Mapo ransomware decryption instruction

- 1. Make sure that the ransomware is no longer running, it can encrypt your files again, rendering the whole decryption process futile.
- 2. Download Mapo Decryptor (https://nomoreransom.cert.pl/static/mapo_decryptor.exe).
- 3. Obtain the key from https://mapo.cert.pl:

a. Upload the ransom note file (usually **MAPO-Readme.txt**) by clicking on the white field on the website.

CERT.PL >_ Mapo ransomware key retrieval tool						
Upload a ransom note to retrieve the key.						
Click here to upload a ransom note. Chosen file: (none)						
Nie jestem robotem						
Get key						
Contact						
In case of any inquiries please contact us at info@cert.pl.						

b. After choosing the file, the selected filename should be displayed.

,		
	Click here to upload a ransom note. Chosen file: MAPO-Readme.txt	
Vie jestem robotem		
	Get key	

Verify the captcha by clicking on it, then click on "*Get key*" button to retrieve the key.

c. If the ransom note is correct and supported by our decryptor, the key will be returned. Don't close this website just yet.



- 4. Run *mapo_decryptor.exe* (that you downloaded in step 2.) on the infected computer.
- 5. Click "**Yes**" in UAC Window:

D	Do you want to publisher to m		
	Program name: Publisher: File origin:	mapo_decryptor.exe Unknown Hard drive on this computer	mapo_decryp or
•	Show details	Yes No	

- 6. Wait until decryptor asks for key with the following message *"Input the recovered key"*.
- 7. Decryptor will ask you to provide the key obtained from the service in **step 3**, copy the key from website and paste it into the terminal as shown below (right click the title bar first):

C:\Users\ \Desktop\mapo_decryptor.e>	Rostoro		<u>_0×</u>	
[-] C:\Python34\Scripts\easy_ir	Mesuo	.mapo		
L-J GNPython34\Scripts\easy_ir	MOVE	0		
L-J G: NYthon 34 Scripts Naked. e	Size			
[-] C:\Puthon24\Scripts\pip.exe	Minimize			
$[-1]$ C:\Puthon 24\Conjuta\nin2 ov	1. WINTING C			
$[-1]$ C:\Puthon34\tcl\itclstub40	Maximize			
$[-1]$ C:\Puthon34\tcl\tcl86t lib				
[-] C:\Puthon34\tcl\tclConfig.sX	Close			
[-] C:\Python34\tcl\tclooConfid	r da	Made		
[-] C:\Python34\tcl\tclstub86.]		Mark		
[-] C:\Python34\tcl\tk86t.lib.m	Defaults	Copy Enter		mana dage
[-] C:\Python34\tcl\tkstub86.li	Properties	Paste		mapo_oecr
[-] C:\Recovery\180f161b-45c3-1	Troperdes	Culout All	sdi.mapo	
[-] C:\Recovery\180f161b-45c3-11e	7-80be-e11	Select All	.wim.mapo	
[-] C:\Users\Default\NTUSER.DAT{0}	16888bd-6c	Scroll	1e0bcde3ec>.TM.blf.	
mapo		Find		
L-J C:\Users\Default\NTUSER.DAT(0)	L6888bd-6c	THOM	1e0bcde3ec}.TMConta	
iner000000000000000000000000000000000000	.mapo	C 441 0 141 0		
L-J G: NUSEPS NUCLAUIT NIUSEK. DHI (0)	LPAAADU-PCP	f-11de-8d1d-0	91e0bcde3ec7.IMConta	
Ineroooooooooooooooooooooooooooooooooooo	.mapo			
[-] locating warsom note				
[-] Scanning drive C:\				
Input the recovered key:			•	
Linke one recorded and y				

- 8. Entering the key and pressing enter will start the decryption process. After the "*Press* "*Enter*" to exit..." message, all of your files should be decrypted.
- If something didn't work, or not all files were decrypted, don't hesitate to contact cert@cert.pl. Please attach log.txt file, that should be generated next to mapo_decryptor.exe. If you can, attach wrongly decrypted file as well.
- 10. After decryption and making sure that the files have been decrypted correctly you can safely delete encrypted files.