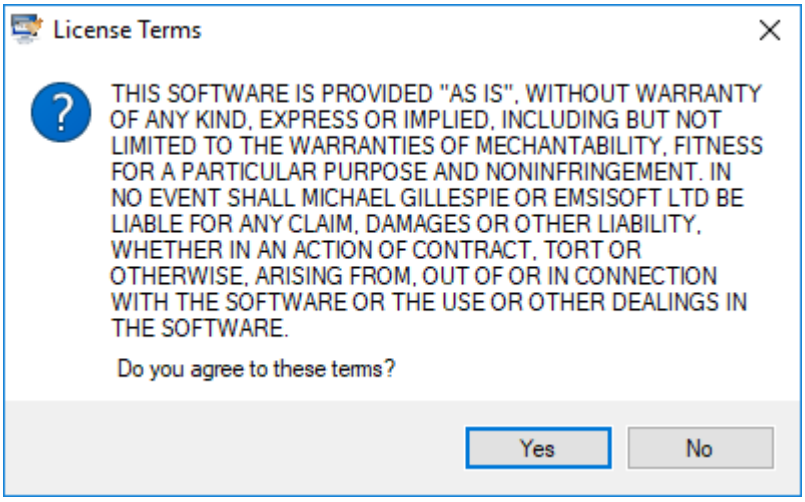
How to use the Emsisoft Decrypter for Aurora

IMPORTANT! Make sure you remove the malware from your system first, otherwise, it will repeatedly lock your system or encrypt files. If your current antivirus solution fails to delete the malware, it can be removed using the free trial version of Emsisoft Anti-Malware. 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.

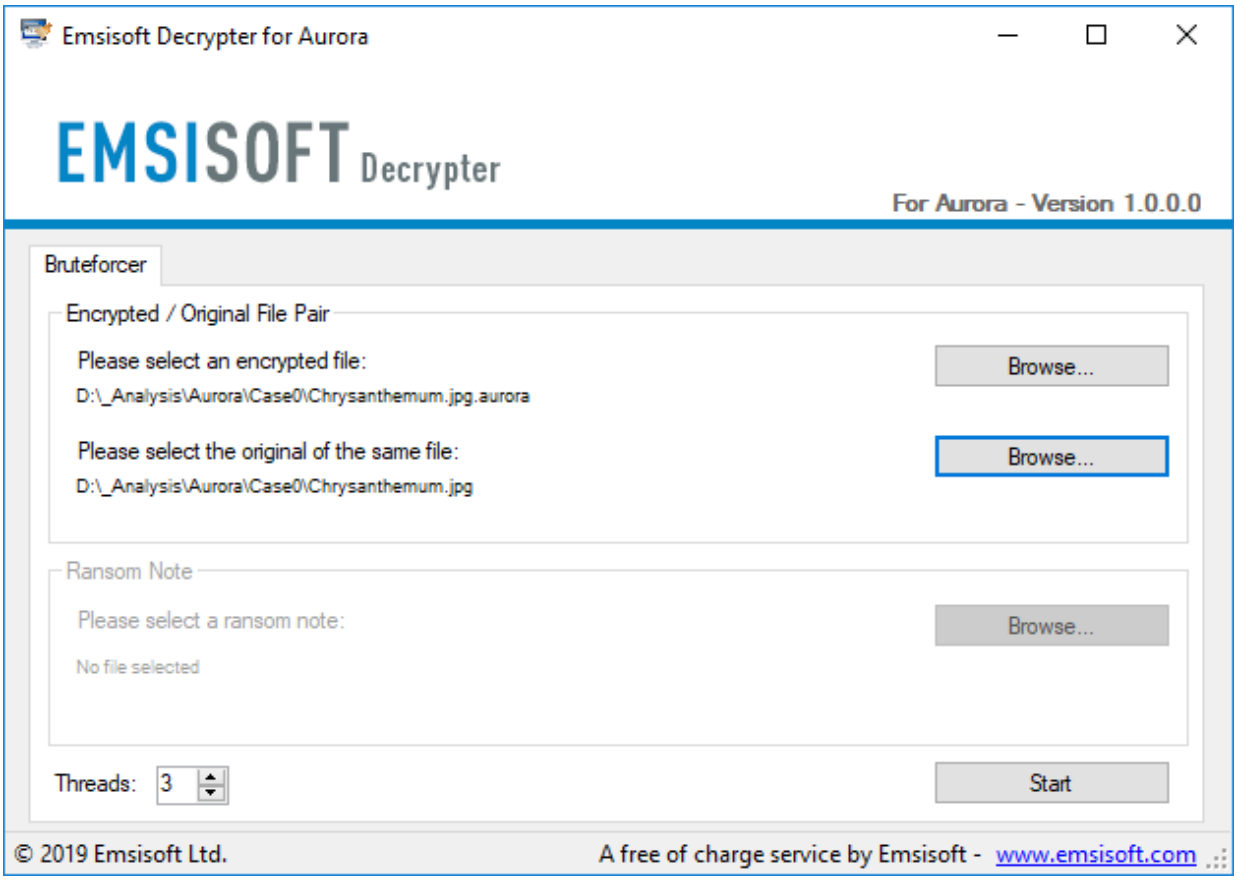
The decrypter requires access to a file pair consisting of one encrypted file and the original, unencrypted version of the encrypted file to reconstruct the encryption keys needed to decrypt the rest of your data. Please do not change the file names of the original and encrypted files, as the decrypter may perform file name comparisons to determine the correct file extension used for encrypted files on your system.

How to decrypt your files

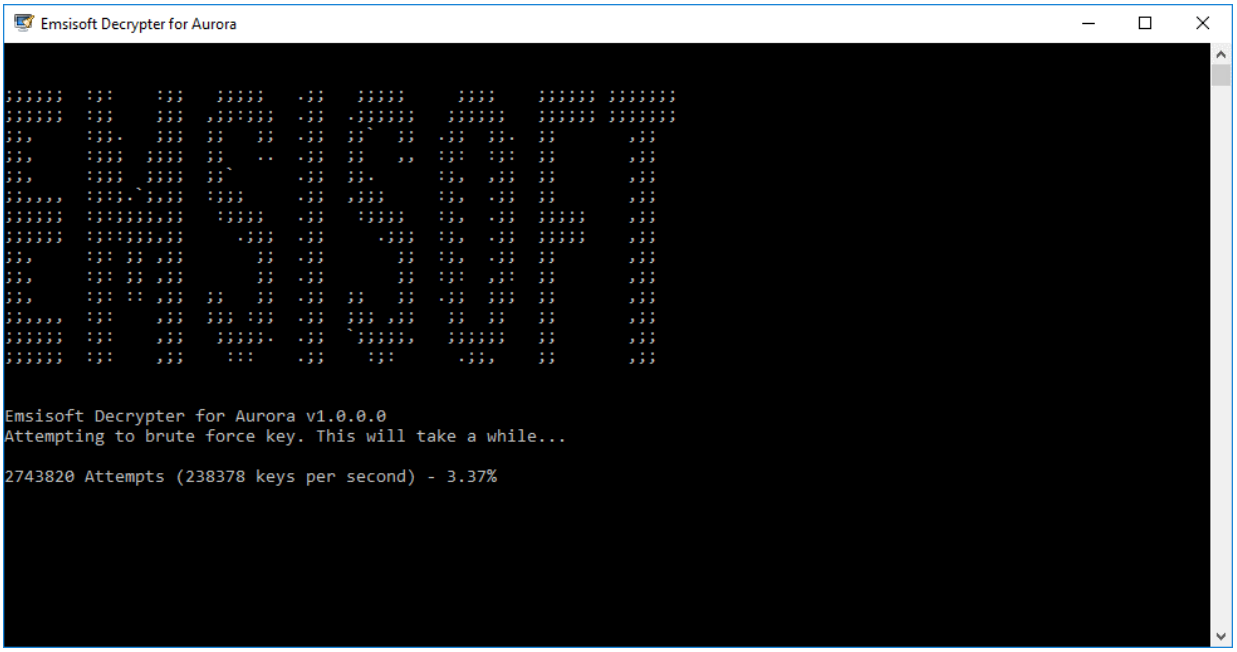
1. Download the decrypter from the same site that provided this "How To" document.
2. Run the decrypter as an administrator. The license terms will show up next, which you have to agree to by clicking the "Yes" button:



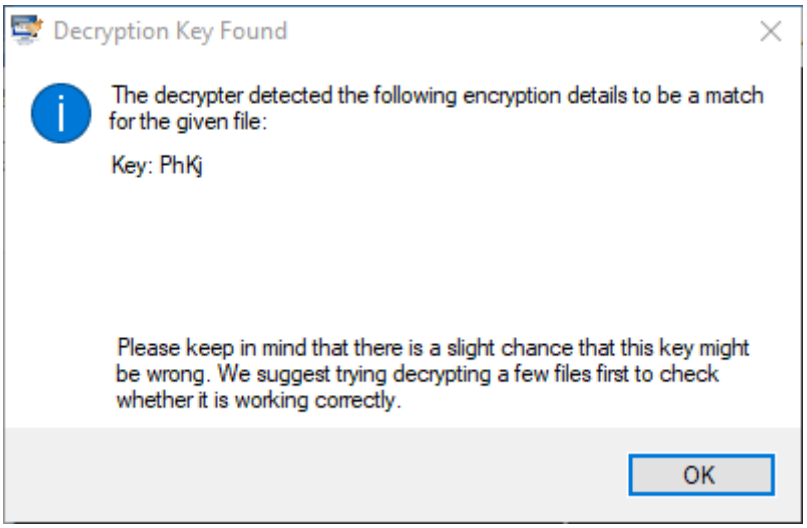
3. After accepting the terms, select your file pair using the "Browse" buttons. Optionally, the number of CPU threads to use may be changed; the default is one less than those available. Then, click the "Start" button.



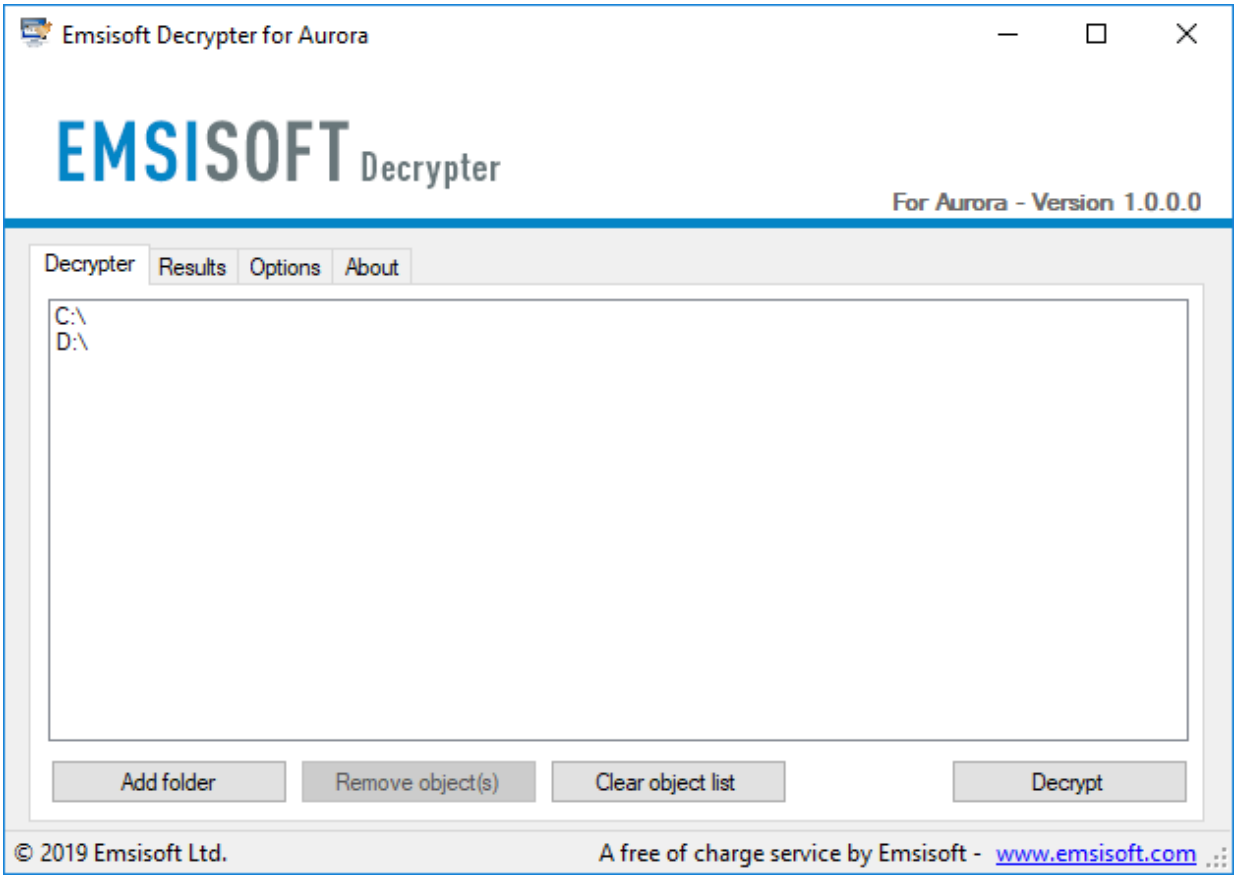
4. The decrypter will start to reconstruct the required encryption parameters. Depending on the ransomware and your computer, this process can take a significant amount of time.



5. The decrypter will display the reconstructed encryption details once the recovery process has finished. The display is purely informational to confirm that the required encryption details have been found:



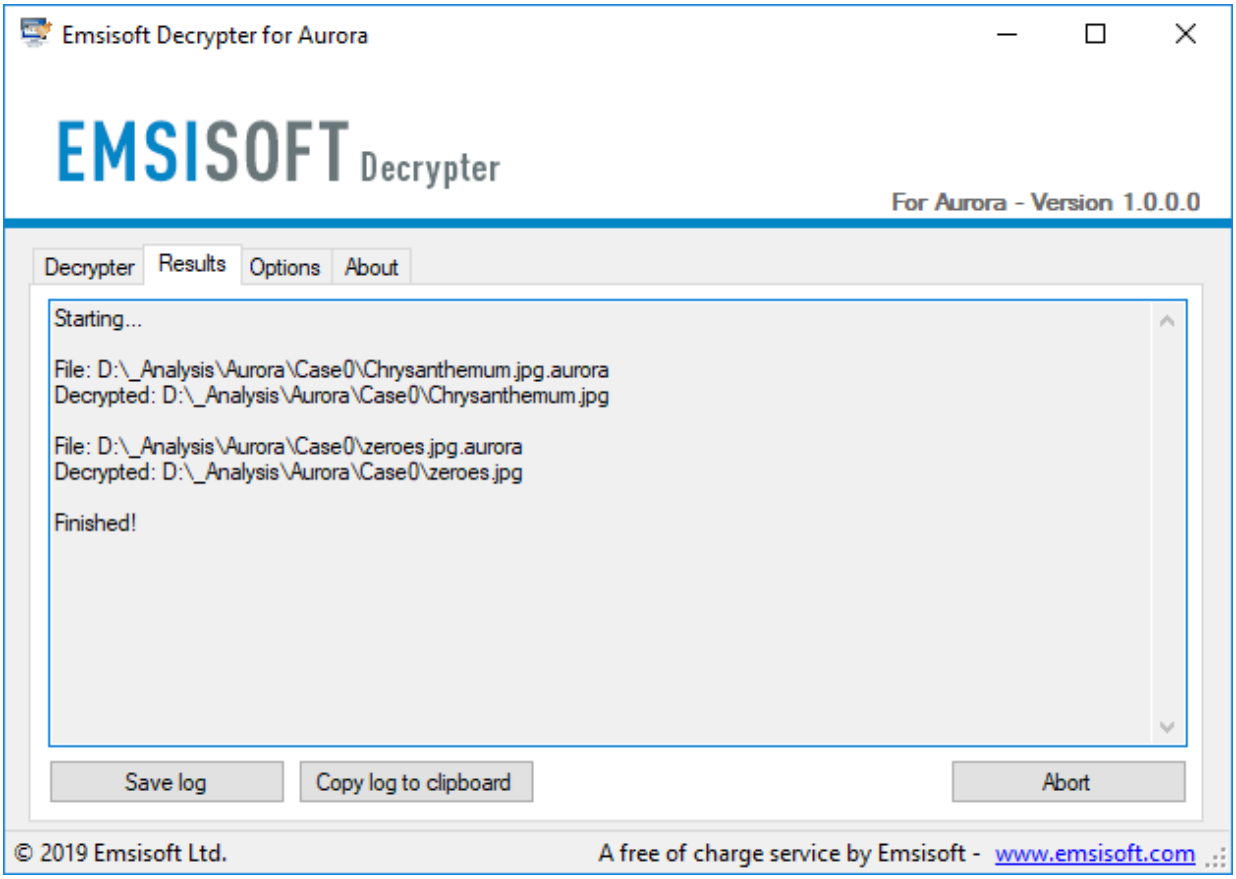
6. Once a key is found, click "OK" to open the primary decrypter user interface:



7. By default, the decrypter will pre-populate the locations to decrypt with the currently connected drives and network drives. Additional locations can be added using the "Add" button.

8. 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.

9. After you have added all the locations you want to decrypt to the list, click the "Decrypt" button 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:



10. 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:

- **Keep encrypted files**
  Since the ransomware does not save any information about the unencrypted files, the decrypter can't guarantee that the decrypted data is identical to the one that was previously encrypted. Therefore, the decrypter by default will opt on the side of caution and not remove any encrypted files after they have been decrypted. If you want the decrypter to remove any encrypted files after they have been processed, you can disable this option. Doing so may be necessary if your disk space is limited.