EMSISOFT

How to use the Emsisoft Decrypter for Amnesia2

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.

How to decrypt your files

- 1. Download the decrypter from the same site that provided this "How To" document.
- 2. Once downloaded, double click the decrypter file to run it.
- 3. The license terms will show up next, which you have to agree to by clicking the "Yes" button:

License terms	\times
THIS SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL FABIAN WOSAR OR EMSISOFT LTD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Do you agree to these terms?	
Yes <u>N</u> o]

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



- 5. 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.
- 6. 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.
- 7. 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:



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

🗊 Emsisoft Decrypter for Amnesia2	_		Х
EMSISOFT Decrypter			
For Amr	nesia2 - Ve	ersion 1	.0.0.41
Decrypter Results Options About			
Encrypted file: C: \Users\Fabian\Desktop\Amnesia\Fourth\Do Not Encrypt\9w0000000 +larP7U0WZcEJyQ+3SB1nVnjfL2QNjL6I7wg3Bf4Fjruw60RD6fPjlZU.onion Trying to determine correct key. Please be patient, this can take some time Destination file: C: \Users\Fabian\Desktop\Amnesia\Fourth\Do Not Encrypt \Black_TextureRay_by_Ethenyl.jpg Status: Successfully decrypted! Encrypted file: C: \Users\Fabian\Desktop\Amnesia\Fourth\Do Not Encrypt\dg000000002 +WiJIMkD1hsEvMqsH1dR4fBiL+-wWdOuf+9I7Ox40zDnD-pBO-IAXq-Mu6ghCowElvk0Vef W2O1.onion Trying to determine correct key. Please be patient, this can take some time Destination file: C: \Users\Fabian\Desktop\Amnesia\Fourth\Do Not Encrypt\Womb of Co Lapis 1920x1080.jpg Status: Successfully decrypted!	23s BRdSQBNp-	s Searing	^
Finished!			~
Save log Copy log to clipboard	A	bort	
© 2017 Emsisoft Ltd	http://wv	w.emsis	oft.com

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.