How to remove CoinVault ransomware from your computer and restore your files

Step 1: Are you infected with CoinVault?

It is fairly easy to see if you are infected with CoinVault, because if you are, you will see an image like that depicted in Figure 1.

Figure 1: CoinVault screenshot

Step 2: Get the Bitcoin wallet address

In the bottom right of Figure 1 you will see the Bitcoin wallet address (surrounded by a black circle). It is very important that you copy and save this address!

Step 3: Get the encrypted file list

In the top left corner of Figure 1 you will see a 'view encrypted filelist' button (surrounded by a blue circle). Click on it and save the output to a file.

Step 4: Remove CoinVault

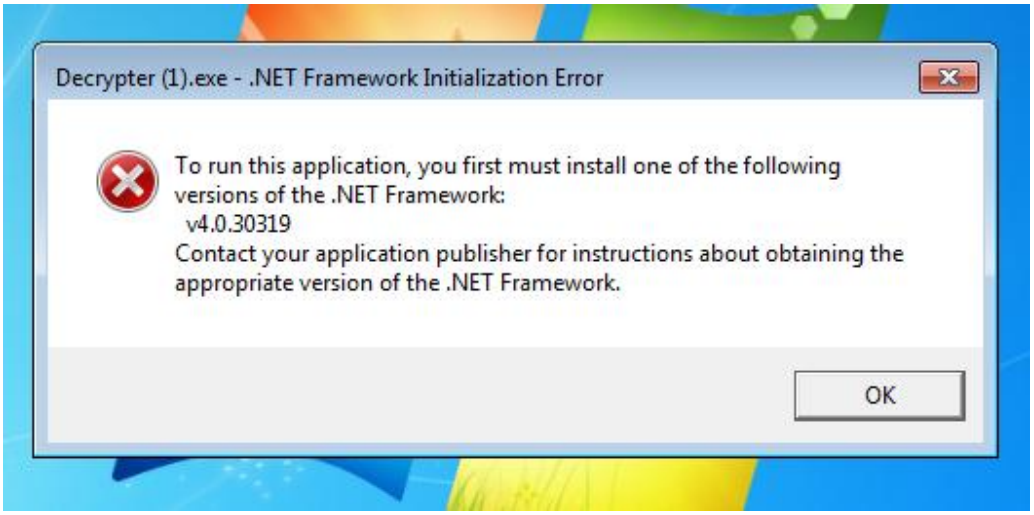
Go to https://kas.pr/kismd-cvault and download the trial version of Kaspersky Internet Security. Install it and it will remove CoinVault from your system.

Step 5: Check https://noransom.kaspersky.com

At https://noransom.kaspersky.com you can submit the Bitcoin wallet address from step 2. If your Bitcoin wallet address is known, the IV and Key will appear on the screen. Please note that multiple keys and IVs may appear. If this is the case, please save all the keys and IVs to your computer, you will need them later.

Step 6: Download the decryption tool

Download the decryption tool from https://noransom.kaspersky.com/ and run it on your computer. If you get an error message, as shown in Figure 2, go to step 7. If not you can go to step 8.

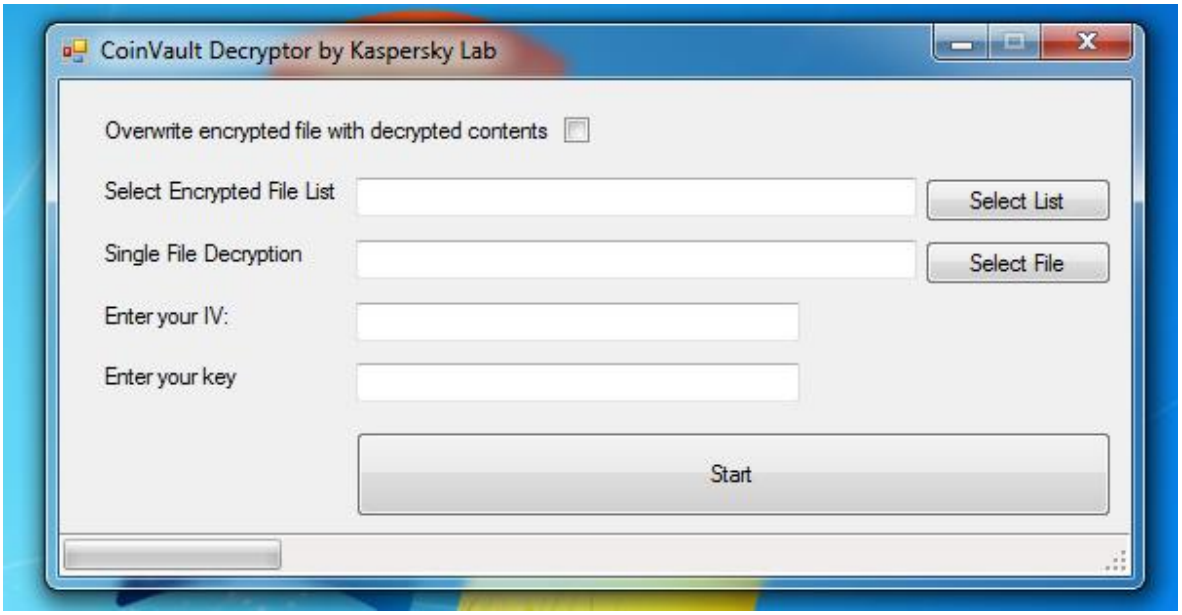


Step 7: Download and install additional libraries

Go to http://www.microsoft.com/en-us/download/details.aspx?id=40779 and following the instructions on the website. Then install the software.

Step 8: Decrypt your files

Start the tool and you will see a screen as in Figure 3.



When running the tool for the first time, we strongly advise the following:

- Click on “select file” in the Single File Decryption box and select the file you want to decrypt;
- Enter the IV from the webpage into the IV box;
- Enter the key from the webpage into the key box;
- Click on “start”.

Verify whether the newly created file is properly decrypted. If this is the case, you can select “Overwrite encrypted file with decrypted contents”, select the file list from step 3, and click on “start” again.

If you received multiple IVs and keys when you entered your Bitcoin wallet address, please be very careful. At the moment we are not 100% sure where the multiple IVs and keys for one Bitcoin wallet come from. Therefore we suggest leaving the “Overwrite encrypted file with decrypted contents” unticked, and trying to decrypt one file first (you can get this file from the list obtained in step 3). If the new file is not properly decrypted, try with another key IV pair until the file is successfully decrypted. This should be done for all the files.