How to use the Emsisoft Decryptor for Maze/Sekhmet/Egregor

IMPORTANT! Be sure to quarantine the malware from your system first, or it may repeatedly lock your system or encrypt files. If your current antivirus solution fails to detect the malware, it can be quarantined using the free trial version of <u>Emsisoft Anti-Malware</u>. 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 decryptor requires the ransom note to decrypt your key.

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:

🔄 License Terms 🛛 🕹 🗙			
?	THIS SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MECHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL MICHAEL GILLESPIE 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 No		

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

Emsisoft Decryptor for MazeSehkmetEgregor	– 🗆 ×
EMSISOFT Decryptor	For MazeSehkmetEgregor - Version 1.0.0.0
Bruteforcer	
Encrypted / Original File Pair	
Please select an encrypted file: No file selected	Browse
Please select the original of the same file: No file selected	Browse
Ransom Note	
Please select a ransom note:	Browse
D:_Analysis\Maze\Case0\DECRYPT-FILES.txt	
Threads: 1	Start
© 2019 Emsisoft Ltd.	A free of charge service by Emsisoft - www.emsisoft.com

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:

Decryption Key Found X			
1	The decryptor detected the following encryption details to be a match for the given file:		
	Key: 0702000000A40000525341320008000001000100F727B8D1DF41C0 2A5D1D0C1AE12103B6749FB7F4AF79479E34346F46574F9A25F66 EAE97BB31170E527E656546D653C94D07654E01A8860A23B909D 54D44B1B11DC192BB913609A6853DCD20724CEE6BA993C02561 C2B0C8E202FEC35B94D43B4F8D818EC86CCEA2009F371F43E6D 043F9F7FF2F476A075A6CA46FFF8BF38AAB095CF4A98979115FD 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.	6	
	ОК]	

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

🔄 Emsisoft Decryptor for MazeSehkmetEgregor — 🗆 🔀				
EMSISOFT Decryptor	For MazeSehkm	etEgregor - Version 1.0.0.0		
Decryptor Results Options About				
C:\ D:\				
Add folder Remove object(s)	Clear object list	Decrypt		
© 2019 Emsisoft Ltd.	A free of charge service by En	nsisoft - <u>www.emsisoft.com</u> :		

- 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.

Emsisoft Decryptor for MazeSehkmetEgregor	– 🗆 X
EMSISOFT Decryptor	For MazeSehkmetEgregor - Version 1.0.0.0
Decryptor Results Options About	
Starting File: D:_Analysis\Maze\Case0\Chrysanthemum.jpg.tXkT(Decrypted: D:_Analysis\Maze\Case0\Chrysanthemum.jp; File: D:_Analysis\Maze\Case0\Desert.jpg.3pcin Decrypted: D:_Analysis\Maze\Case0\Desert.jpg File: D:_Analysis\Maze\Case0\Hydrangeas.jpg.5EFCJm Decrypted: D:_Analysis\Maze\Case0\Hydrangeas.jpg File: D:_Analysis\Maze\Case0\Hydrangeas.jpg File: D:_Analysis\Maze\Case0\zeroes.jpg.kNYUW5 Decrypted: D:_Analysis\Maze\Case0\zeroes.jpg Finished!	
Save log Copy log to clipboard	Abort
2019 Emsisoft Ltd.	A free of charge service by Emsisoft - www.emsisoft.com

- 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.