Dr.WEB®
desde 1992

Proteja lo creado

Troyanos cifradores
Amenaza №1

Los troyanos cifradores son una de las amenazas más actuales hoy día. Los programas nocivos de la familia **Trojan.Encoder** cifran los archivos de usuarios en PCs y dispositivos móviles, y luego extorsionan el pago a la víctima para descifrar.

Los primeros troyanos cifradores de la familia Trojan.Encoder aparecieron en el año **2006–2007**.

A partir del enero del año 2009, ¡el número de variedades de los mismos incrementó apróx. en **1900%!**

Actualmente Trojan.Encoder tiene **varios miles de modificaciones**.

Qué es lo que pierde Vd.

Hoy día los extorsionistas demandan hasta 1 500 bitcoins por descifrar archivos.
1 bitcoin = 272 Euros o 330 USD.
El total del rescate puede alcanzar **49 500 USD**.

Incuso si Vd. paga el rescate al malintencionado, no le dará ninguna garantía de recuperación de la información.

A veces pasan cosas curiosas – ¡una vez, a pesar del rescate pagado, los malintencionados no pudieron descifrar archivos cifrados por Trojan.Encoder (Cryptolocker) **creado por ellos mismos**, y aconsejaron a su víctima... ¡que contactara con el servicio de soporte técnico de Doctor Web!

Cómo los troyanos cifradores penetran en un equipo

En más de 90% de los casos, los usuarios mismos inician (activan) los cifradores en su equipo. Y si es una modificación desconocida para la base antivirus – la destrucción de archivos es inevitable.

Algunas modificaciones de los cifradores no se detectan por ningún antivirus.

Eso pasa porque al crear los troyanos cifradores, los malintencionados hacen las pruebas para que los mismos no puedan ser detecados por las versiones actuales de los medios antivirus. De esta forma, usando solo un antivirus que no contenga protección preventiva, ni control parental, ni otros medios de restringir las posibilidades de penetración y lanzamiento de programas malintencionados, el usuario corre peligro de ser infectado por un troyano cifrador, del cual no le salvará ningún antivirus.

Doctor Web S.L.
125124, Rusia, Moscú, c/3 Yamskogo Polya, 2, edif. 12A

Teléfono (multicanal):
+7 495 789–45–87
Fax: +7 495 789–45–97

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

Dr.WEB®
desde 1992

Cómo ayudará Dr.Web

1. Accione adelantando — use un programa antivirus que contiene las tecnologías de la protección preventiva. Permiten detectar a los cifradores por los algoritmos de comportamiento similares de las modificaciones de los mismos.
   - Protección preventiva de Dr.Web: http://products.drweb.com/technologies/preventive_protection.
2. Para prevenir la pérdida de datos por causa de la acción de los troyanos cifradores, use el componente «Protección contra la pérdida de datos» que forma parte de Dr.Web Security Space (versiones 9 y 10). A diferencia de programas de copia de reserva ordinarios, Dr.Web usa un almacén para las copias de archivos **protegido** contra el acceso no sancionado de los malintencionados. **Y** si aun así un troyano logra cifrar sus archivos (no más de 10), Vd. solo podrá recuperarlos, sin contactar con el servicio de soporte técnico Doctor Web
   - Vídeo sobre la protección contra la pérdida de datos: http://support.drweb.ru/video/security_space.
3. Si su PC se infecta por una modificación del troyano desconocida para Dr.Web, contacte con el soporte técnico de Doctor Web para descifrar, **sin realizar ninguna acción en el equipo infectado**.
   - Reglas de comportamiento en caso de un incidente vinculado con virus: http://legal.drweb.com/encoder.
   - Peritaje de incidentes informáticos vinculados con virus: http://antifraud.drweb.com/expertise.

   Para los usuarios comerciales de productos Dr.Web, el servicio de descifrar de nuestros especialistas es gratuito.
   - Solicitud para descifrar gratis: https://support.drweb.com/new/free_unlocker.

Perspectivas de descifrar

Los troyanos de la familia Trojan.Encoder usan **varias decenas de diferentes algoritmos de cifrado** de archivos de usuarios.

Según las estadísticas de la empresa Doctor Web, es posible descifrar los archivos dañados por un troyano solo en 10% de los casos.

Quiere decir que la mayor parte de los datos de usuarios se pierde sin posibilidad de recuperación.

Desde mediados de abril de 2013 hasta marzo de 2015 el laboratorio de virus de la empresa Doctor Web recibió más de **8 500 solicitudes para descifrar** archivos dañados por las acciones de los troyanos codificadores.

Cada día el personal del laboratorio de virus recibe en promedio unas 40 solicitudes de descifrar.

Solo el personal de la empresa Doctor Web es capaz de descifrar algunas modificaciones de los troyanos— lo confirman los usuarios de los foros.

A partir del mayo del año 2014, el personal de la empresa Doctor Web realizó una investigación científica muy importante sobre la creación de algoritmos para descifrar **Trojan.Encoder.398**. **Hoy día el desarrollador de los antivirus Dr.Web es la única empresa** cuyo personal puede restaurar completamente los datos cifrados por este troyano **con probabilidad de 90%**.

Más información sobre los cifradores: http://antifraud.drweb.com/encryption_trojs/

Doctor Web S.L.

Doctor Web es un productor ruso de los medios de protección de información antivirus bajo la marca Dr. Web. Los productos Dr. Web. se desarrollan a partir del año 1992.

125124, Rusia, Moscú, c/3 Yamskogo Polya, 2, edif. 12A
Teléfono (multicanal): +7 495 789–45–87
Fax: +7 495 789–45–97

www.drweb.com | www.drweb-curenet.com | www.av-desk.com | freedrweb.com | mobi.drweb.com