Stop DJVU ransomware

Yuvaraj Rajendra and Shivam Mishra
pcl2016003@iiita.ac.in & mit2020122@iiita.ac.in
Network Security and Cryptography (NSC) Lab
Indian Institute of Information Technology, Allahabad

Overview:

Introduction

Stop DJVU ransomware is the most widely spread file encrypting virus in 2022. This ransomware comes in various versions and encrypts files using RSA cryptography. The encrypted files are saved with various extensions(like uihj, fefg, nnuz, bbnm, rrbb etc). These ransomware enters computers through cracked softwares, and games.

Immediate measures

1. Disconnect your system from the internet to prevent spread across the networked devices. Pen drives connected to the affected system shouldn't be used elsewhere as it may infect them.
2. Consider your system is compromised. And take the following measures.
    a. Reset all your saved passwords in all your browsers.
    b. Reset passwords that are stored in files, if any.
    c. When running recovery tools don't store the recovered data on the hard disk that contains encrypted data. In general, don't create any new files (avoid copying data) as it may hinder our data recovery process in later stages.
    d. The ransomware in your system is active and needs to be disabled first. To do that you can use any up to date malware removal tool or anti virus software. Depending on the extension used, you can identify the ransomware variant and find help online to disable the virus. But remember these viruses create backdoors for various attack vectors. So we strongly recommend using updated antivirus tools. Perform an entire system scan to detect and quarantine the malicious programs.
    e. Never pay money to the attacker. As it can be misused for other illegal activities or your money may go vain.

Data Recovery from backups:

If you have a backup in your system you can restore the un-encrypted files from your computer.

Data Decryption:

Keys used for encryption are of two types.

Online key: The ransomware after entering your system tries to contact the attackers web server and requests for a key. If successfully contacted your data is encrypted with the remotely generated key. In this case your data can't be decrypted. But can be recovered in other ways. [link]

Offline key: If the ransomware is not able to contact the attacker, it generates a key locally and shares with the attacker later. This offline key is used for encrypting your data.
In this case, victims can use the stop djvu tool [link]. The developers of this tool collect various keys used by this ransomware in a repository. If the used key exists in this repository, this tool decrypt**s** your data. If it is not available, then we have to wait until the key is added to the repository by other users.

Data Recovery Tools:

Victims can use data recovery tools to recover the data from the hard disk. When you delete data from your hard disk. The data is not deleted but it is marked as deleted so the Operating System uses the space to write new data in this marked space. Data recovery tools exploit this property to recover the data. The stop djvu virus encrypts the copies of files. After encryption the original files are deleted. This means we can recover the data unless it is overwritten by new data. To avoid overwriting the deleted data, we should stop creating new data(files) in your system. Running your system creates new files in the main drive that is where your OS is installed. So for the rest of this writeup, we work on the images of your harddisk. Images are nothing but snapshots of your hard disk. It captures the state of your hard disk. Snapshots or images can be created using the command dd or photorec. Multiple data recovery tools like photorec, recuva, easeus etc exist online. Tools like easeus are efficient for NTFS file systems. You can use these data recovery tools to work on the images and recover the data.
It is always better to immediately take the snapshot(images) of the hard disk drives and work on them instead of the system itself as running these tools causes further loss of data by overwriting. All the data can't be recovered. Some of the data may be corrupted or damaged due to overwriting.

Recovering large files: Fortunately the ransomware encrypts only the starting few bytes of a file and not the entire file. Larger files like zip, mp4, VDI etc can be recovered. For repairing VDI images you can follow the below method we used.

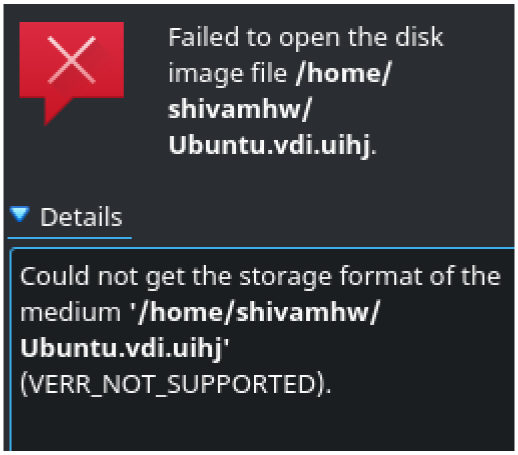
Recovering VDI Image

Files we had

1. Ubuntu.vdi (referred as ubuntu_encr from here) : The ransomware encrypted this file and it has a uihj extension (part of Djvu ransomware class). Supposedly some part of the header was corrupted but the exact number of encrypted bytes was unknown.
2. Ubuntu_recovered.vdi (referred as ubuntu_shadow from here) : This file was recovered from the Windows VSS system using a free utility called shadow explorer. This was supposed to be a clean un-encrypted image of the VDI, But after examining its content using *strings* commands, no ascii text was found (img attached in 2nd step of initial examination). So it must have been corrupted since the partition was almost and it was a 37GB file so it might be possible that other parts of the recovered image could have been overwritten.

Initial Examination

1. Since the original vbox file was missing, we created a dummy virtual machine in oracle virtual box (same version as well as the latest version of virtual box was used) and attached both of the vdi's to the machine. But both of them gave the same error.
2. The next step was to somehow mount the image and try to extract the file system, to do that we tried following on both the VDI's

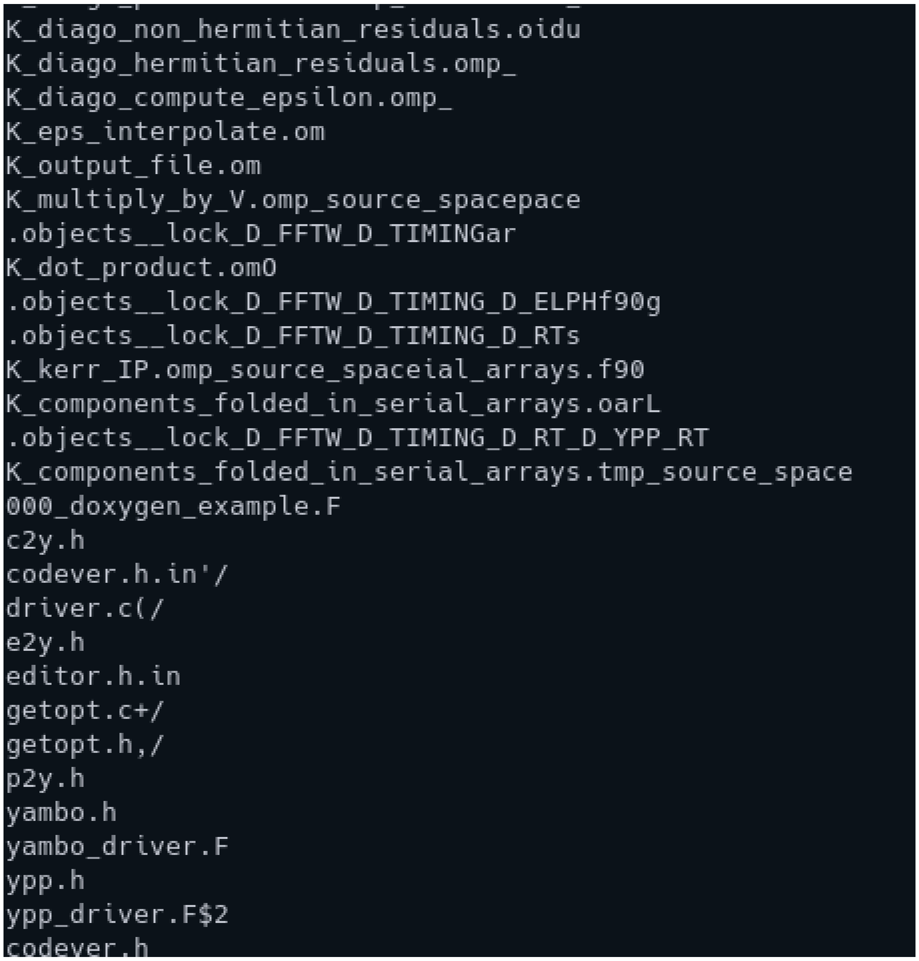
   

   Failed to open the disk image file **/home/shivamhw/Ubuntu.vdi.uihj**.

   Could not get the storage format of the medium '**/home/shivamhw/Ubuntu.vdi.uihj**' (VERR_NOT_SUPPORTED).

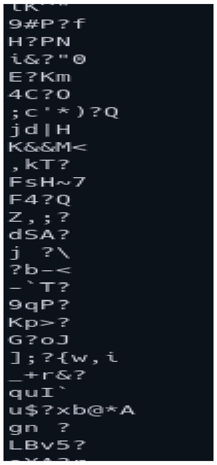
   a. *VBoxManage clonehd --format RAW ubuntu.vdi ubuntu.img* command on linux to try to convert the vdi to standard img file so it could be used with other tools like mount and poweriso. (Got error)
   b. Used *sudo vdfuse -a -f /path-to-vdi-file /mnt* command to directly mount the vdi to the linux system. (error)
   c. Used extracting utilities like 7z to extract something from the VDIs (failed)
   d. Used poweriso in windows (failed)
3. Nothing was working on both the images at first so we dug further using standard *strings* commands.

a. Using strings on ubuntu_encr fetched some recognizable ascii string as well as text that was visible in the strings output.



```
K_diago_non_hermitian_residuals.oidu
K_diago_hermitian_residuals.omp_
K_diago_compute_epsilon.omp_
K_eps_interpolate.om
K_output_file.om
K_multiply_by_V.omp_source_spacepace
.objects__lock_D_FFTW_D_TIMINGar
K_dot_product.omO
.objects__lock_D_FFTW_D_TIMING_D_ELPHf90g
.objects__lock_D_FFTW_D_TIMING_D_RTs
K_kerr_IP.omp_source_spaceial_arrays.f90
K_components_folded_in_serial_arrays.oarL
.objects__lock_D_FFTW_D_TIMING_D_RT_D_YPP_RT
K_components_folded_in_serial_arrays.tmp_source_space
000_doxygen_example.F
c2y.h
codever.h.in'/
driver.c(/
e2y.h
editor.h.in
getopt.c+/
getopt.h,/
p2y.h
yambo.h
yambo_driver.F
ypp.h
ypp_driver.F$2
codever.h
```

b. Using strings on ubuntu_shadow fetched nothing but garbage

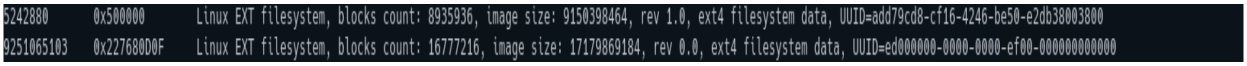


```
9#P?f
H?PN
i&?"@
E?Km
4C?O
;c'*)?Q
jd|H
K&&M<
,kT?
FsH~7
F4?Q
Z,;?
dSA?
j  ?\
?b-<
-`T?
9qP?
Kp>?
G?oJ
];?{w,i
_+r&?
quI`
u$?xb@*A
gn  ?
LBv5?
```

2. It was obvious that the file recovered from shadow explorer was corrupted beyond repair so we moved to the ubuntu_encr file to recover the data.

Recovering data from ubuntu_encr

After further inspection, it was noted that the header part of the file was corrupted but the file system and text files were intect (analyzed from strings output and hex editor output). So we focused our attention on extracting the ext file system that was there on the vdi.
Running *binwalk* on img got promising results as it was able to identify two filesystem partition, (swap and root filesystem)



```
5242880      0x500000      Linux EXT filesystem, blocks count: 8935936, image size: 9150398464, rev 1.0, ext4 filesystem data, UUID=add79cd8-cf16-4246-be50-e2db38003800
9251065103   0x227680D0F   Linux EXT filesystem, blocks count: 16777216, image size: 17179869184, rev 0.0, ext4 filesystem data, UUID=ed000000-0000-0000-ef00-000000000000
```

1. Using binwalk extraction utility however failed, Used binwalk –dd commands which fetched nothing but blocks of bytes.
2. Tried dd to get partition out of main vdi file using *dd if=Ubuntu.vdi.uihj of=f_par skip=5242880 count=<count> iflag=skip_bytes,count_bytes status=progress bs=4M* command from which we got a file which was getting identified as a ext4 filesystem.
3. Tried to mount the file but failed, used *e2fsck* on the extracted file to repair the file system. Got superblocks but repair failed a few times, even when repair got successful, mounting still failed.

The success

After trying multiple software like cloneVDI this particular post caught our attention. (https://forums.virtualbox.org/viewtopic.php?f=6&t=78755) . After this the following steps were performed to extract the file successfully.

1. Create a new VDI of the same size from virtualbox.
2. Open ubuntu_encr and new_vdi in any hex editor (We used neo as fhred was giving error)
3. Copy starting bytes of new_vdi to ubuntu_encr (We used 600 bytes based on hit and trial)
4. Now save ubuntu_encr and load it to cloneVDI and restore the headers by clicking repair.
5. Now get the new VDI generated from cloneVDI and use 7z to extract the file systems.
6. In our case, We got two images from VDI, 0.img and 1.img. By using *file* command we could see the one was swap and the other one is ext4 file system.
7. Mount imgs to linux filesystem using standard *mount* commands.

Conclusion

Even after doing this, the new VDI was still not booting normally. we could only get the emergency recovery shell from grub. But the filesystem was fully intact and grub was working

fine. Also the virtual terminals (Ctrl+Alt+F1-F9) were working fine. So if you have encrypted your home dir with password, no need to worry.
This mostly worked because of the nature of the ransomware which only encrypted the header of the file. Also using cloneVDI to detect any valid VDI should be your first move.
Since the file that we were dealing with was quite large(37GB), each step was taking too much time to produce results. So have a clean backup and try to run multiple utilities on multiple fresh copies of the files. Also binwalk –dd worked in many situations but not in this one.

Preventive measures:

1. Don't use OS which are outdated like windows xp, 7, 8. Upgrade your system to a new OS with active security update support like windows 10, 11.
2. Scan your pen drives before opening files in them.
3. Never download third party software(games, free tools) online. Mostly they contain malicious code.
4. Always keep your system updated with the latest security patches.

Additional material:

1. Emsisoft releases new decryptor for STOP Djvu ransomware
2. How to Recover Ransomware Encrypted or Deleted Files - EaseUS
3. How to use the Emsisoft Decryptor for STOP Djvu
4. Recover Ransomware Encrypted Files
5. Free Ransomware Decryption Tool
6. PhotoRec Step By Step - CGSecurity
7. https://forums.virtualbox.org/viewtopic.php?f=6&t=78755
8. https://stackoverflow.com/questions/36530643/use-binwalk-to-extract-all-files
9. https://stackoverflow.com/questions/66398230/extract-only-one-file-type-with-binwalk
10. https://olinux.net/e2fsck/
11. https://forums.virtualbox.org/viewtopic.php?f=6&t=22422&start=1275