêtre **Modifier la liste**.

Pour supprimer une adresse de la liste :

1. Sélectionnez l'adresse dans la liste.
2. Cliquez sur **Supprimer**.

Dans la fenêtre **Listes noire et blanche** cliquez sur le bouton **OK** pour sauvegarder les modifications apportées.

Liste blanche

Si l'adresse de l'expéditeur est ajoutée dans la blanche liste, le message ne subit pas l'analyse antispam. Cependant, si les noms de domaine du destinataire et de l'expéditeur sont identiques et que ce nom de domaine est inscrit dans la blanche liste avec le symbole « * », le message sera analysé. Méthodes d'entrée :

- afin d'ajouter un expéditeur dans la liste, saisissez son adresse e-mail complète (par exemple `mail@example.net`). Tous les messages provenant de cette adresse seront délivrés sans contrôle antispam ;
- chaque élément de la liste peut comprendre une seule adresse e-mail ou un seul masque d'adresses ;
- pour ajouter des adresses déterminées dans la liste des expéditeurs, entrez un masque déterminant les adresses nécessaires. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses e-mail ainsi que le symbole « * » remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

Par exemple les variantes ci-dessous sont possibles :

- `mailbox@domain.com`
- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`

Le symbole « * » ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole « @ » est obligatoire.

- pour assurer la réception des messages provenant des adresses qui appartiennent à un domaine déterminé, utilisez le symbole « * » à la place du nom d'utilisateur. Par exemple pour recevoir tous les messages provenant des adresses depuis le domaine *exemple.net, saisissez `*@exemple.net ;`
- pour assurer la réception des messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole « * » à la place du nom de domaine. Par exemple, pour recevoir tous les messages provenant des expéditeurs dont le nom de la boîte e-mail est « martin », saisissez `martin@*`.

Liste noire

Si l'adresse de l'expéditeur est ajoutée dans la liste noire, les messages provenant de cette adresse seront classés comme spam sans analyse supplémentaire. Méthodes d'entrée :

- pour ajouter un expéditeur déterminé dans la liste, entrez son adresse e-mail complète (par exemple `spam@spam.com`). Tous les messages provenant de cette adresse seront automatiquement classés comme spam ;
- chaque élément de la liste peut comprendre une seule adresse e-mail ou un seul masque d'adresses ;
- pour ajouter des adresses déterminées dans la liste des expéditeurs, entrez un masque déterminant les adresses nécessaires. Le masque définit un modèle déterminant un objet. Le masque peut comprendre des symboles utilisés dans les adresses e-mail ainsi que le symbole « * » remplaçant toute séquence de n'importe quels symboles y compris une séquence vide.

Par exemple les variantes ci-dessous sont possibles :

- `mailbox@domain.com`
- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`

Le symbole « * » ne peut être mis qu'au début ou à la fin de l'adresse.

Le symbole « @ » est obligatoire.

- pour classer comme spam tous les messages provenant des adresses du domaine déterminé, utilisez le symbole « * » à la place du nom d'utilisateur. Par exemple pour que tous les messages provenant des expéditeurs du domaine spam.com soient classés comme spam, saisissez `*@spam.com ;`
- pour classer comme spam tous les messages provenant des adresses contenant un nom d'utilisateur déterminé, quel que soit le nom de domaine utilisez le symbole « * » à la place du nom de domaine. Par exemple, pour que tous les messages provenant des expéditeurs dont le nom de boîte e-mail est « martin » soient classés comme spam, saisissez `martin@* ;`
- les adresses appartenant au domaine du destinataire ne sont pas traitées. Par exemple, si la BAL du destinataire (votre BAL) se trouve dans le domaine mail.com, les messages provenant du domaine mail.com ne seront pas traités pas le filtre antispam.

11.6.3. Journal des événements

Dr.Web pour Outlook enregistre les erreurs survenues et les événements dans les journaux suivants :

- journal d'événements système (Event Log) ;

- journal texte de débogage.

Journal d'événements système

Le journal d'événement système (Event Log) collecte les informations suivantes :

- messages sur l'arrêt ou le démarrage de l'application ;
- paramètres des modules : scanner, moteur, bases virales (ces informations sont écrites au démarrage ou lors de la mise à jour des modules) ;
- messages sur la détection des virus .

Pour afficher le journal d'événements système :

1. Allez au **Panneau de configuration du système d'exploitation**.
2. Sélectionnez la section **Outils d'administration** → **Observateur d'événements**.
3. Dans la partie gauche de la fenêtre **Observateur d'événements**, sélectionnez l'élément **Application**. La liste des événements enregistrés dans le journal par des applications utilisateur va s'afficher. La source des messages pour Dr.Web pour Outlook est l'application Dr.Web pour Outlook.

Journal texte de débogage

Le journal texte de débogage collecte les informations listées ci-dessous :

- messages sur la détection des virus ;
- messages sur des erreurs survenues lors de l'écriture dans des fichiers ou lors de la lecture depuis des fichiers ainsi que sur des erreurs d'analyse des archives ou des fichiers protégés par mot de passe ;
- paramètres des modules : scanner, moteur, bases virales ;
- messages sur les arrêts urgents du moteur.

Configuration de la journalisation des événements

1. La fenêtre de paramètres du journal s'ouvre.Dans l'onglet **Antivirus Dr.Web**, cliquez sur le bouton **Journal**.
2. Pour obtenir le niveau maximum de détails du fichier de journal, cochez la case **Ecrire le journal détaillé**. Par défaut, la journalisation est paramétrée sur le mode régulier.

   

   Obtenir le niveau maximum de détails des journaux influe sur les performances du serveur ; ainsi, il est recommandé d'activer le niveau maximum de détail uniquement en cas d'erreur de Dr.Web pour Outlook.

3. Cliquez sur **OK** pour sauvegarder les modifications apportées.

La fenêtre **Journal** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous Windows Vista ou supérieur, si vous cliquez sur le bouton **Journal** :

- lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits administrateur sera invité à saisir les informations d'authentification de l'administrateur système ;
- lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

L'affichage du journal des événements

Pour afficher le journal texte des événements, cliquez sur le bouton **Afficher dans le dossier**. Le dossier dans lequel est sauvegardé le journal sera ouvert.

11.6.4. Statistiques

Dans l'application Microsoft Outlook, la section **Outils** → **Options** → l'onglet **Antivirus Dr.Web** (en cas de Microsoft Outlook 2010, allez dans la section **Fichier** → **Options** → **Add-ins**, sélectionnez le module **Dr.Web pour Outlook** et cliquez sur **Options**) offre des informations statistiques sur le total d'objets analysés et traités par l'application.

Les objets sont divisés selon les catégories suivantes :

- **Analysés** : le total des messages analysés ;
- **Infectés** : le total des messages contenant des virus ;
- **Suspects** : le total des messages probablement infectés par des virus (réaction du moteur heuristique) ;
- **Désinfectés** : le total des objets réparés par l'application ;
- **Non vérifiés** : le total des objets dont l'analyse est impossible ou entraîne des erreurs d'analyse ;
- **Sains** : le total des messages qui ne contiennent aucun objet malveillant.

Les informations suivantes seront également affichées :

- **Déplacé** : le total des objets déplacés vers la Quarantaine ;
- **Supprimé** : le total des objets supprimés du système ;
- **Sautés** : le total des objets sautés sans modifications ;
- **Messages spam** : le total des messages classés comme spam.

Par défaut, les statistiques sont sauvegardées dans le fichier drwebforoutlook.stat se trouvant dans le dossier %USERPROFILE%\Doctor Web.

Les informations statistiques sont accumulées au sein d'une session. Après le redémarrage de l'ordinateur ou lors du nouveau lancement de Agent pour Windows, les statistiques sont remises à zéro.

11.7. 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.

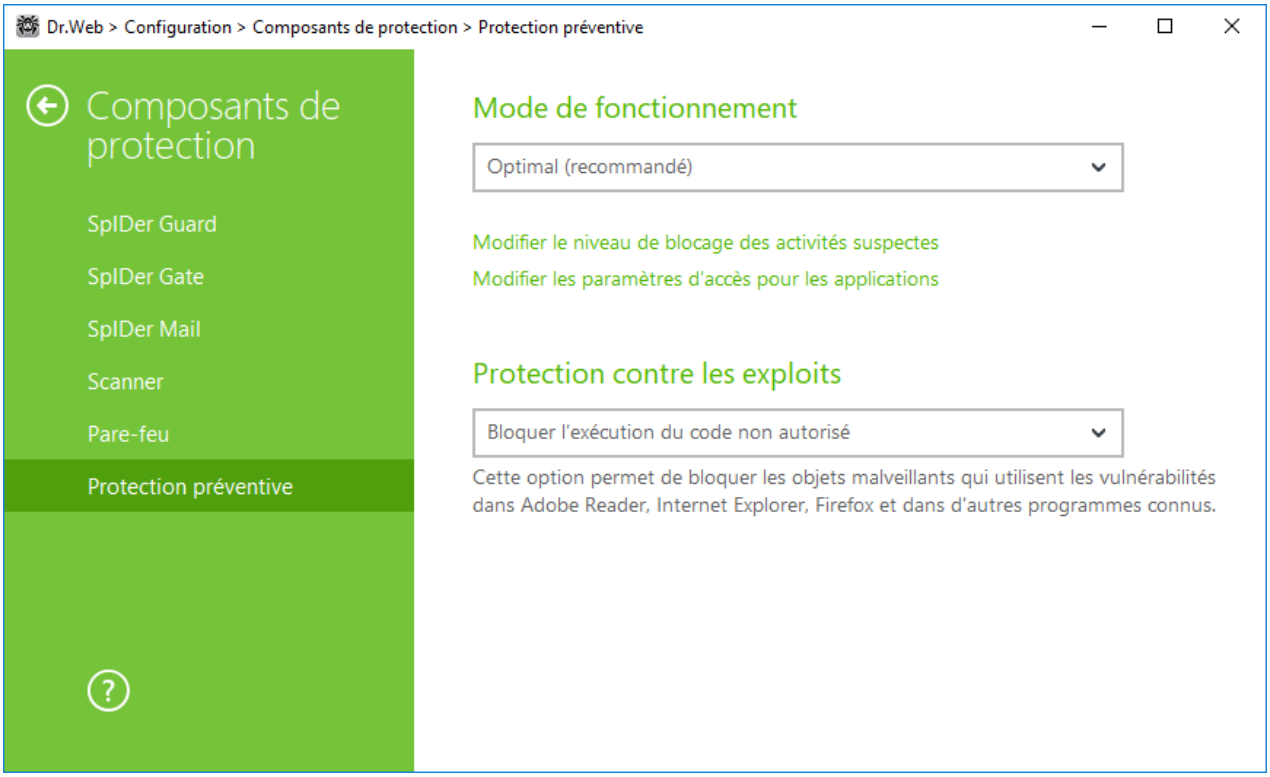

Figure 33. Configuration de la protection préventive

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 déjà créée, sélectionnez-la dans la liste 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**, Dr.Web interdit la modification automatique des objets système, la modification qui indiquerait clairement une tentative malveillante d'endommager le système d'exploitation. L'accès bas niveau au disque est interdit, ainsi que toute modification du fichier HOSTS par les applications dont les actions sont considérées comme tentative d'endommager le système.

Seules les actions des applications qui ne sont pas de confiance sont bloquées.

Vous pouvez choisir le mode **Moyen**, s'il existe un risque élevé d'infection. 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.

Le niveau de protection **Paranoïde** est nécessaire pour avoir un contrôle total de l'accès aux objets Windows critiques. Dans ce mode, Dr.Web fournit également un contrôle interactif sur le chargement de pilotes et le démarrage automatique de programmes.

Dans le mode **Défini 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 Exclusions ne sont pas gérés.
Intégrité des fichiers des utilisateurs	Cette option permet la détection des processus qui modifient les fichiers utilisateur avec un algorithme connu qui indique que le processus peut compromettre la sécurité de l'ordinateur. Les processus qui sont ajoutés à Exclusions ne sont pas gérés.
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

Objet protégé	Description
	Associations de fichiers exécutables : • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (clés) • 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.

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.

12. Statistiques

Cette fenêtre contient les statistiques sur les événements importants de fonctionnement des composants de protection.

Pour consulter les informations sur le fonctionnement des composants, ouvrez le menu 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
- Office Control

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.

Dans le groupe **Office Control**, les statistiques des URL bloquées sont affichées pour chaque compte.

Les informations suivantes sont enregistrées dans le rapport :

- Fréquence de visites ;
- Action ;
- URL.

Pour toutes les entrées du rapport il existe des filtres prédéfinis qui sont disponibles dans la liste déroulante en haut de la page.

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

Activité réseau

Si Pare-feu Dr.Web est installé, le rapport de l'activité réseau est disponible.

Vous pouvez voir les informations sur les applications en cours, le journal des applications et le journal du filtre de paquet. Pour ce faire, sélectionnez l'objet nécessaire dans la liste déroulante.

Dans le rapport, les informations suivantes sont affichées pour chaque application en cours :

- direction de transmission de données ;
- protocole de fonctionnement ;
- adresse locale ;
- adresse distante ;
- taille du paquet de données envoyé ;

- taille du paquet de données reçu.

Dans le journal des applications, vous verrez :

- heure de début du fonctionnement de l'application ;
- nom de l'application ;
- nom de la règle du traitement de l'application ;
- direction de transmission de données ;
- action ;
- adresse cible.

Dans le journal du filtre de paquets, les informations suivantes sont affichées :

- heure de début du traitement du paquet de données ;
- direction de la transmission du paquet de données ;
- nom de la règle de traitement ;
- interface ;
- contenu du paquet.

Avec le bouton  , vous pouvez exporter les entrées des journaux ou effacer les entrées des journaux.

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 **Composant**.

Vous pouvez trier les événements par codes. Pour ce faire, indiquez-les dans le champ **Code (par exemple : 100-103, -102, 403)** en respectant les règles suivants :

- séparez les codes par une virgule ;
- vous pouvez indiquer une plage de codes (par exemple, 100-103) ;
- le symbole « - » devant le code l'exclut de la plage.

Ainsi, une ligne du type suivant « `100-103,-102,403` » signifie qu'il faut afficher tous les événements de « 100 » à « 103 », exclure du filtre le code « -102 » et afficher l'événement « 403 ».

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

13. Messages du serveur

L'administrateur du réseau a la possibilité de configurer l'envoi de notifications de serveurs sur un poste. Cette fonction est pratique pour recevoir les notifications du serveur quand l'administrateur travaille sur un des postes.

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.

Vous pouvez filtrer les messages par les catégories suivantes :

- Postes ;
- Référentiels ;
- Licences ;
- Administrateurs ;
- Autre.

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

Avec le bouton , vous pouvez supprimer, copier ou exporter les messages sélectionnés ou supprimer tous les messages.

14. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

- consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.com/doc/ ;
- lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/ ;
- visitez des forums de Doctor Web à l'adresse https://forum.drweb.com/.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

- remplissez le formulaire de question dans la section correspondante de la rubrique https://support.drweb.com/ ;
- appelez au numéro : 0 825 300 230.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse https://company.drweb.com/contacts/offices/.

15. Annexe A. Paramètres supplémentaires de ligne de commande

Des paramètres de ligne de commande supplémentaires (clés) sont utilisés pour définir les paramètres des programmes lancés via l'ouverture d'un fichier exécutable. Ceci est relatif au Scanner Dr.Web ainsi qu'au Scanner en ligne de commande. Les clés peuvent définir des 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.

15.1. Paramètres du Scanner et du Scanner en ligne de commande

Clé	Description
`/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'imbrication dans l'archive. L'option est désactivée par défaut.
`/AR`	Scanner les archives. L'option est activée par défaut.
`/ARC:<`*taux_de_compression*`>`	Taux maximum de compression. Si le scanner détecte que le taux 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'imbrication*`>`	Niveau maximum d'imbrication 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 taux de compression (la taille minimum du fichier dans l'archive à partir de laquelle s'effectue la vérification du taux de compression), en Ko. Par défaut — illimité.

Clé	Description
/ARX:<*taille*>	Taille maximum des objets archivés à scanner, en Ko. Par défaut — illimité.
/BI	Afficher les informations sur les bases de données virales. L'option est activée par défaut.
/CUSTOM	Lancer le Scanner sur la page de l'analyse personnalisée. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), l'analyse personnalisée des objets spécifiés sera lancée. (Uniquement pour le Scanner).
/CL	Utiliser le service cloud Dr.Web. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).
/DCT	Ne pas afficher la durée calculée d'analyse. (Uniquement pour le Scanner en ligne de commande).
/DR	Scanner les dossiers de manière récursive (analyser les sous-dossiers). L'option est activée par défaut.
/E:<*nombre_de_flux*>	Effectuer une analyse à un nombre spécifié de flux.
/FAST	Lancer le analyse rapide du système. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), les objets spécifiés seront également analysés. (Uniquement pour le Scanner).
/FL:<*nom_du_fichier*>	Analyser les chemins spécifiés dans le fichier.
/FM:<*masque*>	Analyser les fichiers selon un masque. Par défaut, tous les fichiers seront analysés.
/FR:<*expression_régulière*>	Analyser 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 l'analyse ou les paramètres /TM, /TB), l'analyse rapide et l'analyse des objets spécifiés seront lancées. (Uniquement pour le Scanner).
/FX:<*masque*>	Exclure de l'analyse les fichiers qui correspondent au masque. (Uniquement pour le Scanner en ligne de commande).

Clé	Description
/GO	Mode de fonctionnement du Scanner lors duquel les questions impliquant des réponses d'utilisateur sont ignorées ; les décisions impliquant un choix sont prises automatiquement. Il est utile d'utiliser ce mode pour l'analyse automatique des fichiers, par exemple, lors de l'analyse quotidien ou hebdomadaire du disque dur. Dans la ligne de commande, il est nécessaire de spécifier l'objet à analyser. Vous pouvez utiliser les paramètres /LITE, /FAST, /FULL avec le paramètre /GO. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
/H ou /?	Afficher la rubrique d'aide sur le fonctionnement du programme. (Uniquement pour le Scanner en ligne de commande).
/HA	Effectuer une analyse heuristique des fichiers afin d'y rechercher des 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	Effectuer une analyse du système y compris la mémoire vive, les secteurs d'amorçage de tous les disques, effectuer une recherche des rootkits. (Uniquement pour le Scanner).
/LN	Analyser les fichiers par raccourcis associés. L'option est désactivée par défaut.
/LS	Analyser sous le compte LocalSystem. L'option est désactivée par défaut.
/MA	Analyser les fichiers de messagerie. L'option est activée par défaut.
/MC:<*nombre_de_tentatives* >	Spécifier le 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

Clé	Description
	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'arrêt du système après la fin de l'analyse. (Uniquement pour le Scanner).
/NT	Analyser les flux NTFS. L'option est activée par défaut.
/OK	Afficher la liste complète des objets scannés et accompagner les objets sains de la remarque 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'imbrication*>	Niveau d'imbrication maximum des outils de compression d'un fichier exécutable. Si le niveau d'imbrication dépasse la valeur spécifiée, l'analyse va uniquement jusqu'au niveau d'imbrication 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 l'analyse (indépendamment de l'application/non application des actions aux menaces détectées). (Uniquement pour le Scanner).

Clé	Description
/RA:<*nom_du_fichier*>	Ajouter le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal.
/REP	Analyser selon les liens symboliques. L'option est désactivée par défaut.
/RK	Analyse pour la présence de rootkits. L'option est désactivée par défaut.
/RP:<*nom_du_fichier*>	Enregistrer le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal.
/RPC:<*s*>	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

Clé	Description
	commande).
/SST	Afficher la durée du scan. L'option est désactivée par défaut.
/ST	Lancement du Scanner en tâche de fond. Si le paramètre /GO n'est pas spécifié, le mode graphique s'affiche uniquement en cas de détection d'une menace. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
/TB	Analyser les secteurs de boot et les secteurs MBR du disque dur.
/TM	Détecter les menaces dans la mémoire vive (y compris la partie système de Windows).
/TR	Vérifier les points de restauration système.
/W:<*s*>	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]	A 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)) :

Action	Description
/AAD:<action>	actions appliquées aux adwares (actions possibles : DQIR)
/AAR:<action>	actions appliquées aux archives infectées (actions possibles : DQIR)
/ACN:<action>	actions appliquées aux packages d'installation infectés (actions possibles : DQIR)
/ADL:<action>	actions appliquées aux dialers (actions possibles : DQIR)
/AHT:<action>	actions appliquées aux hacktools (actions possibles : DQIR)
/AIC:<action>	actions appliquées aux fichiers incurables (actions possibles : DQR)

Action	Description
/AIN:<action>	actions appliquées aux fichiers infectés (actions possibles : CDQR)
/AJK:<action>	actions appliquées aux canulars (actions possibles : DQIR)
/AML:<action>	actions appliquées aux fichiers de messagerie infectés (actions possibles : QIR)
/ARW:<action>	actions appliquées aux riskwares (actions possibles : DQIR)
/ASU:<action>	actions appliquées aux 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 du paramètre « 0 » signifie que le paramètre est utilisé sans restrictions.

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`.

15.2. Paramètres des packages d'installation

`/compression` <*mode*> : mode de compression du trafic avec le serveur de protection centralisée. Le paramètre <*mode*> peut prendre une des valeurs suivantes :

- `yes` : utiliser la compression.
- `no` : ne pas utiliser la compression.

- `possible` : la compression est possible. La décision est prise en fonction des paramètres du Serveur.

Si la clé n'est pas définie, la valeur `possible` est utilisée par défaut.

`/encryption` <*mode*> : mode de chiffrement du trafic avec le serveur de protection centralisée. Le paramètre <*mode*> peut prendre une des valeurs suivantes :

- `yes` : utiliser le chiffrement.
- `no` : ne pas utiliser le chiffrement.
- `possible` : le chiffrement est possible. La décision est prise en fonction des paramètres du Serveur.

Si la clé n'est pas définie, la valeur `possible` est utilisée par défaut.

`/excludeFeatures` <*composants*> : la liste des composants qui seront exclus lors de l'installation. Si vous spécifiez quelques paramètres utilisez le caractère « , » en tant que séparateur. Les composants disponibles :

- `scanner` : Scanner Dr.Web,
- `spider-mail` : SpIDer Mail,
- `spider-g3` : SpIDer Guard,
- `outlook-plugin` : Dr.Web pour Microsoft Outlook,
- `firewall` : Pare-feu Dr.Web,
- `spider-gate` : SpIDer Gate,
- `parental-control` : Office Control,
- `antispam-outlook` : Antispam Dr.Web pour le composant Dr.Web pour Microsoft Outlook,
- `antispam-spidermail` : Antispam Dr.Web pour le composant SpIDer Mail.

Pour les composants non indiqués directement, le statut d'installation spécifié par défaut est gardé.

`/id` <*station_id*> : identificateur d'un poste sur lequel l'Agent Dr.Web sera installé.

Le paramètre est indiqué avec le mot de passe (clé /pwd) pour une authentification automatique sur le serveur. Si les paramètres d'authentification ne sont pas définis, la décision est prise du côté du Serveur.

`/includeFeatures` <*composants*> : la liste des composants à installer. Si vous spécifiez quelques paramètres utilisez le caractère « , » en tant que séparateur. Les composants disponibles :

- `scanner` : Scanner Dr.Web,
- `spider-mail` : SpIDer Mail,
- `spider-g3` : SpIDer Guard,
- `outlook-plugin` : Dr.Web pour Microsoft Outlook,
- `firewall` : Pare-feu Dr.Web,

- `spider-gate` : SpIDer Gate,
- `parental-control` : Office Control,
- `antispam-outlook` : Antispam Dr.Web pour le composant Dr.Web pour Microsoft Outlook,
- `antispam-spidermail` : Antispam Dr.Web pour le composant SpIDer Mail.

Pour les composants non indiqués directement, le statut d'installation spécifié par défaut est gardé.

`/installdir` <*folder*> : dossier d'installation.

Si le paramètre n'est pas défini, le dossier d'installation par défaut est Program Files\DrWeb folder sur le disque système.

`/instMode` <*mode*> : mode de lancement de l'installateur. Le paramètre <*mode*> peut prendre une des valeurs suivantes :

- `remove` : supprimer le produit installé.

Si le paramètre n'est pas défini, l'installateur détermine par défaut automatiquement le mode de lancement.

`/lang` <*code_de_la_langue*> : langue de l'installateur et du produit installé. Le code de la langue est indiqué au format ISO-639-1.

Si le paramètre n'est pas défini, la langue système est utilisée par défaut.

`/pubkey` <*chemin*> : chemin complet vers le certificat ou le fichier de la clé publique du serveur.

Si le certificat ou la clé publique n'est pas défini, après le lancement de l'installation locale, l'installateur utilise automatiquement le certificat (avec l'extension .pem) ou la clé publique (drwcsd.pub) de son propre dossier de lancement. Si le certificat ou la clé publique est située dans un autre dossier que le dossier de l'installateur, vous devez indiquer manuellement le chemin complet vers le fichier de certificat ou de clé publique.

Si vous lancez le package d'installation généré dans le Centre de Gestion, le certificat ou la clé publique est inclus au package d'installation et il n'est pas nécessaire de l'indiquer encore une fois.

`/pwd` <*mot de passe*> : mot de passe de l'Agent Dr.Web pour accéder au serveur.

Le paramètre est indiqué avec l'identificateur du poste (clé /id) pour une authentification automatique sur le Serveur. Si les paramètres d'authentification ne sont pas définis, la décision d'authentification est prise du côté du serveur.

`/regagent` <*mode*> : détermine si l'Agent Dr.Web sera enregistré dans la liste des programmes installés. Le paramètre <mode> peut prendre une des valeurs suivantes :

- `yes` : enregistrer l'Agent Dr.Web dans la liste des programmes installés.
- `no` : ne pas enregistrer l'Agent Dr.Web dans la liste des programmes installés.

Si le paramètre n'est pas défini, la valeur `no` est utilisée par défaut.

`/retry` <*number*> : nombre de tentatives de localisation du Serveur par l'envoi de requêtes multicast. Si le Serveur n'a pas répondu alors que le nombre de tentatives a été atteint, le Serveur est considéré comme introuvable.

Si le paramètre n'est pas défini, 3 tentatives pour trouver le Serveur sont effectuées.

`/server` [<*protocol*>/]<*server_address*>[:<*port*>] : l'adresse du Serveur depuis lequel l'installation de l'Agent Dr.Web sera effectuée et auque l'Agent Dr.Web se connecte après l'installation.

Si le paramètre n'est pas défini, le serveur est recherché par défaut : par l'envoi de requêtes multicast.

`/silent` <*mode*> : détermine si l'installateur sera lancé en tâche de fond. Le paramètre <*mode*> peut prendre une des valeurs suivantes :

- `yes` : lancer l'installateur en tâche de fond.
- `no` : lancer l'installateur en mode graphique.

Si la clé n'est pas définie, l'installation de l'Agent Dr.Web s'effectue par défaut en mode graphique.

`/timeout` <*time*> : délai d'attente de chaque réponse lors de la recherche du Serveur. Défini en secondes. La réception de messages de réponse continue tant que le délai de réponse est inférieur à la valeur indiquée.

Si le paramètre n'est pas défini, 3 secondes sont utilisées par défaut.

15.3. 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.

Code de retour	Événement
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 ».

16. 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.

16.1. 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 des informations 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 programmes « gris » ou « programmes potentiellement indésirables ». 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. Les macros, ce sont des programmes 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 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.

16.2. 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 de copies de programmes malveillants, 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 dans 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. Par exemple, la désinfection d'un ver d'ordinateur signifie la destruction de toutes ses 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 l'objet malveillant sont bloquées. Le renommage signifie que l'extension du fichier est modifiée, ce qui le rend inopérant.

17. 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 https://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.

Préfixes 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 messagerie ;
- `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 la fonction de RAT (Remote Administration Tool – utilitaire d'administration à distance) ;
- `IRC` : Trojan qui utilise des canaux Internet Relay Chat ;
- `DownLoader` : Trojan qui télécharge discrètement différents programmes malveillants sur Internet ;
- `MulDrop` : Trojan qui télécharge discrètement 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 l'utilisateur vers un site spécial (ou des sites) ;
- `KeyLogger` : Trojan spyware qui suit et enregistre des touches saisies ; il peut envoyer les données collectées à un cybercriminel ;
- `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 destinés à attaquer certaines vulnérabilités connues des systèmes d'exploitation afin de provoquer l'arrêt du système attaqué ;
- `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 où 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'interprète 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.