

How do I clean a Trustezeb.A or Matsnu infection using the Trustezeb.A cleaner?

[Click here to download the most recent version of this document](#)

Note: We do not recommend running the decryptor on files located on USB flash drives.

1. Download the [ESETTrustezebAdecoder.exe tool](#) and save the file to your Desktop.
2. Double-click ESETTrustezebAdecoder.exe on your Desktop to run the cleaner.
3. Click the **Decode** button.
4. When prompted, select your **Desktop** folder to decrypt all encrypted files in your Desktop and Desktop's subdirectories. To decrypt a different folder, for example, all in the C drive, select **C:**.

Decode using clean file

If you receive the message *"Can't find window's original wallpaper file. Try to decode with clean file."*:

1. Click **Decode using clean file**.
2. When prompted, select a clean file and click **OK**.
3. When prompted, select an encrypted version of the same file and click **OK**.
For example, a document or photo (step 2) in your backup or sent emails which was encrypted by Trustezeb.A. Decryptor requires you to select both versions of the file in order to decrypt all other files correctly.
4. When prompted, select a directory to decrypt all its files and subdirectories and click **OK**.
5. The FilecoderAR cleaner tool will run. If an infection is discovered, TrustezebA cleaner will decode the file and display the *"Decoded and written: x file(s)"* message.

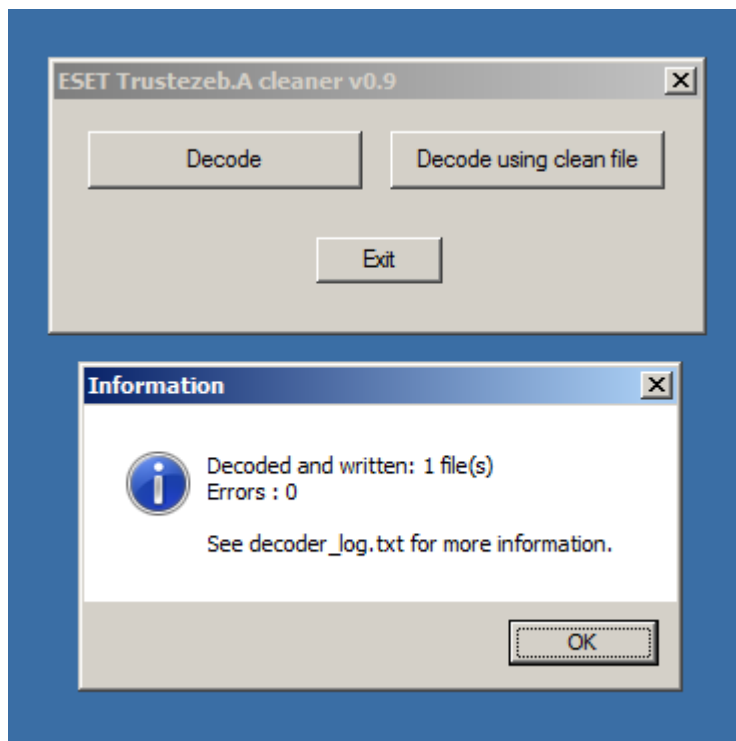


Figure 1 // ESET Trustezeb.A cleaner

Related articles:

- [Best practices to protect against Filecoder \(ransomware\) malware](#)
- [Minimize the risk of a malware attack](#)
- [Stand-alone malware removal tools](#)