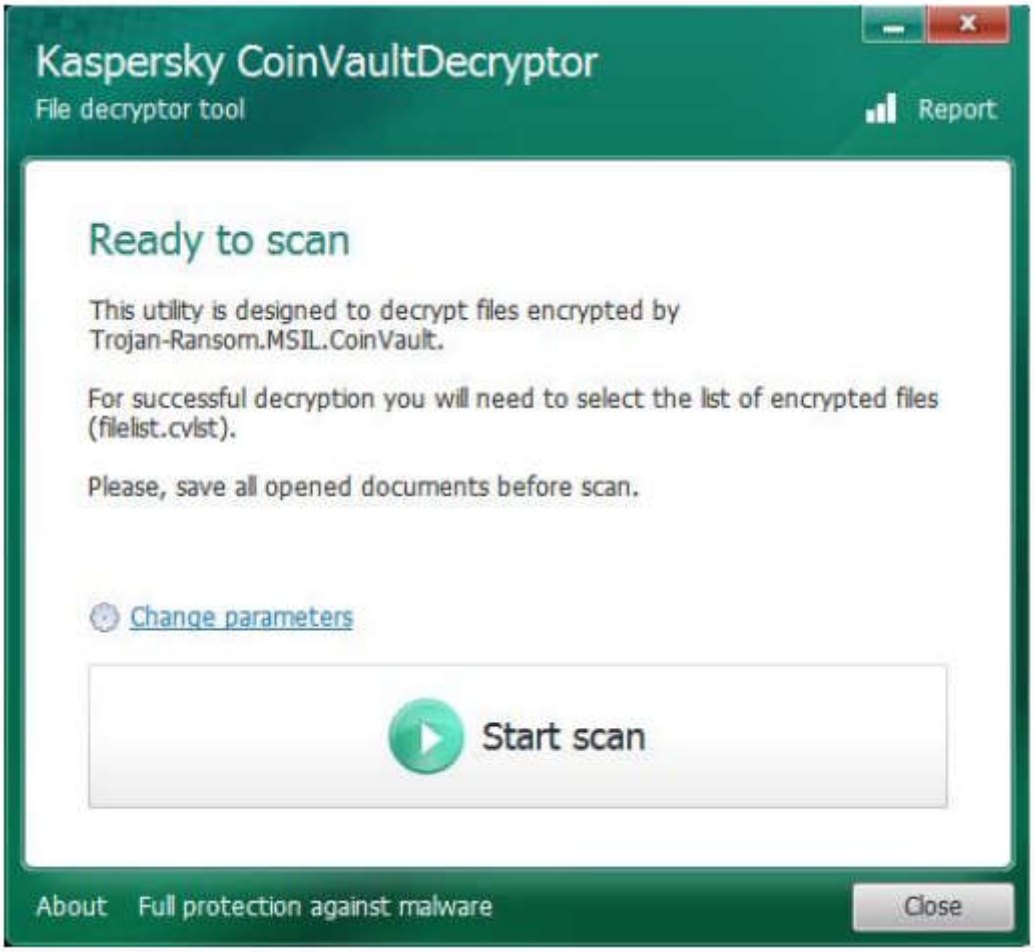
How-to guide.

IMPORTANT! Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

To decrypt the files:

1. Download the **CoinVaultDecryptor.zip** archive and extract the files using a file archiver (for example, 7zip).
2. Doublle-click the **CoinVaultDecryptor.exe** file.
3. Press the **"Start Scan"** button on the application's main screen.



4. A **"File Selection"** dialog pops up. You should locate the file called **"filelist.cvlst"**, that is usually left behind after a CoinVault infection.
5. Click **Open.**
6. If you can't find the **"filelist.cvlst"** file on your system, you have to **place all the encrypted files in a single folder** in order to decrypt them. The utility assumes that every single file in the folder is encrypted and will try to decrypt them all.

7. To operate in this mode, you have to click the **"Change Parameters"** button on the application's main
   screen and select the "Folder with Encrypted Files" option.
8. The Kaspersky **CoinVaultDecryptor** finds a suitably encrypted file for key search, tries every single CoinVault key until it finds your personal key and then decrypts all the files provided.
9. By default, the application renames the decrypted files by adding "decryptedKLR" to the file name: **Somefile.doc -> Somefile.decryptedKLR.doc**
10. This is an additional safeguard against improper file handling. If you have additional backup copies and don't want to manually rename your files, there is an additional parameter under the **"Change Parameters"**: **"Replace encrypted files with decrypted ones"** If you select it, the encrypted files will be decrypted under their original names.