How-to guide.

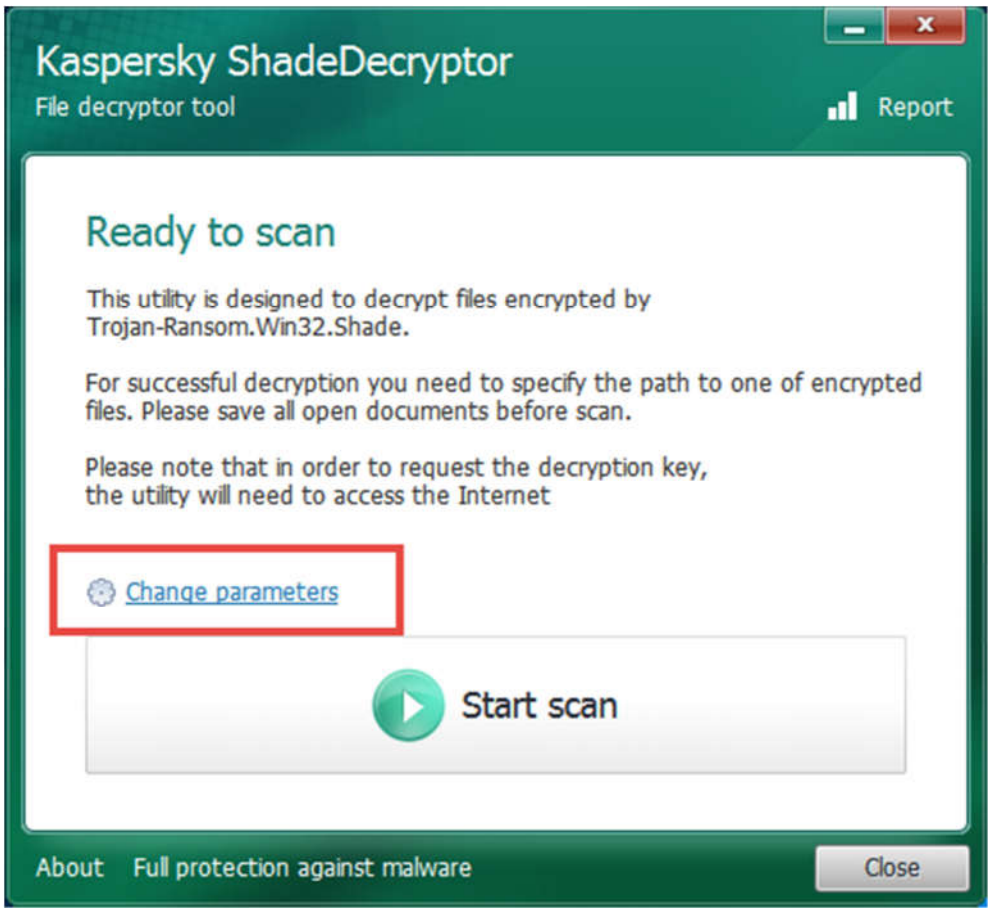
IMPORTANT! Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

First, the tool searches for the decryption key in its database. If the key is present in the database, the files are decrypted and become accessible. If the key is not present in the databases, the tool sends the request to the server in search for additional keys. This action requires access to the Internet.

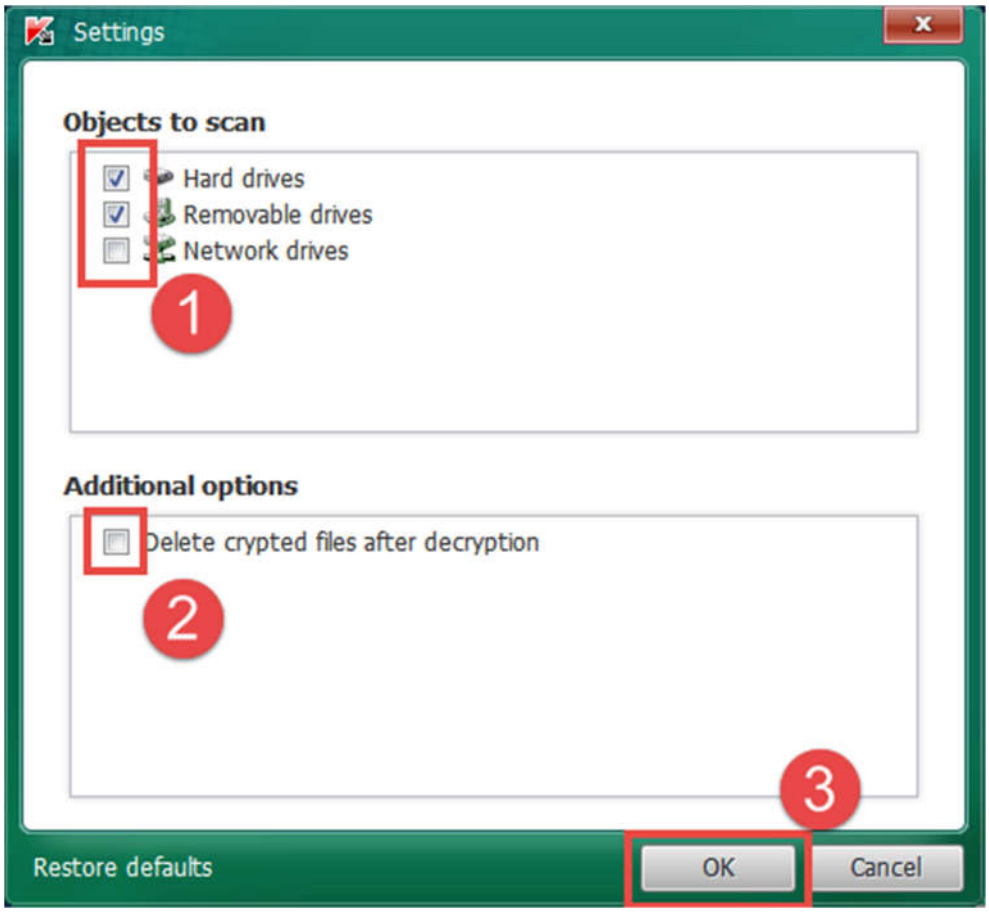
To decrypt the files:

1. Download the **ShadeDecryptor.zip** archive and extract the files using a file archiver (for example, **7zip**).
2. Doublle-click the **ShadeDecryptor.exe** file.

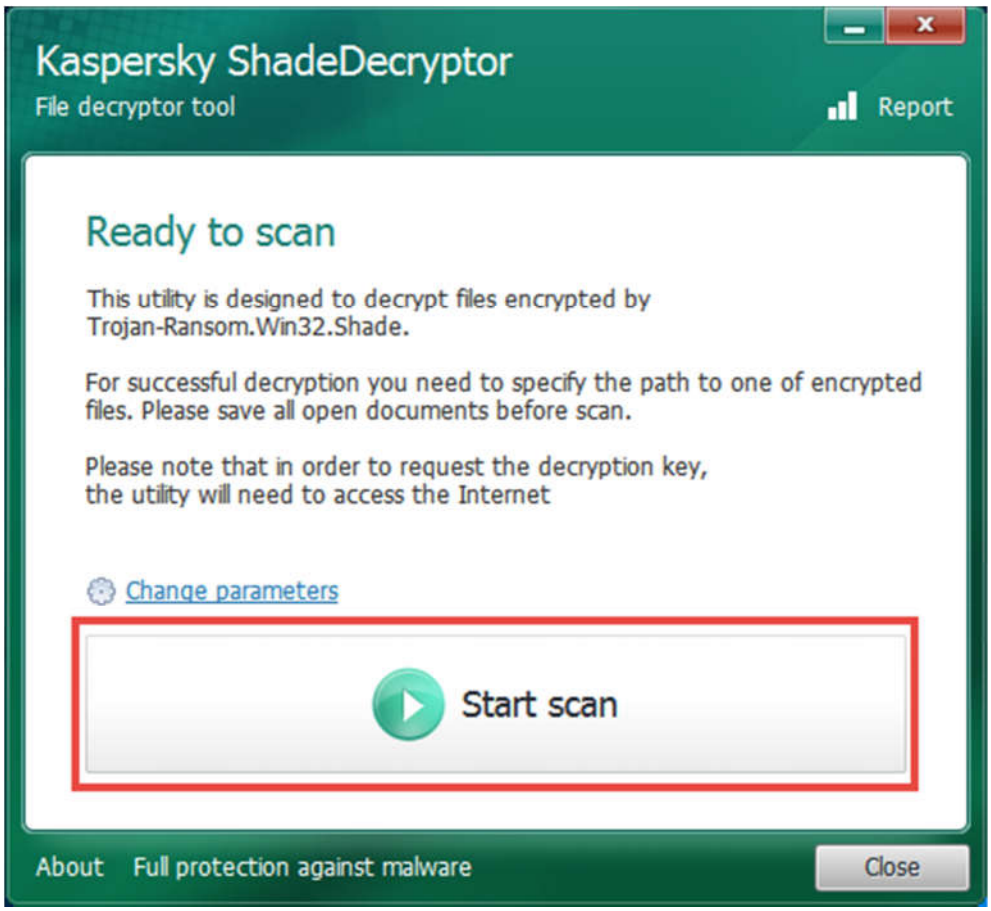
3. In the **User Account Control** (**UAC**) window, enter the administrator password and click **Yes**.
4. In the **Kaspersky ShadeDecryptor** window, specify the scan scope by clicking **Change parameters**.



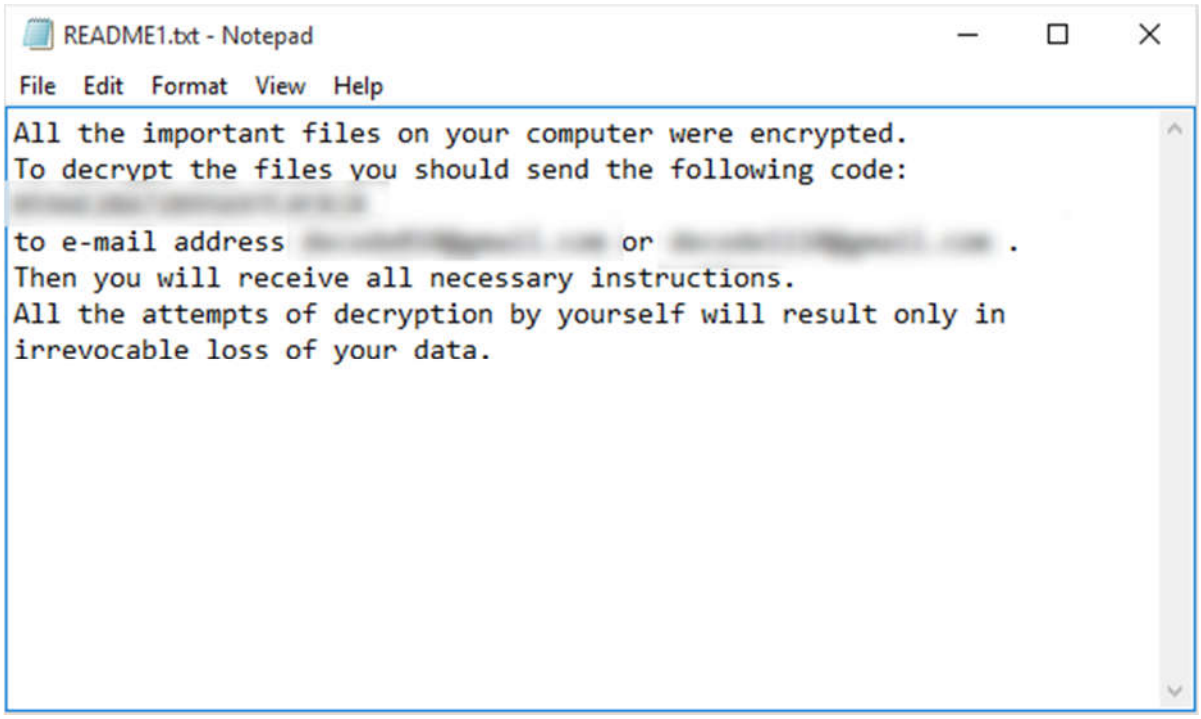
5. In the Settings window, select the drives to scan in the **Objects to scan** section. To delete the encrypted files after scan, select the check box in the **Additional options** section.
6. Click **OK**.



7. In the **Kaspersky ShadeDecryptor** window, click **Start scan**.



8. In the window **Specify the path to one of encrypted files**, select the location of one of the files.
9. Click **Open**.
10. If the tool is unable to detect the infection identification, it will request a path to the **readme.txt** file.



11. To view the information about the scan, click the **details** link.

12. To view the history of performed scans, click **Report** in the upper-right corner of the **Kaspersky ShadeDecryptor**window.