Dr.WEB®
seit 1992

Defend what you create

Verschlüsselungstrojaner
Bedrohung №1

Die Verschlüsselungstrojaner stellen heute die Bedrohung #1 dar. Sie verschlüsseln auf PCs und mobilen Geräten Benutzerdateien und fordern vom Opfer Lösegeld für die Entschlüsselung.

Die ersten Verschlüsselungstrojaner der Familie Trojan.Encoder sind in den Jahren **2006–2007** aufgetaucht.

Seit Januar 2009 ist die Anzahl ihrer Muster um etwa **1 900%** gewachsen!

Zurzeit hat Trojan.Encoder **mehrere tausend Varianten**.

Was verlieren Sie?

Heute fordern die Übeltäter bis zu 1 500 Bitcoins für die Entschlüsselung von Dateien.
1 Bitcoin = € 272 oder $ 330.
Das Lösegeld kann den Betrag von bis zu **$ 49 500** erreichen.

Auch wenn Sie das Lösegeld bezahlt haben, gibt es keine Garantie dafür, dass Ihre Daten wiederhergestellt werden können.

Manchmal wird es kritisch, wenn die Übeltäter die durch Trojan.Encoder verschlüsselten Dateien nicht entschlüsseln können und sich an den technischen Support von Doctor Web wenden müssen!

Wie dringen Verschlüsselungstrojaner in Ihren PC ein?

In über 90% der Fälle werden die Verschlüsselungstrojaner durch den Benutzer selbst gestartet. Wenn es sich um eine unbekannte Modifikation von Trojanern handelt, ist die Vernichtung von Dateien nicht zu vermeiden.

Einige Varianten des Trojaners können durch keine Antivirensoftware erkannt werden.

Dies ist vor allem darauf zurückzuführen, dass sie zunächst auf aktuellen Versionen von Antivirensoftware getestet werden. Deshalb sind die Benutzer, die Antivirensoftware ohne Präventivschutz- oder Kinderschutzfunktion verwenden, einer größeren Infektionsgefahr durch einen Verschlüsselungstrojaner ausgesetzt.

Doctor Web
Deutschland GmbH

Rodenbacher Chaussee 6
D-63457 Hanau
Tel.: + 49 (0)6039 9395414
Fax: + 49 (0)6039 9395415

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

Dr.WEB®
seit 1992

Wie kann Dr.Web helfen?

1. Seien Sie auf der Überholspur – benutzen Sie Antivirensoftware mit einer Präventivschutzfunktion. Diese ermöglicht die Erkennung von Verschlüsselungstrojanern aufgrund von ähnlichen Verhaltensregeln.
   - **Dr.Web Präventivschutz:** http://products.drweb-av.de/technologies/preventive_protection.
2. Um dem Datendiebstahl vorzubeugen, benutzen Sie die Funktion **Schutz vor Datendiebstahl** in Dr.Web Security Space (Versionen 9 und 10). Im Unterschied zu regulären Backup-Programmen, benutzt Dr.Web ein **geschütztes Datenlager**, wo die unerlaubte Einschleusung von außen nicht möglich ist. Sollte der Trojaner Ihre Dateien (⩽10) trotzdem verschlüsseln, können Sie diese selbständig wiederherstellen, ohne dass Sie sich an den technischen Support von Doctor Web wenden müssen.
   - **Video zum Schutz vor Datendiebstahl:** http://support.drweb.ru/video/security_space.
3. Wenn Ihr Rechner durch eine unbekannte Modifikation des Trojaners infiziert wurde, wenden Sie sich bitte an den technischen Support von Doctor Web. **Unterlassen Sie beliebige Aktionen auf Ihrem infizierten Rechner**.
   - **Verhaltensregeln bei virenabhängigen Vorfällen:** http://legal.drweb.com/encoder.
   - **Analyse von virenabhängigen Vorfällen:** http://antifraud.drweb.ru/expertise.

   Für kommerzielle Dr.Web Benutzer ist die Dekodierung von verschlüsselten Dateien kostenlos.
   - **Kostenlose Entschlüsselung beantragen:** https://support.drweb-av.de/new/free_unlocker/for_decode/?lng=de.

Ist die Entschlüsselung möglich?

Trojan.Encoder nutzen **Dutzende von Verschlüsselungsalgorithmen**.

Laut Statistiken ist die Entschlüsselung nur in 10% der Fälle möglich.

Dies bedeutet, dass Benutzer, die den Präventivschutz vernachlässigt haben, Ihre Daten unwiderruflich verloren haben.

Von April 2013 bis März 2015 sind etwa **8 500 Dekodierungsanfragen** von Benutzern eingegangen, die wegen Verschlüsselungstrojanern zu Schaden gekommen sind.

Täglich gehen ca. 40 Dekodierungsanfragen im Virenlabor von Doctor Web ein.

Einige Trojaner-Modifikationen **können** nach Aussagen der Benutzer nur **durch Sicherheitsspezialisten von Doctor Web entschlüsselt werden**.

Seit Mai 2014 haben die Virenanalysten von Doctor Web viel Arbeit in die Entwicklung von Entschlüsselungsalgorithmen für **Trojan.Encoder.398** investiert. **Heute ist Doctor Web das einzige Unternehmen**, das die durch diesen Trojaner verschlüsselten Dateien mit **90%-iger Wahrscheinlichkeit** wiederherstellen kann.

Mehr zu Verschlüsselungstrojanern: http://antifraud.drweb-av.de/encryption_trojs**.**

Doctor Web Deutschland GmbH

Doctor Web ist ein führender russischer Anbieter hauseigener IT-Sicherheitslösungen. Dr.Web Antivirensoftware wird seit 1992 weiterentwickelt.

Rodenbacher Chaussee 6
D-63457 Hanau
Tel.: + 49 (0)6039 9395414
Fax: + 49 (0)6039 9395415

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