General guidelines for decoding ransomware

In this guide, TipsMake.com will try to help unfortunate readers infected with ransomware and encrypted files on the computer.

In this guide, **TipsMake.com** will try to help unfortunate readers infected with ransomware and encrypted files on the computer. The instructions below will show you some possible methods that allow you to decrypt any files locked by ransomware.

However, you have to remember that there are a large number of ransomware viruses out there, so this guide can help you unlock some encrypted files, but may also fail to recover data that is believed. Hackers are holding. Cannot be sure that following this guide can unlock all files on your computer. However, you should still try the instructions on this page and only if they don't work, consider implementing some other methods.

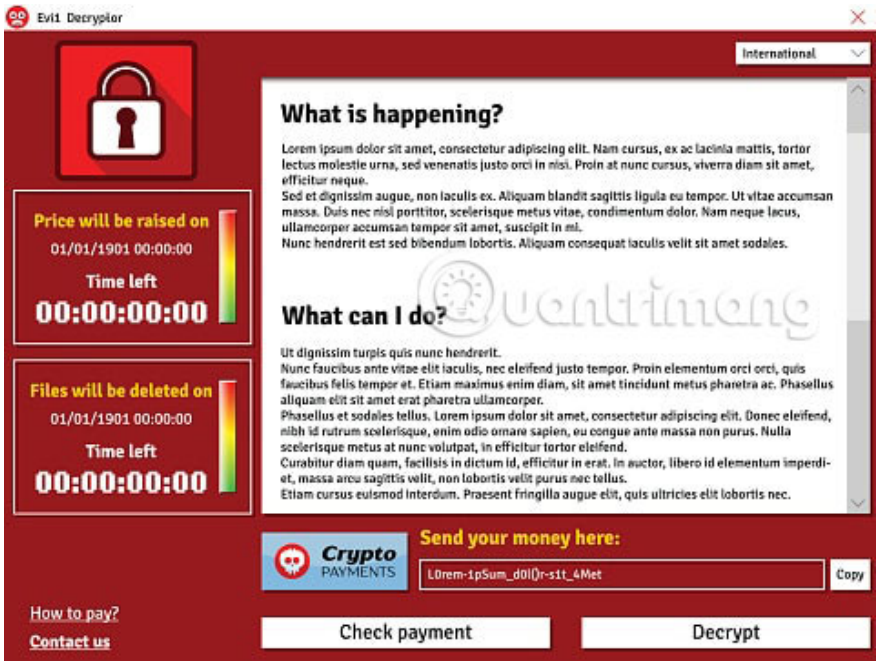
Do you know how to decode ransomware?

1. Identify ransomware
    1. Check the ransom notice section
    2. Use ID Ransomware
2. Restore shadow copy
3. Use decoding tool
    1. Trend Micro Decryptor tool (free)
    2. Emisoft Decryptors (Free)
    3. Decryptor for Petya (Free)
    4. .locked decryptor (Rakhni Ransomware) (Free)

Identify ransomware

Before decrypting the file, first make sure you really know the type of ransomware that has been encrypted for your data. There are several ways to identify.

Check the ransom notice section



The first and easiest way to learn the name of ransomware is to simply read the ransom information section. Depending on the ransomware you are dealing with, the ransom notification may be displayed as a banner on the screen or the virus will create a file notepad on the desktop and in some other folders. In addition to the ransom notification method presented, the content inside requires information about the virus and perhaps its name is also written in it. Therefore, check this notification section and see if you can learn the malware name that way.

Use ID Ransomware

If you are struggling to find out the name of the ransomware has been infected with your computer, you can use a free online tool called ID ransomware. Visit: *https://id-ransomware.malwarehunterteam.com/index.php.* Once you have reached the ransomware ID, you will have to upload ransom note files, as well as a sample of the

encrypted file. If there is no ransom note file, there is a field where you can add other virus information such as email or IP address that ransomware has provided for you. Once you have uploaded the file and filled in all the necessary information, this online tool will identify the virus, if the malware is in its library.

Warning!

Before continuing, you must make sure that the actual malware has been removed from the system, so that it cannot re-encrypt any files you have decrypted, if the virus has not been deleted, all files that you decrypted may be locked again. In addition, you should also back up files and then upload them to a separate device (preferably a flash drive, instead of a computer or smartphone). Some ransomware threaten to delete the locked data, if you try to decode it and not pay ransom. That is why backing up plays a very important role.

Restore shadow copy

The first method you should try to combat ransomware encryption is to recover your data through shadow copies. When the virus encrypts your data, it first deletes the original files and replaces them with encrypted identical copies. However, the original deleted can still be recovered, if you're lucky. The tool that the article will cover here is capable of doing that.

1. Access this link to download Data Recovery Pro - a free shadow copy recovery tool.

2. Install and run the program.

3. Select a scanning option. You should perform a full scan for the best results and also perform a scan of all files.

4. After the scan is complete (the full scan option may take a while, be patient!), Browse through the list of files and select the files you want to recover.

Use decoding tool

There are many ransomware decoding tools. However, note that most new ransomware models do not yet have decoders developed specifically for them. If you're lucky, the following list of decoding programs may include tools that can unlock your files. The article will provide download links for the tools listed here, so you can directly download the tools you need and put them to use.

Trend Micro Decryptor tool (free)

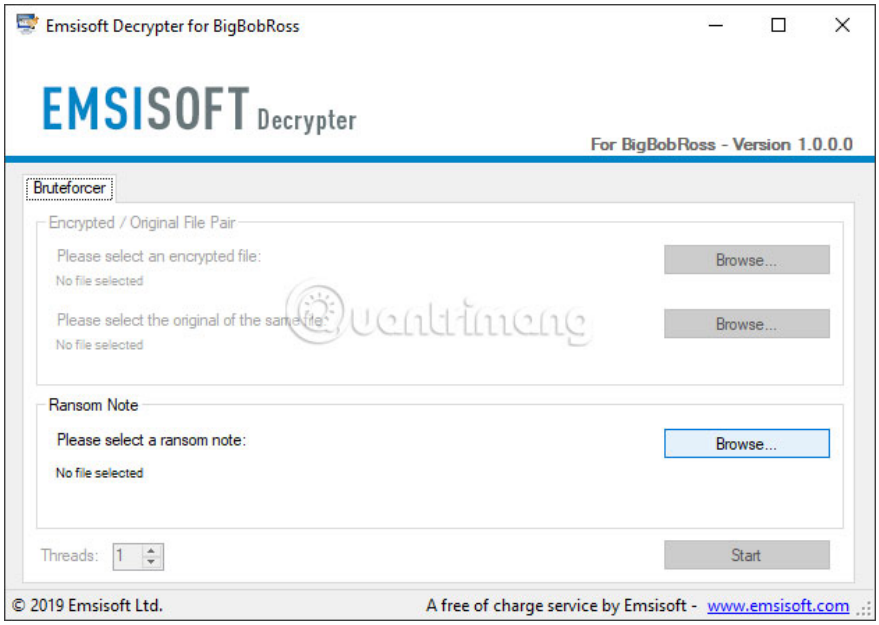
This software tool developed by Trend Micro, can decode the encryption of some ransomware types. Also, after a period of time, Trend Micro Decryptor receives updates for new ransomware that it can decrypt. You can download Trend Micro Decryptor tool here.

This is also a list of viruses that this decoder can currently handle

1. CryptXXX V1, V2, V3
2. CryptXXX V4, V5
3. TeslaCrypt V1
4. TeslaCrypt V2
5. TeslaCrypt V3
6. TeslaCrypt V4
7. SNSLocker
8. AutoLocky
9. BadBlock
10. 777
11. XORIST
12. XORBAT
13. CERBER V1
14. Stampado
15. Nemucod
16. Chimera
17. LECHIFFRE
18. MirCop
19. Jigsaw
20. Globe / Purge
21. DXXD

22. Teamxrat / Xpan
23. Crysis
24. TeleCrypt

Emisoft Decryptors (Free)



Another security company offers a significant number of decoding options as Emisoft. Emisoft has created its own decoding tools for a large number of ransomware viruses and is also developing new tools. You can visit the Emisoft website and download the decoder you need here.

Here are some ransomware versions that Emisoft introduced and created the corresponding decoders:

1. NumecodAES
2. Amnesia
3. Amnesia2
4. Cry128
5. Cry9
6. Damage
7. CryptON
8. MrCr
9. Malboro
10. Globe3
11. OpenToYou
12. etc .

Decryptor for Petya (Free)

Ransomware Petya works differently from most other similar viruses. It directly blocks access to the PC, making it impossible for you to boot into Windows until you make the ransom request. Unlocking your PC is much harder than decoding some files.

First, you need to unplug the PC's HDD and plug it into another PC. In this case, the new computer needs a reliable antivirus program. Next, download Petya Sector Extractor (developed by Wosar) and run it. The necessary data will be extracted and you need to fill them in the corresponding page. After sending the required data, you will receive a code that you must record on paper or on another device. Put the hard drive back into the PC and when the Petya screen appears, enter the code you received.

.locked decryptor (Rakhni Ransomware) (Free)

To decrypt Rakhni-locked files (add .locked extensions to your files after encryption), use this link to download the decoder and unlock your data.

Refer to the following articles:

1. How to decode ransomware InsaneCrypt (Everbe 1.0)
2. How to decode Stupid Ransomware with StupidDecrypter

Note for readers

So far, it's the developers and related ransomware decoders that the article can find.**TipsMake.com** will try to update as soon as new information is available. Unfortunately, there are still many annoying ransomware viruses that don't have a decoder or a successful removal method. Security experts are working hard to provide solutions for newer versions of these malicious malware types. Therefore, keep in mind that it is better to stay safe and not be the prey of malicious viruses, instead of having to handle what they have caused with your data or PC.

Last but not least, if you have suggestions about a decoder that the article missed or is looking for information about a type of ransomware not mentioned here, please leave a comment in the section. comment below.

Wish you soon find a suitable solution!