Safety 101: Virus-fighting utilities

Tool for decrypting files affected by Trojan-Ransom.MSIL.CoinVault

Back to "Virus-fighting utilities"
2017 Mar 30 ID: 13331

When the malware of the Trojan-Ransom.MSIL.CoinVault family infects the computer, it encrypts all user's files and shows the notification on the screen claiming money for decrypting the files.

Use the CoinVaultDecryptor tool to restore the encrypted files. To disinfect the system and decrypt the files:

1. Run the antivirus scan

2. Restore the encrypted files with the CoinVaultDecryptor tool

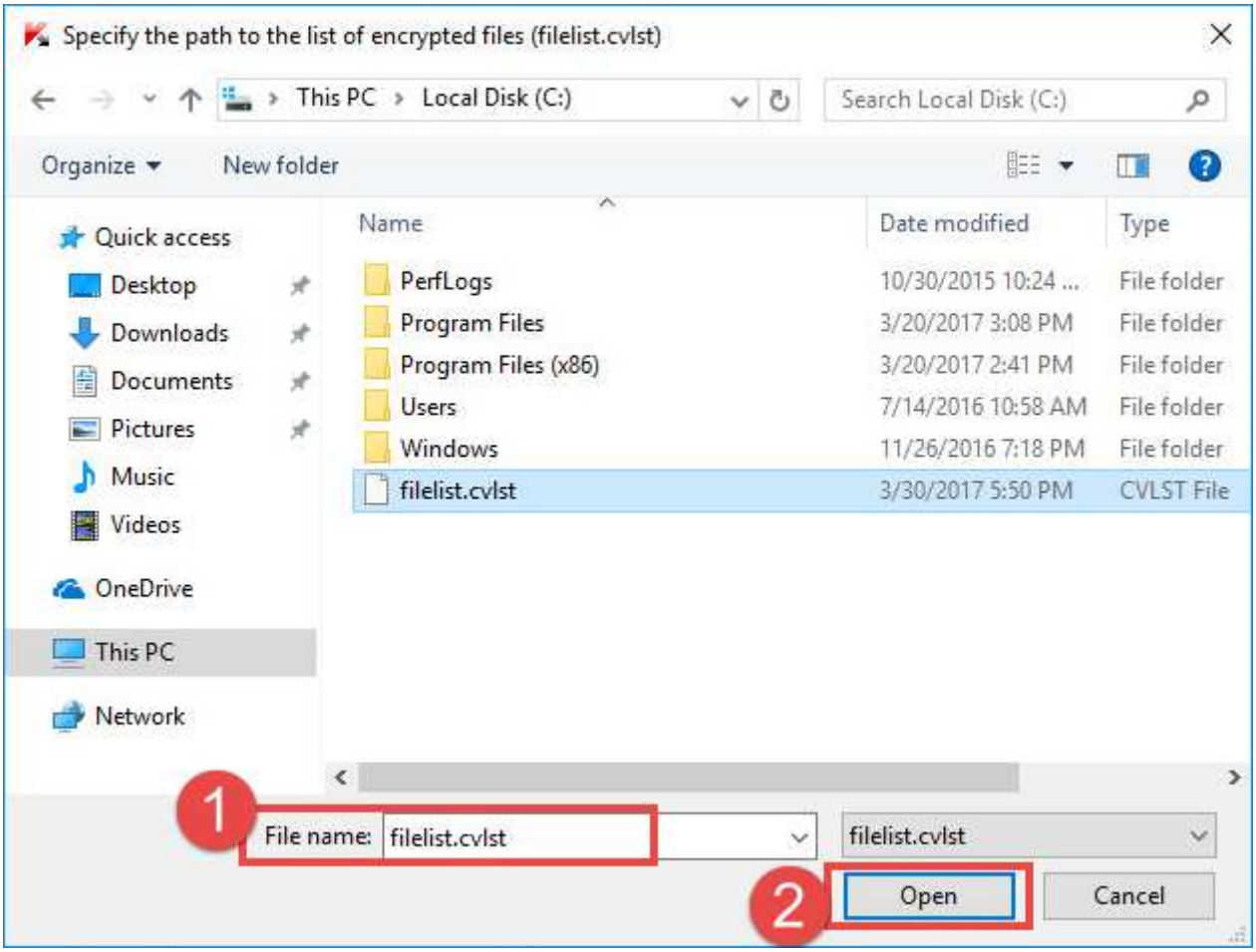
The CoinVaultDecryptor restores the encrypted files in two ways:

- Using the **filelist.cvlst** file. The Trojan-Ransom.MSIL.CoinVault malware creates the **filelist.cvlst** file on the computer. The file contains the list of encrypted files. Usually, the file is located in the temporary folder (**TEMP**) or in the root folder of disk **C**. If you search for the **filelist.cvlst** manually, enable display of hidden files and folders.
- Using the folder with the encrypted files If you cannot find the **filelist.cvlst** file, create a new folder and copy the encrypted files into it.

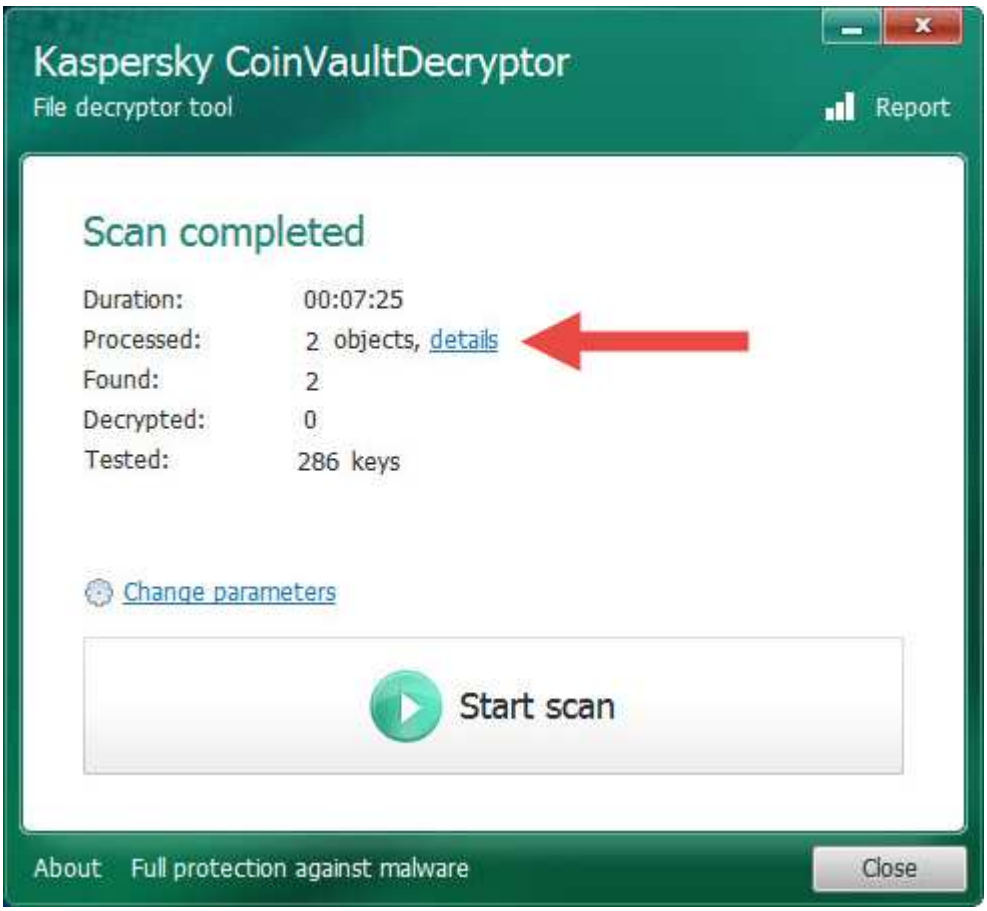
To restore the encrypted files using **filelist.cvlst**:

1. Download CoinVaultDecryptor.zip and run CoinVaultDecryptor.exe.
2. In the main window, click **Start scan**.

3. Specify the path to the **filelist.cvlst** file and click **Open**.

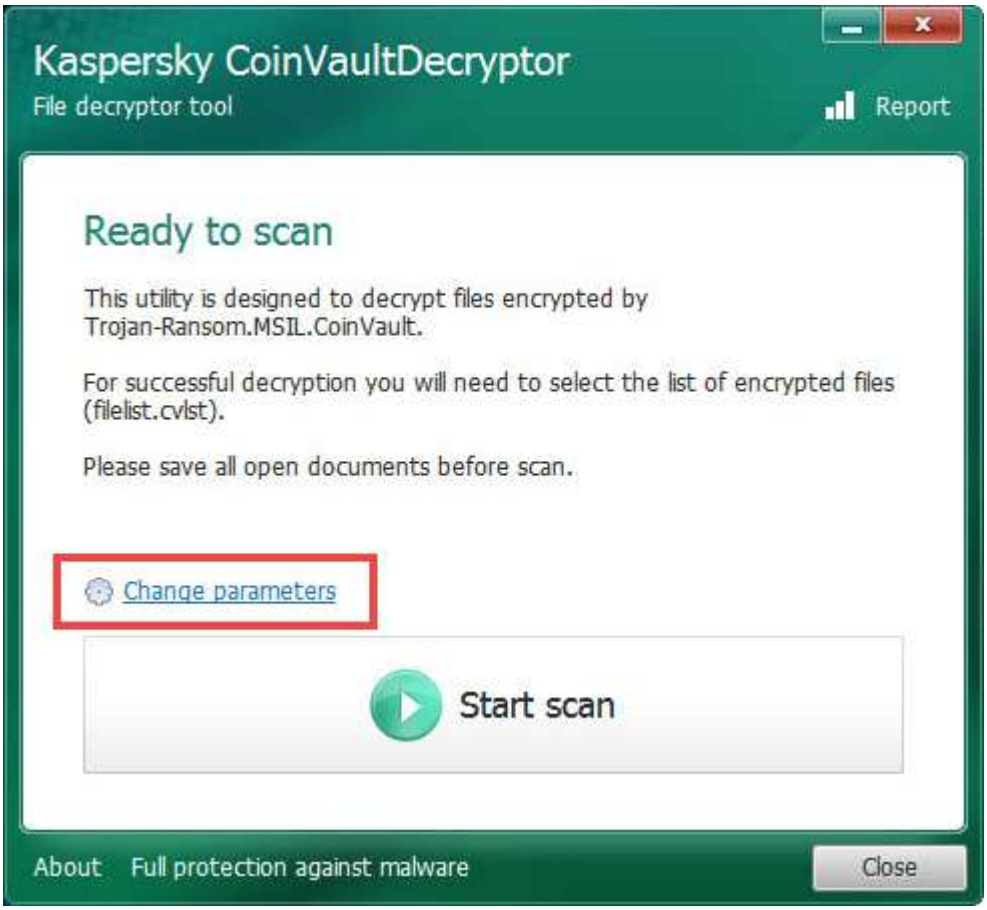


4. Wait until the files are found and decrypted.
5. To view the information about the task, click **Details**.

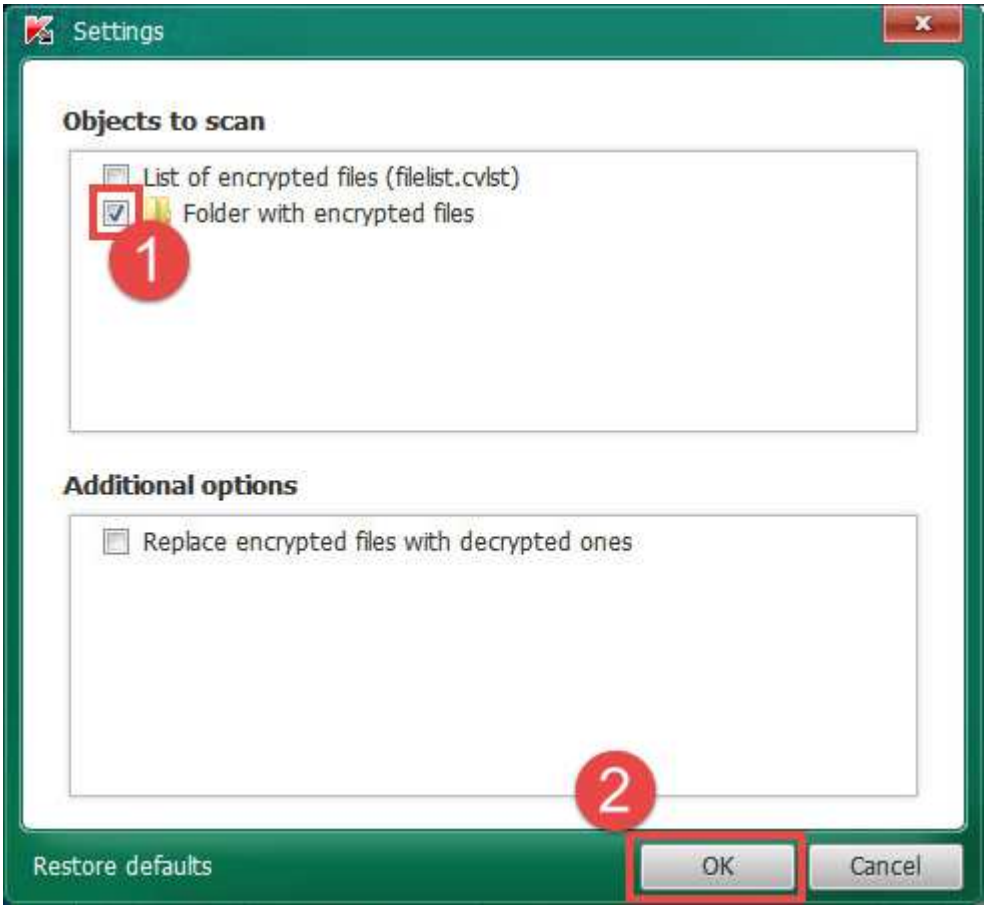


To restore the encrypted files from the folder:

1. Download CoinVaultDecryptor.zip and run CoinVaultDecryptor.exe.
2. Click **Change parameters**.



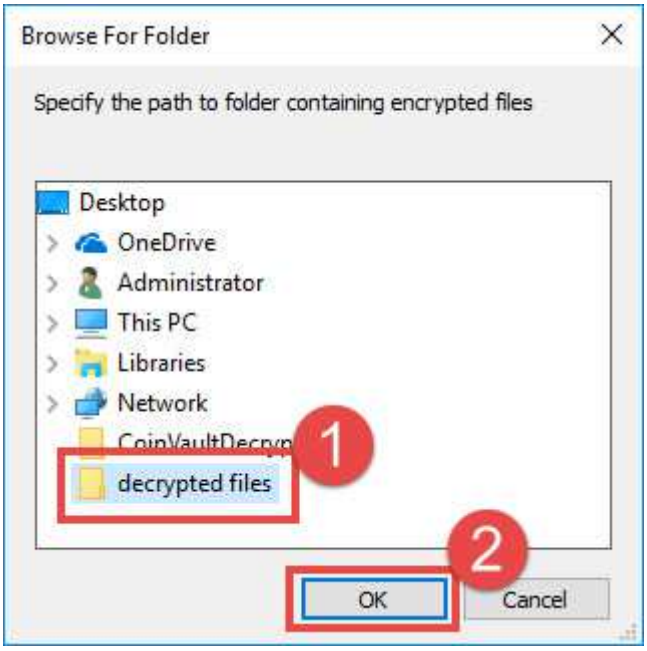
3. In the **Settings** window, select the check box for **Folder with encrypted files** and click **OK**.



4. In the main window, click **Start scan**.

5. In the warning window, click **Continue**.

6. In the **Browse For Folder** window, specify the folder where the encrypted files are located and click **OK**.



7. Wait until the files are found and decrypted.
8. To view information about the scan task, click **Details**.

If the file was encrypted by Trojan-Ransom.MSIL.CoinVault, the tool will save the files to their original location with the extension **decryptedKLR.**. If you select the option **Delete encrypted files after decryption**, the decrypted file will be saved under the original name.

Was this information helpful?
Yes No

Useful references

Forum: Virus-related issues
Free virus-fighting utilities tools

Back to "Virus-fighting utilities"

Support for Home

Consumer Support Contacts
Contact support via My Kaspersky
Knowledge Base for Home
How-to Videos
Forum

Virus-fighting tools & services

Scan file or URL for viruses
Report a false alarm
Kaspersky Virus Removal Tool
Kaspersky Rescue Disk
Other virus-fighting tools

Support for Small Business

Small Business Support Contacts
Contact support via My Kaspersky
Knowledge Base for Small Business
Forum

Software Downloads

Buy online
Renew license
Get updates
Free trial download

Support terms and conditions
(updated April 12, 2017)

Support for Business

Business Support Contacts
Contact support via CompanyAccount
Knowledge Base for Business
Product Support Lifecycle
Premium Support Plans
Licensing by Subscription
Forum
Online Trainings
Subscribe to news

Site Feedback

Privacy Policy Contact Us About us

-

Have you found what you were looking for?

Please let us know how we can make this website more comfortable for you

Enter your feedback here (max. 500

Send feedback Send feedback

Thank you!

Thank you for submitting your feedback.
We will review your feedback shortly.