How-to guide.

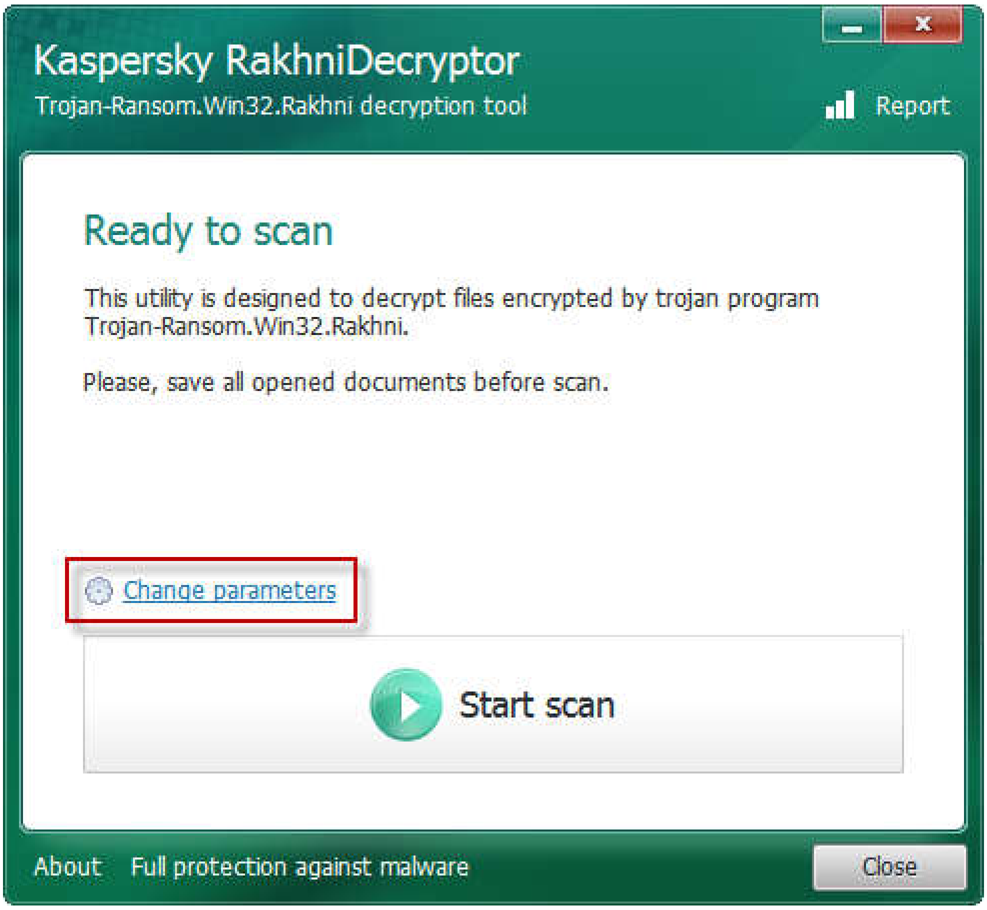
IMPORTANT! Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

Note: Rakhni creates the **exit.hhr.oshit** file that contains an encrypted password to user's files. If this file remains on the computer, it will make decryption with the **RakhniDecryptor** utility faster. If the file has been removed, it can be recovered with file recovery utilities. After the file is recovered, put it into **%APPDATA%** and run the scan with the utility once again. The **exit.hhr.oshit** file has the following path:

- **Windows XP:** C:\Documents and Settings\<username>\Application Data
- **Windows 7/8:** C:\Users\<username>\AppData\Roaming

To decrypt the files, do the following:

1. Download the **RakhniDecryptor.exe** file. The instructions on how to download a file are available below:
   - For **Windows 8** users
   - For **Windows 7** users
   - For **Windows Vista** users
2. Run the **RakhniDecryptor.exe** file on the infected computer.
3. In the **Kaspersky RakhniDecryptor** window click the **Change parameters** link.



Kaspersky RakhniDecryptor

Trojan-Ransom.Win32.Rakhni decryption tool

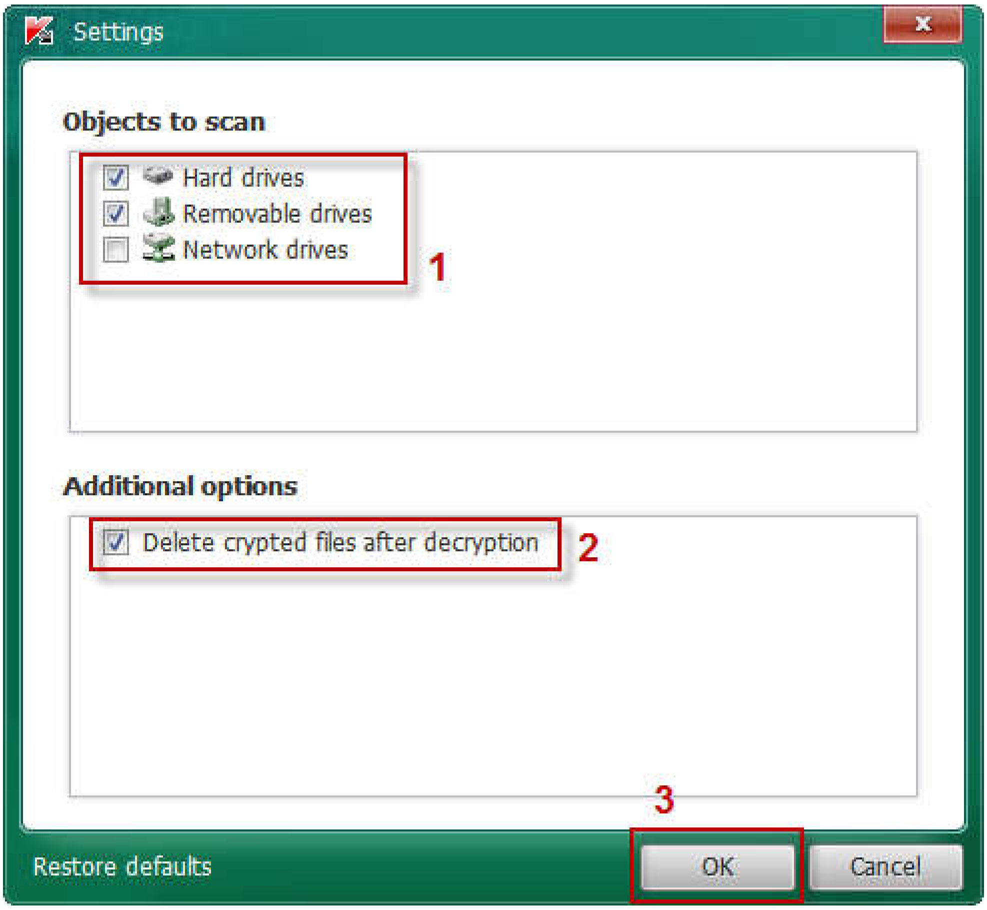
Ready to scan

This utility is designed to decrypt files encrypted by trojan program Trojan-Ransom.Win32.Rakhni.

Please, save all opened documents before scan.

4. In the **Settings** window select the objects to scan (**hard drives** / **removable drives** / **network drives**).

5. Select the checkbox **Delete crypted files after decryption** (the utility will be deleting copies of original files with the **.locked**, **.kraken** and **.darkness** extensions).
6. Click **OK**.



Settings

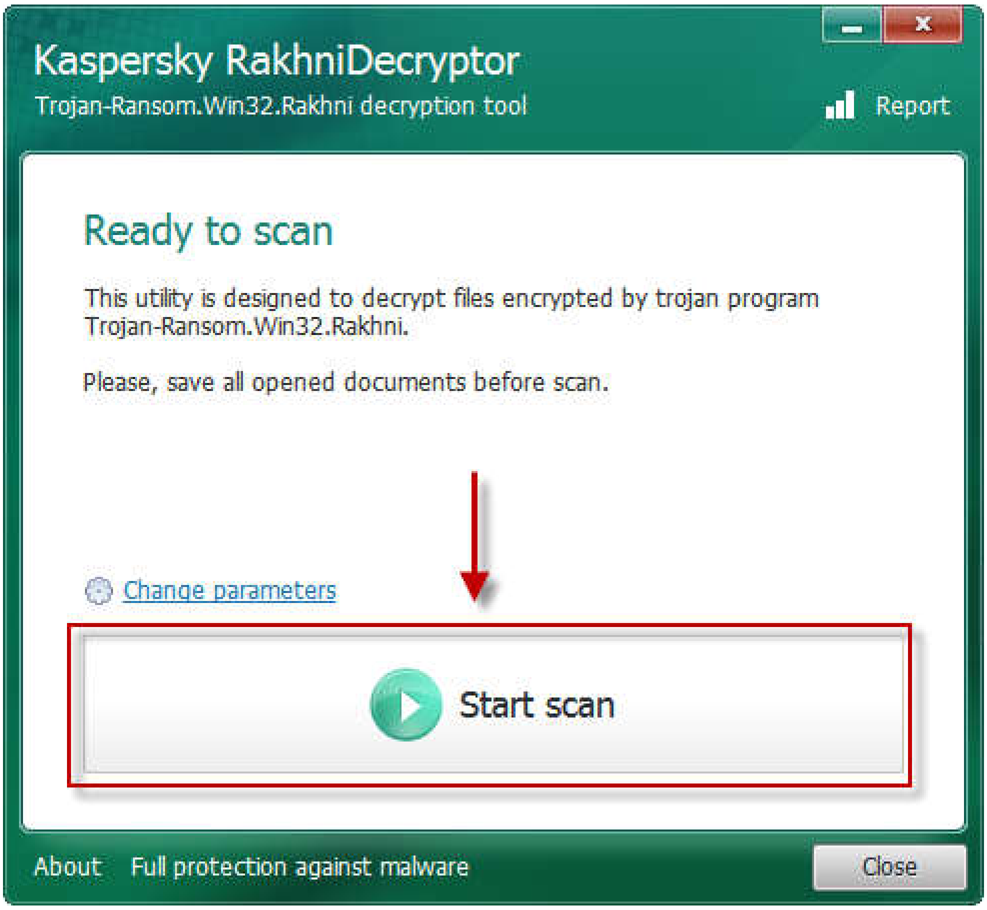
Objects to scan

☑ Hard drives
☑ Removable drives
☐ Network drives

Additional options

☑ Delete crypted files after decryption

7. In the **Kaspersky RakhniDecryptor**, click the **Start scan** button.



Kaspersky RakhniDecryptor

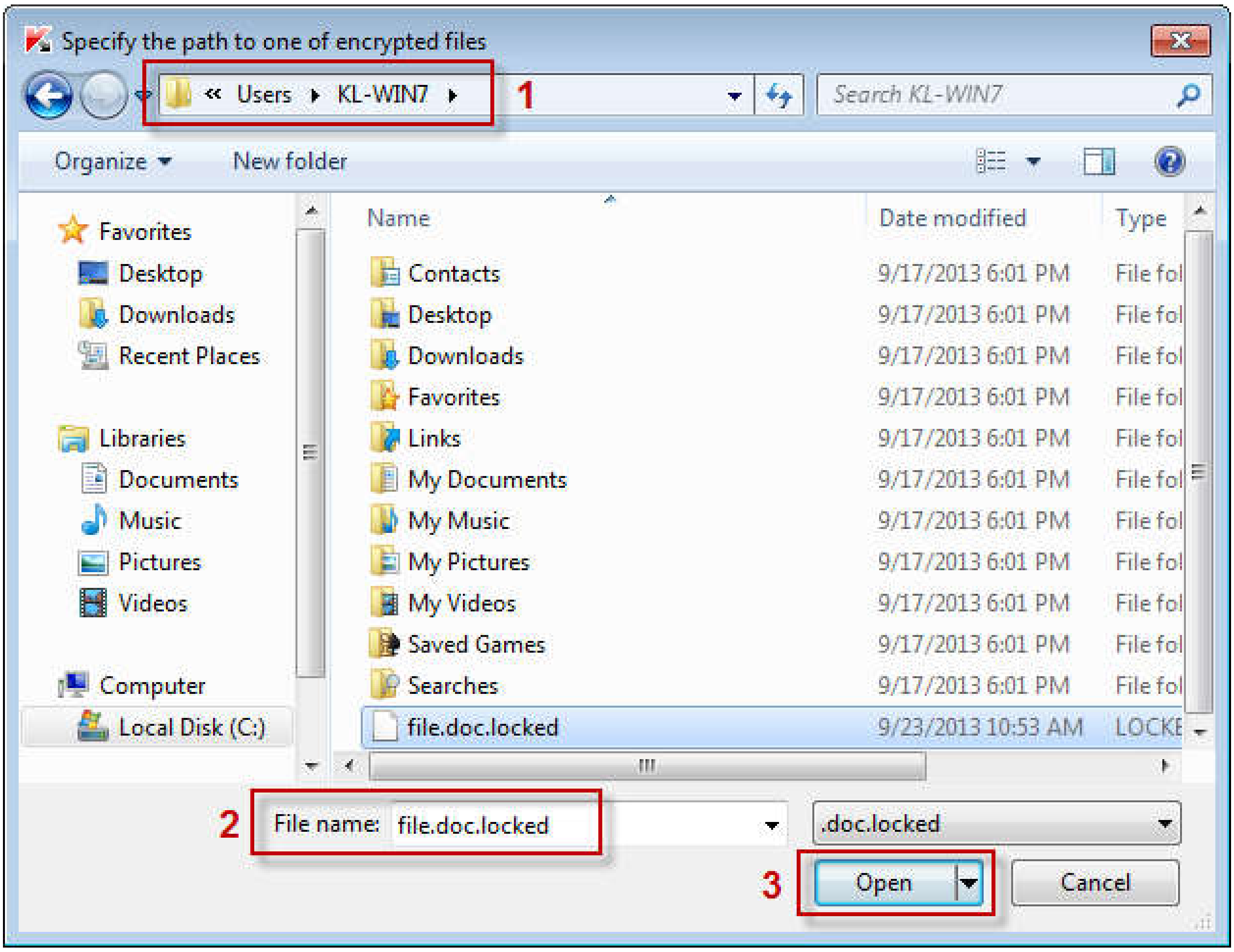
Trojan-Ransom.Win32.Rakhni decryption tool

Ready to scan

This utility is designed to decrypt files encrypted by trojan program Trojan-Ransom.Win32.Rakhni.

Please, save all opened documents before scan.

8. In the **Specify the path to one of encrypted files**, select the file you need to restore and click **Open**.



Specify the path to one of encrypted files

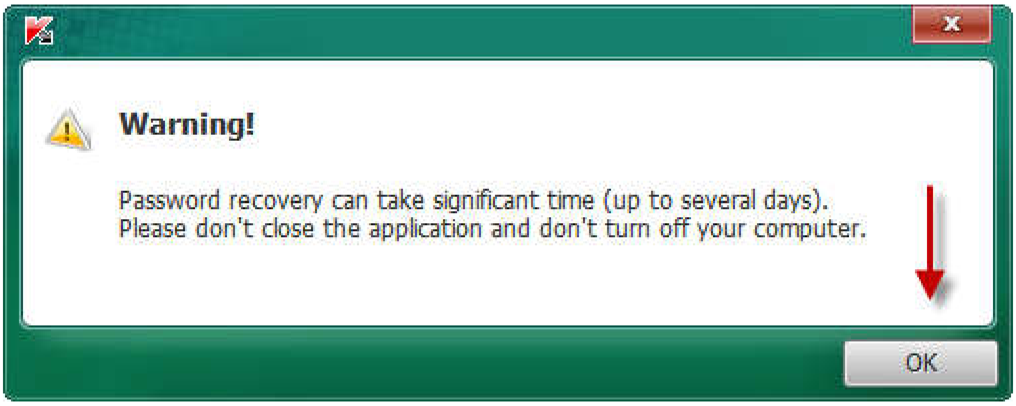
« Users ▸ KL-WIN7 ▸

Name	Date modified	Type
Contacts	9/17/2013 6:01 PM	File fol
Desktop	9/17/2013 6:01 PM	File fol
Downloads	9/17/2013 6:01 PM	File fol
Favorites	9/17/2013 6:01 PM	File fol
Links	9/17/2013 6:01 PM	File fol
My Documents	9/17/2013 6:01 PM	File fol
My Music	9/17/2013 6:01 PM	File fol
My Pictures	9/17/2013 6:01 PM	File fol
My Videos	9/17/2013 6:01 PM	File fol
Saved Games	9/17/2013 6:01 PM	File fol
Searches	9/17/2013 6:01 PM	File fol
file.doc.locked	9/23/2013 10:53 AM	LOCKE

File name: file.doc.locked

.doc.locked

9. The utility will start recovering the password. Please mind the **Warning!** window message.



Warning!

Password recovery can take significant time (up to several days).
Please don't close the application and don't turn off your computer.

10. Wait until the utility is done with decrypting the file (do not exit the program or shut down the computer).