The ShadeDecryptor tool for defending against Trojan-Ransom.Win32.Shade

support.kaspersky.com/13059

Back to "Recovery tools"
Latest update: June 15, 2021 ID: 13059

Do you want to prevent infections? Install Kaspersky Internet Security.

To download the ShadeDecryptor utility, click **Download**.

Download
The Trojan-Ransom.Win32.Shade malware encrypts the files on the user's computer and makes them inaccessible. Using the ShadeDecryptor tool, you can try to decrypt files with the following extensions:

- xtbl
- breaking_bad
- ytbl
- heisenberg
- better_call_saul
- los_pollos
- da_vinci_code
- magic_software_syndicate
- windows10
- windows8
- no_more_ransom
- tyson
- crypted000007
- crypted000078
- dexter
- miami_california
- rsa3072
- decrypt_it

The tool searches for the decryption key in its database. If the key is found in the database, the files are decrypted. If the key is not in the databases, the tool sends a request to the server for additional keys. This requires Internet access.

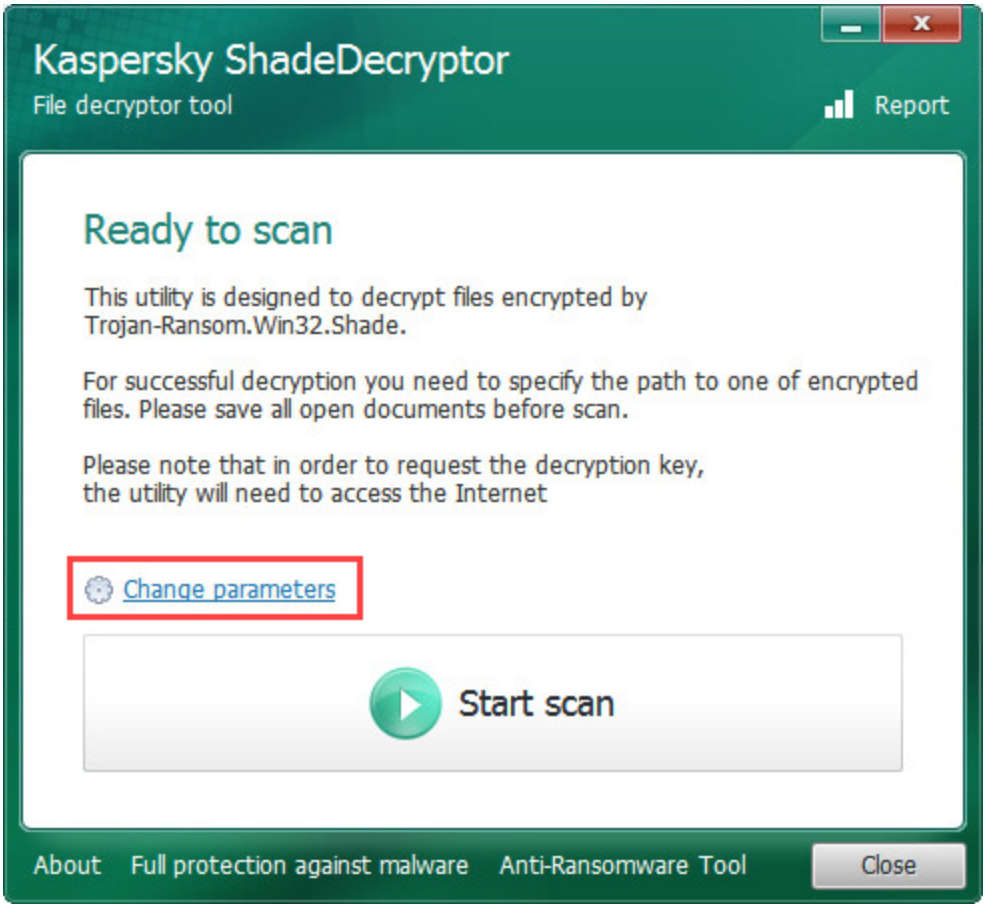
To avoid infection:

- Download and install Kaspersky Internet Security, which protects your PC against file-encrypting and screen-locking malware.
- Follow the instructions in this article.

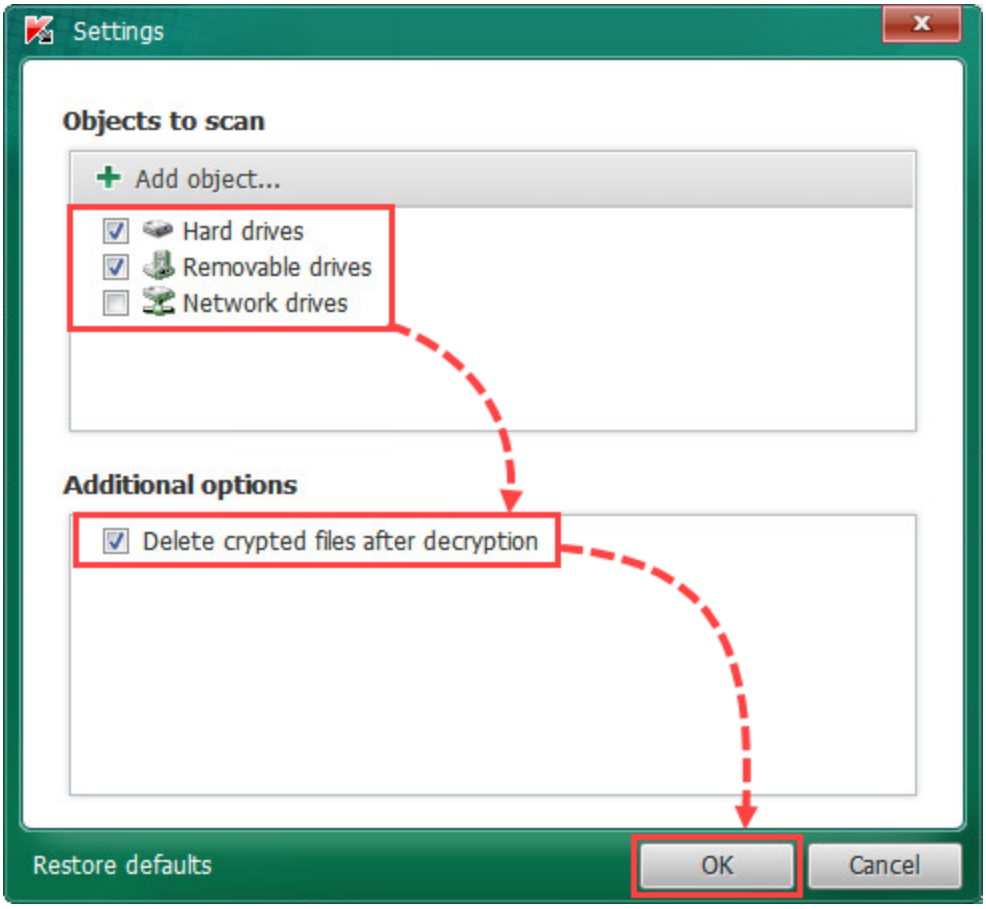
How to decrypt files using ShadeDecryptor

1. Download the ShadeDecryptor.zip archive and extract the files from it. Use an archiver such as 7-Zip.
2. Run the ShadeDecryptor.exe file on the infected computer.

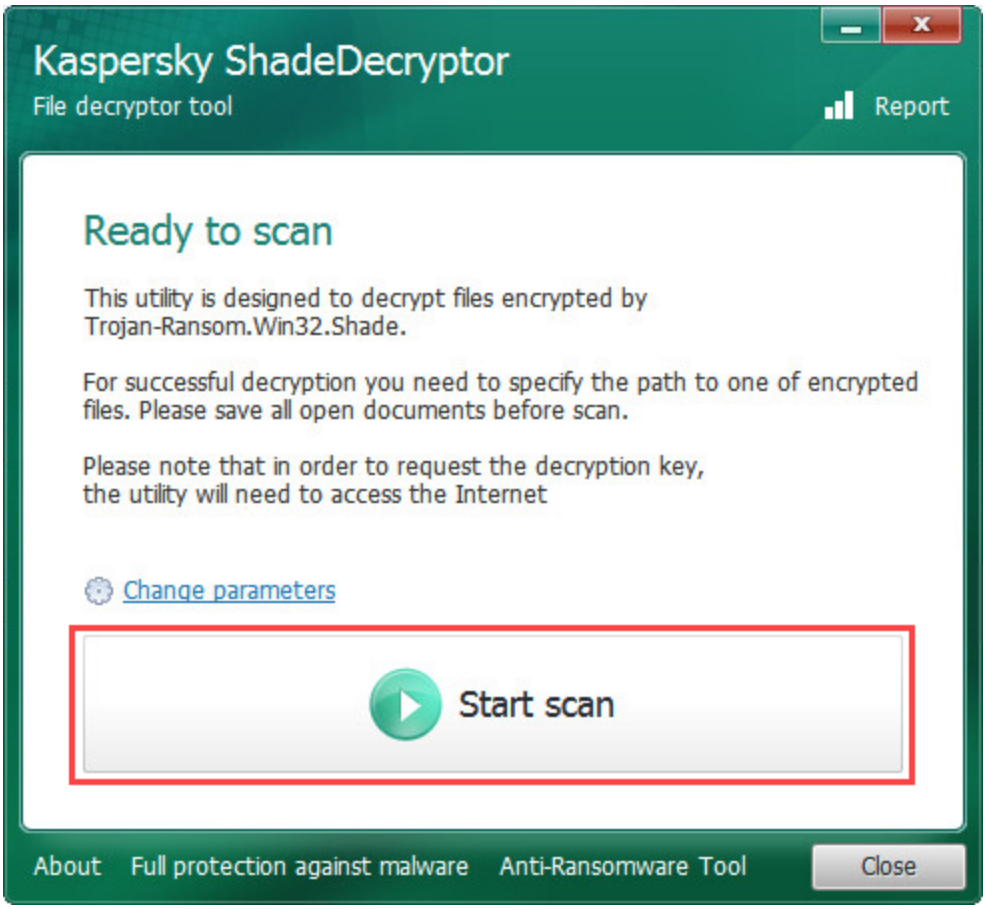
1. Read through the End User License Agreement carefully. Click **Accept** if you agree to the terms.
2. Click **Change parameters**.



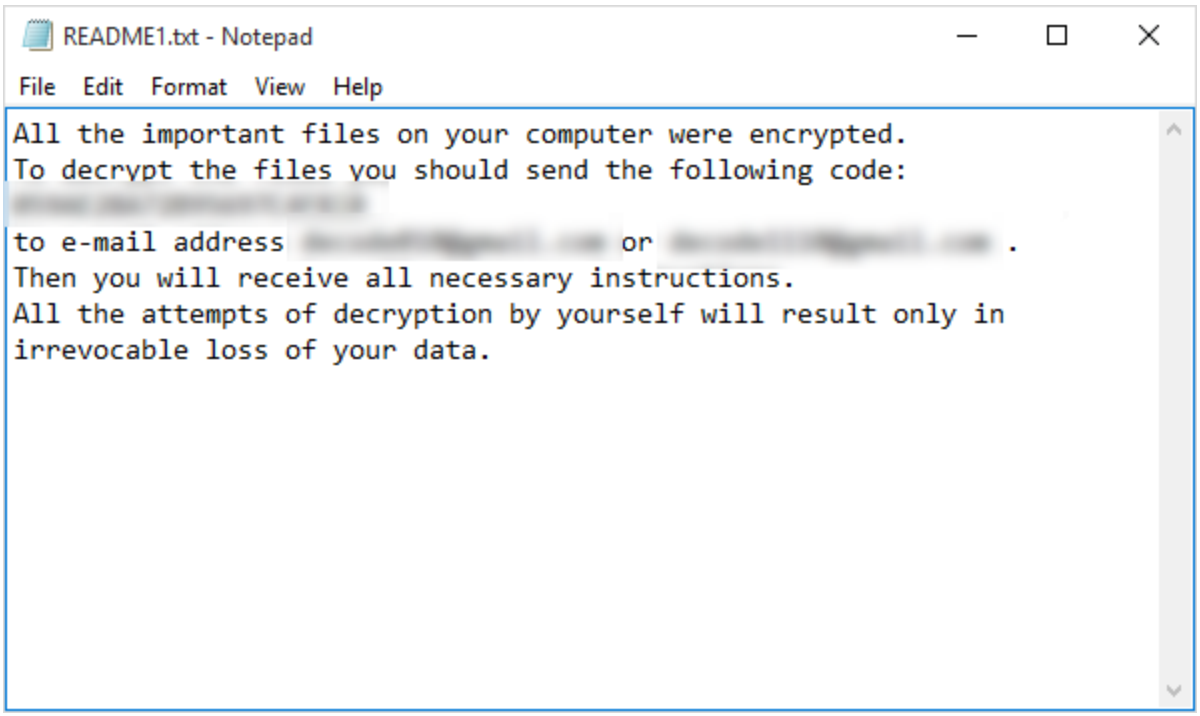
1. In the **Objects to scan** section, select the drives you want to scan. To delete encrypted files after they have been decrypted, select the checkbox in the **Additional options** section.
2. Click **OK**.



1. Click **Start scan**.



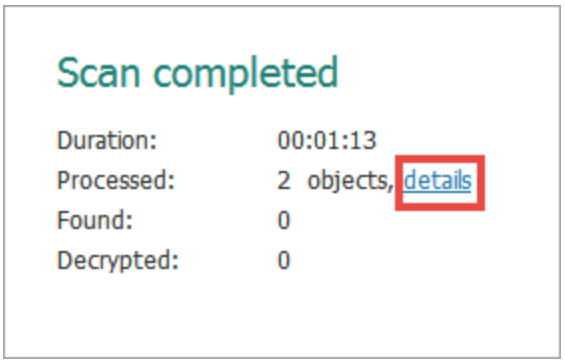
1. Specify the path to one of the encrypted files. If the tool is unable to detect the infection ID, it will request the path to the readme.txt file.



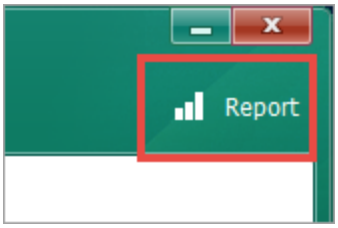
The files will be decrypted and their copies will be deleted.

To view:

Information about the scan, click **Details**.



A history of all scans performed previously, click **Report** in the top-right corner.



What to do if the tool did not help

If the error persists, contact Kaspersky technical support by choosing the topic and filling out the form.

For more information about the Kaspersky technologies for defending against file-encrypting and screen-locking malware, see TechnoWiki.
Back to "Recovery tools"