Possible removal of Ransomware

Advanced ransomware utilizes a technique in which it encrypts the user's files, making them inaccessible, and demands a ransom payment to decrypt them.

Keep in mind that even after you pay the ransom, there is no assurance that your files will be decrypted.

Get your personal files decrypted

For certain known ransomware, it is possible to recover your files with the help of free software. Unfortunately, none of the free software is capable to provide recovery solutions for all known ransomware. In fact, you will have to find a decryption program specifically made for a certain type of ransomware.

Initially, you need to find out which ransomware has encrypted your files.

The following services may help with this:

ID-Ransomware: on the website, you can upload the file in which the attackers have delivered their message. Furthermore, an upload button for encrypted files is provided. You can also enter the blackmailer's email address if you have received one from the criminals to contact them.

The service utilizes this data to identify the ransomware used in the attack. It already recognises over 1100 malware samples.

NO MORE RANSOM: The service not only helps to identify the exact blackmail virus, but additionally offers the right encryption tool - if there is one.

The website offers ransomware advice plus a '**Crypto Sheriff**' tool. Over here you can fill out a form for bitcoin or TOR onion network addresses, website URLs and emails from the ransom demand, as well as the ability to upload encrypted files.

Next the website will check if the type of ransomware is known and whether there is a solution available. If there is, they will provide you with the link to download the decryption solution.

Following other vendors provide free decrypting tools for specific types of ransomware.

- **Avast anti-ransomware tools** avast.com/c-topic-ransomware provides some more information about ransomware and how to remove ransomware from MAC and Windows computers.

Possible removal of Ransomware

You will find the currently available decryptors at: avast.com/ransomware-decryption-tools. These tools can help decrypt files encrypted by more than 20 forms of ransomware. Just click a name to see the signs of infection and get the free fix.

- **AVG ransomware decryption tools** avg.com/en-gb/ransomware-decryption-tools#apocalypse offers tools to decrypt files encrypted by the following forms of ransomware:
  - Apocalypse
  - BadBlock
  - Bart
  - Crypt888
  - Legion
  - SZFLocker
  - TeslaCrypt

- **Kaspersky Lab decryptors** noransom.kaspersky.com/ is designed for small to medium sized businesses. Kaspersky Lab hosts a wide range of decryptors claiming to decrypt lots of nasty types of ransomware.

Ransomware type	Decrypts files affected by
Rakhni Decryptor	Rakhni, Agent.iih, Aura, Autoit, Pletor, Rotor, Lamer, Cryptokluchen, Lortok, Democry, Bitman (TeslaCrypt) version 3 and 4, Chimera, Crysis (versions 2 and 3), Jaff, Dharma, new versions of Cryakl ransomware, Yatron, FortuneCrypt
Rannoh Decryptor	Rannoh, AutoIt, Fury, Cryakl, Crybola, CryptXXX (versions 1, 2 and 3), Polyglot aka Marsjoke
Wildfire Decryptor	Wildfire ransomware
CoinVault decryptor	CoinVault and Bitcryptor ransomware
Shade Decryptor	Shade version 1 and 2
Xorist Decryptor	Xorist and Vandev
Rector Decryptor	Decrypts files affected by Rector

In case you haven't found a solution here, make a search on the web for the ransomware that has infected your device.