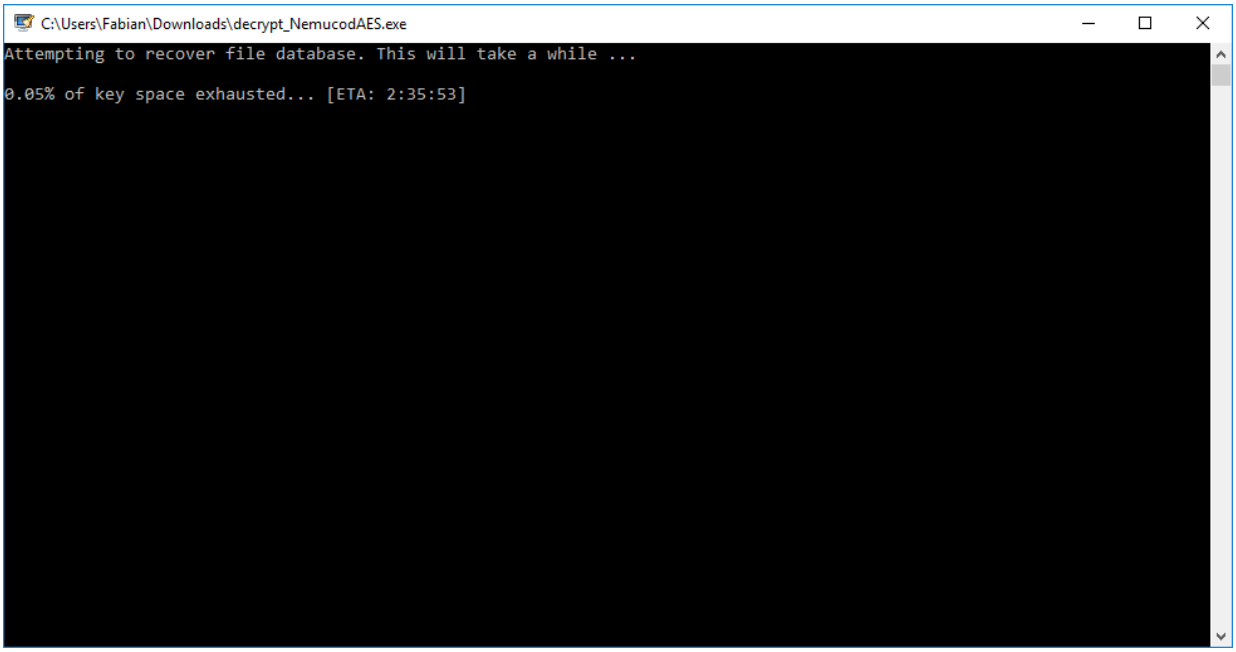
# How to use the Emsisoft Decrypter for NemucodAES

**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. If your system was compromised through the Windows Remote Desktop feature, we also recommend changing all passwords of all users that are allowed to login remotely and check the local user accounts for additional accounts the attacker might have added.**

The decrypter requires access to a database file located inside your %TEMP% directory in order to restore your files. It is therefore important to pause any system optimisers and cleaner software you have installed to avoid them removing said database file. If the database file is removed, recovery is unfortunately impossible even by paying the ransom.

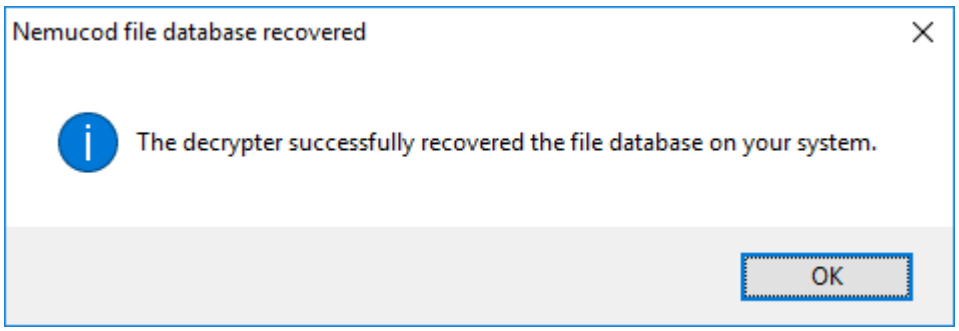
## How to decrypt your files

1. Download the decrypter from the same site that provided this "How To" document.
2. Run the decrypter executable. It will start looking for the NemucodAES file database on your system and attempt to decrypt the data it contains.

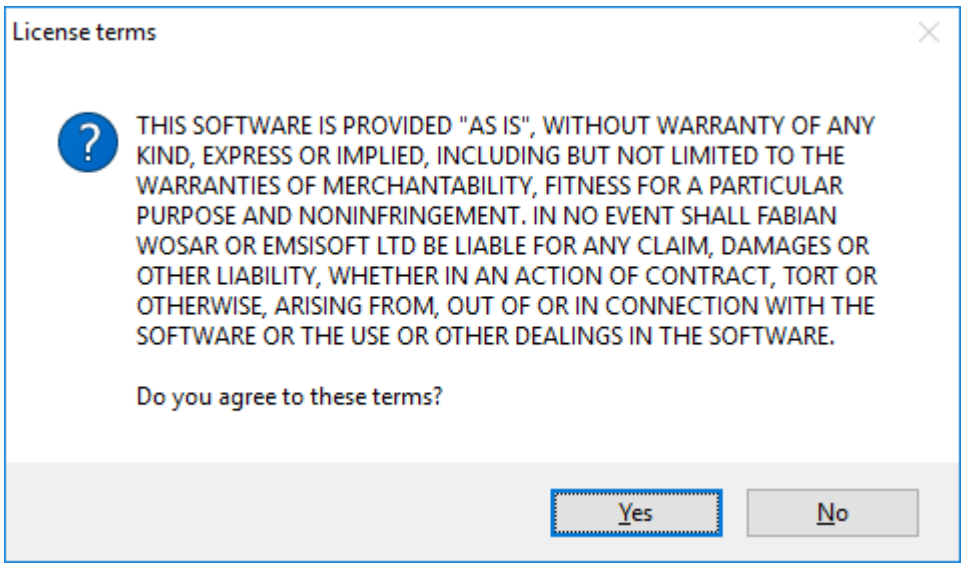


Depending on the speed of your system, this process can take a significant amount of time.

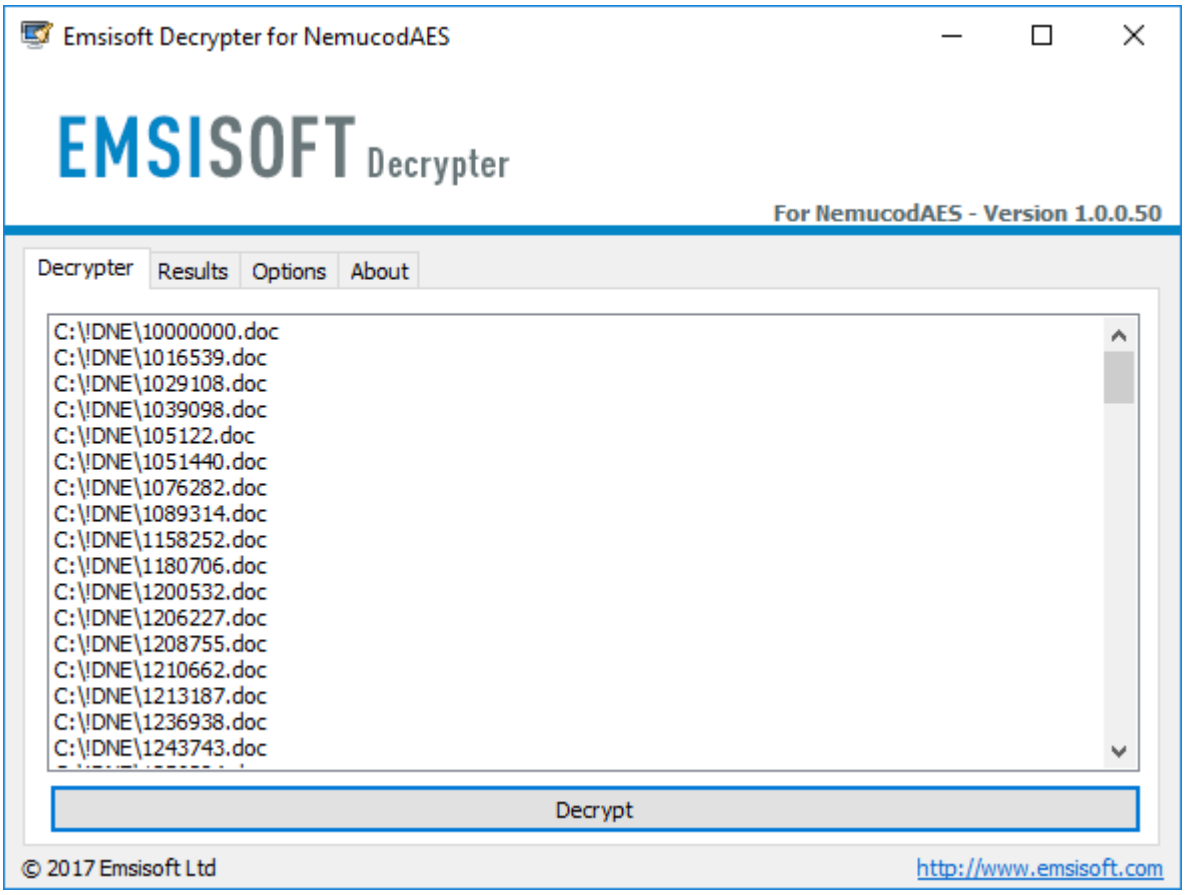
3. The decrypter will display a message as soon as the reconstruction has finished:




4. The license terms will show up next, which you have to agree to by clicking the "Yes" button:



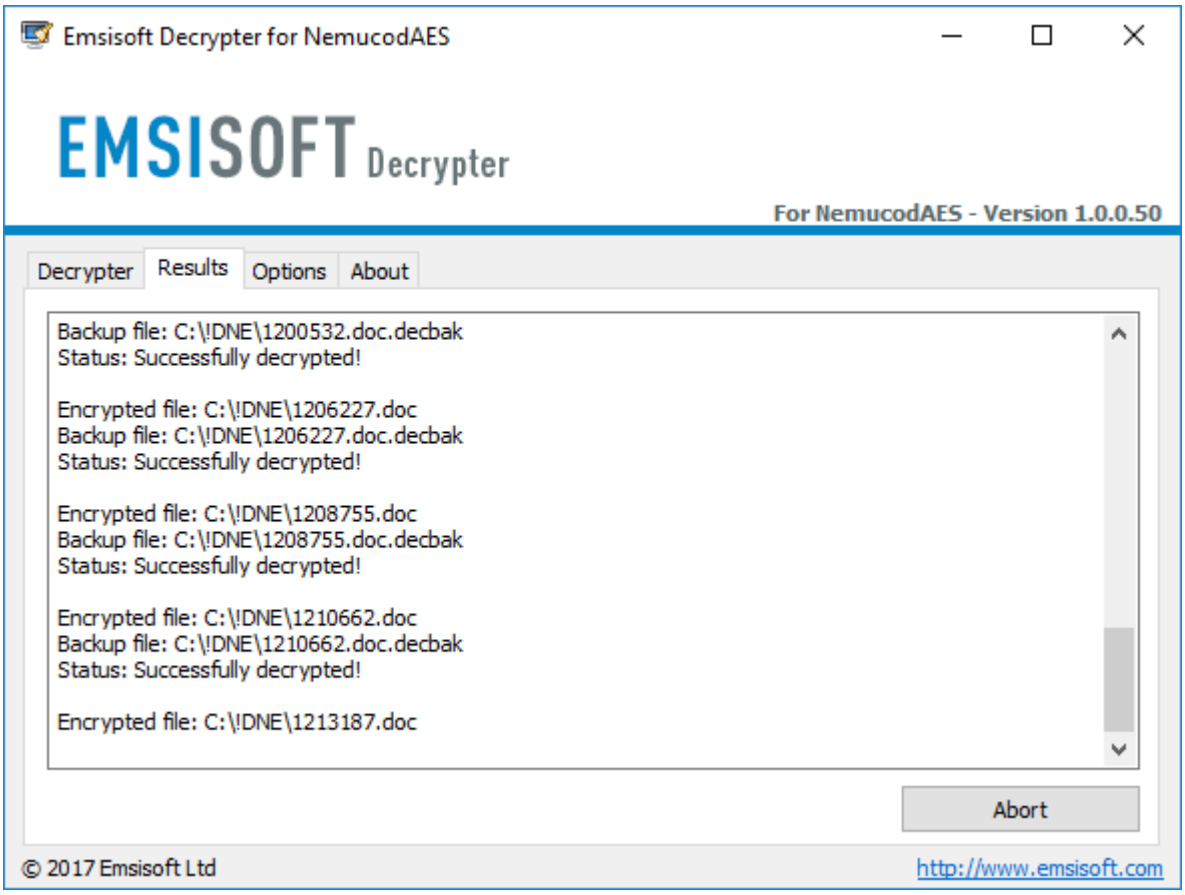

5. Once the license terms are accepted, the primary decrypter user interface opens:



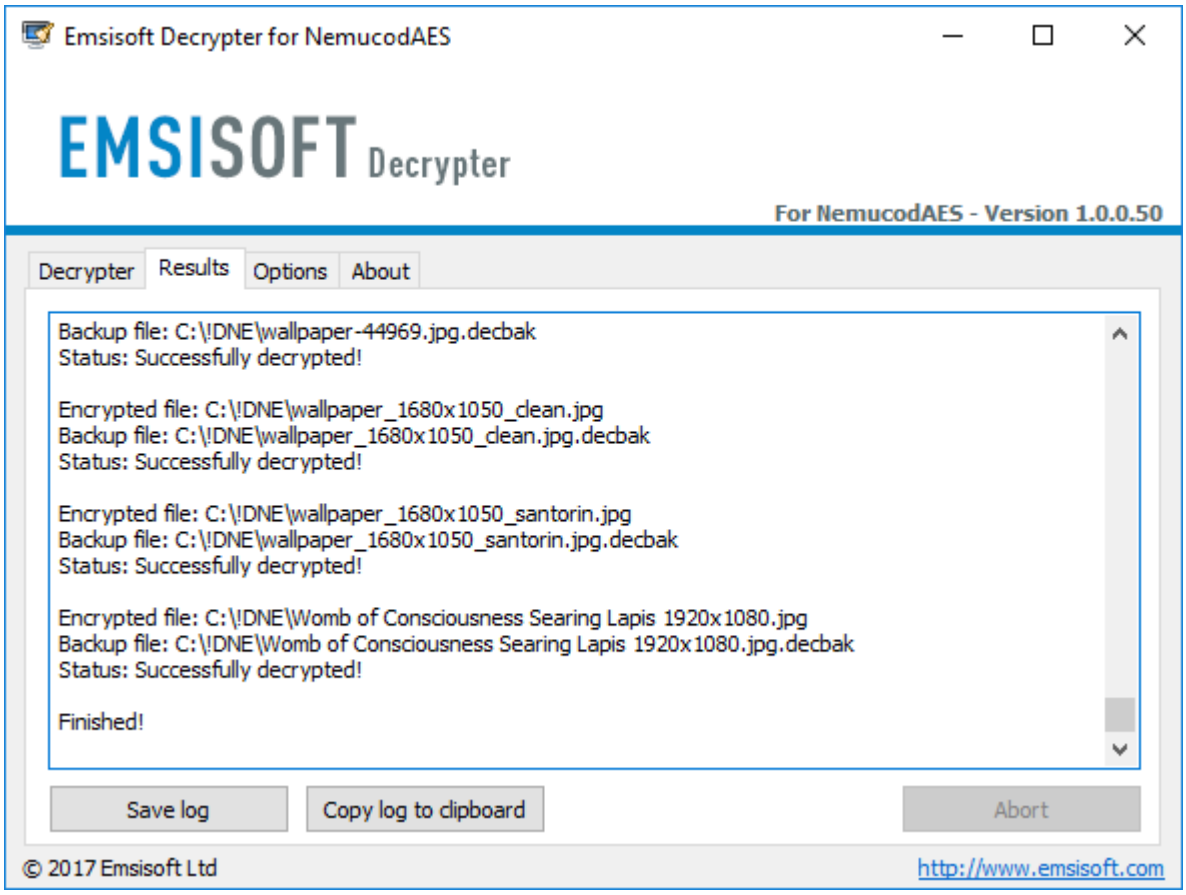

6. By default, the decrypter will pre-populate the list of files to decrypt using the information from the restored file database.

7. Decrypters typically offer various options depending on the particular malware family. The available options are located in the Options tab and can be enabled or disabled there. You can find a detailed list of the available Options below.

8. Click "Decrypt" to start the decryption process. The screen will switch to a status view, informing you about the current process and decryption status of your files:




9. The decrypter will inform you once the decryption process is finished:




If you require the report for your personal records, you can save it by clicking the "Save log" button. You can also copy it straight to your clipboard to paste it into emails or forum posts if you are asked to.

# Available decrypter options

The decrypter currently implements the following options:

- **Backup old encrypted files**
  It is unfortunately not possible for the decrypter to know for sure that a file has been decrypted correctly. If this option is enabled, the decrypter will therefore keep the encrypted version of the file around. If something goes wrong, the user can always restore the encrypted state of the system to allow for an additional recovery attempt.