

Protection contre les nouveaux virus

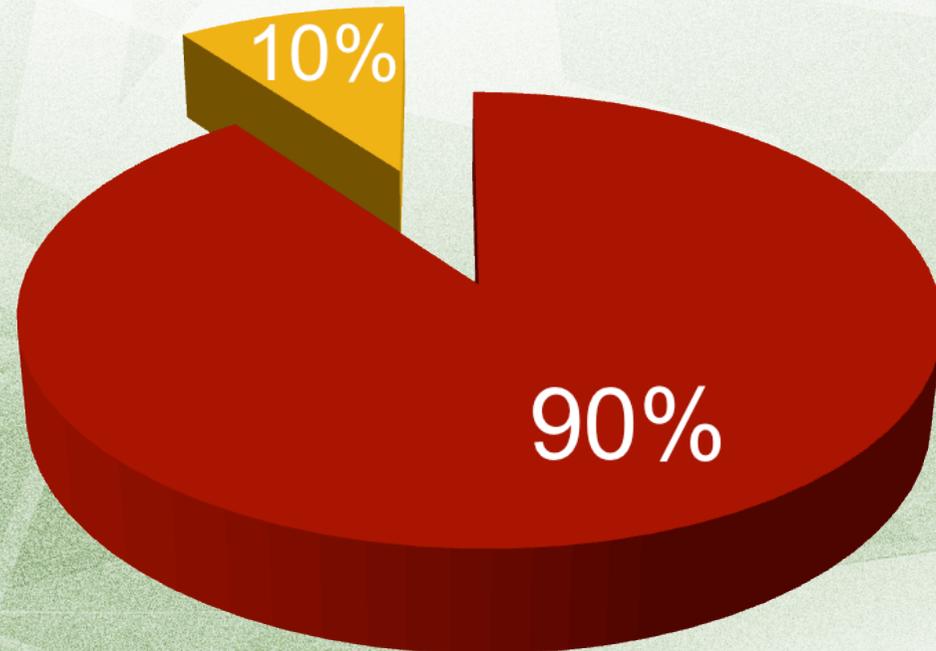
Nouveautés de Dr.Web 9.0





Les menaces actuelles.

Les Trojans des familles Encoder, Winlock, Inject, Exploit représentent **presque 90%** des menaces réelles





Par menaces réelles, nous entendons les virus et les trojans pouvant altérer l'ordinateur et causer des dommages à son propriétaire.





A quoi ressemble le monde de malwares actuels ?





1. Depuis un certain temps, l'écriture de virus prend de l'envergure, et c'est devenu un **business illicite à part entière.**





De nouveaux programmes malveillants apparaissent **tous les jours par centaines de milliers** et les analystes **N'ONT PAS LE TEMPS** de traiter de **tels volumes** de fichiers suspects.





Des heures ou des jours passent avant qu'un nouveau virus ne soit répertorié dans la base de données virales. En cas de virus complexe, ce délai peut s'étaler sur plusieurs mois.





**Il y a TOUJOURS UN RISQUE
d'être contaminé
par un virus INCONNU.**





2. Il n'y a que très peu de nouveaux virus.





Le même virus peut être empaqueté plusieurs fois par heure pour être diffusé sous la forme d'un nouveau virus.





Dans ce cas, l'antivirus n'est pas toujours en mesure de le reconnaître.





3. Mais ces virus ont les mêmes comportements dans le système infecté — c'est leur point faible.



Historique



- **1992** : Igor Danilov crée la première version de l'analyseur antivirus de comportement pour MS-DOS et OS/2.



Historique



- **1999** — les développeurs de Dr.Web annoncent la création de la technologie **SpIDer Netting** pour Windows 9.x — **le premier** analyseur de comportement pour MS Windows.





Historique

- 2013

Nouveauté !

Dr.Web Process Heuristic (DPH)

Nouvel analyseur de comportement de Dr.Web.



© Doctor Web

www.drweb.fr



La neutralisation **de logiciels malveillants inconnus** de la base virale de Dr.Web.



Comment Dr.Web Process Heuristic fonctionne-t-il ?

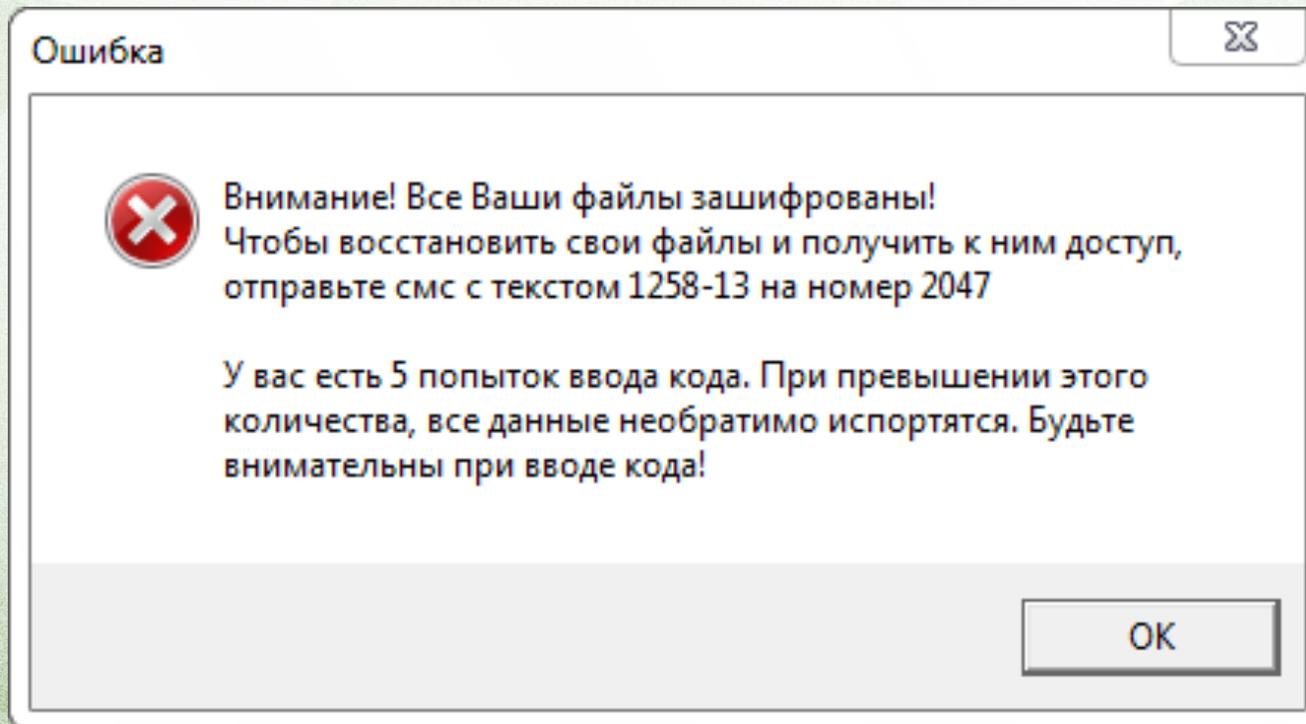


DPH peut détecter les nouvelles menaces en analysant le comportement de logiciels dans le système.

DPH est efficace contre les menaces sophistiquées qui ne sont pas détectées par les autres technologies heuristiques.



Comment Dr.Web Process Heuristic fonctionne-t-il ?



Comment Dr.Web Process Heuristic fonctionne-t-il ?



Une menace a été détectée

Total de menaces détectées et neutralisées: 1

[Plus d'info](#)

▲ [Dr.Web icon] [Network icon] [Speaker icon] FRA 14:43
07/11/2013

A notification window from Dr.Web. It features the Dr.Web logo on the left, which is a green shield with a lightbulb and a red lightning bolt. The main text reads 'Une menace a été détectée' and 'Total de menaces détectées et neutralisées: 1'. There is a link for 'Plus d'info'. The bottom of the window shows system tray icons: an up arrow, the Dr.Web icon, a network icon, a speaker icon, the language 'FRA', and the time '14:43' and date '07/11/2013'.

Comment Dr.Web Process Heuristic fonctionne-t-il ?



Liste de menaces détectées

 Dr.Web a détecté et neutralisé les objets malveillants suivants ::

Objet	Menace	Action	Chemin
fd.exe	DPH:Trojan.Encoder.gen...	Déplacé	C:\Users\User\De...fd.exe

[Aide](#)



Nouvelle protection préventive



Diminue le risque
d'infection en cas de
lancement d'un logiciel
malveillant inconnu de
l'antivirus.



Nouvelle protection préventive



Aucun écran
verrouillé



Pas de problèmes
avec le démarrage
de Windows



Aucune
disparition des
icônes du bureau



Nouvelle protection préventive



Protège l'intégrité des documents, de la musique, des photos et d'autres fichiers de l'utilisateur contre la modification et la suppression.



Nouvelle protection préventive



A screenshot of a Windows Start menu. The menu is open, showing a list of applications and utilities. The items are:

- A propos de
- Enregistrer la licence
- Mon Dr.Web
- Aide
- SplDer Guard
- SplDer Mail
- SplDer Gate
- Contrôle Parental
- Pare-feu
- Updater
- Scanner
- Outils
- Mode administrateur

The taskbar at the bottom shows the system tray with icons for network, volume, and language (FRA).



Nouvelle protection préventive



A screenshot of the Dr.Web software interface. The main menu is open, showing the following options:

- A propos de
- Enregistrer la licence
- Mon Dr.Web
- Aide
- SplDer Guard
- SplDer Mail
- SplDer Gate
- Contrôle Parental
- Pare-feu
- Updater
- Scanner
- Outils** (highlighted)
- Mode utilisateur

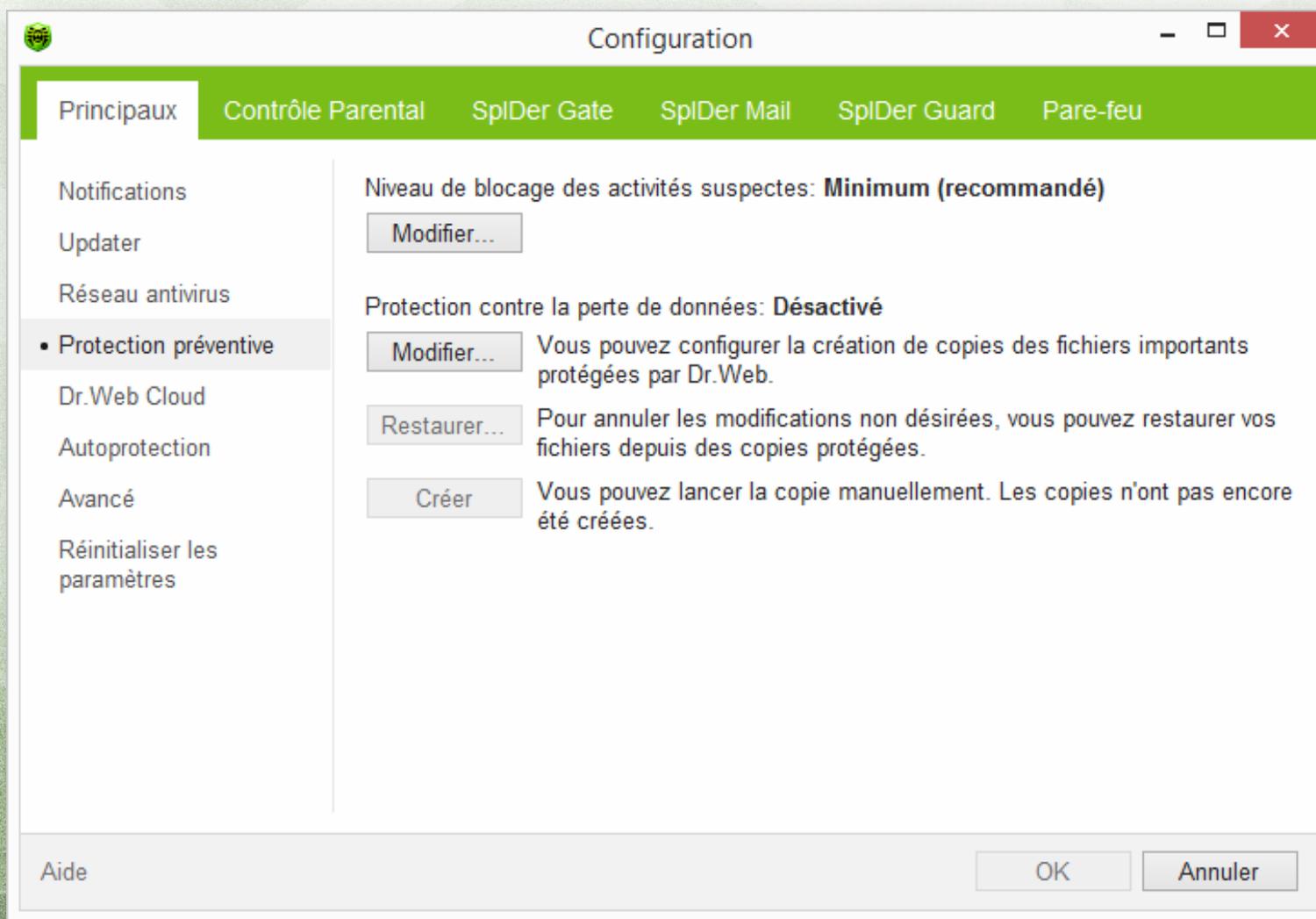
A secondary menu is open over the 'Outils' option, listing the following sub-options:

- Gestionnaire de licence
- Configuration
- Statistiques
- Gestionnaire de Quarantaine
- Réseau antivirus
- Gestionnaire de rapports

The taskbar at the bottom shows system icons for volume, network, and a language indicator set to 'FRA'.



Nouvelle protection préventive



Nouvelle protection préventive



Paramètres de protection de données

Désactiver la protection contre la perte de données
 Activer la protection contre la perte de données

Dossiers	Ajouter	Supprimer
C:\Users\Public\Documents		
C:\Users\Public\Desktop		
C:\Users\User\Documents		
C:\Users\User\Desktop		

Sélectionnez un disque pour stocker les copies protégées

(C:) 13,9 GB de 25,0 GB libre Supprimer les copies

Périodicité

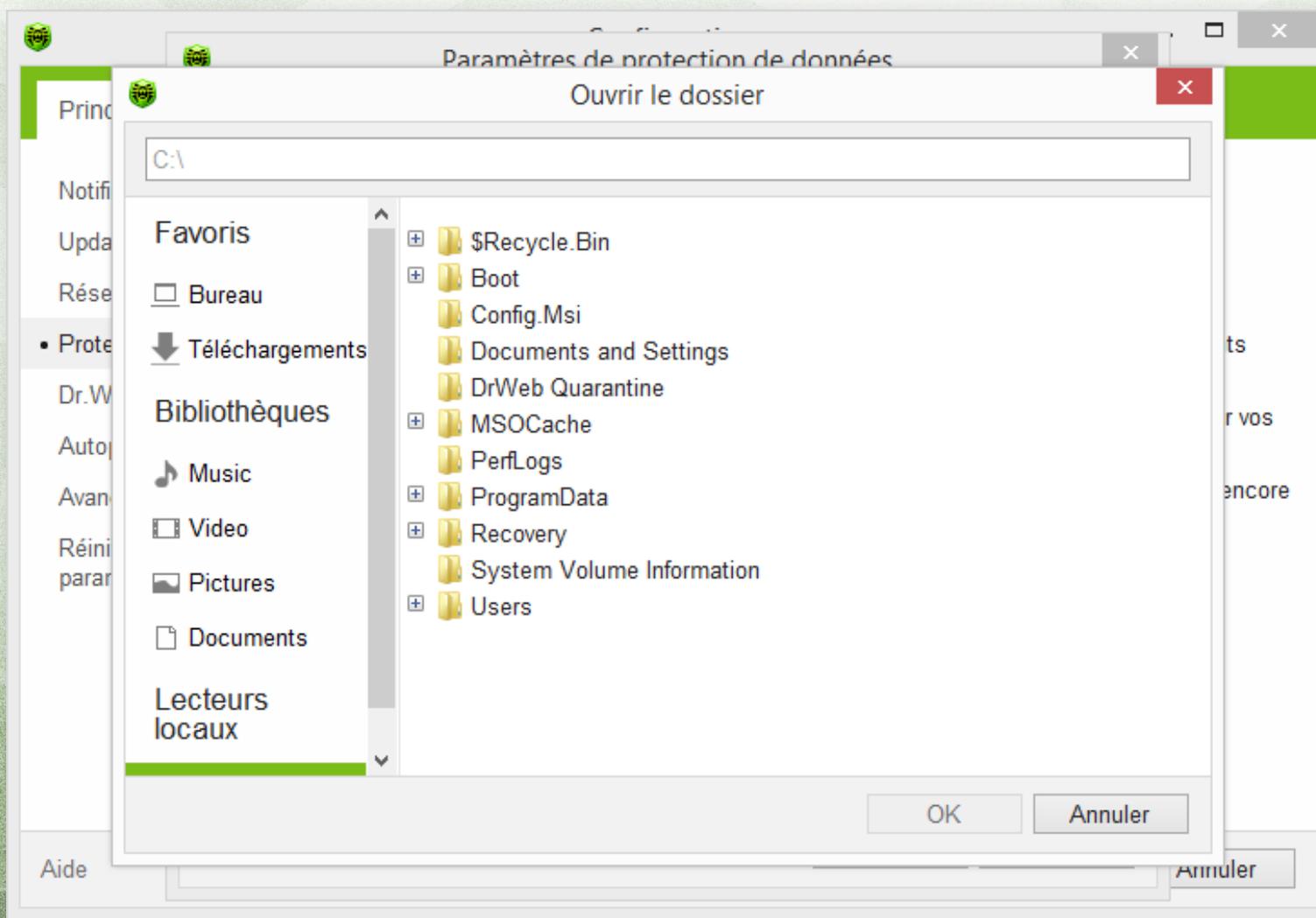
toutes les 24 heures

Ne pas lancer la copie de sauvegarde lorsque vous utilisez la batterie

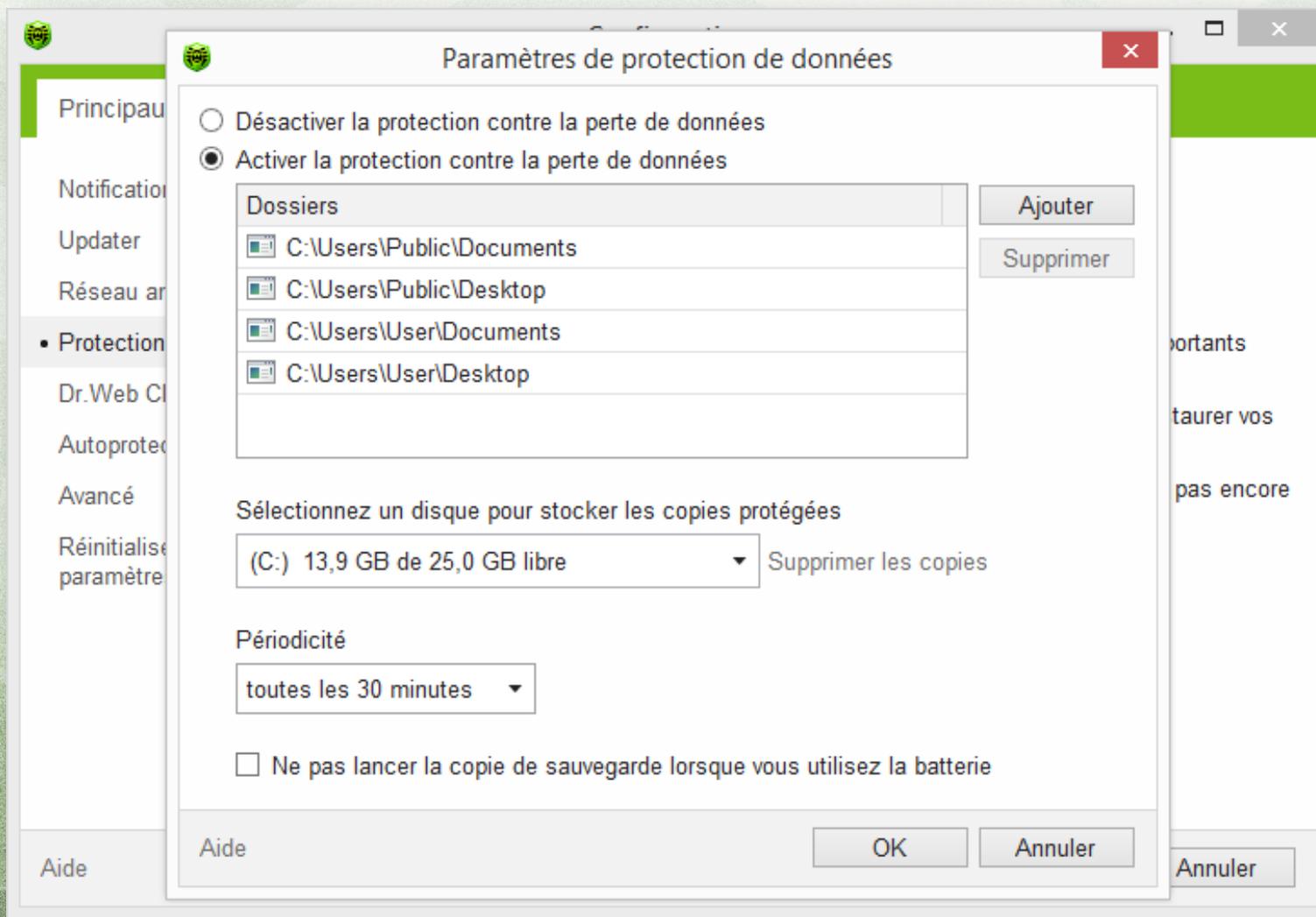
Aide OK Annuler Annuler



Nouvelle protection préventive



Nouvelle protection préventive



Nouvelle protection préventive



Nouvelle protection préventive



Paramètres de protection de données

Désactiver la protection contre la perte de données

Activer la protection contre la perte de données

Dossiers	Ajouter	Supprimer
C:\Users\Public\Documents		
C:\Users\Public\Desktop		
C:\Users\User\Documents		
C:\Users\User\Desktop		

Sélectionnez un disque pour stocker les copies protégées

(C:) 13,9 GB de 25,0 GB libre Supprimer les copies

Périodicité

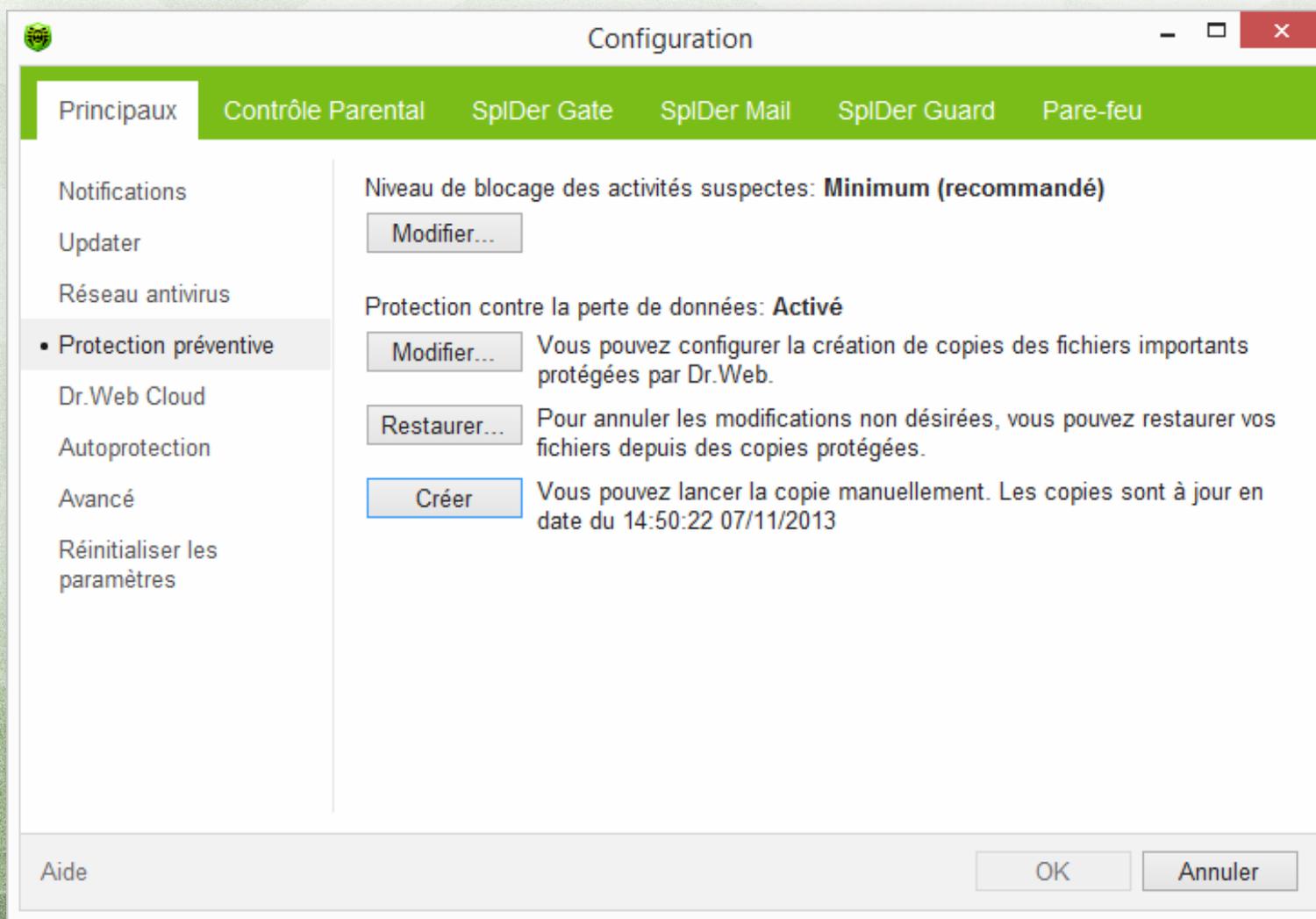
toutes les 30 minutes

Ne pas lancer la copie de sauvegarde lorsque vous utilisez la batterie

Aide OK Annuler Annuler



Nouvelle protection préventive



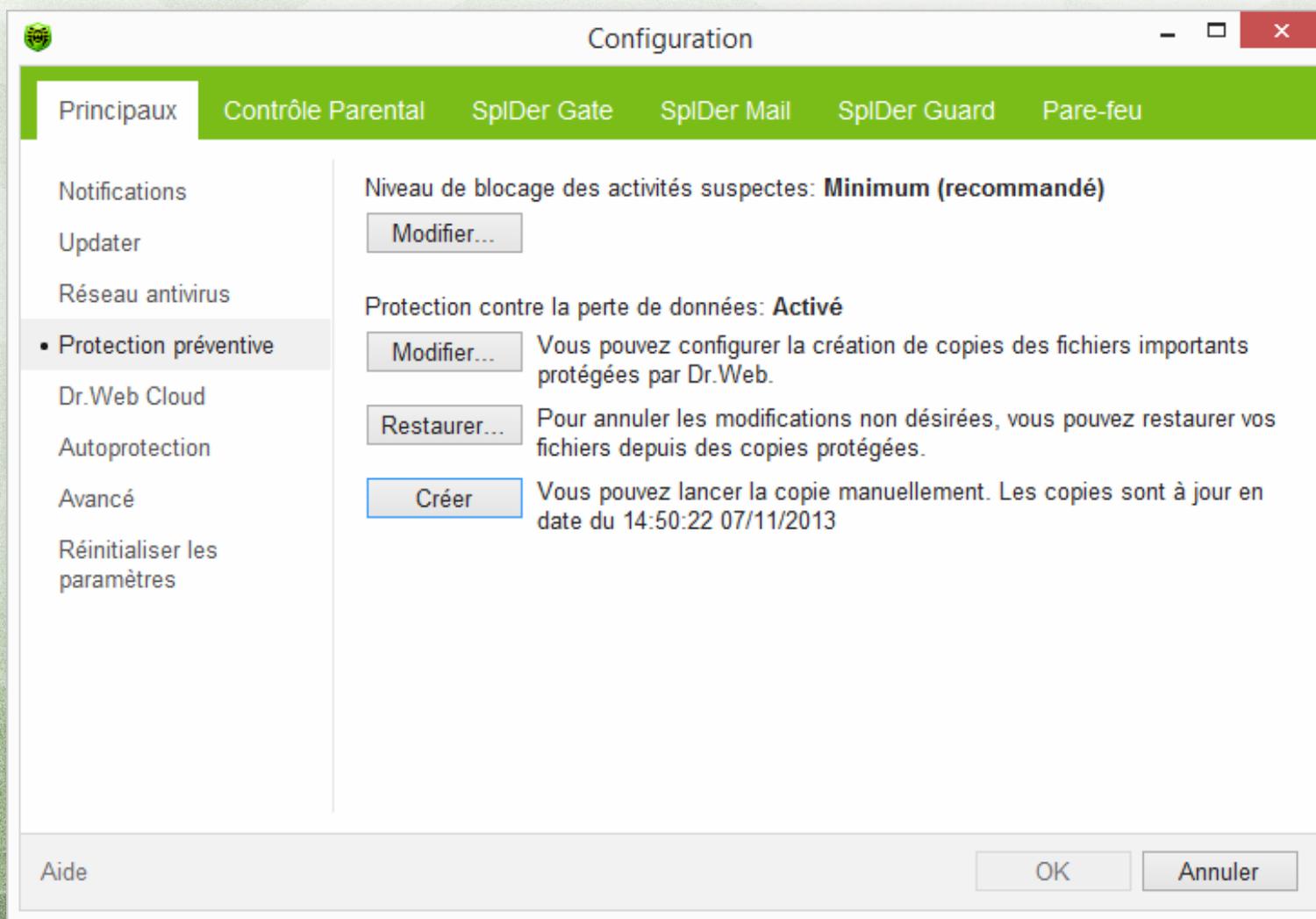
Nouvelle protection préventive



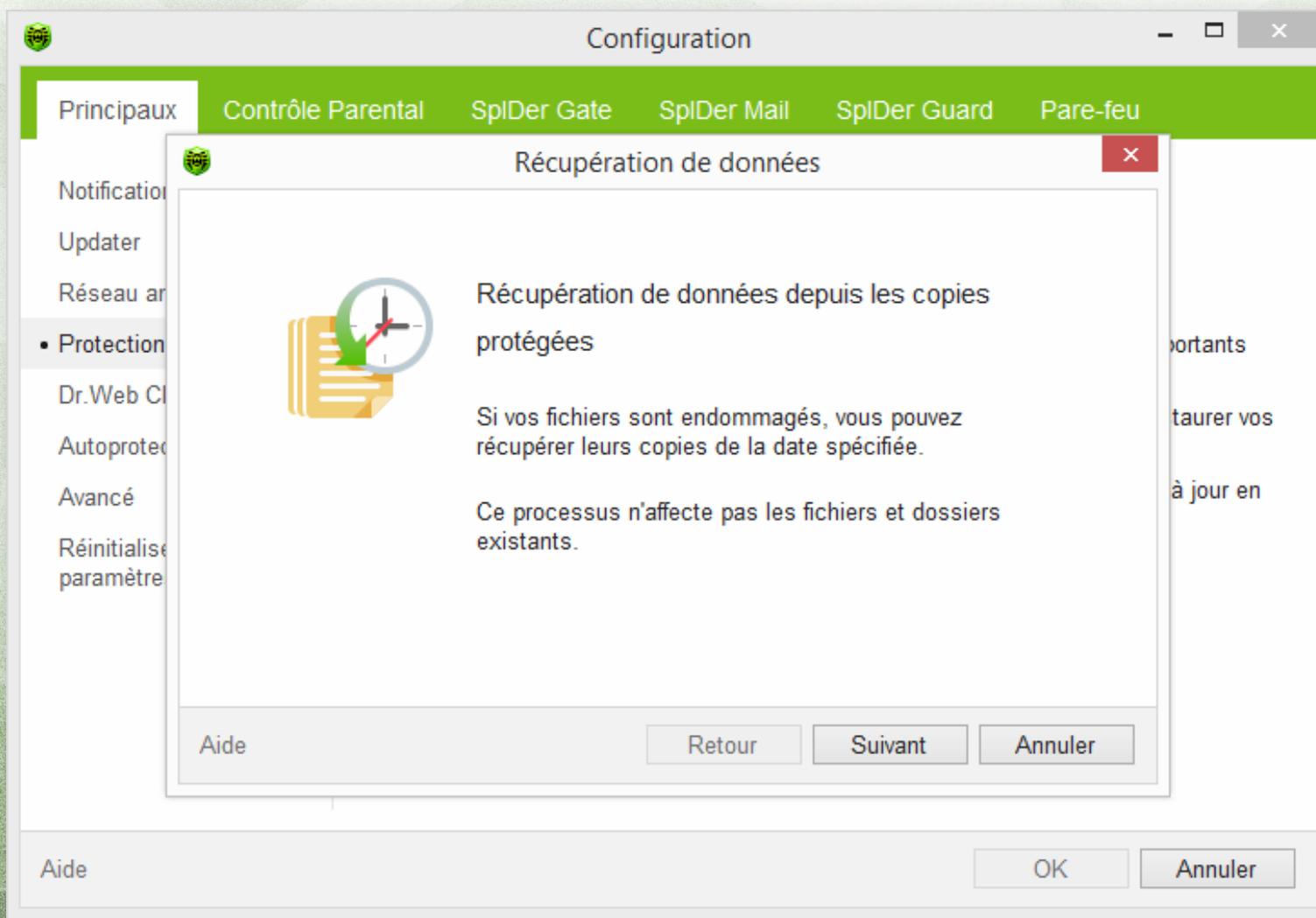
The image shows a screenshot of the Dr.Web Configuration window. The window title is 'Configuration'. The main menu includes 'Principaux', 'Contrôle Parental', 'SpIDer Gate', 'SpIDer Mail', 'SpIDer Guard', and 'Pare-feu'. The 'Protection préventive' section is selected in the left sidebar. The main area shows 'Niveau de blocage des activités suspectes: Minimum (recommandé)' with a 'Modifier...' button, and 'Protection contre la perte de données: Activé'. A 'Nouvelle copie' dialog box is open, prompting the user to enter a description for a new copy, with the text '14-50; 07/11/2013' entered in the text box. The dialog box has 'Aide', 'OK', and 'Annuler' buttons. The main window also has 'Aide', 'OK', and 'Annuler' buttons at the bottom.



Nouvelle protection préventive



Nouvelle protection préventive



Nouvelle protection préventive



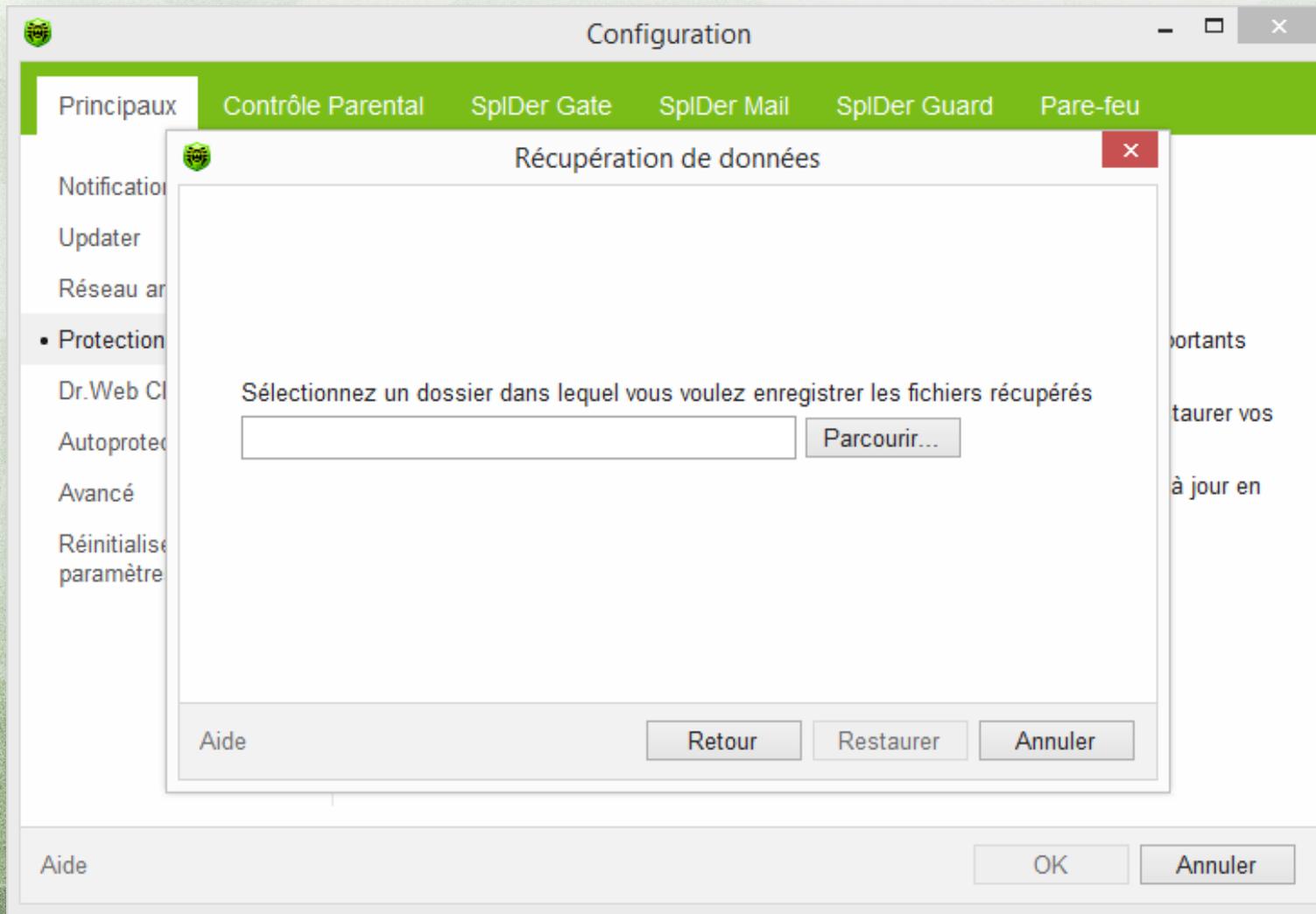
The screenshot shows the 'Configuration' window of Dr.Web software. The 'Principaux' tab is selected, and the 'Protection' section is active in the left sidebar. A dialog box titled 'Récupération de données' is open, prompting the user to select a version of protected copies to recover. The dialog contains a table with the following data:

Date et heure	Description
07/11/2013 14:50:22	14-49; 07/11/2013

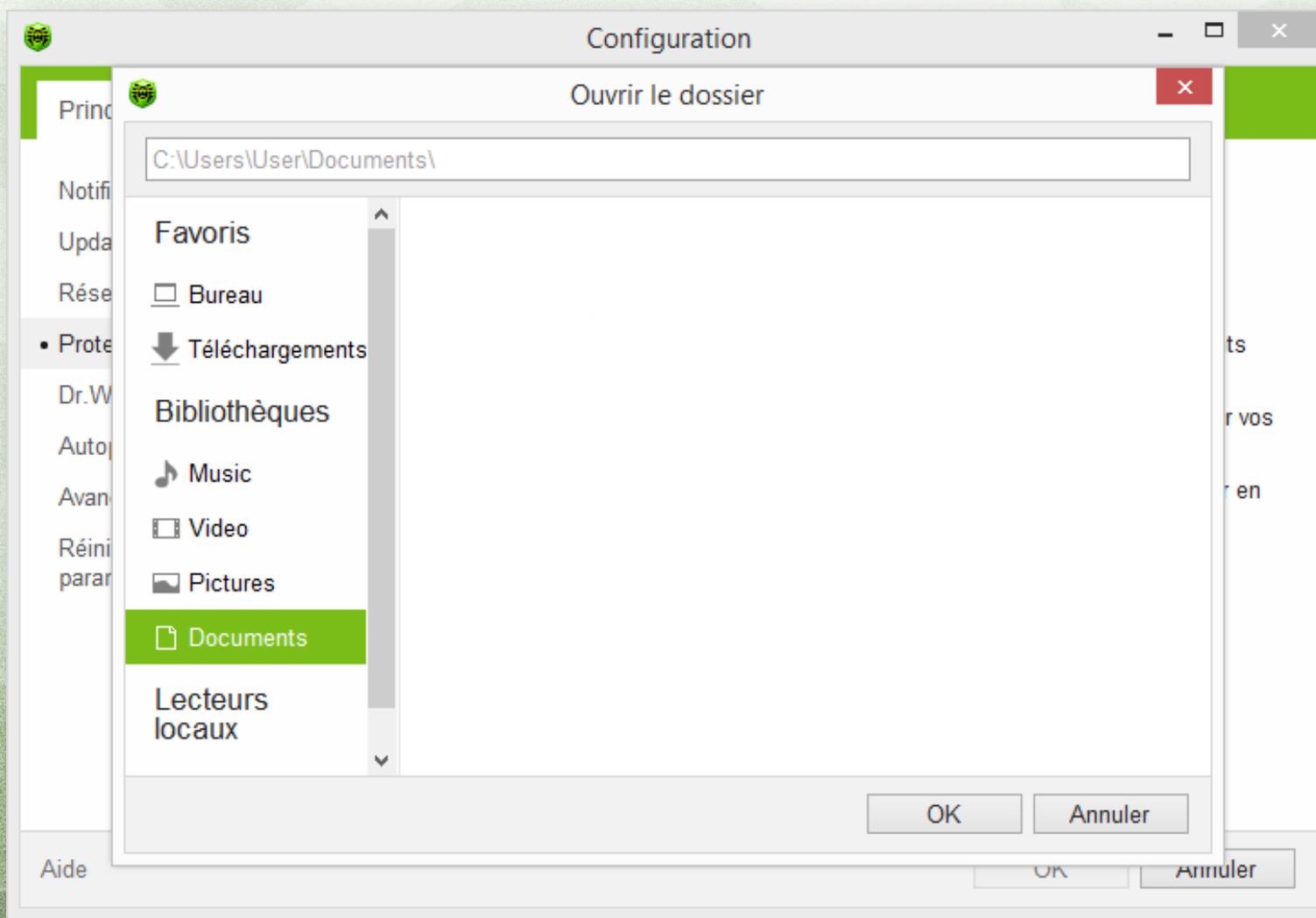
At the bottom of the dialog, there are buttons for 'Aide', 'Retour', 'Suivant', and 'Annuler'. The 'Suivant' button is highlighted with a blue border. The main configuration window also has 'Aide', 'OK', and 'Annuler' buttons at the bottom.



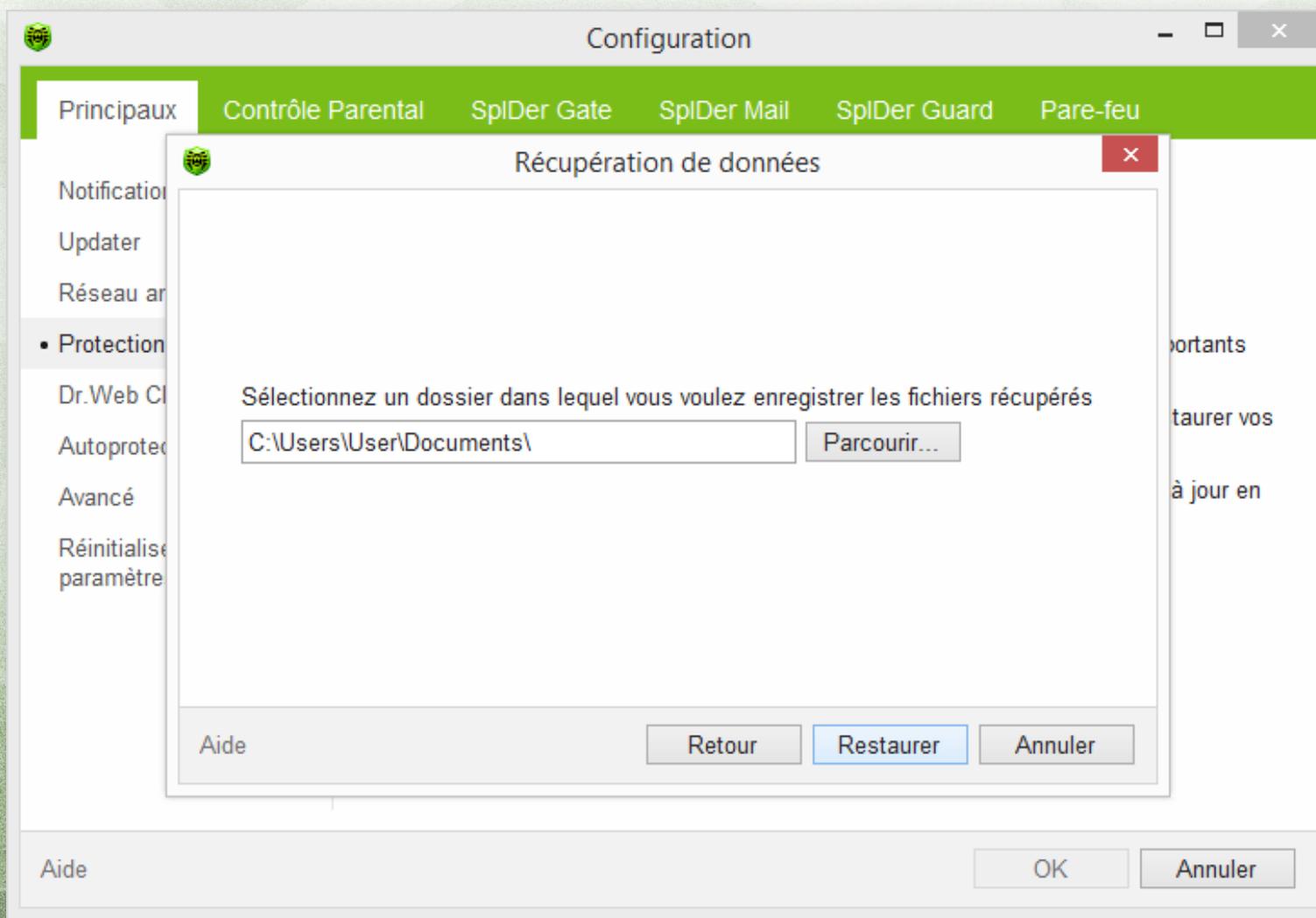
Nouvelle protection préventive



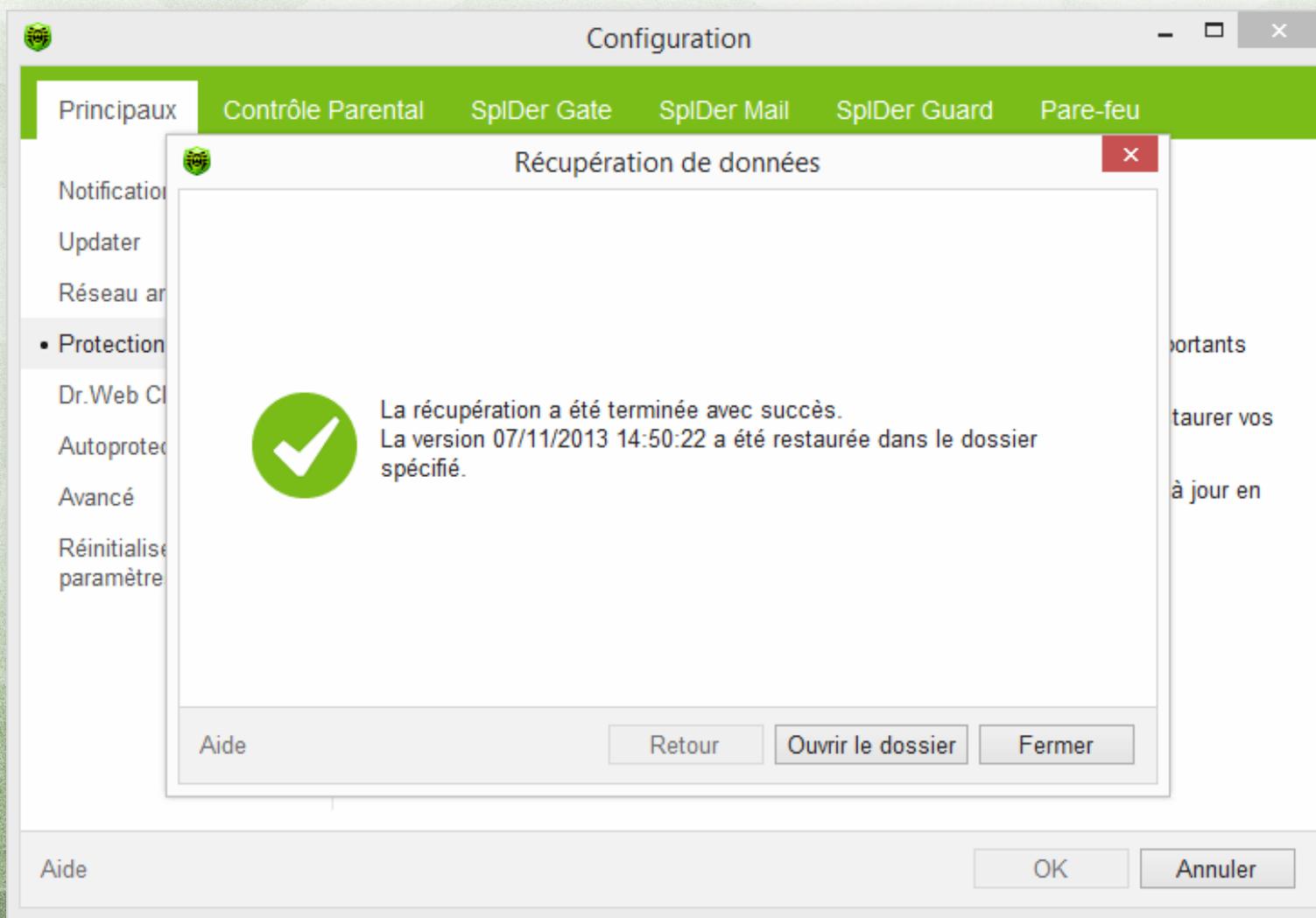
Nouvelle protection préventive



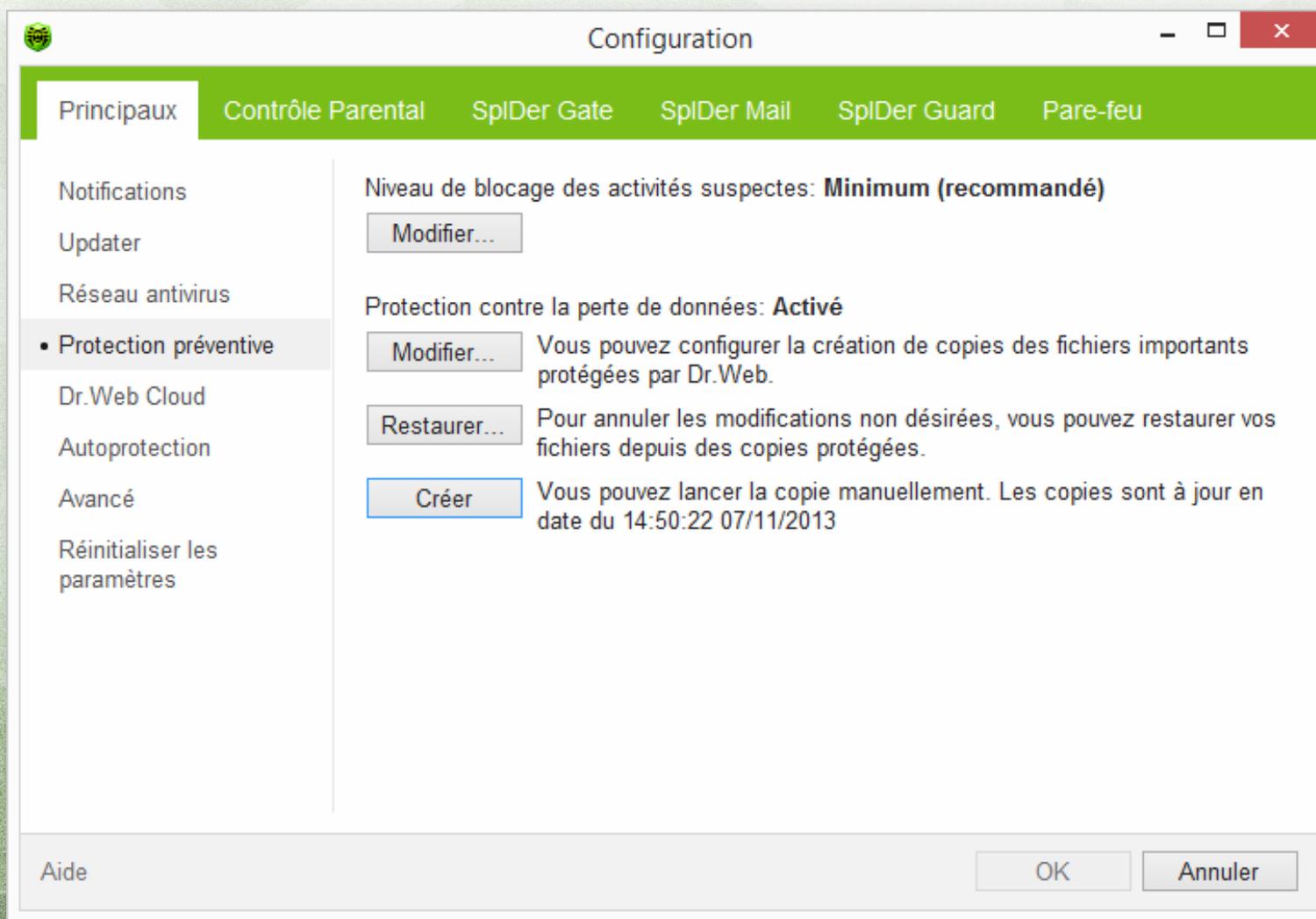
Nouvelle protection préventive



Nouvelle protection préventive



Nouvelle protection préventive



Nouvelle protection préventive



Configuration

Principaux | Contrôle Parental | SpIDer Gate | SpIDer Mail | SpIDer Guard | Pare-feu

Notification
Updater
Réseau ar
• Protection
Dr.Web Cl
Autoprotec
Avancé
Réinitialise
paramètre

Protection préventive

Niveau de blocage des activités suspectes:
Minimum (recommandé)

Objet protégé	Autoriser	Demander	Bloquer
L'intégrité des applications en cours d'e...	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
L'intégrité des fichiers des utilisateurs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Fichier HOSTS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Accès bas niveau au disque	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Téléchargement de pilotes	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Image File Exécution Options	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aide

OK Annuler

Aide

OK Annuler



Nouvelle protection préventive



Configuration

Principaux Contrôle Parental SpIDer Gate SpIDer Mail SpIDer Guard Pare-feu

Notification
Updater
Réseau ar
• Protection
Dr.Web Cl
Autoprotec
Avancé
Réinitialise
paramètre

Protection préventive

Niveau de blocage des activités suspectes:
Minimum (recommandé) ▼
Minimum (recommandé)
Moyen
Paranoïde
Personnalisé

	Autoriser	Demander	Bloquer	
Paranoïde	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Importants
Personnalisé	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Restaurer vos
Intégrité des données des ordinateurs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Mettre à jour en
Fichier HOSTS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Accès bas niveau au disque	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Téléchargement de pilotes	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Image File Exécution Options	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Aide

OK Annuler

Aide

OK Annuler



Nouvelle protection préventive



Configuration

Principaux | Contrôle Parental | SpIDer Gate | SpIDer Mail | SpIDer Guard | Pare-feu

Notification
Updater
Réseau ar
• Protection
Dr.Web Cl
Autoprotec
Avancé
Réinitialise
paramètre

Protection préventive

Niveau de blocage des activités suspectes:
Personnalisé

Objet protégé	Autoriser	Demander	Bloquer
L'intégrité des applications en cours d'e...	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
L'intégrité des fichiers des utilisateurs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Fichier HOSTS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Accès bas niveau au disque	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Téléchargement de pilotes	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Image File Exécution Options	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aide

OK Annuler

Aide

OK Annuler



Autoprotection de Dr.Web



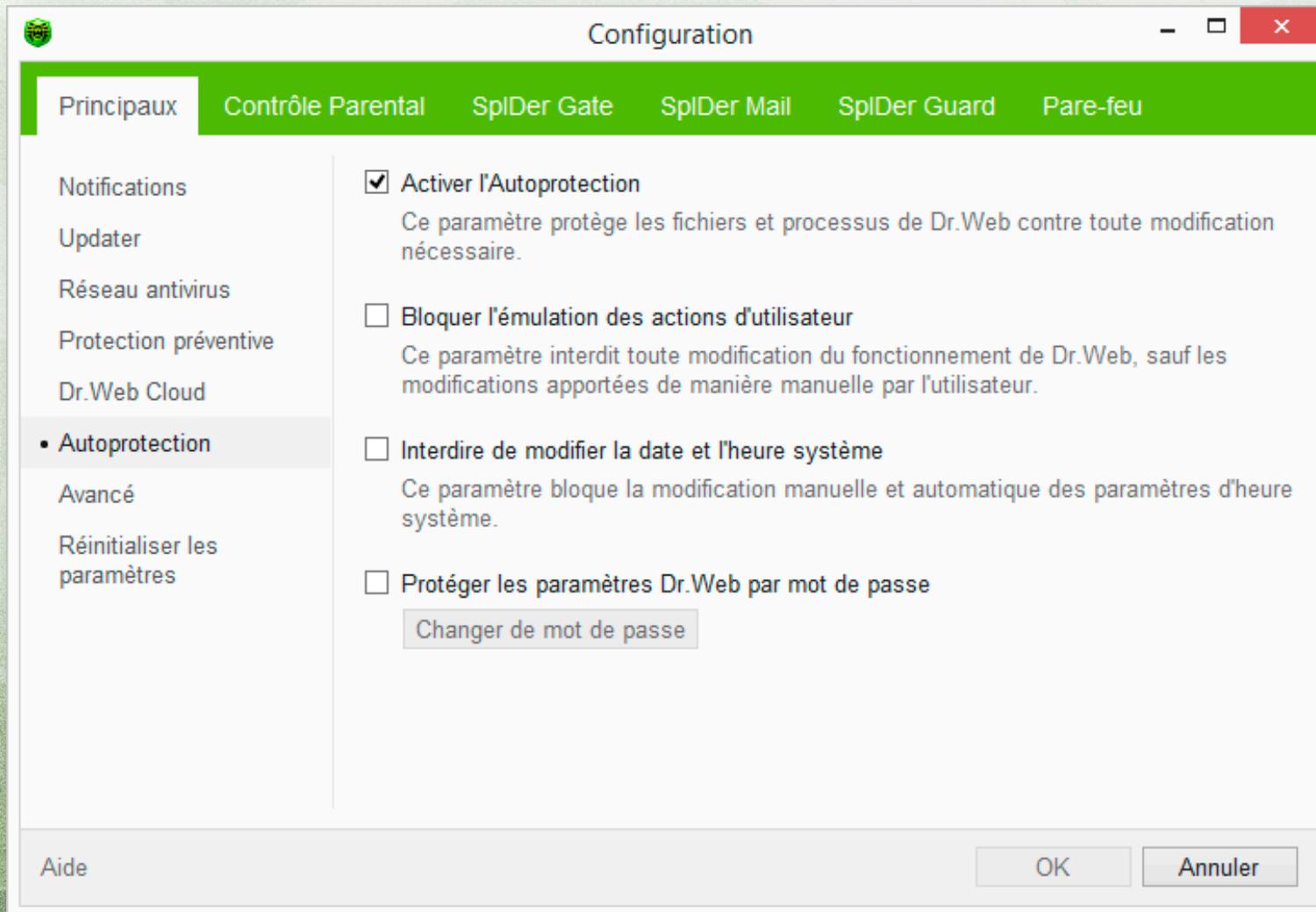
Protège Dr.Web Security
Space 9 contre les attaques
virales



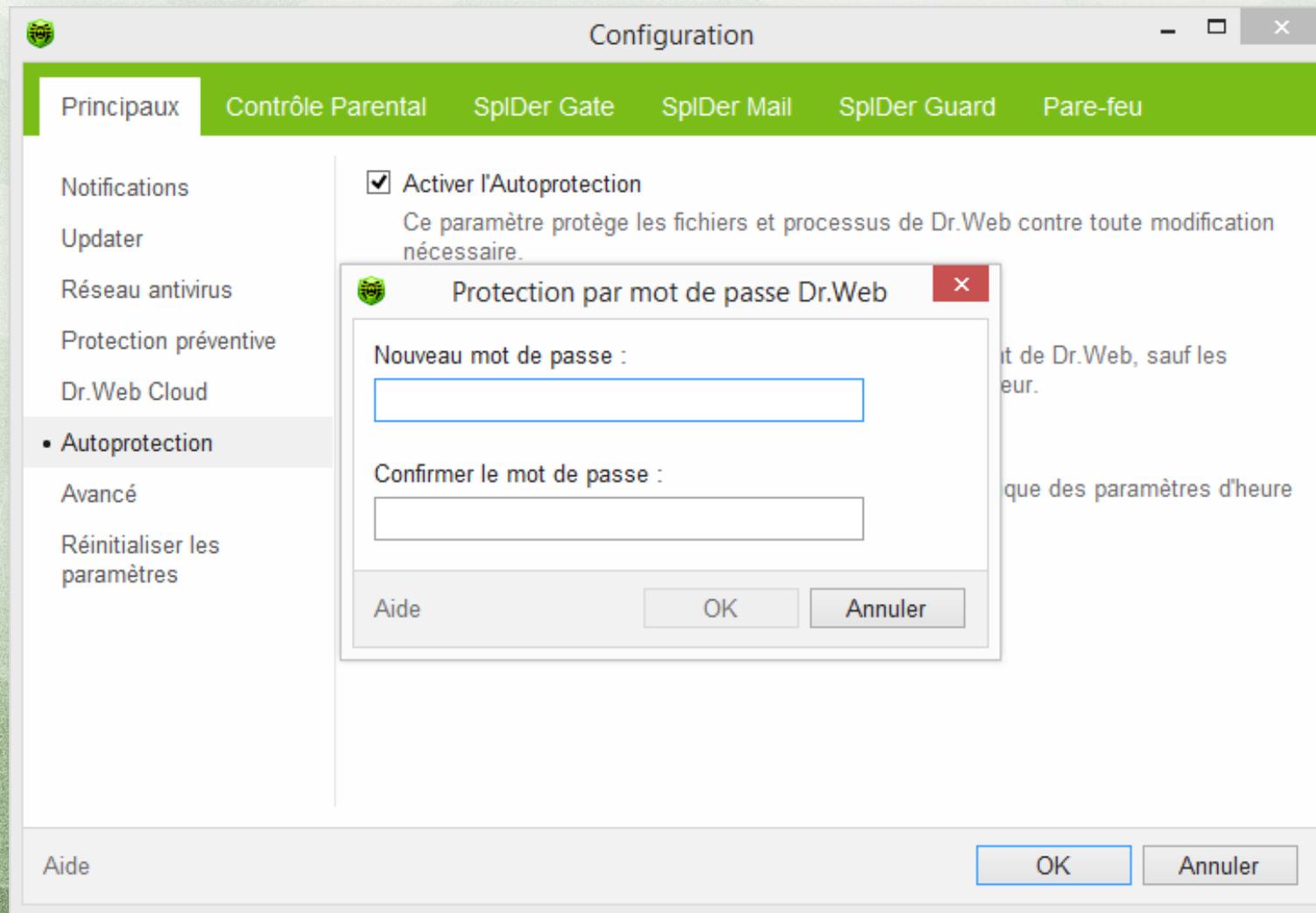
Assure l'intégrité des copies
protégées de documents,
musique, photos et autres
fichiers de l'utilisateur



Autoprotection de Dr.Web



Autoprotection de Dr.Web



Autoprotection de Dr.Web



Configuration

Principaux | Contrôle Parental | SpIDer Gate | SpIDer Mail | SpIDer Guard | Pare-feu

Notifications
Updater
Réseau antivirus
Protection préventive
Dr.Web Cloud
• Autoprotection
Avancé
Réinitialiser les paramètres

Activer l'Autoprotection
Ce paramètre protège les fichiers et processus de Dr.Web contre toute modification nécessaire.

Protection par mot de passe Dr.Web

Nouveau mot de passe :
.....

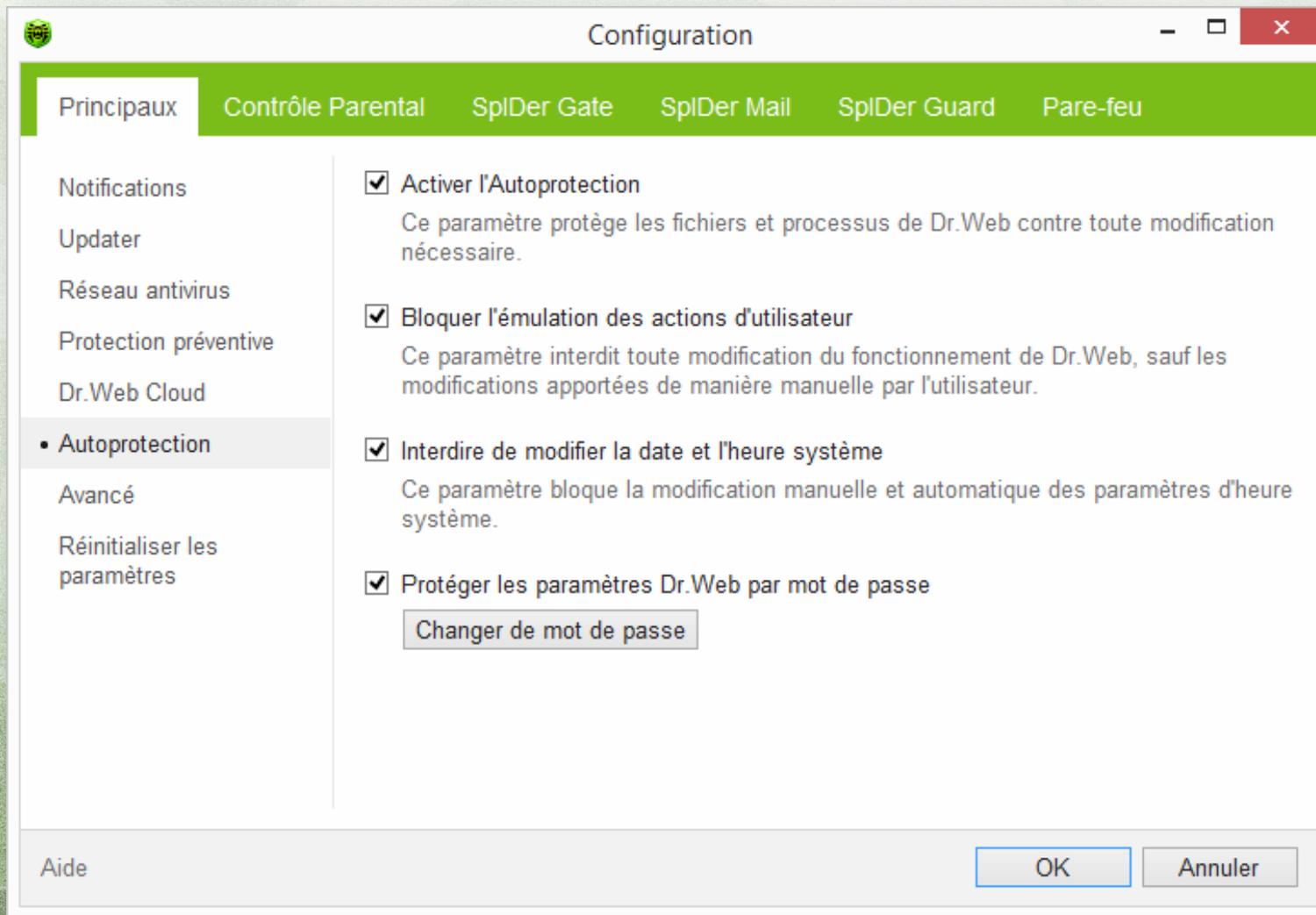
Confirmer le mot de passe :
.....

Aide OK Annuler

Aide OK Annuler



Autoprotection de Dr.Web





Protection préventive Dr.Web - protection fiable contre les menaces **inconnues**





Dr.Web ERA, la nouvelle ère Dr.Web

Efficace. Réactif. Actuel

La nouvelle version Dr.Web 9.0



© Doctor Web

www.drweb.fr