Ransomware Decryption Tool User Manual

- Ragnar -

May 2022

Cryptography & Convergence Team

KISA Korea Internet & Security Agency

Directions for Using Decryption Tool

Caution: Make sure to delete malicious code from the system first. If not, the system can be reinfected even if the infected file is recovered.
KISA is not responsible for any problems caused by misuse.

1. Prepare for recovery

To use Ragnar ransomware decryption tool, **one pair of the infected file and original file of the infected file is required.** The original file can be obtained by installing the same program installed in the infected computer in another computer. In general, when a program distributed in the format of ".exe" is installed, the file is created in various formats, such as a compressed file in the format of ".zip" or ".jar," and a photo file in the format of ".jpeg" or ".png," on the installation path of "Program Files," "Program Files(x86)," etc. Repeating the process to compare the created file with the infected file, the original file can be obtained.

The original file can also be obtained by comparing a file transmitted through email, a file in the USB storage device, and a file saved in cloud storage with the infected file.

For successful recovery, the size of the pair of files must be at least **10MB or larger** each. In addition, the name and version of the files must be the same.

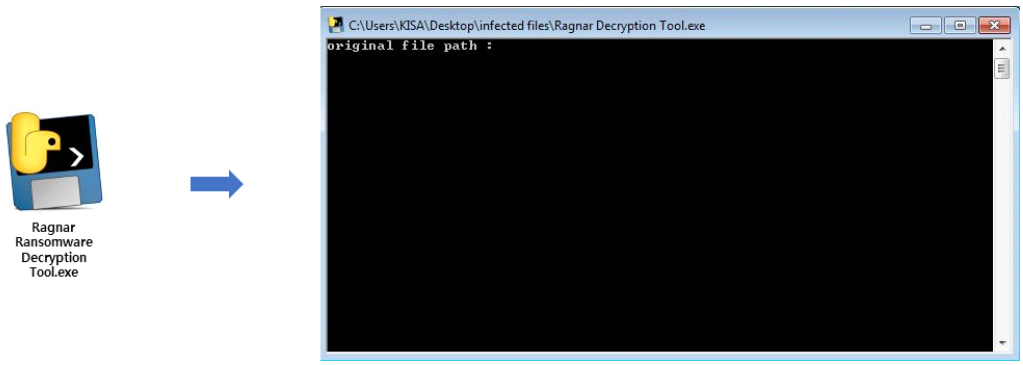
Ragnar ransomware executes encryption by excluding specific folders, files, and extensions. The folders, files, and extensions in [Table 1] do not include infected files. This must be noted when preparing the pair of files for recovery.

Excluded Folders	Windows	Windows.old	Tor browser	Internet Explorer
	Google	Opera	Opera Software	$Recycle.Bin
	Mozilla	Mozilla Firefox	ProgramData	All Users
Excluded Files	autorun.inf	boot.ini	bootfont.bin	bootsect.bak
	desktop.ini	ntldr	ntuser.dat	ntuser.dat.log
	ntuser.ini	thumbs.db	ransom note	
Excluded Extensions	.db	.msi	.sys	.drv
	.dll	.exe	.lnk	

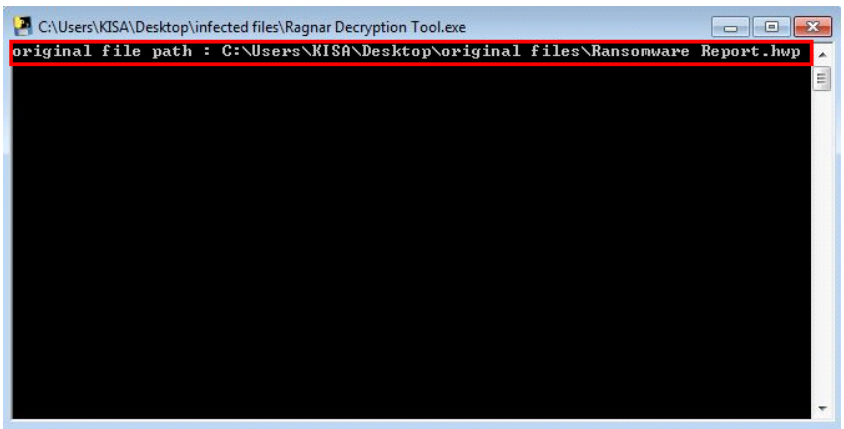
< Table 1 > List of Encryption Exclusion Targets

2. Execute recovery

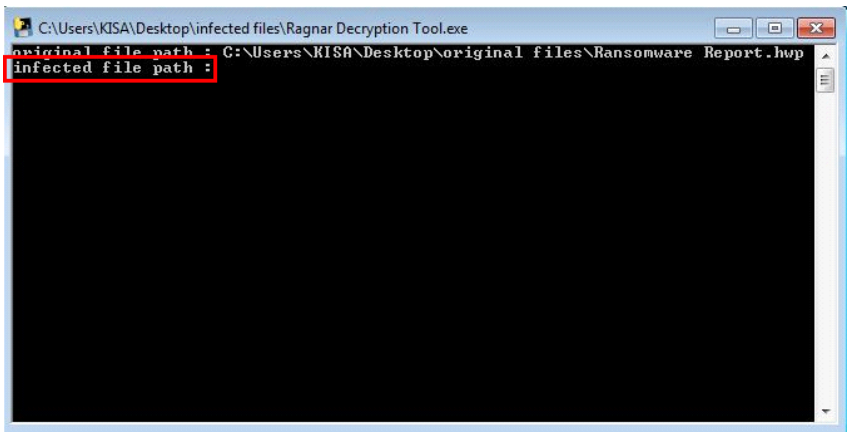
When Ragnar ransomware decryption tool is executed with administrative privilege, a window for entering the path on which the original file of the infected file is located opens.



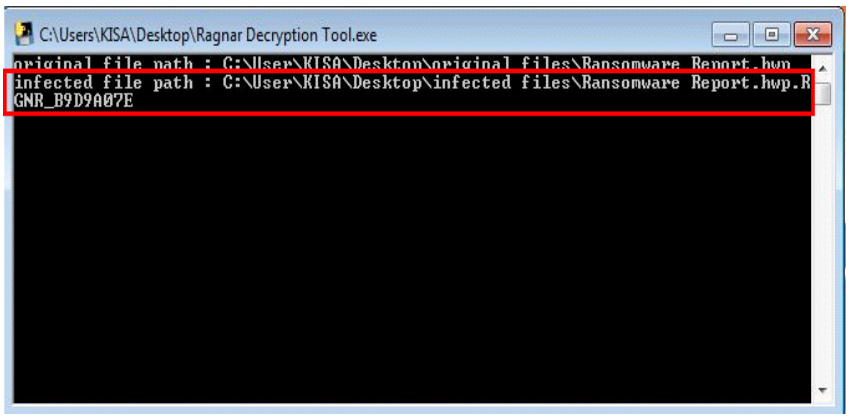
Enter the path including the name and extension of the original file, and press Enter.



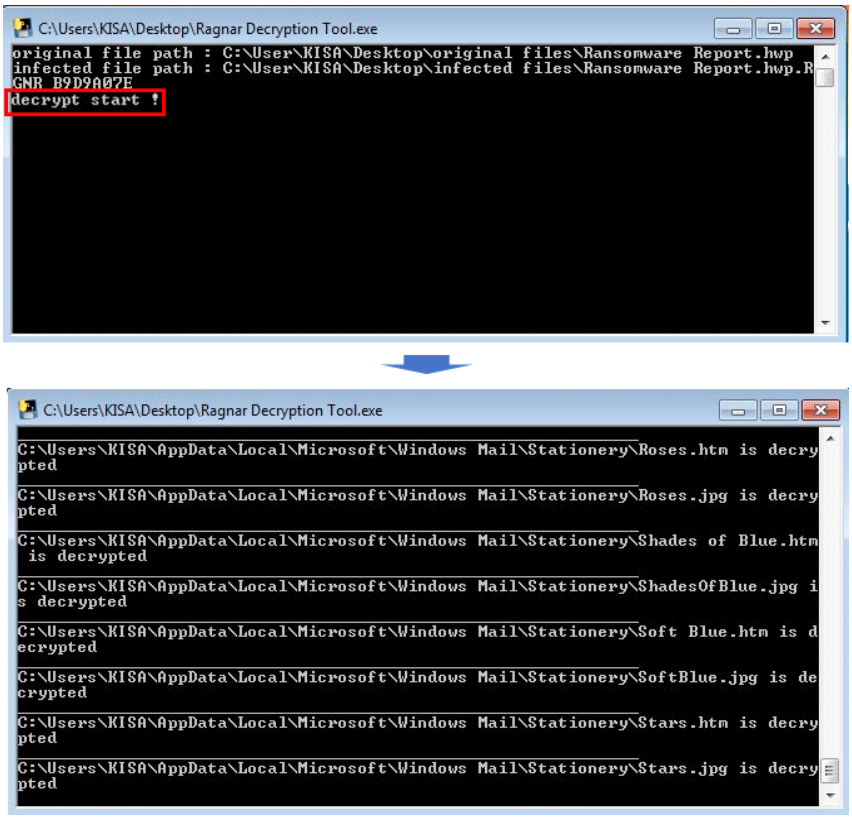
A window for entering the path on which the infected file is located opens.



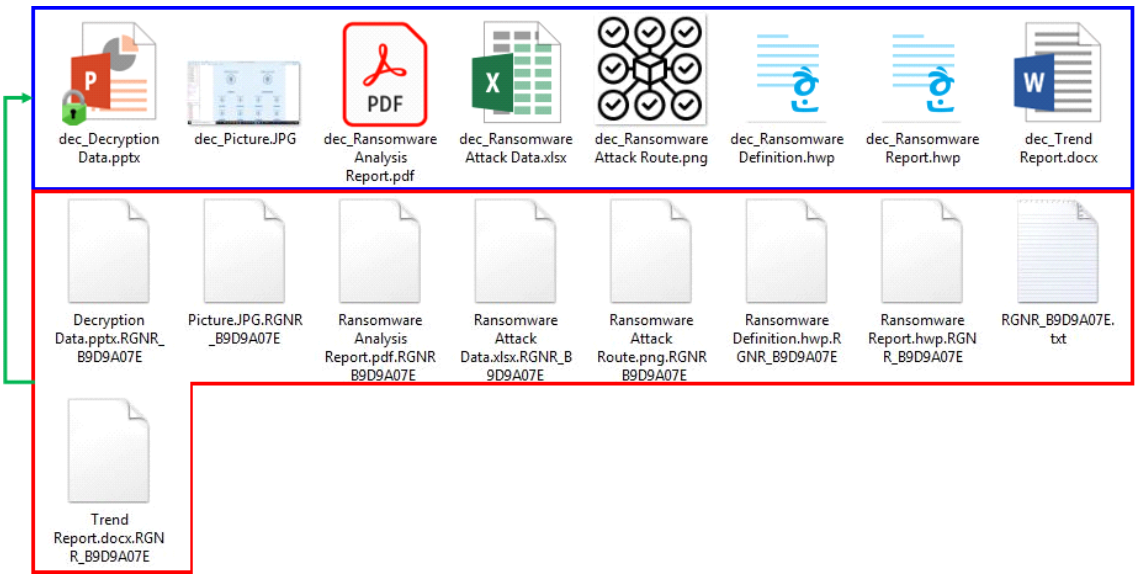
Enter the path including the name and extension of the infected file, and press Enter. For reference, Ragnar ransomware adds "RGNR_(a random eight-digit character string)" extension to the back of the infected file extension. So, when entering a path, make sure to accurately enter it including the added extension.



When path including names and extensions of the original file and infected file is entered, the decryption tool extracts values necessary for encryption key recovery using the files. When encryption key recovery is completed, recovery of the infected file is automatically executed.



The recovered file is created on every path where the infected file is located. A character string, "dec_" is added to the front of the recovered file name. Opening the file, it can be checked that the file is normally executed.



What is Ragnar ransomware?

Ragnar ransomware mainly attacks enterprises. This ransomware encrypts data using stream ciphers. As the condition for data recovery, it demands a large amount of ransom to the infected. Detailed information is available in the analysis report.

※ URL for Ragnar ransomware analysis report download
→ https://seed.kisa.or.kr/kisa/Board/101/detailView.do

Ragnar Ransomware Decryption Tool User Manual

May 2022

Published by KISA Korea Internet & Security Agency