How to use the Emsisoft Decrypter for Xorist

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 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.

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:

View	
l .	s الح
2860.doc Microsoft Word 97 - 2003 Docum 2.79 KB 2.79 KB	decrypt inst.exe Emsison Decrypter for Xorist Emsisoft Ltd
	 Open with Emsisoft Decrypter for Xorist

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:

C:\Users\Fabian\Desktop\NMR\decrypt_xorist.exe	-	х
Attempting to brute force key. This will take a while		^
2.41% of key space exhausted		
		~

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:

Decryption	h key found	×
1	The decrypter detected the following encryption details to be a match for the given file:	
	Key : 7F1675882FC0B1525BA40F8A65ADF5F4 Encryption Rounds: 64 Start Offset: 74 Encryption Limit: 1775620 Algorithm: TEA Please keep in mind that there is a slight chance that this key might be wrong. We suggest trying decrypting a few files first to check whether it is working correctly.	
	ОК]

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

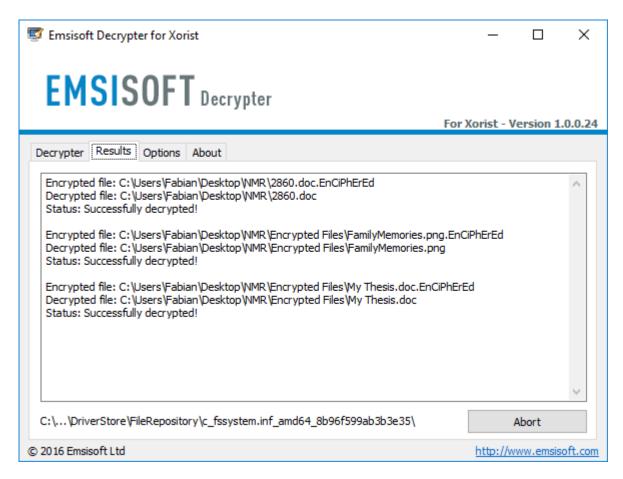
License terms	\times
THIS SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL FABIAN WOSAR OR EMSISOFT LTD BE LIABLE FOR ANY CLAIM, DAMAGES 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?	
<u>Y</u> es <u>N</u> o	

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

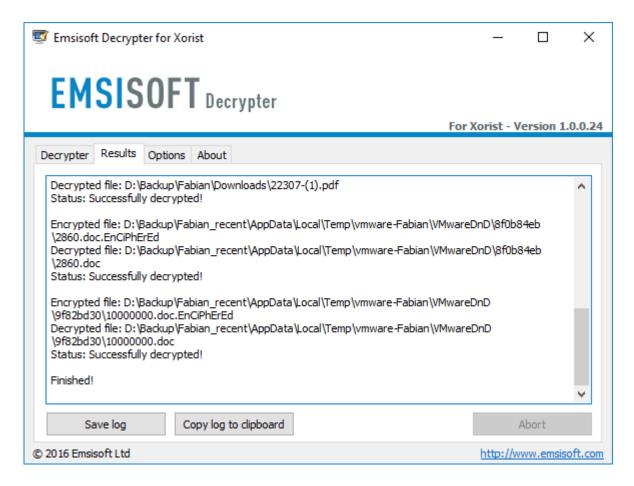
🕼 Emsisoft Decrypter for Xorist			_		×
EMSISO	FT Decrypter				
			For Xorist -	Version 1	.0.0.24
Decrypter Results Option	ons About				
C:\ D:\ E:\					
Add file(s)	Remove file(s)	Clear files		Decrypt	
© 2016 Emsisoft Ltd			http://	www.emsis	oft.com

- 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.