How to use the Emsisoft Decryptor for Muhstik

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.

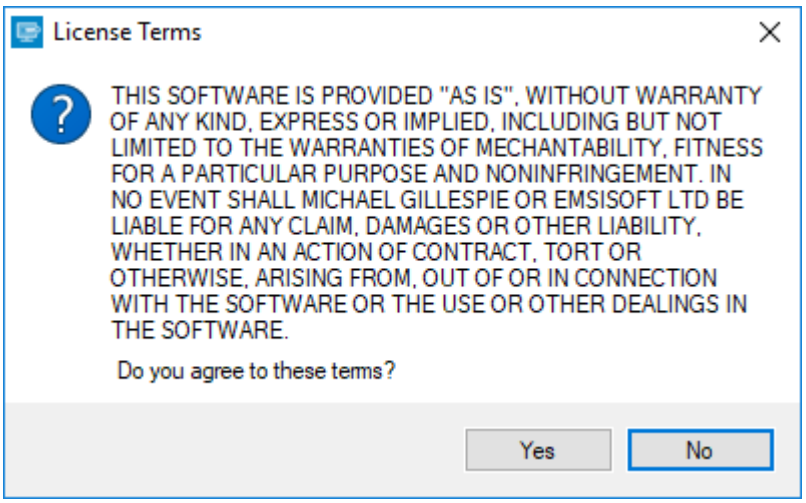
This particular malware spreads via open QNAP shares on the internet. Make sure your network disks are not exposed to the internet, and are password-protected.

Due to how Windows isolates the administrator session by default, your network drive may not be able to be selected to decrypt. You may work around this issue with the registry key "EnableLinkedConnections" as mentioned in this Microsoft article: https://support.microsoft.com/en-us/help/3035277/

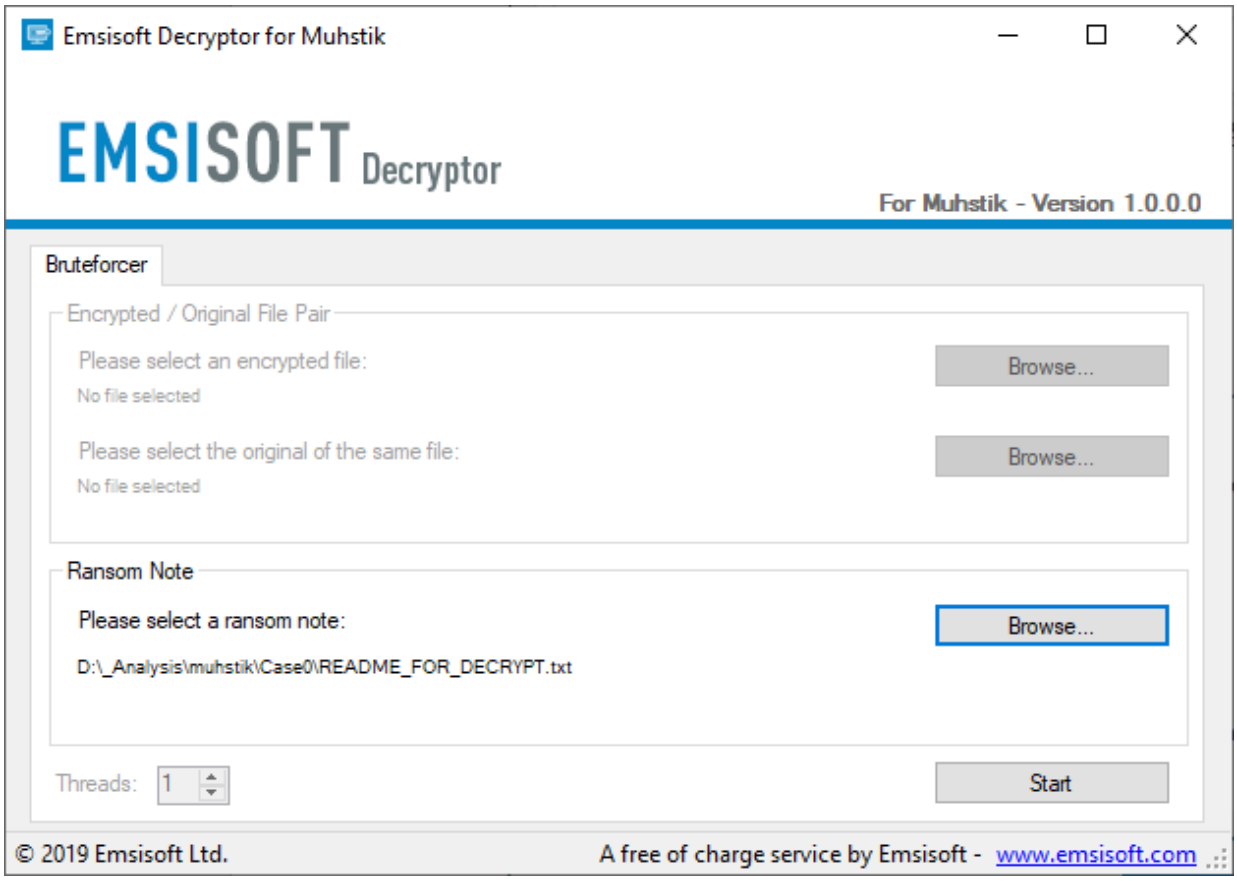
The decryptor requires access to a ransom note left by the malware, typically called "README_FOR_DECRYPT.txt". An internet connection is also required.

How to decrypt your files

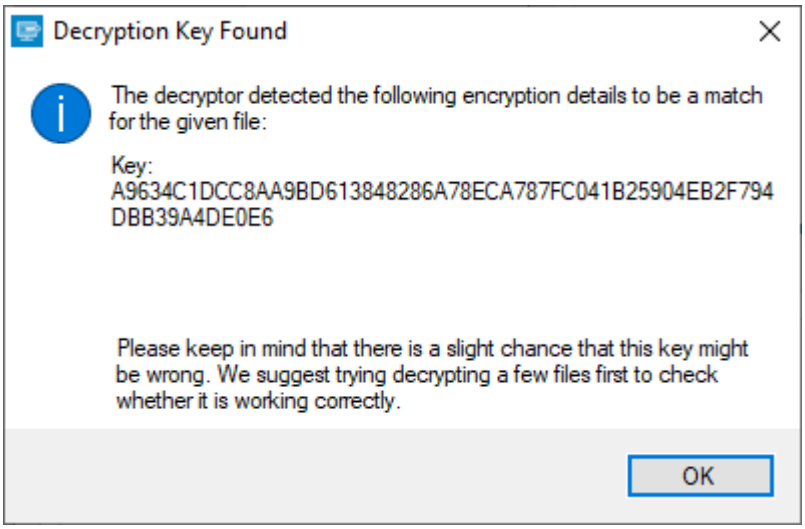
1. Download the decryptor from the same site that provided this "How To" document.
2. Run the decryptor as an administrator. The license terms will show up, which you must agree to by clicking the "Yes" button:



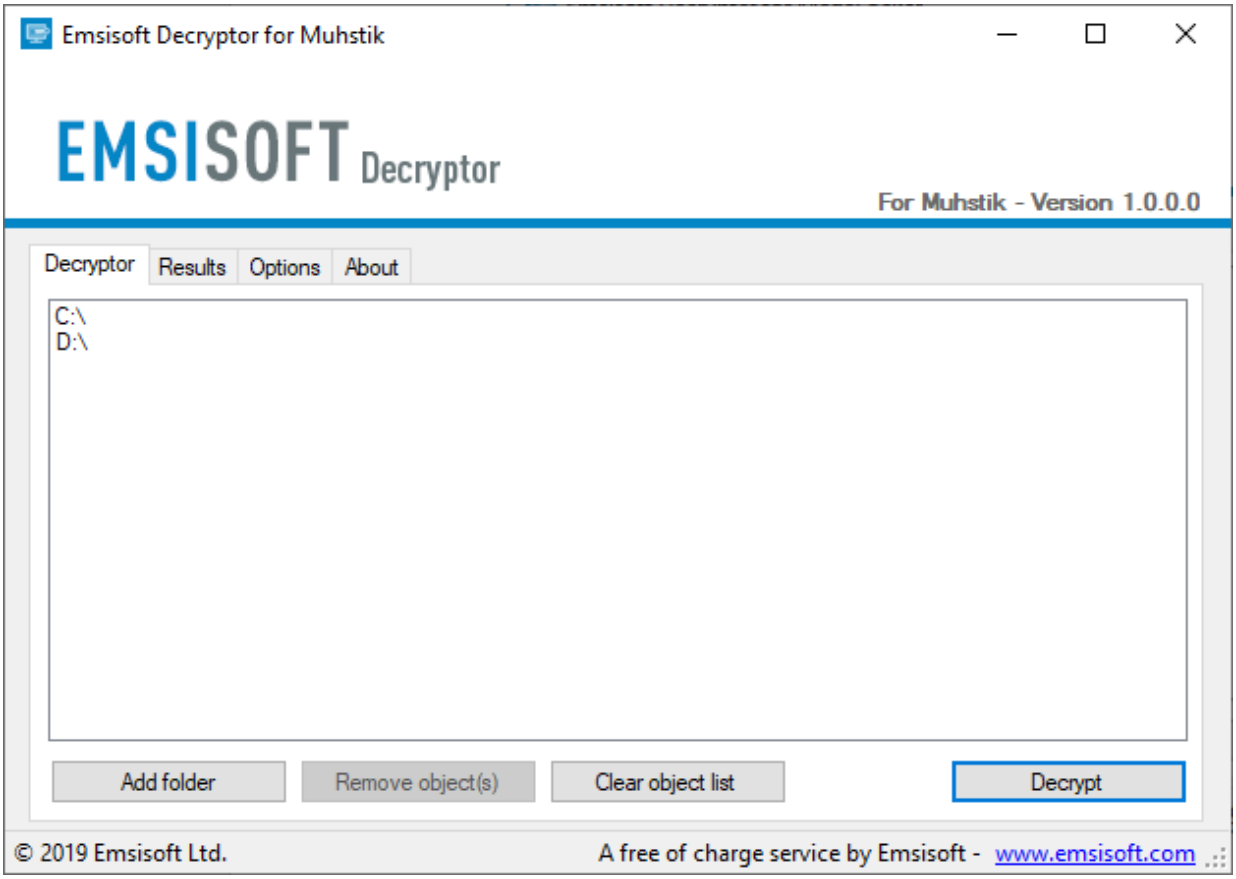
3. After accepting the terms, select a ransom note by clicking the "Browse" button. Then click the "Start" button.



4. The decryptor 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:



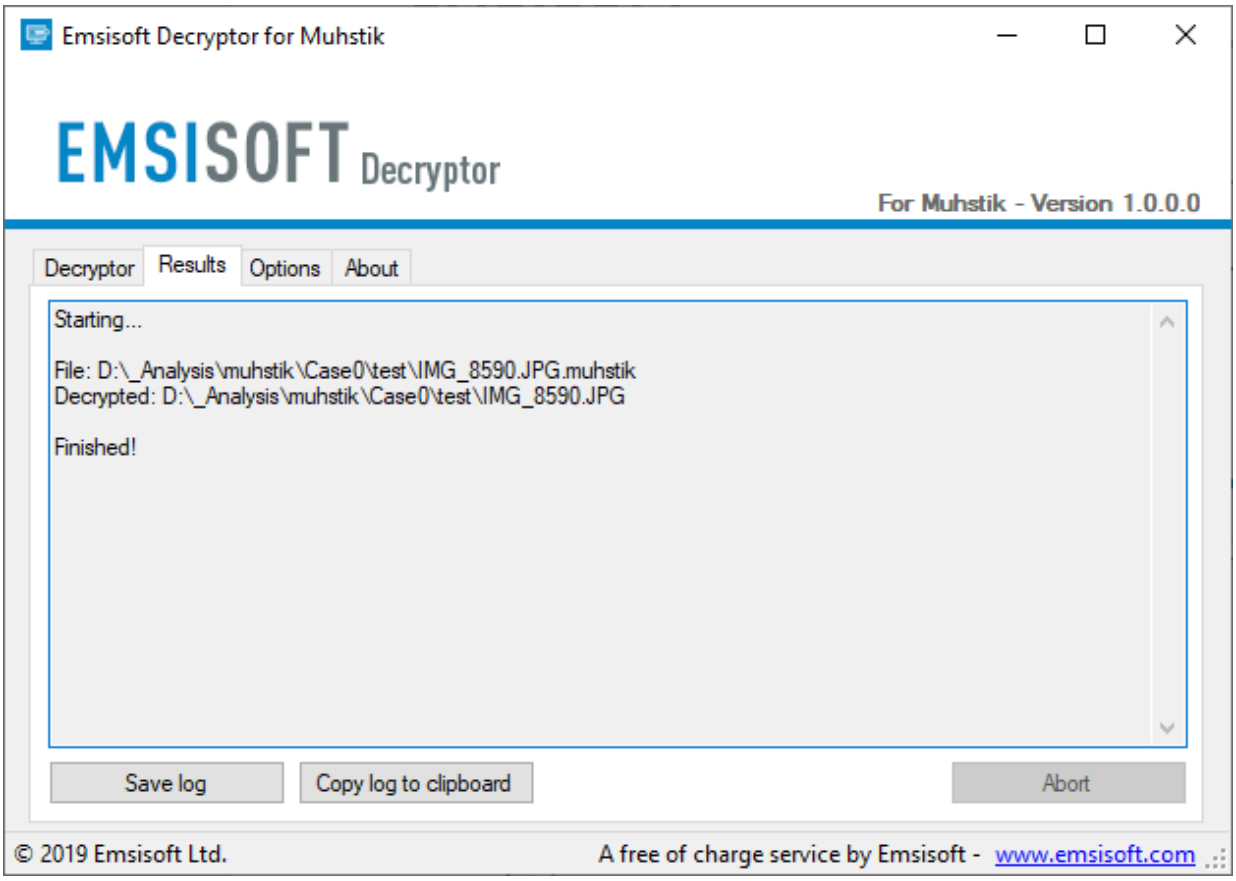
5. Once a key is found, click "OK" to open the primary decryptor user interface:



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

7. Decryptors 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. 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:



9. The decryptor 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 decryptor options

The decryptor currently implements the following options:

- **Keep encrypted files**
  Since the ransomware does not save any information about the unencrypted files, the decryptor can't guarantee that the decrypted data is identical to the one that was previously encrypted. Therefore, the decryptor by default will opt on the side of caution and not remove any encrypted files after they have been decrypted. If you want the decryptor 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.