How to use the Emsisoft Decrypter for MRCR

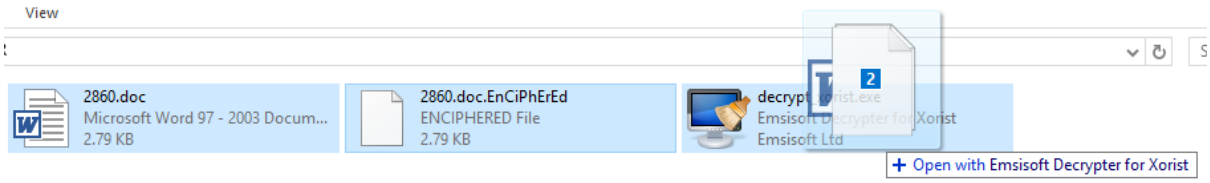
IMPORTANT! Make sure you remove the malware from your system first. Otherwise, it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you. If your system was compromised through the Windows Remote Desktop feature, we also recommend changing all passwords 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 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 file, as the decrypter may perform file name comparisons to determine the correct file extension used for encrypted files on your system.

Due to the mathematical properties of the custom encryption algorithm utilised by the ransomware, it is not possible to determine the correct key based on just one file pair alone in many cases as multiple keys will match the same file pair. Instead, the decrypter will come up with a list of possible keys. You will have to test these keys on your files manually to determine which of the possible key candidates is the correct one. The best way to do that is to gather a couple of encrypted files, then try to decrypt them using the decrypter and check the results. The key used by the decrypter can be switched in the options tab.

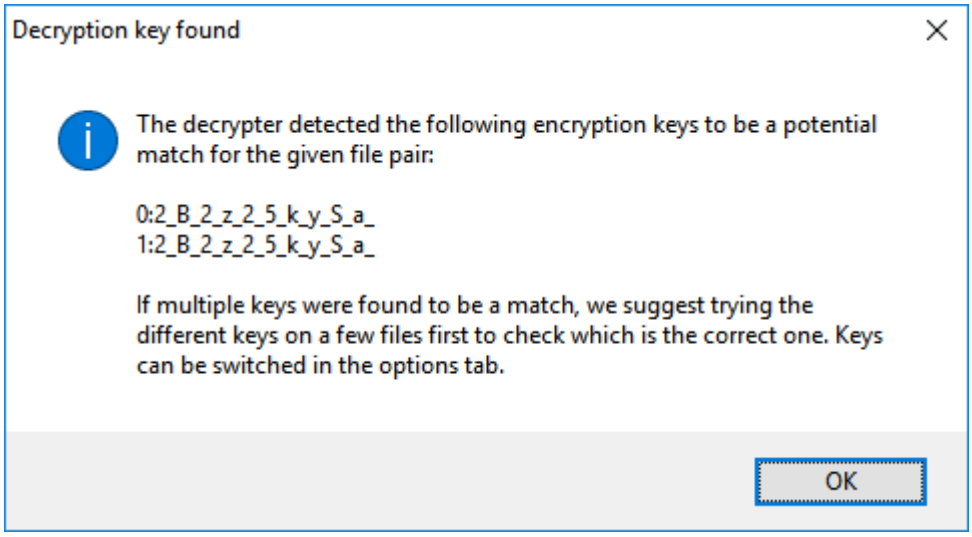
How to decrypt your files

1. Download the decrypter from the same site that provided this "How To" document.
2. Once downloaded, select your file pair, and drag and drop it with your mouse onto the decrypter executable:

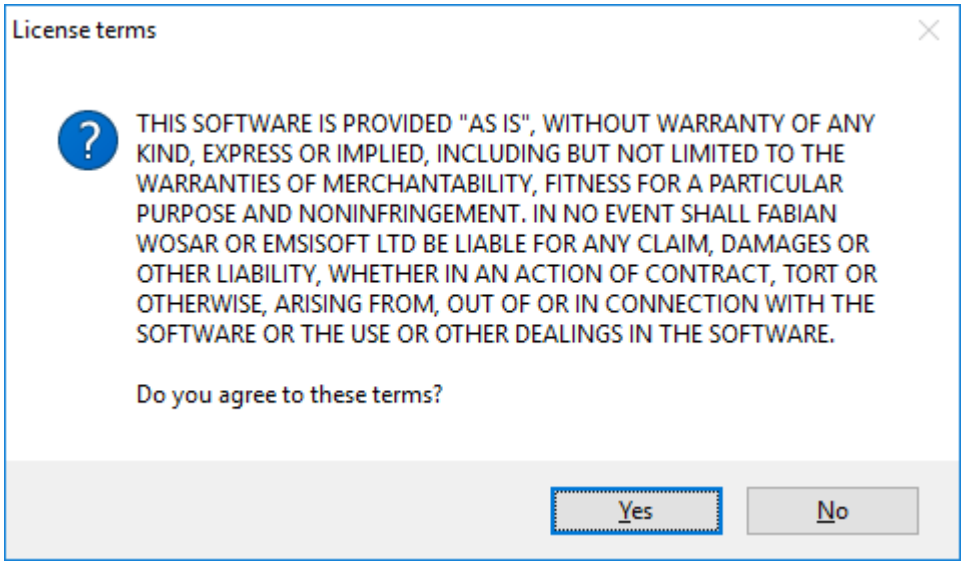


3. Once the mouse key is released, the decrypter will start to reconstruct the required encryption parameters. Depending on the ransomware, this process can take a significant amount of time.
4. The decrypter will display the reconstructed encryption details once the recovery process finished. The display is purely informational to confirm that the required encryption details have

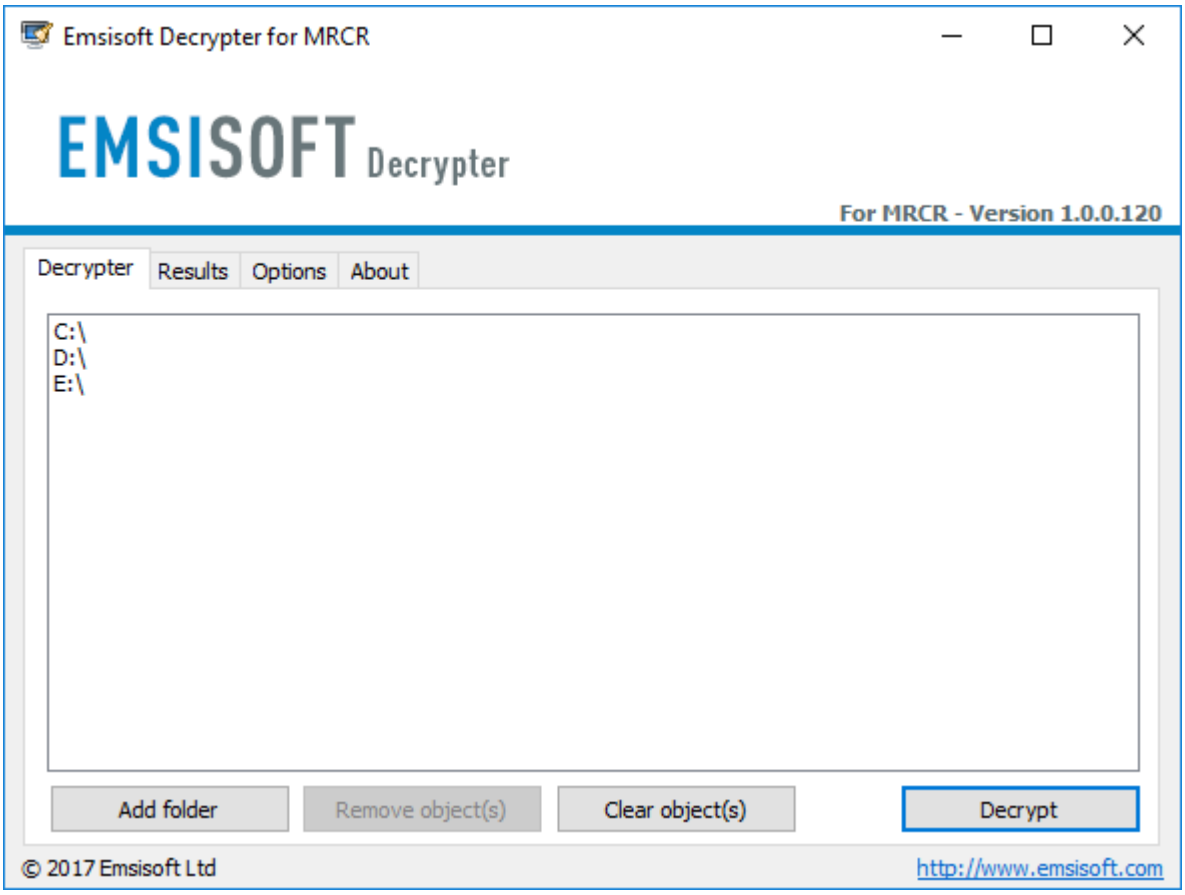
been found:



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



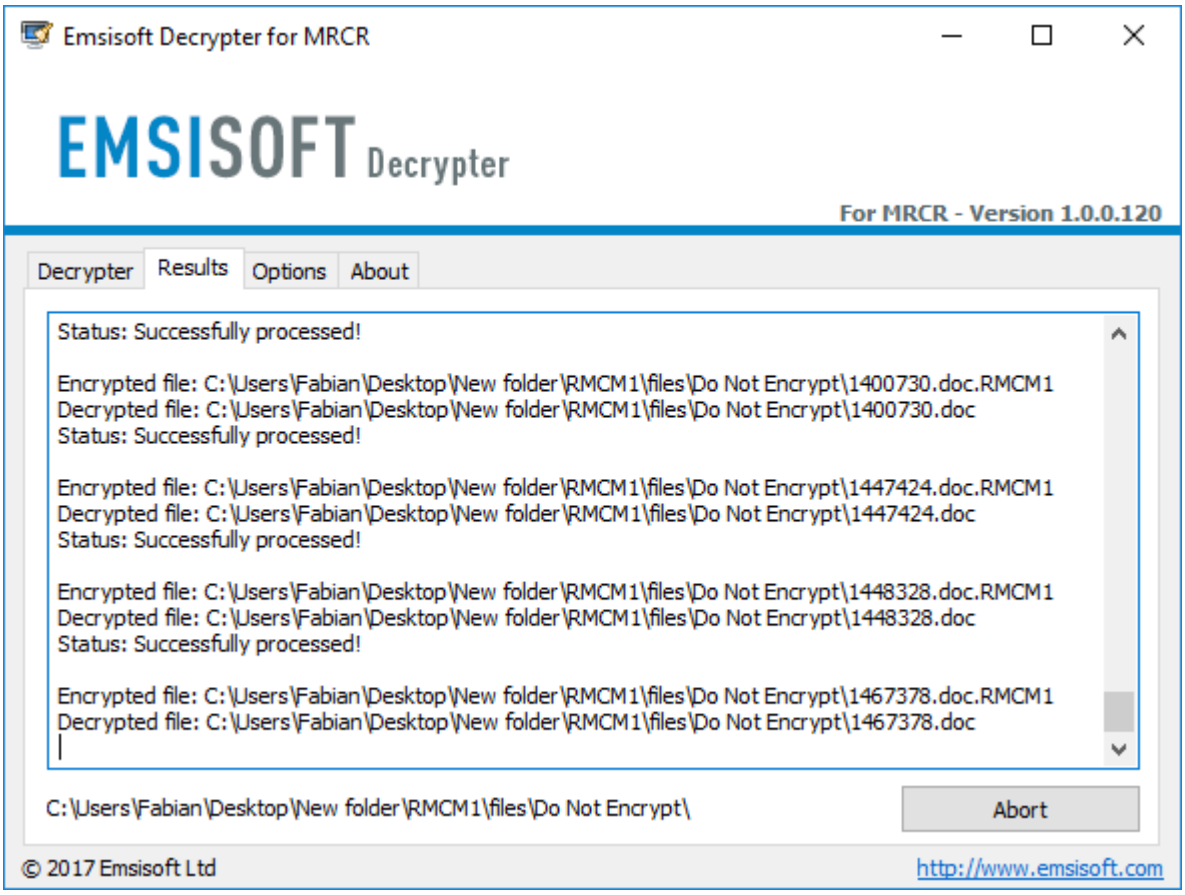
6. Once the license terms are accepted, the primary decrypter user interface opens:



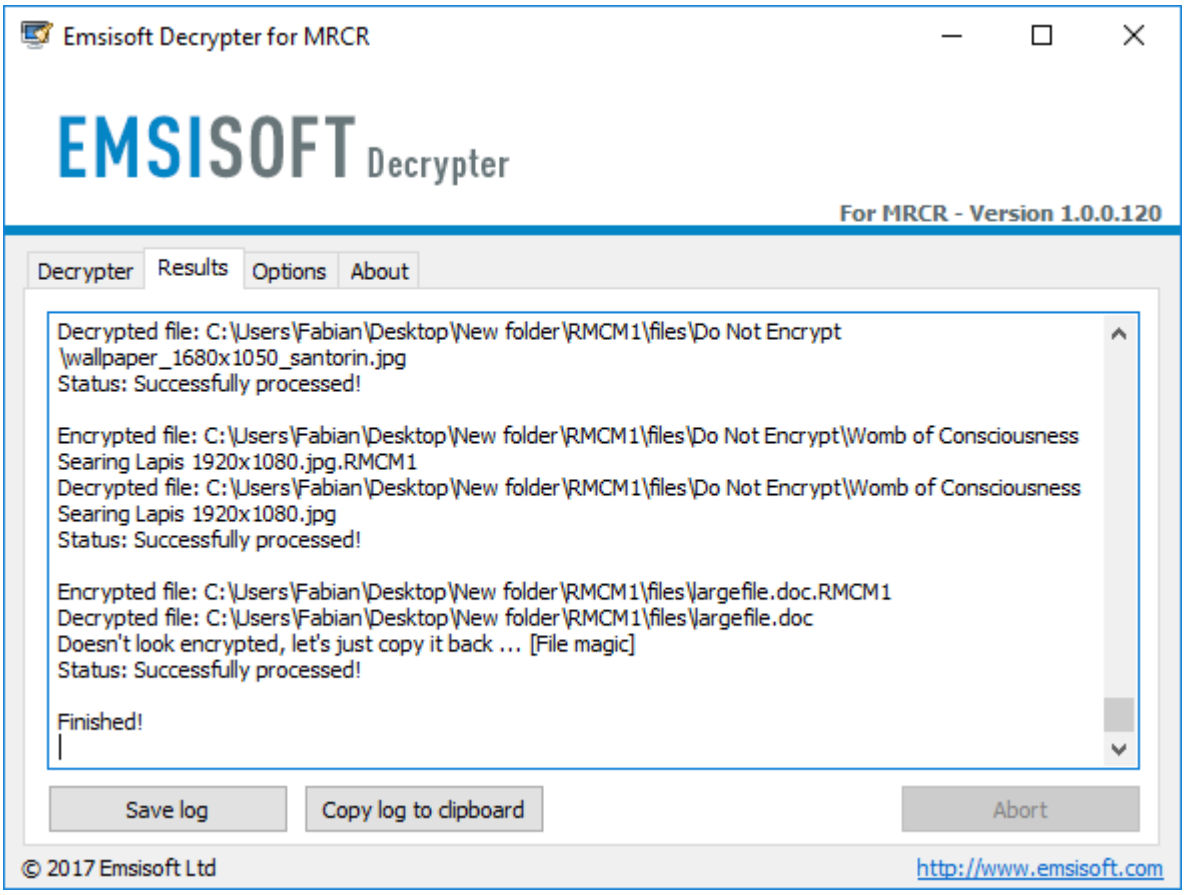
7. By default, the decrypter will pre-populate the locations to decrypt with the currently connected drives and network drives. Additional locations can be added using the "Add" button. Also, the object list accepts files and locations to be added via drag and drop.

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 added all the locations you want to decrypt to the list, 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:



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.
- **Detect failed encryptions**
  Due to a bug in the ransomware, some files are not being encrypted but merely renamed. If enabled, this option will instruct the decrypter to rename files instead of actually attempting to decrypt them.
- **Key selection**
  If multiple keys match your file pair, you can switch between them using the drop-down list.