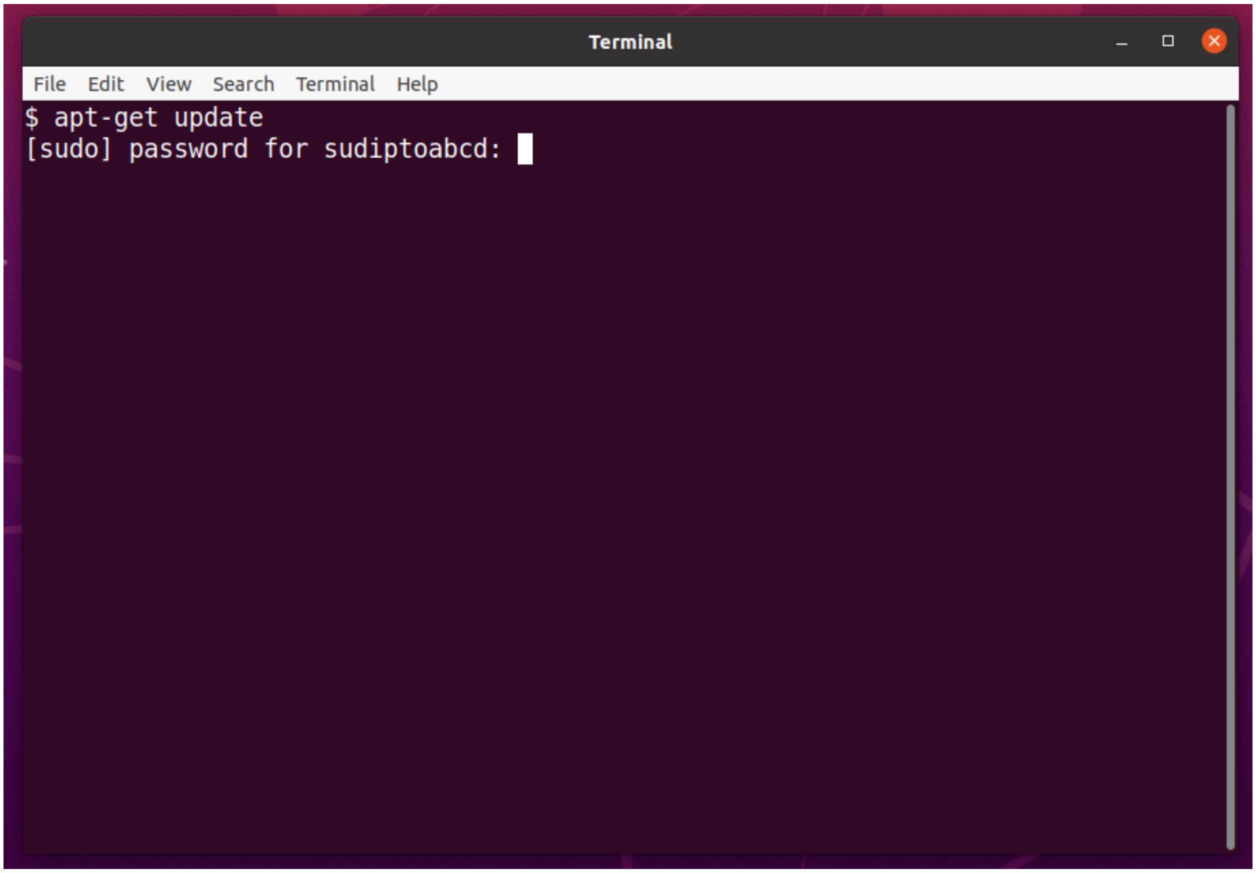
SNS Project

March 30, 2022

Working Flow

Attack 1: Sudo Password Extraction

1. Upon running studio.sh, a new terminal will be opened like this.

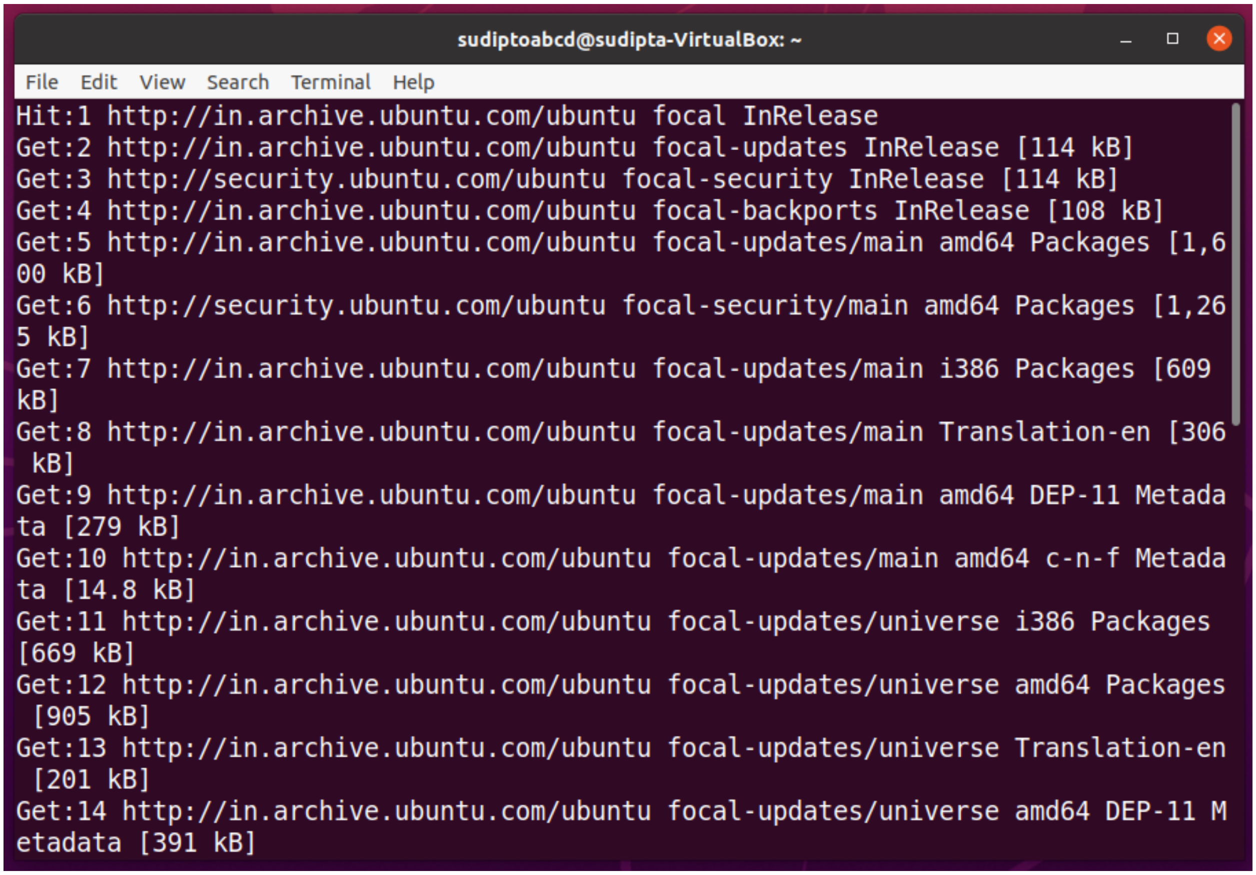


```
$ apt-get update
[sudo] password for sudiptoabcd: 
```

Figure 1

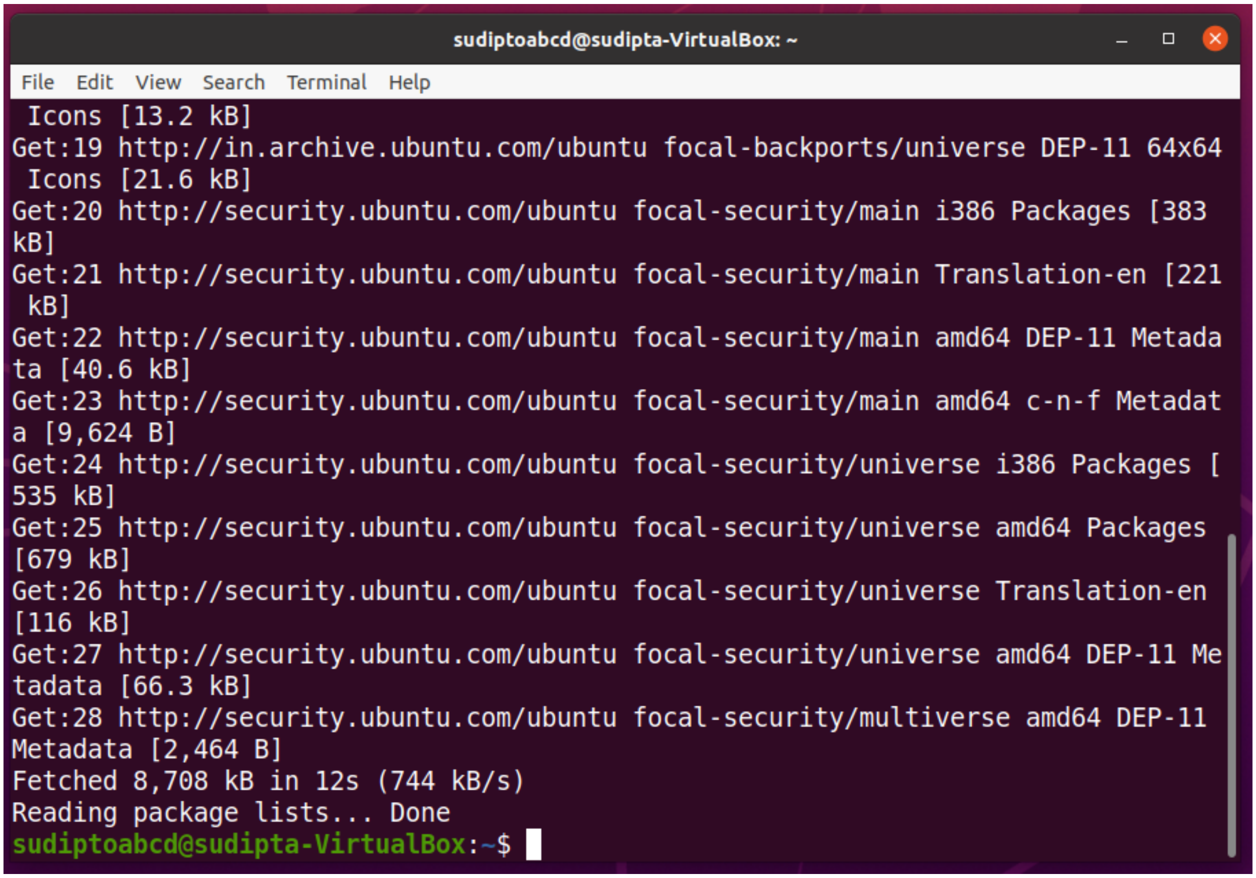
After a few hours of restarting the device, an update popup will ask for sudo password for the purpose of updating the system. User would suspect and close it or enter the wrong password, But the script would keep on popping after a few hours of every restart.

If the user enters the sudo password an update script **(Figure 2 and Figure 3)** will be called, making the user think it was an actual update script, and the popup will not start ever again. This Attack was for sudo password extraction.


sudiptoabcd@sudipta-VirtualBox: ~
File Edit View Search Terminal Help

```
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,6
00 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1,26
5 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [609
kB]
Get:8 http://in.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [306
 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metada
ta [279 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metada
ta [14.8 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages
[669 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages
 [905 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en
 [201 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 M
etadata [391 kB]
```

Figure 2


sudiptoabcd@sudipta-VirtualBox: ~
File Edit View Search Terminal Help

```
 Icons [13.2 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu focal-backports/universe DEP-11 64x64
 Icons [21.6 kB]
Get:20 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [383
kB]
Get:21 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [221
 kB]
Get:22 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metada
ta [40.6 kB]
Get:23 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadat
a [9,624 B]
Get:24 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [
535 kB]
Get:25 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages
[679 kB]
Get:26 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en
[116 kB]
Get:27 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Me
tadata [66.3 kB]
Get:28 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11
Metadata [2,464 B]
Fetched 8,708 kB in 12s (744 kB/s)
Reading package lists... Done
sudiptoabcd@sudipta-VirtualBox:~$
```

Figure 3

Attack 2: Ransomware

2. This Attack is independent of the previous attack. (i.e. This does not require a sudo password to run) Once the system restarts, all the files present in his PC with the following extensions will be encrypted (".jpg,.gif,.png,.pdf,.doc,.docx,.html,.htm,.css,.js,.xls,.xlsx,.xlsm,.txt,.avchd,.ppt,.pptx,.opd,.m4a,.mp3,.odt,.aif,.cda,.mid,.midi,.mpa,.ogg,.wav,.wma,.wpl,.7z,.arj,.deb,.pkg,.rar,.rpm,.tar.gz,.zip,.dmg,.iso,.toast,.vcd,.csv,.dat,.db,.dbf,.log,.mdb,.sav,.sql,.tar,.xml,.email,.eml,.emlx,.msg,.oft,.ost,.pst,.vcf,.apk,.bat,.bin,.cgi,.com,.exe,.gadget,.msi,.wsf,.jpeg,.ico,.php,.xhtml,.ods,.3g2,.avi,.flv,.h264,.m4v,.mkv,.mov,.mp4,.mpg,.mpeg,.rm,.swf,.vob,.wmv,.rtf,.tex,.wpd")

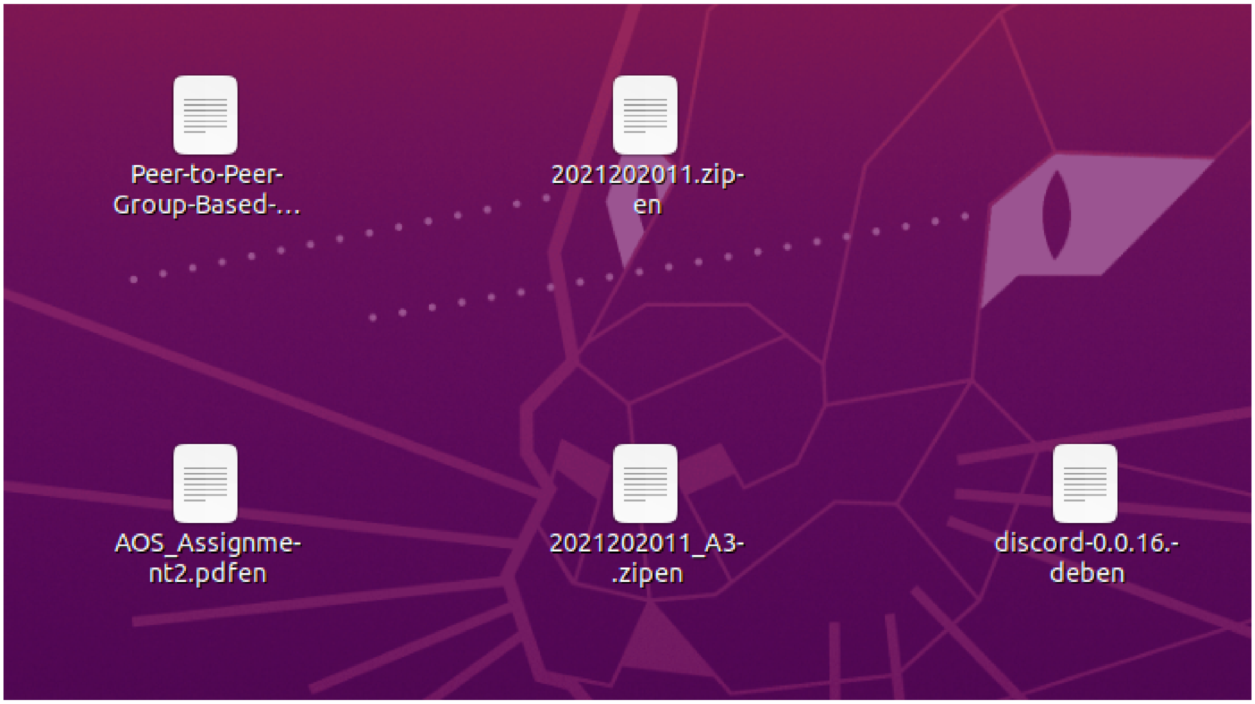
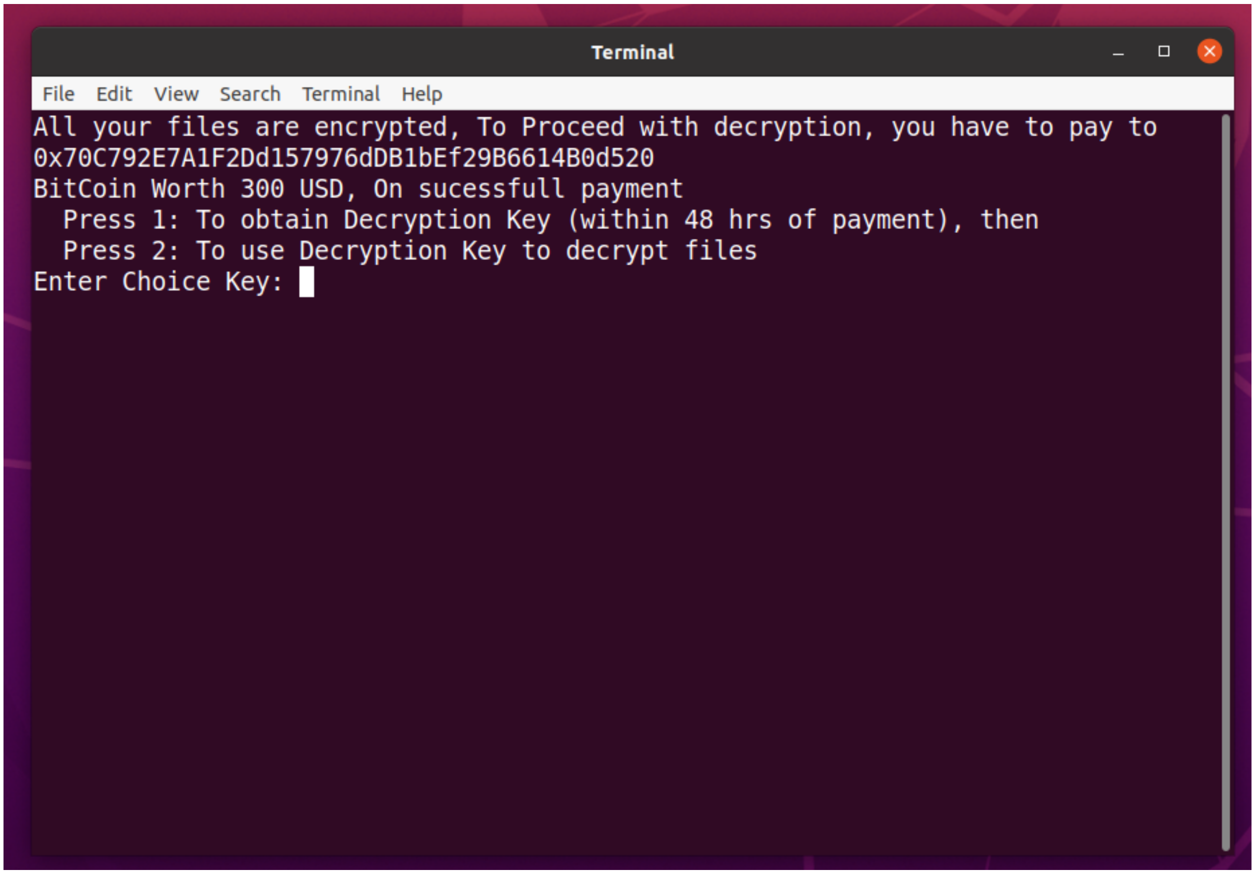


Figure 4

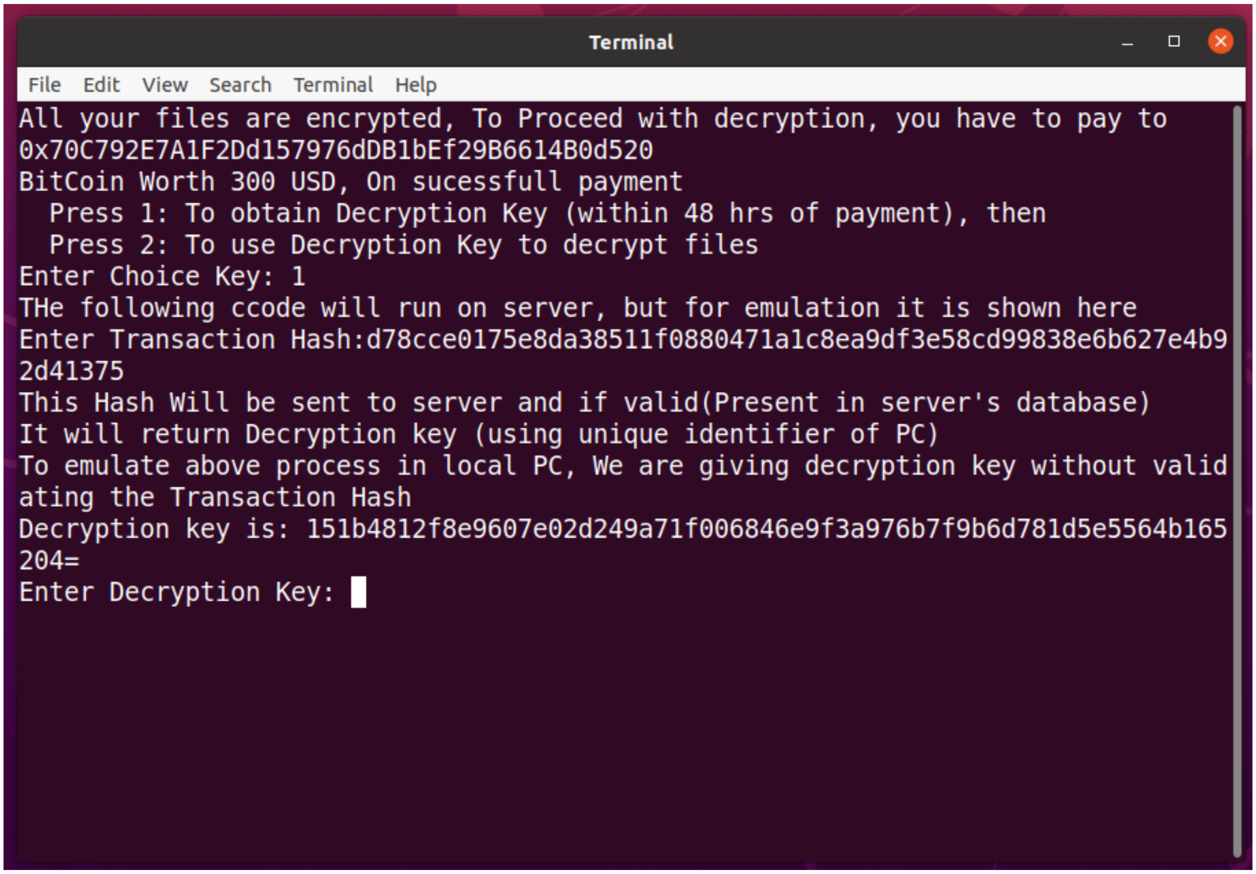
3. To generate the encryption key we have passed user's PC's unique identifier to Pseudo random function generator (PRF) as seed and only the server has the PRF, making it difficult for the user to get this value even if it has the user PC's unique identifier. The output of this PRF is sent to SHA256 and that acts as an encryption key. On next restart user will be prompted to pay to obtain the decryption key.



```
All your files are encrypted, To Proceed with decryption, you have to pay to
0x70C792E7A1F2Dd157976dDB1bEf29B6614B0d520
BitCoin Worth 300 USD, On sucessfull payment
  Press 1: To obtain Decryption Key (within 48 hrs of payment), then
  Press 2: To use Decryption Key to decrypt files
Enter Choice Key: 
```

Figure 5

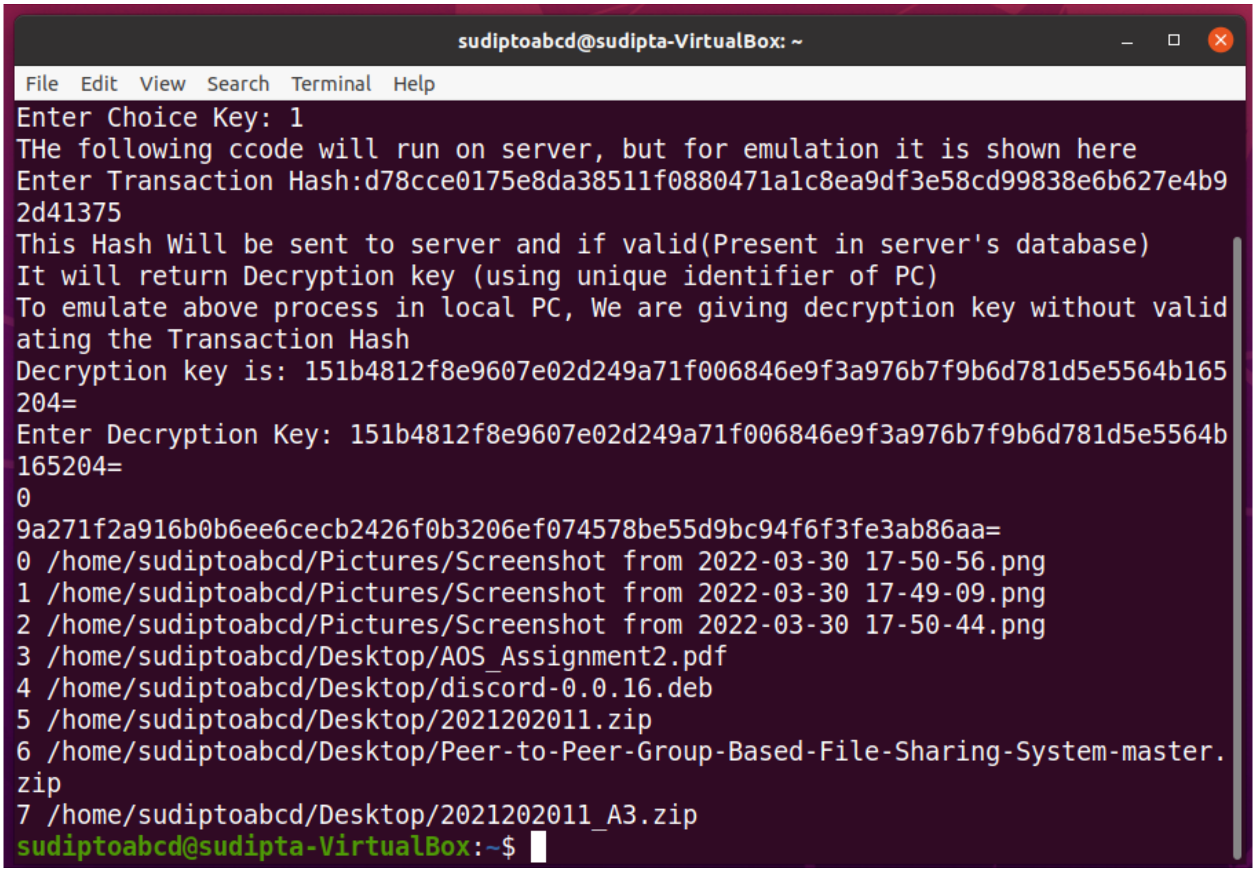
4. User has two choices after this. By pressing ‘2’, he can enter his keys to decrypt the files. But after 3 unsuccessful attempts, all the encrypted files will be deleted. If he does the payment and within 48 hours of payment if he presses 1, he would be asked to enter the transaction hash.



```
All your files are encrypted, To Proceed with decryption, you have to pay to
0x70C792E7A1F2Dd157976dDB1bEf29B6614B0d520
BitCoin Worth 300 USD, On sucessfull payment
  Press 1: To obtain Decryption Key (within 48 hrs of payment), then
  Press 2: To use Decryption Key to decrypt files
Enter Choice Key: 1
THe following ccode will run on server, but for emulation it is shown here
Enter Transaction Hash:d78cce0175e8da38511f0880471a1c8ea9df3e58cd99838e6b627e4b9
2d41375
This Hash Will be sent to server and if valid(Present in server's database)
It will return Decryption key (using unique identifier of PC)
To emulate above process in local PC, We are giving decryption key without valid
ating the Transaction Hash
Decryption key is: 151b4812f8e9607e02d249a71f006846e9f3a976b7f9b6d781d5e5564b165
204=
Enter Decryption Key: 
```

Figure 6

5. On successful verification at the server end, he would be given the decryption key to decrypt the files. He would be asked to type the decryption key that he obtained. Upon typing the correct decryption key, the files in his system will be decrypted [Figure 7].


sudiptoabcd@sudipta-VirtualBox: ~
File Edit View Search Terminal Help

```
Enter Choice Key: 1
THe following ccode will run on server, but for emulation it is shown here
Enter Transaction Hash:d78cce0175e8da38511f0880471a1c8ea9df3e58cd99838e6b627e4b9
2d41375
This Hash Will be sent to server and if valid(Present in server's database)
It will return Decryption key (using unique identifier of PC)
To emulate above process in local PC, We are giving decryption key without valid
ating the Transaction Hash
Decryption key is: 151b4812f8e9607e02d249a71f006846e9f3a976b7f9b6d781d5e5564b165
204=
Enter Decryption Key: 151b4812f8e9607e02d249a71f006846e9f3a976b7f9b6d781d5e5564b
165204=
0
9a271f2a916b0b6ee6cecb2426f0b3206ef074578be55d9bc94f6f3fe3ab86aa=
0 /home/sudiptoabcd/Pictures/Screenshot from 2022-03-30 17-50-56.png
1 /home/sudiptoabcd/Pictures/Screenshot from 2022-03-30 17-49-09.png
2 /home/sudiptoabcd/Pictures/Screenshot from 2022-03-30 17-50-44.png
3 /home/sudiptoabcd/Desktop/AOS_Assignment2.pdf
4 /home/sudiptoabcd/Desktop/discord-0.0.16.deb
5 /home/sudiptoabcd/Desktop/2021202011.zip
6 /home/sudiptoabcd/Desktop/Peer-to-Peer-Group-Based-File-Sharing-System-master.
zip
7 /home/sudiptoabcd/Desktop/2021202011_A3.zip
sudiptoabcd@sudipta-VirtualBox:~$
```

Figure 7

6. He would get back his files like the following.

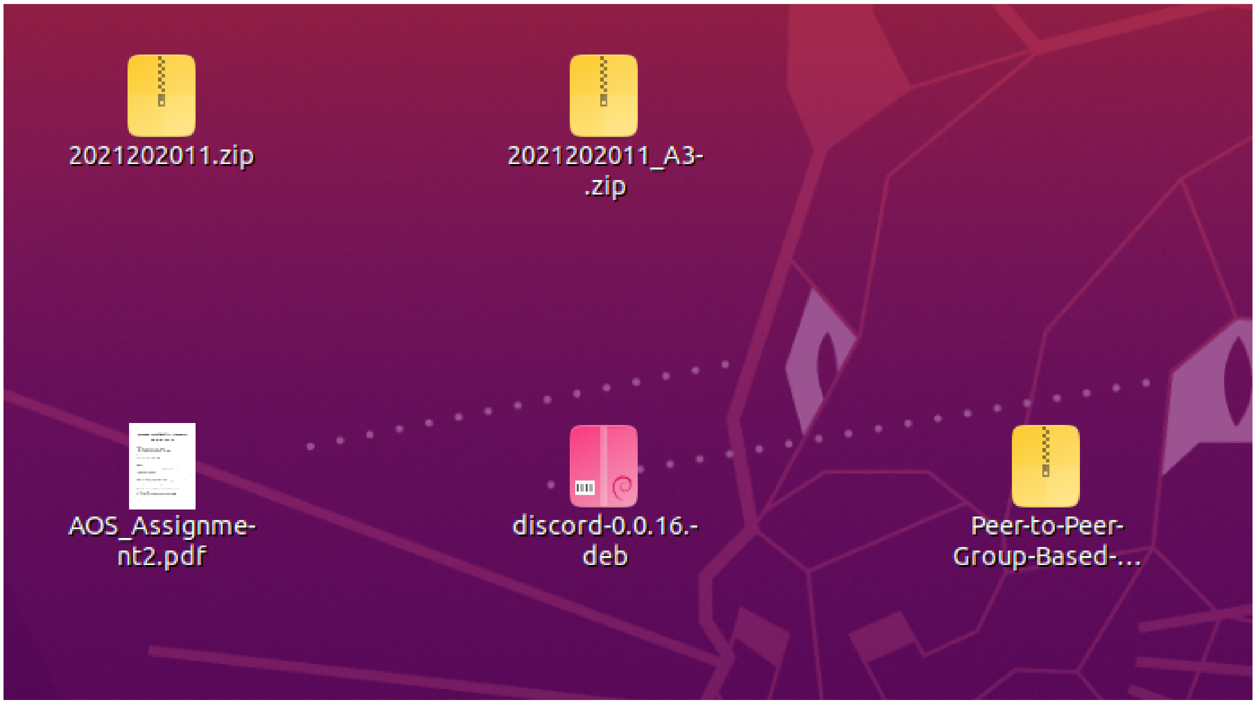
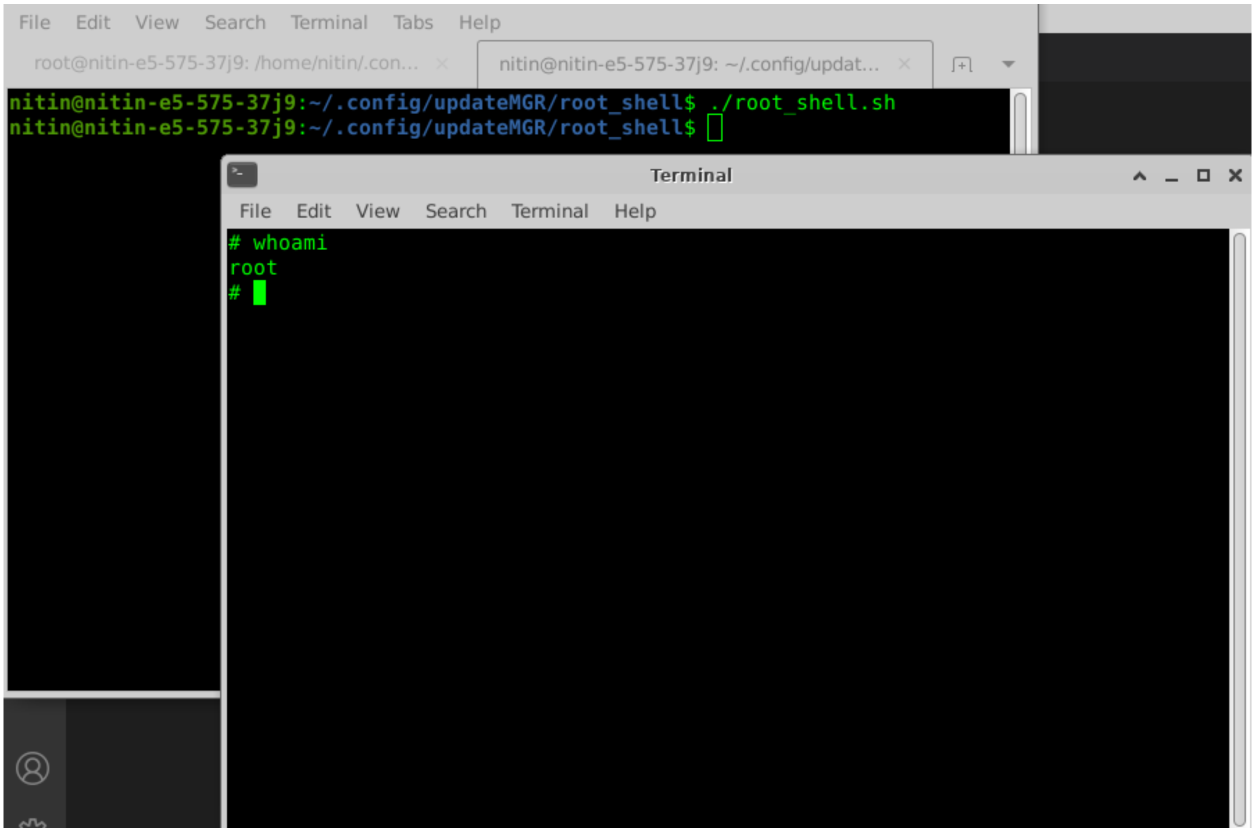


Figure 8

Attack 3: Root Shell

It will work only if the install script which was infected required root access. THe crontab entry can call a simple c++ program which causes stack overflow and shellcode is executed, and based on the file permission root shell is obtained [Figure 9].



File Edit View Search Terminal Tabs Help
root@nitin-e5-575-37j9: /home/nitin/.con...
nitin@nitin-e5-575-37j9: ~/.config/updat...
Terminal
File Edit View Search Terminal Help

```
nitin@nitin-e5-575-37j9:~/.config/updateMGR/root_shell$ ./root_shell.sh
nitin@nitin-e5-575-37j9:~/.config/updateMGR/root_shell$ 
```

```
# whoami
root
# 
```

Figure 9

The only defense against such attacks is to keep the crontab file in check and remove the entries if required using crontab -r .