Dr.WEB®
depuis 1992

Protégez votre univers

Trojans — Encoders

Menace №1.

Les Trojans Encodeurs représentent une des menaces les plus actuelles. Les malwares de la famille **Trojan.Encoder** cryptent les fichiers sur le PC ou appareil mobile, puis demandent une rançon pour le décryptage.

Les premiers malwares de la famille **Trojan.Encoder** sont apparus en **2006–2007**.

Depuis janvier 2009, leur nombre a cru de **1900% !**

Actuellement, le Trojan.Encoder possède **plusieurs milliers de modifications à son actif**.

Les pertes potentielles.

Aujourd'hui, les malfaiteurs demandent en général une rançon de 1 500 bitcoins pour décrypter les fichiers qu'ils ont infectés.

1 bitcoin = 272 euros ou 330 dollars.

Le total peut attendre 49 500 dollars.

Même si vous payez une rançon aux attaquants, personne ne peut garantir que les fichiers seront restaurés.

Certains faits sont incroyables – il s'est trouvé une fois qu'une victime a payé la rançon mais que les malfaiteurs n'ont pas réussi à décrypter les fichiers cryptés par leur Trojan.Encoder et ont proposé de contacter le support technique de Doctor Web !

Comment les Trojans pénètrent-ils les ordinateurs des victimes ?

Dans 90% des cas, les utilisateurs lancent (activent) eux-mêmes les Trojan.Encoder sur leur ordinateur. Et si c'est une modification inconnue – la destruction de fichiers est inévitable.

Certaines modifications des Trojans Encoders sont indétectables par aucun antivirus.

Parce que les cybercriminels peuvent tester leurs Trojans Encoders sur toutes les solutions antivirus actuelles. Ainsi, en utilisant seulement un antivirus standard, qui n'inclut pas de protection préventive, de contrôle parental, ou d'autres moyens pour limiter la possibilité de pénétration et de lancement des malwares inconnus de la base virale, l'utilisateur ne peut pas assurer la protection contre les Encoders, indétectables par l'antivirus.

Doctor Web France Sarl
333b, avenue de Colmar –
67100 Strasbourg

Téléphone :
+33 (3) 90 40 40 20
Fax : +33 (3) 90 40 40 21

www.drweb.fr
www.drweb.com
www.drweb-curenet.com
www.av-desk.com
freedrweb.com

Dr.WEB®
depuis 1992

Que propose Dr.Web ?

1. D'utiliser un logiciel antivirus avancé qui comprend des technologies de protection préventive. Elles permettent de détecter les Encoders par leurs algorithmes de comportement qui sont similaires entre les différentes modifications des Trojans.
   - Protection préventive de Dr.Web : http://products.drweb.ru/technologies/preventive_protection.
2. Pour prévenir la perte de données cryptées par les Trojans Encoders, veuillez utiliser le composant " Prévention de la perte de données " inclus à Dr.Web Security Space (en versions 9 et 10). Contrairement aux logiciels de sauvegarde classiques, Dr.Web crée et **protège** le stockage de copies de fichiers contre un accès non autorisé. Si vos fichiers sont cryptés par un Trojan (pas plus de 10), vous pourrez restaurer vous-même les fichiers originaux sauvegardés sans avoir besoin de contacter le support technique Doctor Web.
   - La vidéo sur la prévention de la perte de données : http://support.drweb.ru/video/security_space.
3. Si votre PC est infecté par une version du Trojan inconnue de la base virale de Dr.Web, contactez le support technique de Doctor Web sans effectuer aucune action sur l'ordinateur infecté.
   - Comment agir en cas d'accident informatique viral http://legal.drweb.ru/encoder.
   - L'examen des incidents informatiques viraux : http://antifraud.drweb.ru/expertise.

   Le décryptage de fichiers est gratuit pour les utilisateurs de licences commerciales Dr.Web.
   - Requête pour le décryptage gratuit : https://support.drweb.fr/new/free_unlocker/for_decode/?lng=fr.

Perspectives de décryptage.

Les représentants de la famille **Trojan.Encoder** utilisent **des douzaines d'algorithmes de chiffrement différents** pour crypter les fichiers de l'utilisateur.

Selon les spécialistes de Doctor Web, il est possible de décrypter les fichiers cryptés par un Trojan dans 10% des cas.

Cela signifie que pour les utilisateurs qui ont négligé d'utiliser des moyens de protection importants, la majorité des données personnelles sont perdues à jamais.

De mi-avril 2013 à mars 2015, le support technique de Doctor Web a reçu plus de **8 500 demandes pour déchiffrer des fichiers** cryptés par des Trojans Encodeurs.

Les spécialistes de Doctor Web reçoivent environ 40 demandes par jour pour déchiffrer des fichiers.

Certaines modifications du Trojan **semblent pouvoir être décryptées uniquement par les spécialistes de Doctor Web** d'après les utilisateurs sur les forums.

Depuis le mois de mai 2014, les spécialistes de Doctor Web ont effectué un travail de recherche approfondi sur le décryptage des fichiers touchés par le **Trojan.Encoder.398. À ce jour, Doctor Web est le seul éditeur antivirus** qui peut décrypter les fichiers avec une probabilité **de 90%**.

Plus d'infos sur les Encoders. http://antifraud.drweb.com/encryption_trojs/

Doctor Web France Sarl
Doctor Web est un éditeur russe de produits antivirus développés depuis 1992
333b, avenue de Colmar – 67100 Strasbourg
Téléphone : +33 (3) 90 40 40 20
Fax: +33 (3) 90 40 40 21
www.drweb.fr | www.drweb.com | www.drweb-curenet.com | www.av-desk.com | freedrweb.com