Ransomware Integrated Decryption Tool User Manual

- Hive Version1 to Version4 -

June 2022

Cryptography & Convergence Team

KISA Korea Internet & Security Agency

Directions for Using Decryption Tool

Precautions : Make sure to delete malicious code from the system first. If not, the system can be reinfected even if the infected file is recovered.

Due to the cryptographic nature of Hive ransomware, it is difficult to recover 100%.

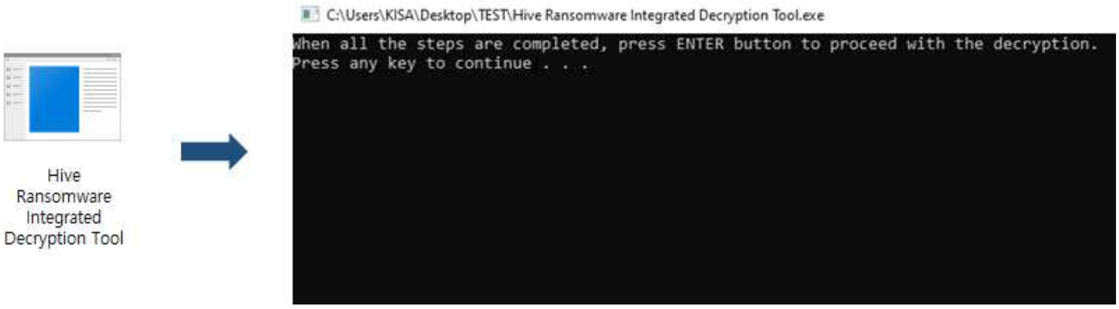
KISA is not responsible for any problems caused by misuse.

As the integrated decryption tool operates continuously, it is impossible to recover files if you exit the program in the middle.

The integrated decryption tool can decrypt Hive ransomware version 1 to 4. However, in the version 2, it is possible to decrypt only if the extension of the infected file is ‘.w2tnk’, ‘.uj1ps’.

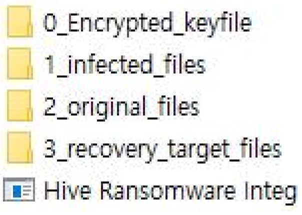
1. Run the integrated decryption tool

When Hive Ransomware Integrated Decryption Tool.exe is run with administrator privileges, a Command Prompt(CMD) window appears.



```
C:\Users\KISA\Desktop\TEST\Hive Ransomware Integrated Decryption Tool.exe
When all the steps are completed, press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

Then, 4 folders are created in the path where the decryption tool is located. If the encryption key file encrypted by the ransomware attacker, the infected file, the original file, and the file to be decryted are copied to the created folder, preparation for file decryption is completed.



```
0_Encrypted_keyfile
1_infected_files
2_original_files
3_recovery_target_files
Hive Ransomware Integ
```

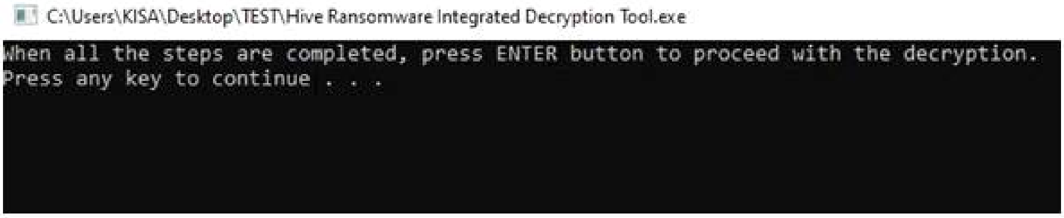
Folder name		Copy to
0_Encrypted_keyfile	⇨	Encryption key file encrypted by attacker
1_infected_files	⇨	Infected file
2_original_files	⇨	The original file of the infected file
3_recovery_target_files	⇨	File to be decrypted

2. Check the version

For the Hive ransomware version, check the file extension and size of the encryption key encrypted by the ransomware attacker created on the C drive when infected. However, in the version1, if the execution program is not run with administrator privileges, an encrypted encryption key is created in the virtualization folder. For the virtualization folder, refer to the details in the table of contents of '3.1.1. Version1'.

Version	File name	File extension	File size	Example
1	random string	.hive	about 10MB	Jub3Ee9tNMK1Wy0PRwuVTw.**key.hive**
2		.w2tnk	about 10MB	Ns9SQ_476LclOK71vDYbAwrFKbt.**key.w2tnk**
		.uj1ps		wMeaAeiQD-vkcgjVMdenTtLGAST.**key.uj1ps**
3		random string	about 3KB, 100KB, 1MB	xDKszTbfp3gyp7ixGWIWuZp5iS0B.**key.fayg2**
4		random string	about 3MB	VICqe_MNCP-TubaUvhZ4IU5f1rqr.**key.bvddx**

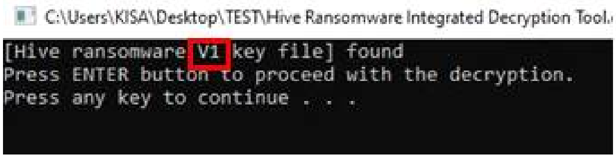
After copying the encrypted encryption key to the 0_Encrypted_keyfile folder, enter the Enter key in the previous window to check the Hive ransomware version and see the result.



C:\Users\KISA\Desktop\TEST\Hive Ransomware Integrated Decryption Tool.exe

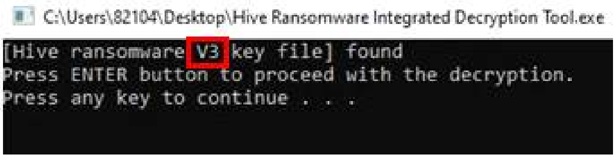
```
When all the steps are completed, press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

Enter the Enter key



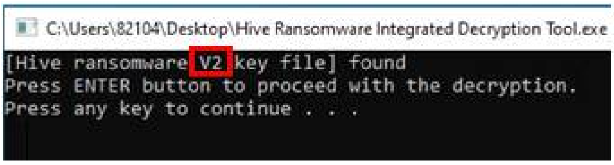
C:\Users\KISA\Desktop\TEST\Hive Ransomware Integrated Decryption Tool.

```
[Hive ransomware V1 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```



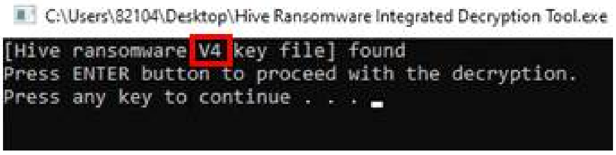
C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V3 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```



C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V2 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```



C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V4 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

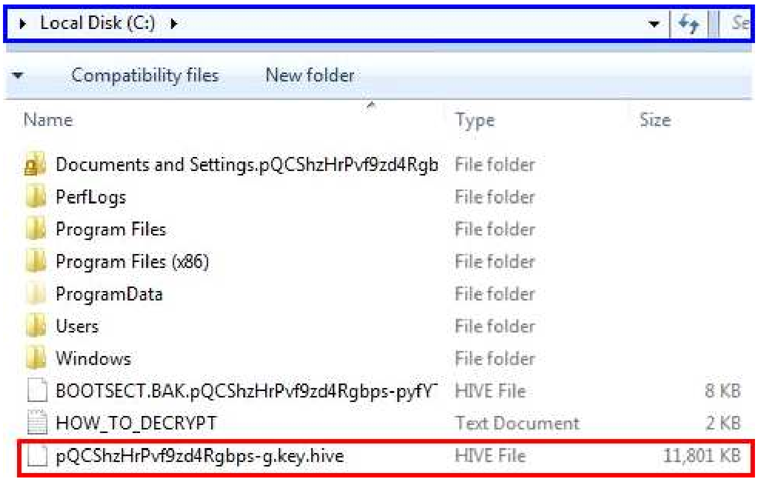
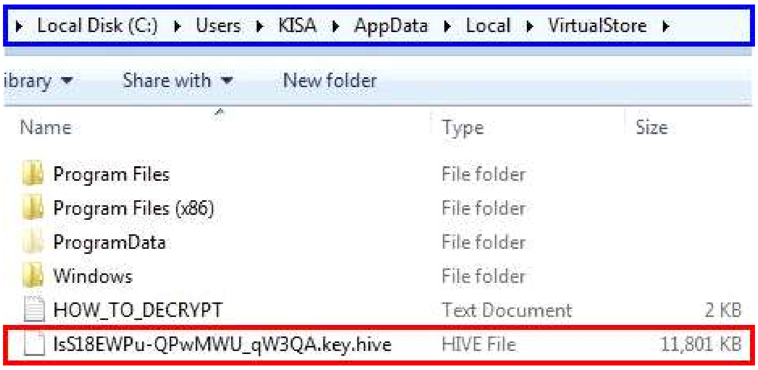
3. Collect original files

3.1. How to collect original files by version

To use the Hive ransomware integrated decryption tool, the infected file and the original file of the infected file are needed. From version 1 to version 4, the method of collecting original files is basically the same. However, in version 1, if the ransomware execution program is not run with administrator privileges, the original file must be collected in another way.

3.1.1. Version1

Whether the Hive ransomware version 1 execution program is run with administrator privileges can be checked through the location of the file encryption key encrypted by the attacker. The encrypted file encryption key exists in the root directory(C drive) if it is run with administrator privileges, otherwise in the virtualization folder (C:\Users\<User_name>\AppData\Local\VirtualStore). The file name is 'random string.key.hive', and the file size is about 10MB.

Whether to run with administartor privileges	Encrypted file encryption key location
Run with administartor privileges (C drive)	 Local Disk (C:) Name / Type / Size Documents and Settings.pQCShzHrPvf9zd4Rgb / File folder PerfLogs / File folder Program Files / File folder Program Files (x86) / File folder ProgramData / File folder Users / File folder Windows / File folder BOOTSECT.BAK.pQCShzHrPvf9zd4Rgbps-pyfY / HIVE File / 8 KB HOW_TO_DECRYPT / Text Document / 2 KB pQCShzHrPvf9zd4Rgbps-g.key.hive / HIVE File / 11,801 KB
Not run with administrator privileges (VirtualStore)	 Local Disk (C:) ▸ Users ▸ KISA ▸ AppData ▸ Local ▸ VirtualStore Name / Type / Size Program Files / File folder Program Files (x86) / File folder ProgramData / File folder Windows / File folder HOW_TO_DECRYPT / Text Document / 2 KB IsS18EWPu-QPwMWU_qW3QA.key.hive / HIVE File / 11,801 KB

① **When run with administrator privileges**

When the Hive ransomware is run with administrator privileges, the infected file is not created in the Virtualization folder(VirtualStore), but the infected file is created in the 'Program Files', 'Program Files (x86)', and 'ProgramData' folder of the C drive and the original file of the corresponding file is deleted.

In this case, reinstall the same version of the program installed on the infected PC to collect the original files. When the program is reinstalled, various formats of files such as library files of '.lib', '.dll' format, photo files of '.jpeg', '.png', format are created in installation paths such as "Program Files" and "Program Files" (x86). If the process of comparing the file with the infected file is repeated, a large amount of original files can be collected.

In addition, there is also a method to collect original files by comparing files sent and received via email, files on USB storage devices, and files stored in cloud storage with infected files.

② **When not run with administrator privileges**

If the Hive ransomware is not run with administrator privileges, the infected file is created in the Virtualization folder(VirtualStore). The original file of the infected file is located in the ‘Program Files’, ‘Program Files (x86)’, ‘ProgramData’ folders of the C drive. The encryption key can be decrypted using the original file and the infected file in the VirtualStore, and files such as infected document, photo, and video from which the original file has been deleted can be decrypted.

3.1.2. Version2 to Version4

The method of collecting the original file of infected files of Hive ransomware version 2 to version 4 is the same as the case ① When run with administrator privileges of "3.1.1. Version 1". Thus, the original files of the infected files can be collected using the corresponding method.

3.2. Conditions

When collecting the infected files and original files, three conditions have to be met. If decryption is performed in a state where the conditions are not satisfied, an error occurs or the decryption tool program is ended. The conditions are as follows.

> Infected files and original files
>
> ① **The name** has to be the same.
> ② **The total number** has to be the same.
> ③ **The version** has to be the same.

Due to the cryptographic characteristics of Hive ransomware, the number of files required for decryption is variable and difficult to quantify, so it is recommended to refer to the description below.

In the version1, the number of files required for decryption varies according to the total size of the files. If the total size of the files is 50 KB or less, 500 to 1,000 files are required, if the size is between 1 to 5 MB, more than 100 files are required, and if the size is 25 MB, 30 to 50 files are required.

Version	Total size of file	Number of file required
1	50KB or less	500 to 1,000 files
	1 to 5MB	more than 100 files
	25MB	30 to 50 files

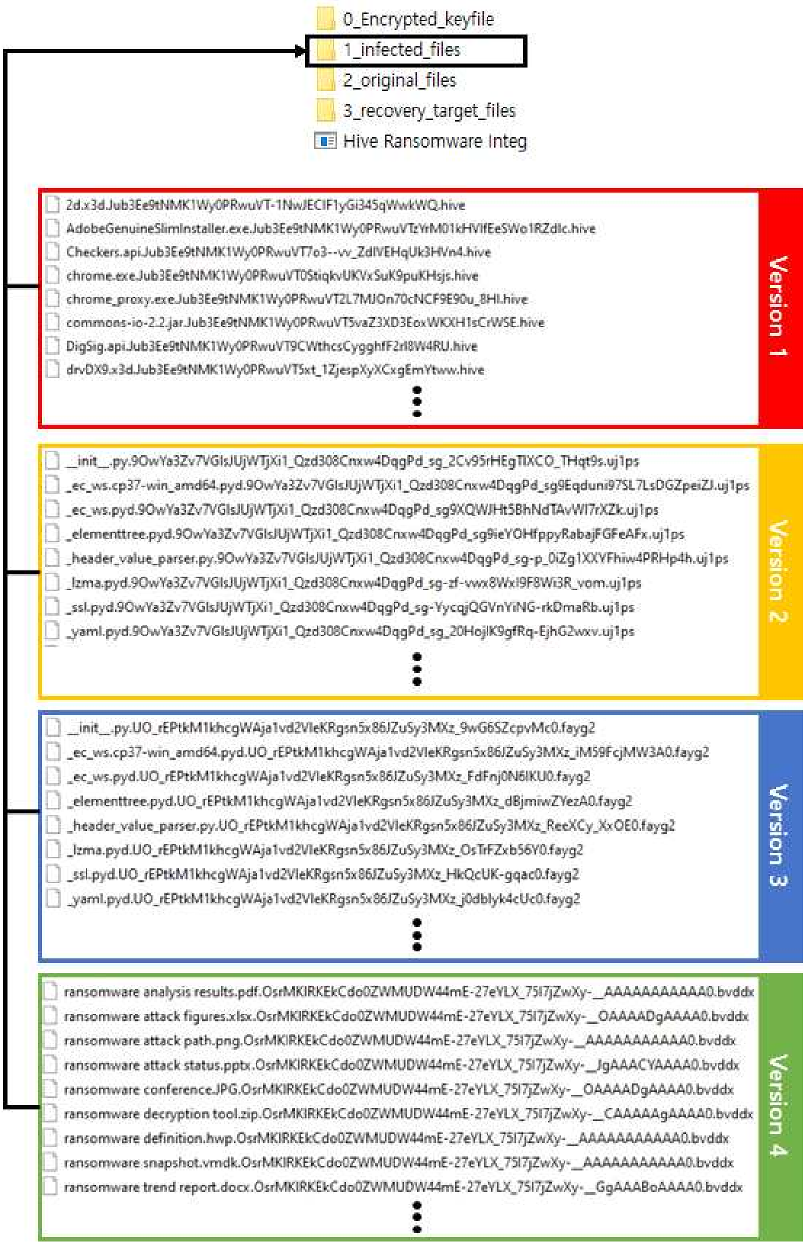
From version2 to version4, the number of files required for decryption varies according to the size of individual file. If the extension of the infected file among version 2 is '.w2tnk', 500 to 1,000 files with a size of more than 86 KB are required, and for '.uj1ps', 1,000 files with a size of more than 128 KB are required or 500 files with a size of more than 345 KB are required. For version 3, 100 files with a size of more than 128 KB, and for version 4, at least 5 files with a size of more than 5 KB are required.

Version		Size of individual file	Number of file required
2	**w2tnk**	more than 86KB	500 to 1,000 files
	uj1ps	more than 128KB	1,000 files
		more than 345KB	500 files
3		more than 128KB	100 files
4		more than 5KB	more than 5 files

The number of files required for decryption is inversely proportional to the total size of files or the size of individual file depending on the version, so the user can arbitrarily adjust the number of files required, and the decryption rate may vary accordingly. However, if the number is too small, it is not possible to extract the values necessary for encryption key decryption, so this needs to be noted(except version 4).

4. Perform decryption

After the collection of original files is completed, copy the infected file to the '1_infected_files' folder.



```
0_Encrypted_keyfile
1_infected_files
2_original_files
3_recovery_target_files
Hive Ransomware Integ
```

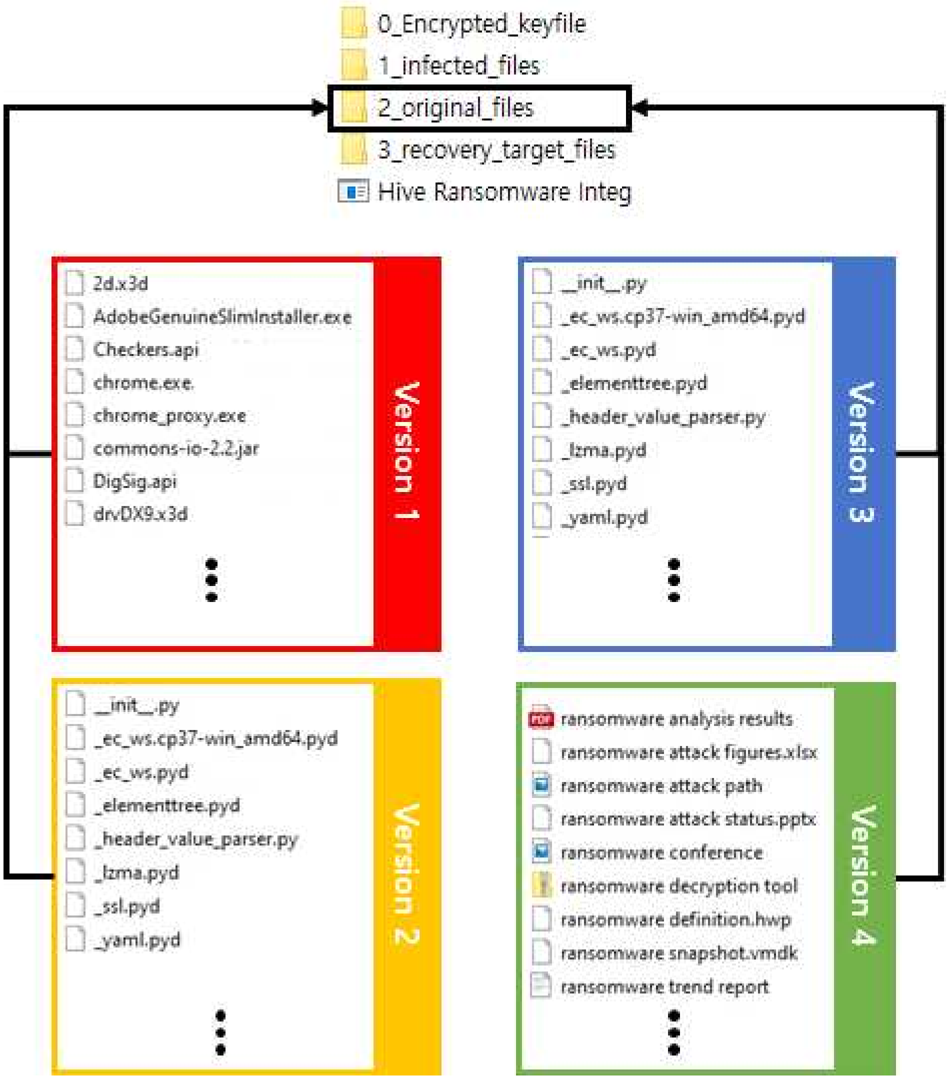
```
2d.x3d.Jub3Ee9tNMK1Wy0PRwuVT-1NwJECIF1yGi345qWwkWQ.hive
AdobeGenuineSlimInstaller.exe.Jub3Ee9tNMK1Wy0PRwuVTzYrM01kHVIfEeSWo1RZdlc.hive
Checkers.api.Jub3Ee9tNMK1Wy0PRwuVT7o3--vv_ZdlVEHqUk3HVn4.hive
chrome.exe.Jub3Ee9tNMK1Wy0PRwuVT0StiqkvUKVxSuK9puKHsjs.hive
chrome_proxy.exe.Jub3Ee9tNMK1Wy0PRwuVT2L7MJOn70cNCF9E90u_8HI.hive
commons-io-2.2.jar.Jub3Ee9tNMK1Wy0PRwuVT5vaZ3XD3EoxWKXH1sCrWSE.hive
DigSig.api.Jub3Ee9tNMK1Wy0PRwuVT9CWthcsCygghfF2rl8W4RU.hive
drvDX9.x3d.Jub3Ee9tNMK1Wy0PRwuVT5xt_1ZjespXyXCxgEmYtww.hive
⋮
```

```
__init__.py.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_2Cv95rHEgTlXCO_THqt9s.uj1ps
_ec_ws.cp37-win_amd64.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9Eqduni97SL7LsDGZpeiZJ.uj1ps
_ec_ws.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9XQWJHt5BhNdTAvWI7rXZk.uj1ps
_elementtree.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9ieYOHfppyRabajFGFeAFx.uj1ps
_header_value_parser.py.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-p_0iZg1XXYFhiw4PRHp4h.uj1ps
_lzma.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-zf-vwx8WxI9F8Wi3R_vom.uj1ps
_ssl.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb.uj1ps
_yaml.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_20HojlK9gfRq-EjhG2wxv.uj1ps
⋮
```

```
__init__.py.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_9wG6SZcpvMc0.fayg2
_ec_ws.cp37-win_amd64.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_iM59FcjMW3A0.fayg2
_ec_ws.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_FdFnj0N6IKU0.fayg2
_elementtree.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_dBjmiwZYezA0.fayg2
_header_value_parser.py.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_ReeXCy_XxOE0.fayg2
_lzma.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_OsTrFZxb56Y0.fayg2
_ssl.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0.fayg2
_yaml.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_j0dblyk4cUc0.fayg2
⋮
```

```
ransomware analysis results.pdf.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware attack figures.xlsx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0.bvddx
ransomware attack path.png.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware attack status.pptx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__JgAAACYAAAA0.bvddx
ransomware conference.JPG.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0.bvddx
ransomware decryption tool.zip.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__CAAAAAgAAAA0.bvddx
ransomware definition.hwp.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware snapshot.vmdk.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware trend report.docx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__GgAAABoAAAA0.bvddx
⋮
```

Then, copy the original file to the ‘2_original_files’ folder.



0_Encrypted_keyfile
1_infected_files
2_original_files
3_recovery_target_files
Hive Ransomware Integ

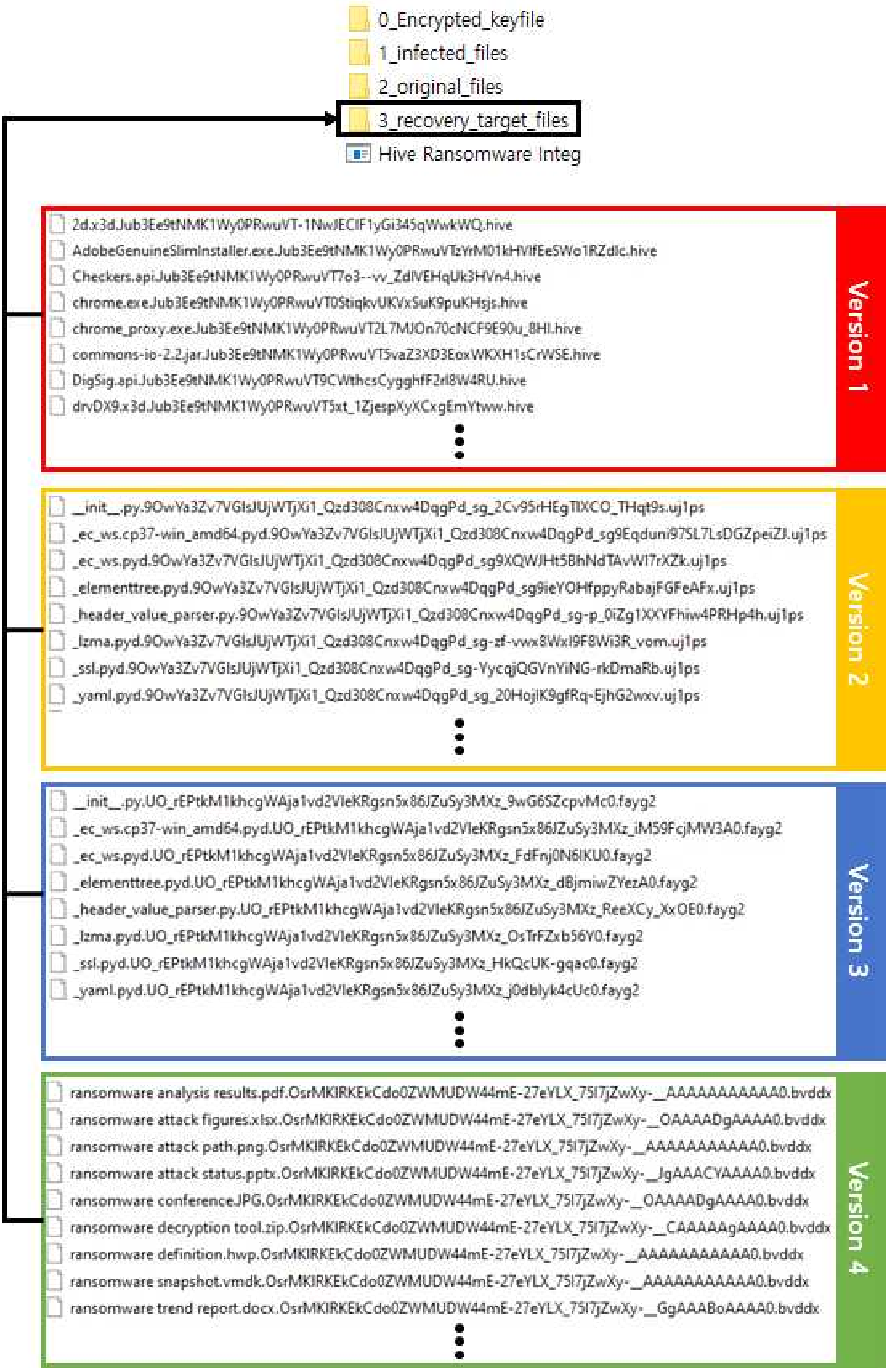
2d.x3d
AdobeGenuineSlimInstaller.exe
Checkers.api
chrome.exe
chrome_proxy.exe
commons-io-2.2.jar
DigSig.api
drvDX9.x3d
⋮

__init__.py
_ec_ws.cp37-win_amd64.pyd
_ec_ws.pyd
_elementtree.pyd
_header_value_parser.py
_lzma.pyd
_ssl.pyd
_yaml.pyd
⋮

__init__.py
_ec_ws.cp37-win_amd64.pyd
_ec_ws.pyd
_elementtree.pyd
_header_value_parser.py
_lzma.pyd
_ssl.pyd
_yaml.pyd
⋮

ransomware analysis results
ransomware attack figures.xlsx
ransomware attack path
ransomware attack status.pptx
ransomware conference
ransomware decryption tool
ransomware definition.hwp
ransomware snapshot.vmdk
ransomware trend report
⋮

Finally, copy the files to be decrypted to the '3_recovery_target_files' folder.



```
0_Encrypted_keyfile
1_infected_files
2_original_files
3_recovery_target_files
Hive Ransomware Integ
```

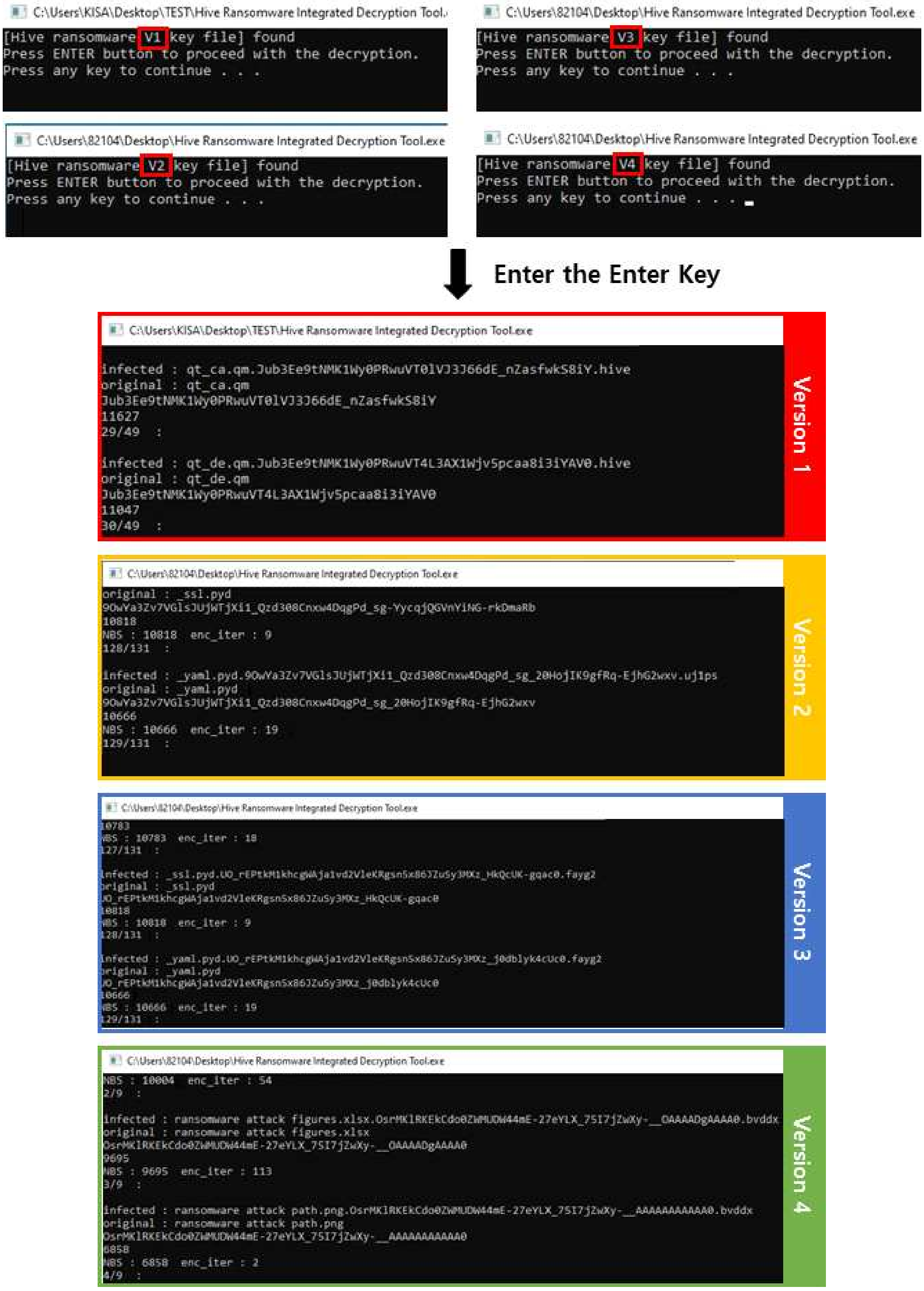
```
2d.x3d.Jub3Ee9tNMK1Wy0PRwuVT-1NwJECIF1yGi345qWwkWQ.hive
AdobeGenuineSlimInstaller.exe.Jub3Ee9tNMK1Wy0PRwuVTzYrM01kHVIfEeSWo1RZdlc.hive
Checkers.api.Jub3Ee9tNMK1Wy0PRwuVT7o3--vv_ZdlVEHqUk3HVn4.hive
chrome.exe.Jub3Ee9tNMK1Wy0PRwuVT0StiqkvUKVxSuK9puKHsjs.hive
chrome_proxy.exe.Jub3Ee9tNMK1Wy0PRwuVT2L7MJOn70cNCF9E90u_8HI.hive
commons-io-2.2.jar.Jub3Ee9tNMK1Wy0PRwuVT5vaZ3XD3EoxWKXH1sCrWSE.hive
DigSig.api.Jub3Ee9tNMK1Wy0PRwuVT9CWthcsCygghfF2rl8W4RU.hive
drvDX9.x3d.Jub3Ee9tNMK1Wy0PRwuVT5xt_1ZjespXyXCxgEmYtww.hive
⋮
```

```
__init__.py.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_2Cv95rHEgTlXCO_THqt9s.uj1ps
_ec_ws.cp37-win_amd64.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9Eqduni97SL7LsDGZpeiZJ.uj1ps
_ec_ws.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9XQWJHt5BhNdTAvWI7rXZk.uj1ps
_elementtree.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg9ieYOHfppyRabajFGFeAFx.uj1ps
_header_value_parser.py.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-p_0iZg1XXYFhiw4PRHp4h.uj1ps
_lzma.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-zf-vwx8WxI9F8Wi3R_vom.uj1ps
_ssl.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb.uj1ps
_yaml.pyd.9OwYa3Zv7VGIsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_20HojlK9gfRq-EjhG2wxv.uj1ps
⋮
```

```
__init__.py.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_9wG6SZcpvMc0.fayg2
_ec_ws.cp37-win_amd64.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_iM59FcjMW3A0.fayg2
_ec_ws.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_FdFnj0N6lKU0.fayg2
_elementtree.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_dBjmiwZYezA0.fayg2
_header_value_parser.py.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_ReeXCy_XxOE0.fayg2
_lzma.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_OsTrFZxb56Y0.fayg2
_ssl.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0.fayg2
_yaml.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_j0dblyk4cUc0.fayg2
⋮
```

```
ransomware analysis results.pdf.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware attack figures.xlsx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0.bvddx
ransomware attack path.png.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware attack status.pptx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__JgAAACYAAAA0.bvddx
ransomware conference.JPG.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0.bvddx
ransomware decryption tool.zip.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__CAAAAAgAAAA0.bvddx
ransomware definition.hwp.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware snapshot.vmdk.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
ransomware trend report.docx.OsrMKIRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__GgAAABoAAAA0.bvddx
⋮
```

After copying the files required for decryption and the files to be decrypted to each folder, press the Enter key in the previous window. The decryption tool extracts the values necessary for decryption using the infected file and the original file and recovers the encryption key. The time that it takes to recover the encryption key may vary depending on the number of infected files and original files.



C:\Users\KISA\Desktop\TEST\Hive Ransomware Integrated Decryption Tool.

```
[Hive ransomware V1 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V3 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V2 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
[Hive ransomware V4 key file] found
Press ENTER button to proceed with the decryption.
Press any key to continue . . .
```

C:\Users\KISA\Desktop\TEST\Hive Ransomware Integrated Decryption Tool.exe

```
infected : qt_ca.qm.Jub3Ee9tNMK1Wy0PRwuVT0lVJ3J66dE_nZasfwkS8iY.hive
original : qt_ca.qm
Jub3Ee9tNMK1Wy0PRwuVT0lVJ3J66dE_nZasfwkS8iY
11627
29/49  :

infected : qt_de.qm.Jub3Ee9tNMK1Wy0PRwuVT4L3AX1Wjv5pcaa8i3iYAV0.hive
original : qt_de.qm
Jub3Ee9tNMK1Wy0PRwuVT4L3AX1Wjv5pcaa8i3iYAV0
11047
30/49  :
```

C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
original : _ssl.pyd
9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb
10818
NBS : 10818  enc_iter : 9
128/131  :

infected : _yaml.pyd.9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_20HojIK9gfRq-EjhG2wxv.uj1ps
original : _yaml.pyd
9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg_20HojIK9gfRq-EjhG2wxv
10666
NBS : 10666  enc_iter : 19
129/131  :
```

C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
10783
NBS : 10783  enc_iter : 18
127/131  :

infected : _ssl.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0.fayg2
original : _ssl.pyd
UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0
10818
NBS : 10818  enc_iter : 9
128/131  :

infected : _yaml.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_j0dblyk4cUc0.fayg2
original : _yaml.pyd
UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_j0dblyk4cUc0
10666
NBS : 10666  enc_iter : 19
129/131  :
```

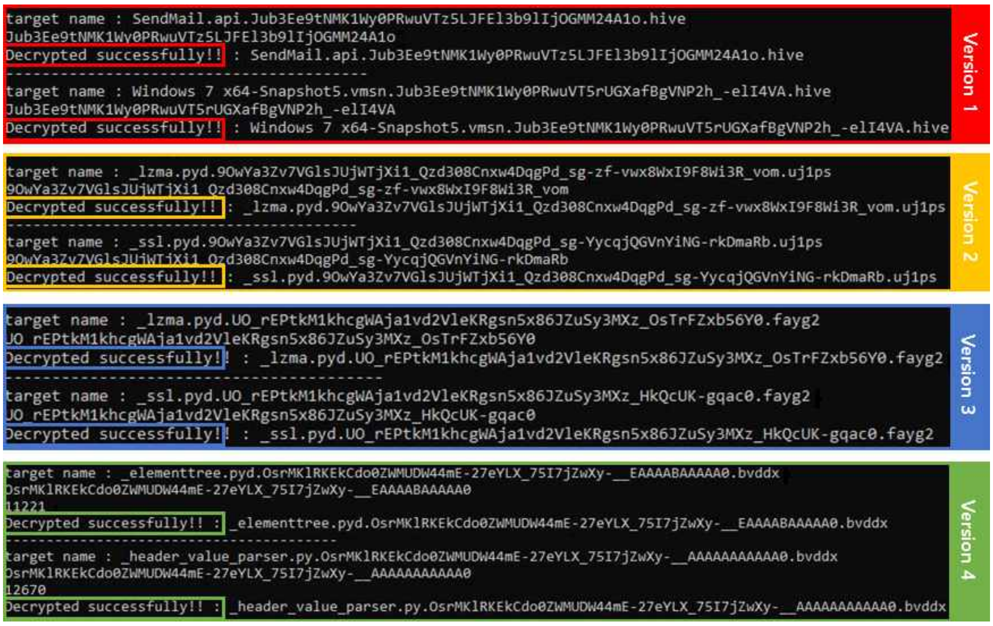
C:\Users\82104\Desktop\Hive Ransomware Integrated Decryption Tool.exe

```
NBS : 10004  enc_iter : 54
2/9  :

infected : ransomware attack figures.xlsx.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0.bvddx
original : ransomware attack figures.xlsx
OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__OAAAADgAAAA0
9695
NBS : 9695  enc_iter : 113
3/9  :

infected : ransomware attack path.png.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
original : ransomware attack path.png
OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0
6858
NBS : 6858  enc_iter : 2
4/9  :
```

When encryption key recovery is completed, decryption is performed targeting the files in the ‘3_recovery_target_files’ folder. For files that have been successfully decrypted, the string 'Decrypted successfully!!' is displayed in the window.



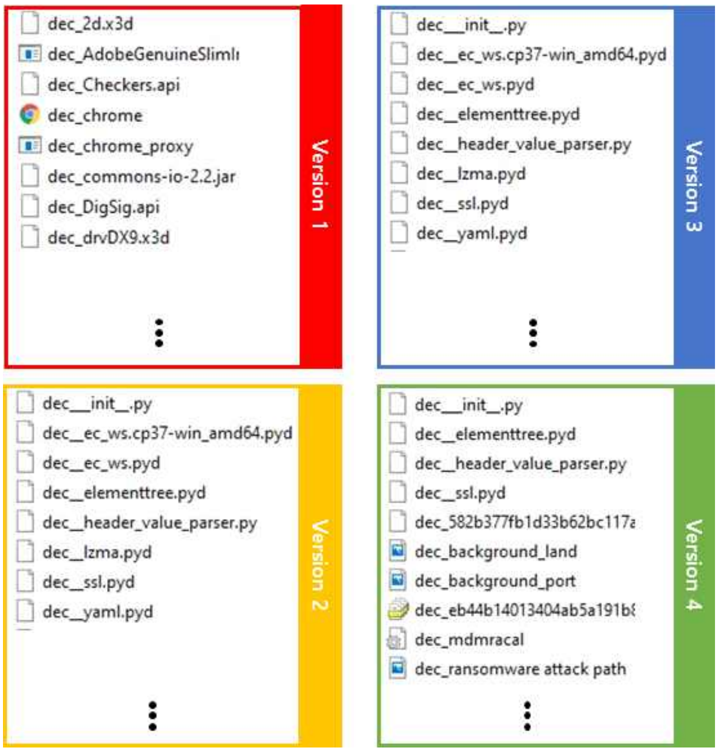
```
target name : SendMail.api.Jub3Ee9tNMK1Wy0PRwuVTz5LJFEl3b9lIjOGMM24A1o.hive
Jub3Ee9tNMK1Wy0PRwuVTz5LJFEl3b9lIjOGMM24A1o
Decrypted successfully!! : SendMail.api.Jub3Ee9tNMK1Wy0PRwuVTz5LJFEl3b9lIjOGMM24A1o.hive
----------------------------------------
target name : Windows 7 x64-Snapshot5.vmsn.Jub3Ee9tNMK1Wy0PRwuVT5rUGXafBgVNP2h_-elI4VA.hive
Jub3Ee9tNMK1Wy0PRwuVT5rUGXafBgVNP2h_-elI4VA
Decrypted successfully!! : Windows 7 x64-Snapshot5.vmsn.Jub3Ee9tNMK1Wy0PRwuVT5rUGXafBgVNP2h_-elI4VA.hive
```

```
target name : _lzma.pyd.9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-zf-vwx8WxI9F8Wi3R_vom.uj1ps
9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-zf-vwx8WxI9F8Wi3R_vom
Decrypted successfully!! : _lzma.pyd.9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-zf-vwx8WxI9F8Wi3R_vom.uj1ps
----------------------------------------
target name : _ssl.pyd.9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb.uj1ps
9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb
Decrypted successfully!! : _ssl.pyd.9OwYa3Zv7VGlsJUjWTjXi1_Qzd308Cnxw4DqgPd_sg-YycqjQGVnYiNG-rkDmaRb.uj1ps
```

```
target name : _lzma.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_OsTrFZxb56Y0.fayg2
UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_OsTrFZxb56Y0
Decrypted successfully!! : _lzma.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_OsTrFZxb56Y0.fayg2
----------------------------------------
target name : _ssl.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0.fayg2
UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0
Decrypted successfully!! : _ssl.pyd.UO_rEPtkM1khcgWAja1vd2VleKRgsn5x86JZuSy3MXz_HkQcUK-gqac0.fayg2
```

```
target name : _elementtree.pyd.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__EAAAABAAAAA0.bvddx
OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__EAAAABAAAAA0
11221
Decrypted successfully!! : _elementtree.pyd.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__EAAAABAAAAA0.bvddx
----------------------------------------
target name : _header_value_parser.py.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0
12670
Decrypted successfully!! : _header_value_parser.py.OsrMKlRKEkCdo0ZWMUDW44mE-27eYLX_75I7jZwXy-__AAAAAAAAAAA0.bvddx
```

When decryption is completed, the decrypted file is created in the ‘3_recovery_target_files’ folder. The string ‘dec_’ is added in front of the file name to distinguish it from an infected file.



dec_2d.x3d
dec_AdobeGenuineSlimI
dec_Checkers.api
dec_chrome
dec_chrome_proxy
dec_commons-io-2.2.jar
dec_DigSig.api
dec_drvDX9.x3d
⋮

dec__init__.py
dec__ec_ws.cp37-win_amd64.pyd
dec__ec_ws.pyd
dec__elementtree.pyd
dec__header_value_parser.py
dec__lzma.pyd
dec__ssl.pyd
dec__yaml.pyd
⋮

dec__init__.py
dec__ec_ws.cp37-win_amd64.pyd
dec__ec_ws.pyd
dec__elementtree.pyd
dec__header_value_parser.py
dec__lzma.pyd
dec__ssl.pyd
dec__yaml.pyd
⋮

dec__init__.py
dec__elementtree.pyd
dec__header_value_parser.py
dec__ssl.pyd
dec_582b377fb1d33b62bc117a
dec_background_land
dec_background_port
dec_eb44b14013404ab5a191b8
dec_mdmracal
dec_ransomware attack path
⋮

What is Hive Ransomware?

Hive Ransomware is a ransomware discovered in June 2021 and mainly attacks companies. It uses a variety of methods to penetrate the target system and distribute ransomwares. Currently, various strains are continuously being found, so special attention is needed to prevent infection.

Ransomware Integrated Decryption Tool User Manual

June, 2022

Published by KISA Korea Internet & Security Agency