Dr.WEB®
since 1992

Defend what you create

Encryption ransomware
Threat №1

Encryption ransomware is one of today's gravest threats. **Trojan.Encoder** programs encrypt files on PCs and handhelds and demand a ransom for their decryption.

The first **Trojan.Encoder** ransomware species appeared in **2006–2007**.

Since January 2009, the number of modifications of those initial species has increased by **1,900%**!

Now the Trojan.Encoder family incorporates **thousands of malware modifications**.

What it can cost you

Today criminals demand up to 1,500 bitcoins for decryption.
1 bitcoin equals 272 euros or 330 dollars.
A ransom demand can reach **49,500 dollars**.

Even if you pay your attacker a ransom, there is no guarantee you'll get your data back.

Things can even get rather peculiar. In one situation, a user paid a ransom, but their attackers could not decipher the files encrypted by their own Trojan.Encoder and advised the user to seek help... from Doctor Web's technical support service!

How encryption ransomware penetrates computers

In over 90% of incidents, users are responsible for launching encryption ransomware on their computers. And if the modification is one with which the virus database is unfamiliar, files will inevitably be destroyed.

Some encryption ransomware modifications are not recognized by any anti-virus.

Virus makers test encryption Trojans against up-to-date versions of known anti-viruses to make sure that their malware can bypass anti-virus security. Protected only by an anti-virus that has no proactive protection features, parental control, or any other means by which to prevent malware programs from penetrating and launching themselves, a system faces a higher risk of becoming infected by encryption ransomware from which no anti-virus can protect it.

3d street Yamskogo polya 2-12A, Moscow, Russia, 125040

Phone: +7 495 789–45–87
Fax: +7 495 789–45–97

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

Dr.WEB®
since 1992

How Dr.Web can help

1. Stay one step ahead—use an anti-virus that incorporates proactive protection technologies. They will enable the anti-virus to detect encryption ransomware by identifying similarities in the behavioural patterns of their various modifications.
   - Dr.Web preventive protection: http://products.drweb.ru/technologies/preventive_protection.
2. To prevent data loss caused by encryption ransomware, use the Data loss prevention feature of Dr.Web Security Space (versions 9 and 10). Unlike conventional backup programs, Dr.Web creates backups and protects them from intruders. And, even if a Trojan encrypts your files (as many as 10), you will be able to restore them on your own without having to request support from Doctor Web.
   - Watch video tutorial about data loss prevention http://support.drweb.ru/video/security_space.
3. If your PC is infected with encryption ransomware with which Dr.Web is unfamiliar, do not perform any actions with the infected machine and ask Doctor Web technical support to restore your files.
   - Rules of conduct in the event of a virus-related computer incident: http://legal.drweb.ru/encoder.
   - Investigation of virus-related computer incidents http://antifraud.drweb.ru/expertise.

   Doctor Web provides decryption free of charge to users of commercial Dr.Web licenses.
   - File a free decryption request: https://support.drweb.com/new/free_unlocker/for_decode/?lng=en.

Prospects for decryption

Trojan.Encoder programs use **dozens of different encryption algorithms**.

According to Doctor Web's statistics, the probability of restoring corrupted files is roughly 10%.

This means that users who do not take the necessary protective measures, will lose most of their data for good.

From mid-April 2013 to March 2015, Doctor Web's virus laboratory has received more than **6,500 decryption requests** to restore files affected by Trojan encoders.

On average, Doctor Web's virus laboratory receives 40 decryption requests daily.

User feedback on forums indicates that **files compromised by some versions of these Trojans can be decrypted only by Doctor Web's security experts**.

Since May 2014, Doctor Web has been conducting a major research and development project to design routines for recovering data affected by Trojan.Encoder.398. Currently **Doctor Web is the only company** whose experts are able to recover compromised files with a 90% probability of success.

More about encryption ransomware http://antifraud.drweb.com/encryption_trojs/

Doctor Web

Doctor Web is a Russian anti-virus vendor with a software development record dating back to 1992.

3d street Yamskogo polya 2-12A, Moscow, Russia, 125040

Phone: +7 495 789–45–87
Fax: +7 495 789–45–97

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