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.

- 1. Open and extract the **<u>WildfireDecryptor.zip</u>** archive, using an archiver (for example, **7zip**).
- 2. Double click the left mouse button at **WildfireDecryptor.exe**.



- 3. In the **User Account Control** (**UAC**) window, enter the password with the administrator permissions and click **OK**.
- 4. In the **Kaspersky WildfireDecryptor** window, specify the folders with the files to scan: click the **Change parameters** link.



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

🔀 Settings		x
Objects to scan		
Termovable drives		
Additional options		
Delete crypted files after decryption		
Restore defaults	ОК	Cancel

7. In the Kaspersky WildfireDecryptor window, click Start scan.



- 8. In the **Specify the path to one of encrypted files** select a folder for the file. Click **Open**.
- 9. To view information about the scan task, click **Details.**
- 10. To view the history of performed scans, in the upper right corner of the **Kaspersky WildfireDecryptor** window, click **Report**.

Caspersky W le decryptor tool	/ildfireDecryptor	_ Keport
Scan com	pleted	
Duration:	01:32:30	
Processed:	0 objects, details	
Found:	0	
Decrypted:	0	
🛞 <u>Change par</u>	ameters	
8	Start scan	
out Full protect	ion against malware	Close