Dr.WEB®
depuis 1992

Configurer la protection Dr.Web contre les ransomwares !

Recommandations visant à minimiser le risque de contamination par un ransomware.

Les ransomwares à chiffrement (famille Trojan.Encoder) sont des programmes malveillants qui cherchent sur les disques durs ou dans la mémoire les fichiers de l'utilisateur, puis les chiffrent et demandent une rançon pour le déchiffrement.

Tous les Encoders sont considérés comme des fichiers malveillants (Trojans) qui **ne sont pas capables de se propager ou de se lancer eux-mêmes**. D'après les statistiques de Doctor Web,

Dans plus de 90% des cas,	**Le déchiffrement est possible**
les utilisateurs lancent eux-mêmes des ransomwares sur leurs ordinateurs sans le savoir	dans environ 10 % des cas seulement

Ce que vous devez savoir

Les groupes criminels impliqués dans le développement de logiciels malveillants testent leurs malwares afin qu'ils soient **indétectables** par toutes les solutions antivirus actuelles. Cela augmente donc significativement le nombre de malwares non détectés au moment de leur pénétration dans un système, au moins jusqu'à ce que l'antivirus reçoive les mises à jour correspondantes.

Les représentants de cette famille peuvent pénétrer un ordinateur même s'il est protégé par un antivirus, si ce Trojan est inconnu de la base virale ou si l'antivirus n'inclut pas la fonctionnalité de protection préventive qui assure la protection des données contre les menaces inconnues. Aucun antivirus n'est en mesure de détecter tous les programmes malveillants à tout moment.

Cela signifie que personne n'est à l'abri d'être contaminé par un nouveau ransomware inconnu.

Si vous n'avez pas encore configuré votre système de protection.

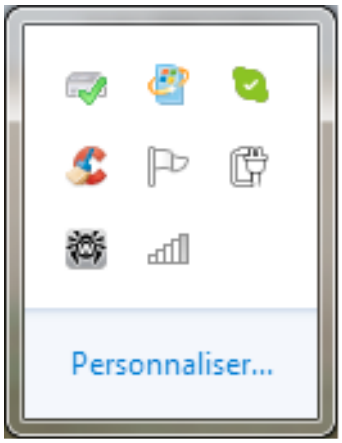
Configurez Dr.Web !

Les règles de base relatives à la configuration de Dr.Web aident à prévenir la contamination par les ransomwares même si ces derniers sont inconnus du moteur antivirus.

Dr.Web doit toujours être activé

Et si votre ordinateur est connecté à Internet ou qu'un support amovible y est connecté et qu'il n'a pas été scanné avant la connexion, il est fortement déconseillé de désactiver Dr.Web.

L'icône dans la zone de notification doit montrer que Dr.Web est actif et protège votre PC.



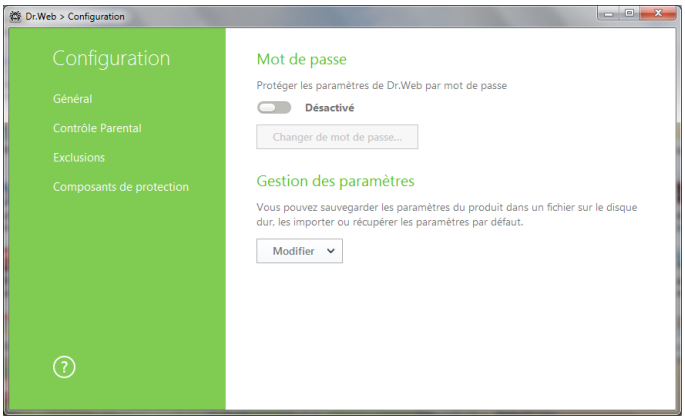
L'absence de l'icône de l'agent ou l'apparence de l'icône avec un point d'exclamation ou une croix signifie que Dr.Web est désactivé et que l'ordinateur est laissé sans protection antivirus. Dans ce cas, redémarrez immédiatement l'ordinateur. Si le problème persiste, contactez le support technique de Doctor Web.

Votre Dr.Web est-il activé actuellement ?

Dr.Web doit être protégé par un mot de passe

L'installation d'un mot de passe garantit qu'il est impossible de désactiver la protection Dr.Web de manière non autorisée et vous protège contre le piratage.

Pour définir un mot de passe permettant d'accéder à Dr.Web



Cliquez sur l'icône (elle va apparaître ainsi) et en cliquant sur l'icône qui apparaît , dans le menu **Configuration**, sélectionnez **Général**. Ensuite, bougez le commutateur et cliquez sur **Modifier le mot de passe** .

Attention ! *Il est déconseillé de mettre un mot de passe qui correspond à celui défini pour accéder à l'ordinateur ou à un périphérique. Le mot de passe pour Dr.Web ne doit pas être stocké sur le même ordinateur.*

Votre Dr.Web est-il protégé par un mot de passe ?

Tous les composants de protection Dr.Web doivent toujours être activés.

Chaque composant de Dr.Web Security Space est impliqué dans la protection contre les ransomwares.

La désactivation d'un de ces composants, même si c'est temporaire, signifie une baisse inévitable du niveau de protection.

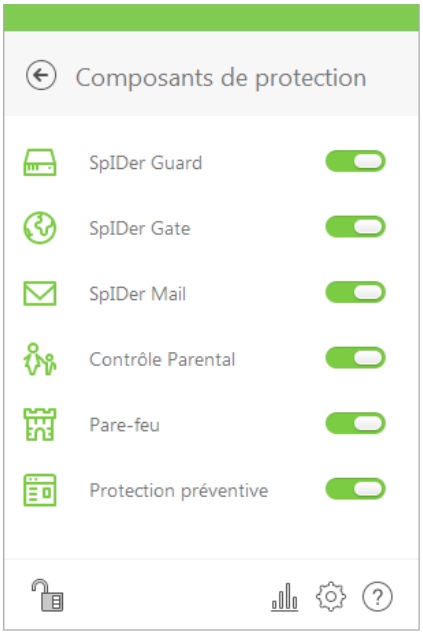
- **Dr.Web SpIDer Guard** détecte les logiciels malveillants lors de leur lancement, même si les composants malveillants ont été reçus au format chiffré et n'ont pas été détectés lors de leur téléchargement.

- Un ransomware peut pénétrer le système via un e-mail. Dans la plupart des cas, ce message contient une pièce jointe malveillante ou un lien. L'antispam Dr.Web filtre les emails en se basant sur les caractéristiques typiques des messages malveillants, même si le moteur n'a pas encore été mis à jour avec des informations sur les dernières menaces.
  L'antispam Dr.Web n'a pas besoin d'apprentissage, il sait comment agir !
- **Les modules Dr.Web SpIDer Gate et Contrôle parental** vous éviteront d'accéder à un site considéré comme dangereux, si un lien de téléchargement d'un Trojan vous parvient dans un email. Le service de scan du trafic mail et du trafic web au sein de Dr.Web Security Space est basé sur des algorithmes uniques qui assurent une haute vitesse de scan et une bonne qualité de détection des logiciels malveillants.
- Le Pare-feu Dr.Web permet de configurer des restrictions pour les programmes ayant accès à Internet.

Et d'autres composants Dr.Web vous protègent contre les virus et les Trojans !

Pour vérifier s'il y a des composants désactivés dans votre Dr.Web :

Regardez la zone de notification : s'il y des composants désactivés, l'icône Dr.Web va avoir l'apparence suivante :



Pour voir quels composants sont désactivés

Cliquez sur l'icône de Dr.Web Agent, puis cliquez sur **Composants de protection**, le menu de Dr.Web Agent va s'ouvrir.

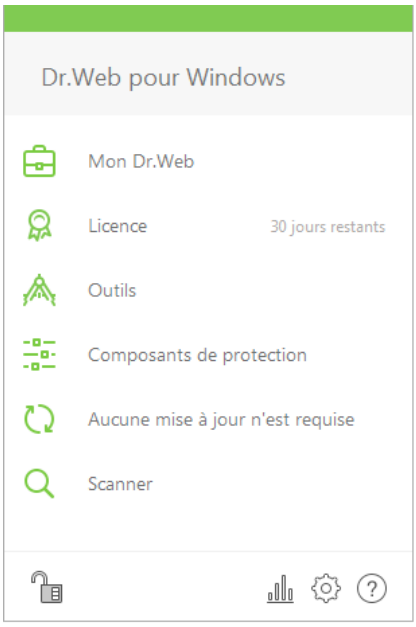
Est-ce que tous les composants de Dr.Web sont actifs ?

L'antivirus doit être mis à jour fréquemment.

Il faut le faire dès réception des mises à jours.
Pour cela, il suffit d'activer les mises à jour automatiques.

Mais il est également très important de redémarrer le PC après les mises à jour nécessitant un redémarrage, quelle que soit la fréquence des demandes de redémarrage affichées par Dr.Web. C'est seulement après le redémarrage que les nouveaux pilotes d'interception des programmes inconnus auparavant peuvent être installés, de plus, ceci est nécessaire pour corriger les vulnérabilités potentielles de la protection Dr.Web.

Attention ! *Chaque jour, le laboratoire antivirus de Doctor Web reçoit jusqu'à 1 million de nouveaux fichiers potentiellement dangereux à analyser. Si Dr.Web n'est pas mis à jour pendant quelques heures seulement, ceci signifie qu'il y a une possibilité de laisser passer des centaines de fichiers malveillants précédemment inconnus (y compris les fichiers inconnus de l'analyseur heuristique Dr.Web). Tandis qu'il suffit de 1 à 3 minutes pour qu'un Trojan bancaire puisse voler de l'argent sur le compte d'un utilisateur.*



Pour vérifier la date et l'actualité des mises à jour.

Cliquez sur l'icône dans la zone de notification. Dans le menu qui apparaît, le statut des mises à jour sera affiché.

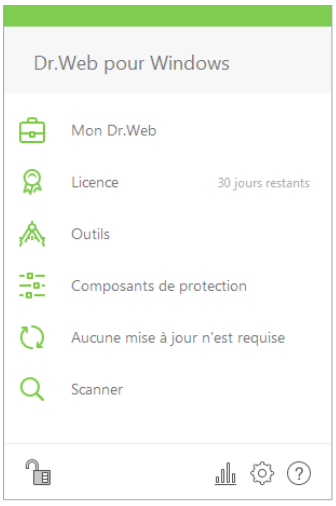
Quand Dr.Web a-t-il été mis à jour pour la dernière fois ?

Des exclusions de l'analyse peuvent être paramétrées uniquement dans des cas spécifiques.

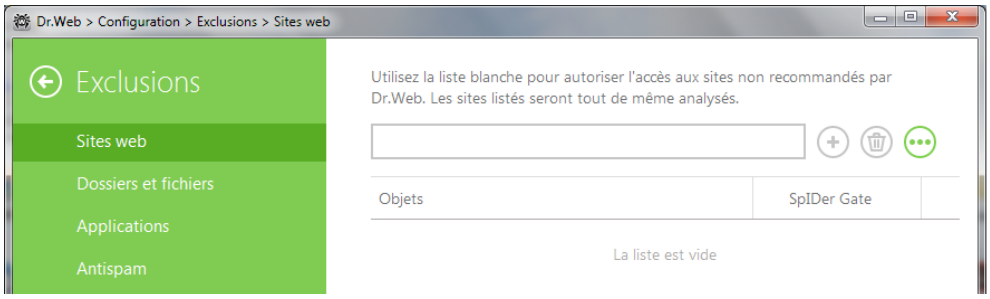
Les exclusions de l'analyse permettent d'accélérer le processus du scan, mais souvent cela provoque aussi une baisse du niveau de sécurité. Les auteurs de virus savent ce que les utilisateurs aiment à exclure de l'analyse et ils l'utilisent activement.

Nos logiciels sont optimisés au maximum et épargnent les ressources de l'ordinateur. Nous ne recommandons pas aux utilisateurs d'exclure quoi que ce soit de l'analyse par Dr.Web. Les exclusions sont un moyen de contourner des situations problématiques. Mieux vaut avoir l'avis des spécialistes du Support technique de Doctor Web pour le faire correctement.

Pour vérifier s'il y a des exclusions dans votre Dr.Web pouvant affaiblir la protection.



Cliquez sur l'icône dans la zone de notification. Dans le menu qui apparaît, cliquez sur l'icône (elle va apparaître ainsi), ensuite cliquez sur l'icône qui apparaît, sélectionnez **Configuration → Exclusions**.



Attention ! *Si dans les exclusions, il y a des masques spécifiés de type *.exe ou *.dll, alors Dr.Web n'analysera pas tous les objets qui correspondent à ce masque – autrement dit, tous les fichiers exécutables et les bibliothèques de logiciels !*

Attention ! *Il n'est pas recommandé d'exclure l'analyse du trafic pour les programmes utilisés, car cela signifie qu'aucun malware téléchargé par ces programmes ne sera scanné.*

Y a-t-il des exclusions configurées dans votre Dr.Web

La Protection préventive doit être activée

Aujourd'hui, la protection préventive est l'un des composants les plus importants dans le système de protection complète avec Dr.Web.

La protection préventive Dr.Web analyse la ressemblance de programmes suspects (qui ne sont pas encore connus de Dr.Web) avec les modèles de comportement habituel des programmes malveillants déjà connus. Ainsi, elle sait identifier et bloquer ces programmes en utilisant un ensemble de technologies agissant de manière préventive et ne dépendant pas de la présence des signatures correspondantes dans la base virale Dr.Web.

Il n'est pas recommandé de désactiver la protection préventive — son fonctionnement assure la protection contre les Trojans-Encoders, bloqueurs, Trojans bancaires et autres malwares.

Important ! *Pour assurer une protection supplémentaire contre les ransomwares, dans les paramètres du composant " Protection préventive ", il faut toujours cocher la case " Interdire " pour les éléments " L'intégrité des applications en cours d'exécution " et " L'intégrité des fichiers d'utilisateurs".*

Ce paramètre est-il activé dans votre Dr.Web ?

Si l'ordinateur est connecté à Internet, la Protection préventive reçoit les données sur les algorithmes de neutralisation des nouvelles menaces depuis le service Dr.Web Cloud. Ceci offre une protection contre les logiciels malveillants analysés par les spécialistes de Dr.Web après la dernière mise à jour de votre antivirus. En général, l'antivirus est actualisé une fois par heure. Dr.Web Cloud, lui, est toujours à jour, car il est actualisé chaque fois que les spécialistes de Dr.Web reçoivent les données.
L'utilisation de la base de données Cloud augmente significativement la protection contre les menaces Internet, y compris celles utilisant les vulnérabilités zero-day.

Est-ce que Dr.Web Cloud est activé dans votre Dr.Web ?

Par défaut, la Protection préventive Dr.Web fonctionne en mode Optimal. Pour plus d'information sur la configuration de la Protection préventive Dr.Web, consultez cette page.

La protection préventive fonctionne avec un système de profils qui permettent de créer des règles flexibles pour les applications de confiance afin d'éviter des conflits logiciels. Pour en savoir plus sur la configuration des profils de la Protection préventive Dr.Web, consultez la documentation.

La Protection contre la perte de données doit être activée et configurée

La " Protection contre la perte de données "sauvegarde les fichiers les plus importants dans un stockage spécialisé et protégé par Dr.Web.

Contrairement aux logiciels de sauvegarde classiques, Dr.Web crée et protège les copies de fichiers contre un accès non autorisé. Même si un nouveau Trojan (encore inconnu de Dr.Web) pénètre dans votre PC, l'utilisation de la « Protection contre la perte de données » permettra de sauver vos fichiers. Au cas où vos fichiers sont chiffrés par un Trojan, vous pourrez restaurer vous-même les fichiers originaux sauvegardés sans avoir besoin de contacter le support technique Doctor Web.

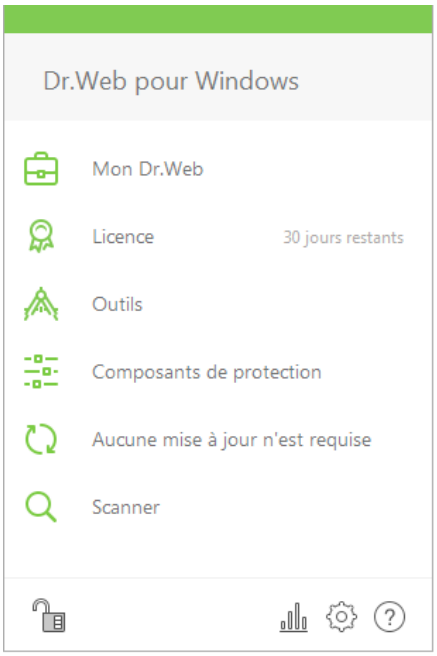
Par défaut, cette fonctionnalité n'est pas activée, car pour qu'elle fonctionne, vous devez spécifier les données que vous souhaitez enregistrer et définir le lieu et le mode de stockage des données.

Et vous, avez-vous activé et configuré "La protection contre la perte de données " dans votre Dr.Web?

La licence Dr.Web doit être valide

Pour que Dr.Web protège votre PC, vous devez avoir une licence active (valide).

Après l'expiration de la licence, tous les composants de la protection de Dr.Web arrêtent de fonctionner.



Pour connaître date d'expiration de votre licence Dr.Web

Cliquez sur l'icône dans la zone de notification. Si la licence est valide, vous pourrez voir dans le menu qui s'ouvre, le nombre de jours restant jusqu'à la date d'expiration de la licence.

Vous pouvez également consulter les dates de validité de la licence Dr.Web dans Le gestionnaire de licence sur le site.

Est-ce que votre licence Dr.Web est active ?

Règles de comportement en cas de contamination par un ransomware.

Pour que les spécialistes de Doctor Web puissent restaurer les fichiers chiffrés, l'utilisateur ne doit pas :

- modifier l'extension des fichiers cryptés ;
- réinstaller le système d'exploitation ;
- utiliser des logiciels pour décrypter/restaurer des données ;
- supprimer/changer le nom des fichiers et des programmes (y compris temporaires) ;
- effectuer des actions irréversibles sur le traitement/ suppression des objets malveillants.

A cause de ces actions, l'utilisateur peut perdre ses données à jamais, car même un utilitaire de déchiffrement spécialisé ne pourra pas les restaurer.

Par conséquent, il vaut mieux de ne pas toucher l'ordinateur contaminé avant la réception d'une réponse du support technique de Doctor Web concernant la possibilité de restauration des fichiers.

Règles de comportement face à une contamination par un ransomware.	Exemples de plaintes à la police

Restauration gratuite des fichiers chiffrés par un ransomware.

Le service est gratuit pour les titulaires de licences commerciales actives Dr.Web Security Space, Dr.Web Enterprise Security Suite (Protection complète) et pour les abonnés au service Dr.Web Antivirus (Formule Dr.Web Premium) — s'ils ont respecté les conditions au moment de l'incident.

Pour les utilisateurs des autres antivirus, ce service est payant. Si les fichiers peuvent être restaurés, l'utilisateur peut acheter Dr.Web Rescue Pack.

Les composants du pack.

- Un utilitaire de déchiffrement
- Une licence Dr.Web Security Space 1 PC / 2 ans

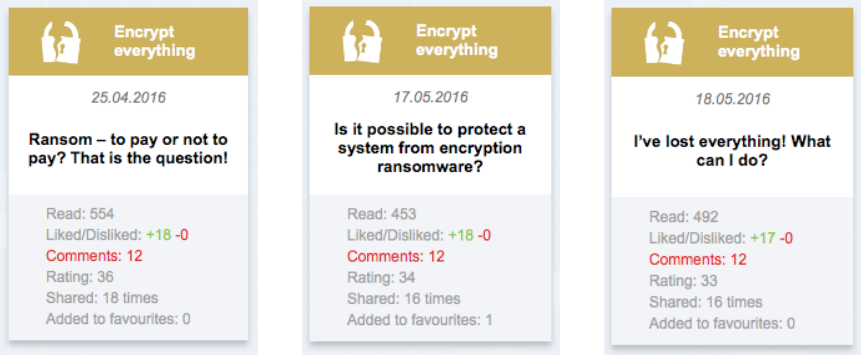
Demande pour un déchiffrement

La connaissance est une arme puissante contre les ransomwares à chiffrement

Pour en savoir plus sur la configuration correcte du système de protection contre les ransomwares à chiffrement, consultez le cours **DWCERT-070-6 « Protection des postes de travail et serveurs de fichiers Windows contre les ransomwares à chiffrement »**, que vous pouvez télécharger depuis ce lien https://training.drweb.com/users?lng=fr.

Mensonge partout ? Le projet " Lumières sur la sécurité " peut également vous aider !

Comment lutter contre les ransomwares ? Lisez les articles du projet " Lumières sur la sécurité " dans la rubrique " Tout chiffrer ".



Tous les articles du projet

La prévention des risques

Les ransomwares sont propagés de manière massive via email, en imitant des messages courrier provenant de l'administration, de vos amis ou sous couvert de CV ou de documents de comptabilité etc. Si vous avez reçu un message suspect et que Dr.Web n'a pas réagi, cela peut signifier qu'il contient un ransomware qui est encore inconnu de l'antivirus.

Envoyez cette pièce jointe pour analyse au Labo de Doctor Web https://vms.dr.web.ru/sendvirus et attendez la réponse d'un spécialiste.

Ce faisant, vous pourrez non seulement vous aider (vous prévenez le chiffrement de données), mais aider également des milliers de victimes potentielles.

Vous pouvez aider à arrêter les cybercriminels.

Le chiffrement de données est une menace dangereuse, et des fichiers corrompus représentent un problème grave. Mais il est possible de lutter contre cette menace. http://legal.drweb.com/templates.

Dr.WEB®
depuis 1992

A propos de Doctor Web

Doctor Web, éditeur russe, développe les produits antivirus Dr.Web depuis 1992.
La société est un acteur clé sur le marché russe et est présent en Europe, au Japon et en Chine.

Doctor Web est l'un des rares éditeurs dans le monde à posséder
ses propres technologies de détection et de traitement des programmes malveillants.
La société possède son propre Laboratoire et un service de surveillance virale.

L'objectif stratégique de la société est de créer les meilleurs outils de protection antivirus afin de répondre aux enjeux d'aujourd'hui en matière de sécurité numérique, ainsi que de développer de nouvelles solutions technologiques qui permettent aux utilisateurs de faire face à toutes sortes de menaces informatiques.

Formation
Espace personnel pour les cours à distance Dr.Web (inscription requise)
Cours pour les ingénieurs | Cours pour les utilisateurs | Brochures

Éducation
" Lumières sur la sécurité " | Brochures

Contacts
Doctor Web France
333b, avenue de Colmar
67100 Strasbourg

Contacts

Plan d'accès

Contact presse

Bureaux hors Russie

www.drweb.fr | free.drweb.fr | www.av-desk.com | curenet.drweb.com

Rejoignez-nous sur les réseaux sociaux