CSCE 5550-001 Introduction to Computer Security

Project

Ransomware

Group-13

Sai Ashrith Gavini
Nikhil Makkena
Nikita Makkena
Sonu Sri Nenavath
Manasa Nimmagadda

1. Abstract

Ransomware is a type of malware which is a very fast-growing security threat that either locks a device or encrypts files on a target computer, making it impossible for the user to access them. The attacker then demands a ransom from the user in return for the key that unlocks the data, extorting them. It has received the majority of the public eye over the past couple of years because of many attacks that have taken place against highly established financial, education, municipalities, infrastructure, and healthcare institutions, which have been big targets. Some of the main causes of ransomware infections are lack of cyber security training, spamming or phishing emails, easy access management because of weak passwords, malicious websites, easy accessibility of malware kits which help in creating new types of malwares based on the demand in the world, use of web interpreters like JavaScript to create cross site scripting. These vectors of cyberattacks usually have a variety of attacking or infecting techniques like phishing, Drive-by downloading, Remote Desktop Protocol (RDP) compromise, and direct infiltration. To defend any system against these kinds of malware attacks, have your system files securely backed up into a secured location, make sure the system is up to date, use only secured networks etc. To achieve ransomware, in this project, we will be looking into phishing attack caused to any files or folder by infecting with malware. We have used monitoring, detection, and mitigation plans to detect and remove the malware infected into the files.

2. Introduction

Files on a computer are encrypted by ransomware, a sort of malware, making it hard for the user to access them. To obtain the key that unlocks the data, the attacker then extorts the user by requesting a ransom. In this project, we are trying to perform a ransomware attack by phishing email technique. We sent out an email with the subject line of free giveaway for thanksgiving. We then include the malicious executable link of malware in the email where the target user will have to click on the link to claim their gift. Once the recipient clicks on it, an executable will be downloaded automatically, and we are providing the steps to run the executable in the malicious web page that we have created. Once it is run, all the sub-directories in the main directory are encrypted. The target user must pay the ransom amount to get the secret key which is used to decrypt the files.

The steps used as approach for this project is divided into 5 components which are Action, Infection, Monitoring, Detection, and Mitigation. In Action component, we have written codes for encryption and decryption of the files and the encryption code has been converted into an executable one using PyInstaller. This executable code is sent to the target user as a link using phishing email. Once the user downloads and runs the malware in his system, the attack starts and encrypts all the files in the directory. In the Infection component, the target user runs the executable file that contains the malware, and all the data will get encrypted. In Monitoring component, the system will keep watching if any malware attacks are being injected into the system’s files using ‘inotifywait’. Here, in our project, we will keep an eye on the files in the "Downloads" directory while the malware is downloaded and begins the attack there, and we will send out an alert of a possible attack if any of the files are changed by any other source apart from the owner of the files, i.e., if the files are encrypted.

In the Detection component, if the files get infected with malware, monitoring module will give a pop-up about the malware attack and clean the entire folder by deleting all the files from that location. In the Mitigation component, using the ‘crontab’ scheduler, we backed up all the files into a root folder, as a zip file, which backs up all the files in the directory every day at 12am and when the malware detection happens and the whole folder gets deleted, the zip file containing original files from root folder will be copied over to the working folder for user’s convenience.

3. Related Works

3.1. WannaCry Ransomware Attack 2017

Many healthcare, educational, government, and corporate institutions have become victims of the largest ransomware attack occurred in 2017 where around 200,000 individual’s devices have been locked and ransom was demanded in order to regain access to their system data. This attack locks the system data and only leaves two files with directions of what the device owner should do to get the data back. Here, the system locked is because it has been encrypted and to decrypt, ransom is demanded by the users and once it is paid, the key to decrypt program will be given by attackers. Some of the preventive measures that the study proposed are keeping all the software, system, browsers, and anti-virus up to date; use only safe and reliable networks; do not click on spam or suspicious emails. As a conclusion, the study explains that easiest way for ransomware attack is by phishing emails, and it is required that individuals don not open suspicious emails and always make sure to back up their system data in a secured location. [9]

3.2. Study of ransomware attacks using web search logs

This study analyzed ransomware using a web search engine “BING” by making a machine learning algorithm to retrieve the queries searched by users that were attacked by ransomware. Using the obtained queries, they have performed a linked analysis based on geographical location and hourly time. The analysis explained the research team of Microsoft that, there has been particular features where the number of times a query had been searched and the number of clicks has been correlated with attacks. Further, they have researched on an attack called Nemty which is a type of ransomware infecting windows where the system data gets encrypted any hint of shadowed copies in the system will be deleted and the only way to restore the data was by paying the ransom to get the data decrypted. [7]

3.3. Comprehensive survey on ransomware attack: A growing Havoc cyberthreat

This study explains in a comprehensive basis about ransomware analysis and how these cryptographic techniques evolved as a threat through their operation modes and what preventive measures have to be taken to avoid falling into the traps of these attacks as they continue to grow widely among all parts of the world as a cyber-plague. Preventive measures the study suggests to keep systems safe from any malicious cyber-attacks is by backing data on a regular basis, have mail servers and file sharing mechanisms as less sophisticated as possible, using secured network, have awareness among users about cyber-attacks, disabling extra features of windows. To prevent the attackers from taking control of systems, all the anti-virus MNCs, security agencies, any research centers will have to always be leveled up to make sure any kind of attacks cannot infect systems. [6]

Survey of Crypto Ransomware attack detection methodologies: An evolving outlook

The study in this paper gives an insight into early observation of ransomware. The paper described that issue with early notice of attack will not give out enough behavioral patterns of the attack and if the mitigation has to be decided, then they will have to follow existing rigid approaches which will have a negative impact on the material. They have concluded that innovative approaches to investigate the likelihood of capturing data and support any kind of malicious software can be achieved by looking into the relation between any events that relate to process and the API. [8]

4. Approach

Ransomware requires to get access to a target system, encrypt the files inside, and then demand a ransom from the victim to function. Although the technical details differ from one ransomware variety to the next, our ransomware attack goes as follows when a device is exposed to the infected code:

4.1. Action

To implement the ransomware attack we need an encryption code to encrypt the files. The encryption code is written using Python programming language. Python has a cryptography library that enables us to encrypt and decrypt data. We have utilized Fernet cryptographic library available in Python3. The cryptography package's fernet module includes built-in functions for the creation of the key, encryption of plaintext into ciphertext, and decryption of ciphertext into plaintext using the encrypt and decode methods, respectively [1]. We have created “virus.py”, “decrypt.deb” files for this purpose. The python code for encryption is converted into an executable file using PyInstaller [2] which is then renamed as “GTA5.deb”. PyInstaller is a tool that freezes Python scripts into standalone executables for Windows, Linux, Mac OS X, FreeBSD, Solaris, and AIX. When this executable file is downloaded and installed in the target system, it encrypts the ‘.txt’ files present in the directory. The “decrypt.py” file decrypts the files using secret key which is given to the target user once the victim pays the ransom.

4.2. Infection

Like other viruses, ransomware can access a system of an organization in a variety of methods. However, the people who run ransomware frequently favor a few distinct infection channels. Phishing emails are one of these. Phishing is the practice of pretending to be a trustworthy organization, usually a website connected to a business, to steal passwords, credit card numbers, and other private information without consent. So, to infect the target system, we have crafted a phishing email saying that the target user is eligible for a free game download. This email has a link to the malicious website which contains our executable encryption code. The executable file, disguised as an executable of a game, gets downloaded into the target’s system once the user clicks on the link. To run the malware in the target system, the executable file's user rights must be properly [3]. So, the malicious website also displays the steps involved in installing the ‘game’ once the file is downloaded. By following the steps given on the website, the user rights of the file will be changed using ‘chmod 777’ command and then the executable file containing the encryption code is run in the terminal. Once the commands are executed by the target user, the ransomware attack begins and encrypts all the text files present in the directory.

To retrieve the victim’s files, we, the owner of the ransomware will give a copy of the secret key if the demanded ransom is paid. The key is then entered in the terminal by the target user after executing the “decrypt.deb” file to undo the encryption and allow the user to access their files once again.

4.3. Monitoring and Detection

Ransomware attack can be avoided by monitoring and detecting suspicious behavior or unauthorized system changes, security monitoring entails gathering and evaluating information. It also requires deciding which sorts of conduct should result in alerts and responding to those alerts as necessary. Here, in our project, we will be monitoring the files in ‘Downloads’ directory as the malware is getting downloaded and starting the attack in that directory and create an alert if the files in it are modified.

We are using bash script named ‘prevention.sh’ to accomplish monitoring of the files and detecting the attack in the directory. The bash script should be up and running all the time. To run the script, we will be giving user rights by utilizing ‘chmod 777’ command and then run it. In this script, we are using ‘inotifywait’ which uses the ‘inotify’ interface in Linux to effectively wait for file changes. The ‘inotifywait’ [4] works well for monitoring file changes made by shell scripts. Either it can stop running after an event occurs or it can keep running and output events as they happen. To execute this, in the shell script, we are storing the location of the file which is to be monitored in a variable. To monitor the events of the files. i.e., to monitor the files if they are modified, opened, closed etc., we are using ‘modify’ event. When any user apart from the owner of the files tries to modify the data in the files, an alert will pop-up on the screen of the user as “Some One tried to hack you so we stopped him and removed the malware.”. This pop-up is being displayed by using the ‘zenity’ UI package [5]. When the pop-up appears that the attack happens, we click on the ‘OK’ button and all the files in the directory are removed.

4.5. Mitigation

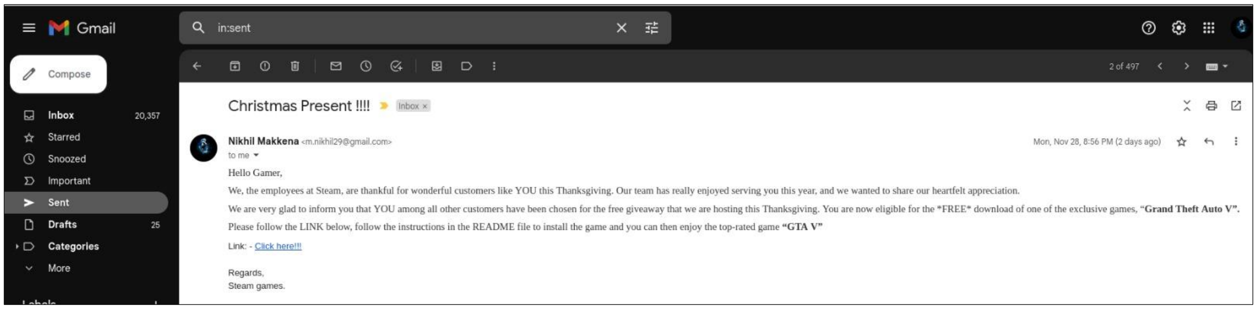
To reduce the impact of ransomware attack, it is important to cautiously design the networks, systems, and backups. The mitigation component that we are using in our project is by backing up all the files in the directory at a regular interval of 24 hours i.e., every day at 12am the files are being backed up in the root folder. This is achieved we have created ‘crontab’. Using the UNIX command crontab, we can compile a set of commands into a table that the operating system will run one by one at predetermined intervals.

When the attack happens, the pop-up displays, the files are changed due to encryption, "inotifywait" notices the changes and notifies the user that an attack has occurred. When the attack occurs, we remove every file in the target directory including the malware executable file to stop the attack. We are restoring this zip file, which is the back-up file, from the root folder to its original location in the "Downloads" directory for the user's convenience. We were able to remove the malware and restore our data to their original directory as a result. So, the files are being regularly backed up in the original directory. After the attack takes place, an alert is sent to the user and all the backed-up files in the directory are removed and the zip file which is being backed-up in regular intervals is then restored in the original directory after removing the malware.

5. Results

5.1. Action

The phishing email with the malicious link is displayed below:



Christmas Present !!!!

Nikhil Makkena <m.nikhil29@gmail.com>
to me
Mon, Nov 28, 8:56 PM (2 days ago)

Hello Gamer,

We, the employees at Steam, are thankful for wonderful customers like YOU this Thanksgiving. Our team has really enjoyed serving you this year, and we wanted to share our heartfelt appreciation.

We are very glad to inform you that YOU among all other customers have been chosen for the free giveaway that we are hosting this Thanksgiving. You are now eligible for the *FREE* download of one of the exclusive games, **"Grand Theft Auto V".**

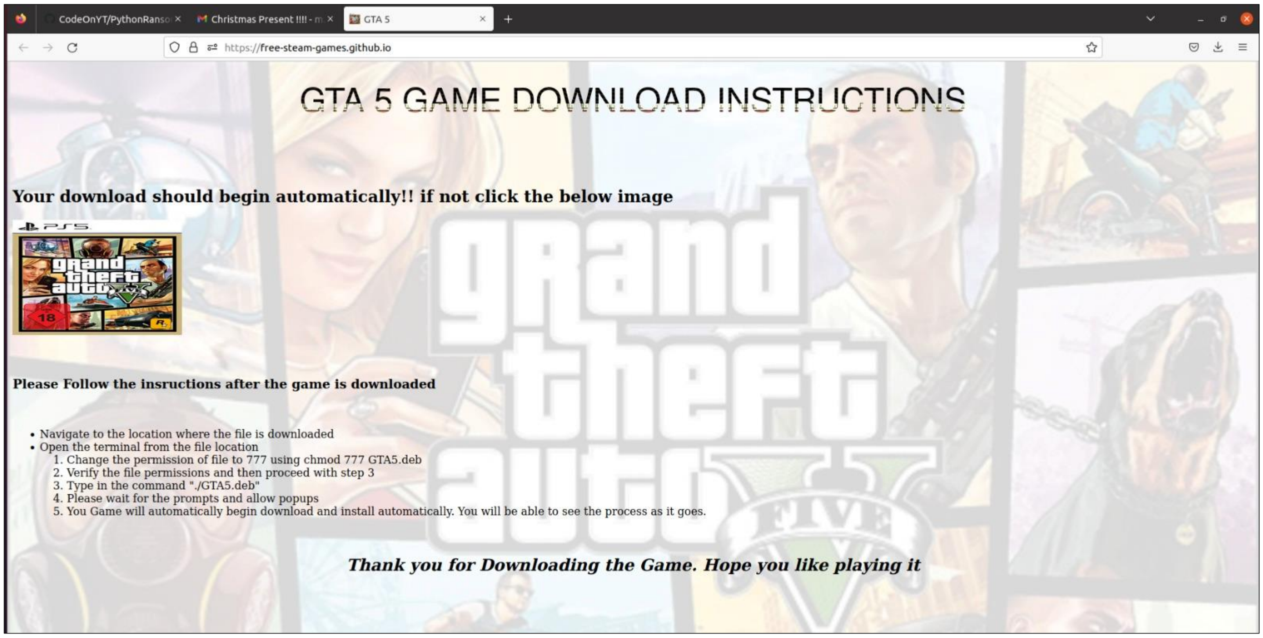
Please follow the LINK below, follow the instructions in the README file to install the game and you can then enjoy the top-rated game **"GTA V"**

Link: - Click here!!!

Regards,
Steam games.

Figure 5.1.1. The phishing email with the malicious link

The malicious webpage containing the installation steps once the file is downloaded:



CodeOnYT/PythonRanso
Christmas Present !!!! - m
GTA 5
https://free-steam-games.github.io
PS5
grand theft auto
18
FIVE

GTA 5 GAME DOWNLOAD INSTRUCTIONS

Your download should begin automatically!! if not click the below image

Please Follow the insructions after the game is downloaded

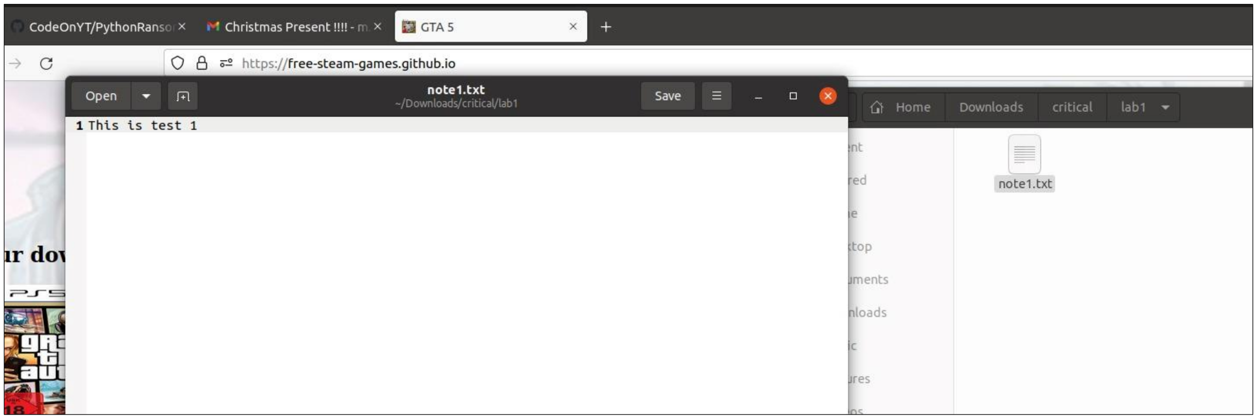
- Navigate to the location where the file is downloaded
- Open the terminal from the file location
  1. Change the permission of file to 777 using chmod 777 GTA5.deb
  2. Verify the file permissions and then proceed with step 3
  3. Type in the command "./GTA5.deb"
  4. Please wait for the prompts and allow popups
  5. You Game will automatically begin download and install automatically. You will be able to see the process as it goes.

Thank you for Downloading the Game. Hope you like playing it

Figure 5.1.2. The malicious webpage containing the installation steps

5.2. Infection

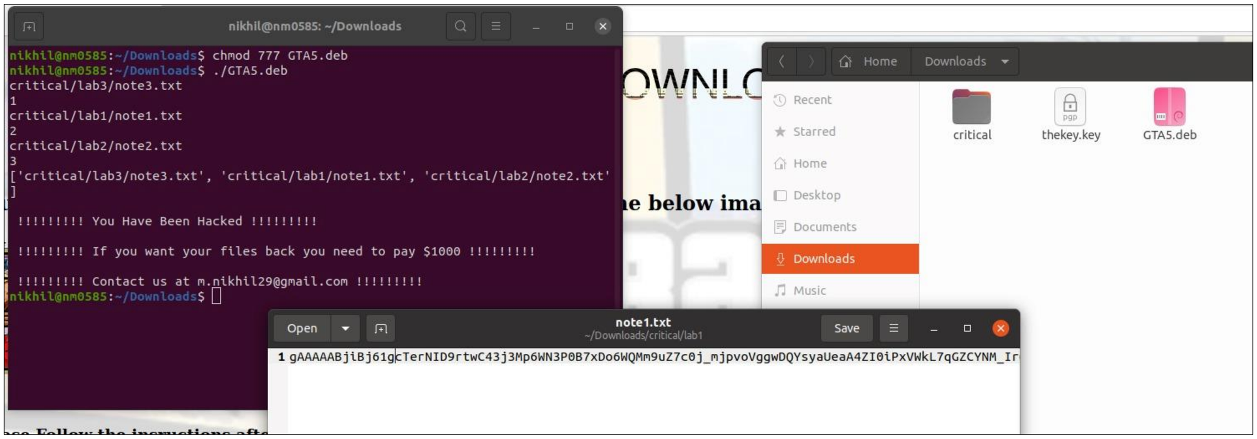
Contents of the one of files before encryption:


CodeOnYT/PythonRanso
Christmas Present !!!! - m
GTA 5
https://free-steam-games.github.io
Open
note1.txt
~/Downloads/critical/lab1
Save
Home
Downloads
critical
lab1
note1.txt

```
This is test 1
```

Figure 5.2.1. Contents of the ‘note1.txt’ file in ‘lab1’ folder before encryption

Messages displaying that the attack has happened and asking for ransom. Contents of the files are encrypted as shown below:

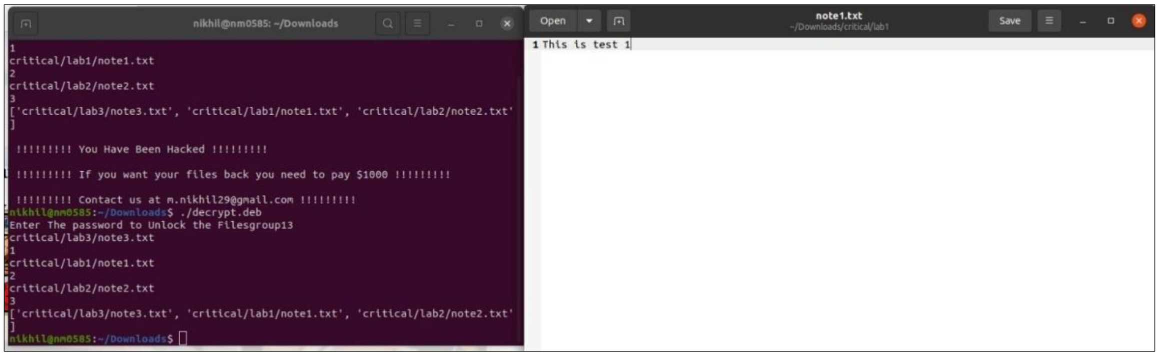


```
nikhil@nm0585:~/Downloads$ chmod 777 GTA5.deb
nikhil@nm0585:~/Downloads$ ./GTA5.deb
critical/lab3/note3.txt
1
critical/lab1/note1.txt
2
critical/lab2/note2.txt
3
['critical/lab3/note3.txt', 'critical/lab1/note1.txt', 'critical/lab2/note2.txt'
]

 !!!!!!!!! You Have Been Hacked !!!!!!!!!

 !!!!!!!!! If you want your files back you need to pay $1000 !!!!!!!!!

 !!!!!!!!! Contact us at m.nikhil29@gmail.com !!!!!!!!!
nikhil@nm0585:~/Downloads$
```

```
gAAAAABjiBj61gcTerNID9rtwC43j3Mp6WN3P0B7xDo6WQMm9uZ7c0j_mjpvoVggwDQYsyaUeaA4ZI0iPxVWkL7qGZCYNM_Ir
```

Figure 5.2.2. Contents of the ‘note1.txt’ file in ‘lab1’ folder after encryption

Contents of the file have been restored to original after entering the secret key for decryption:



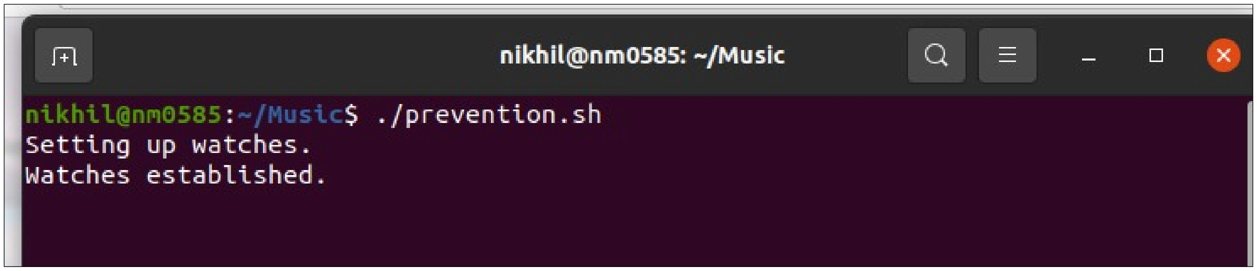
```
1
critical/lab1/note1.txt
2
critical/lab2/note2.txt
3
['critical/lab3/note3.txt', 'critical/lab1/note1.txt', 'critical/lab2/note2.txt'
]

 !!!!!!!!! You Have Been Hacked !!!!!!!!!

 !!!!!!!!! If you want your files back you need to pay $1000 !!!!!!!!!

 !!!!!!!!! Contact us at m.nikhil29@gmail.com !!!!!!!!!
nikhil@nm0585:~/Downloads$ ./decrypt.deb
Enter The password to Unlock the Filesgroup13
critical/lab3/note3.txt
1
critical/lab1/note1.txt
2
critical/lab2/note2.txt
3
['critical/lab3/note3.txt', 'critical/lab1/note1.txt', 'critical/lab2/note2.txt'
]
nikhil@nm0585:~/Downloads$
```

```
This is test 1
```

Figure 5.2.3. Contents of the ‘note1.txt’ file in ‘lab1’ folder after decryption

5.3. Monitoring and Detection

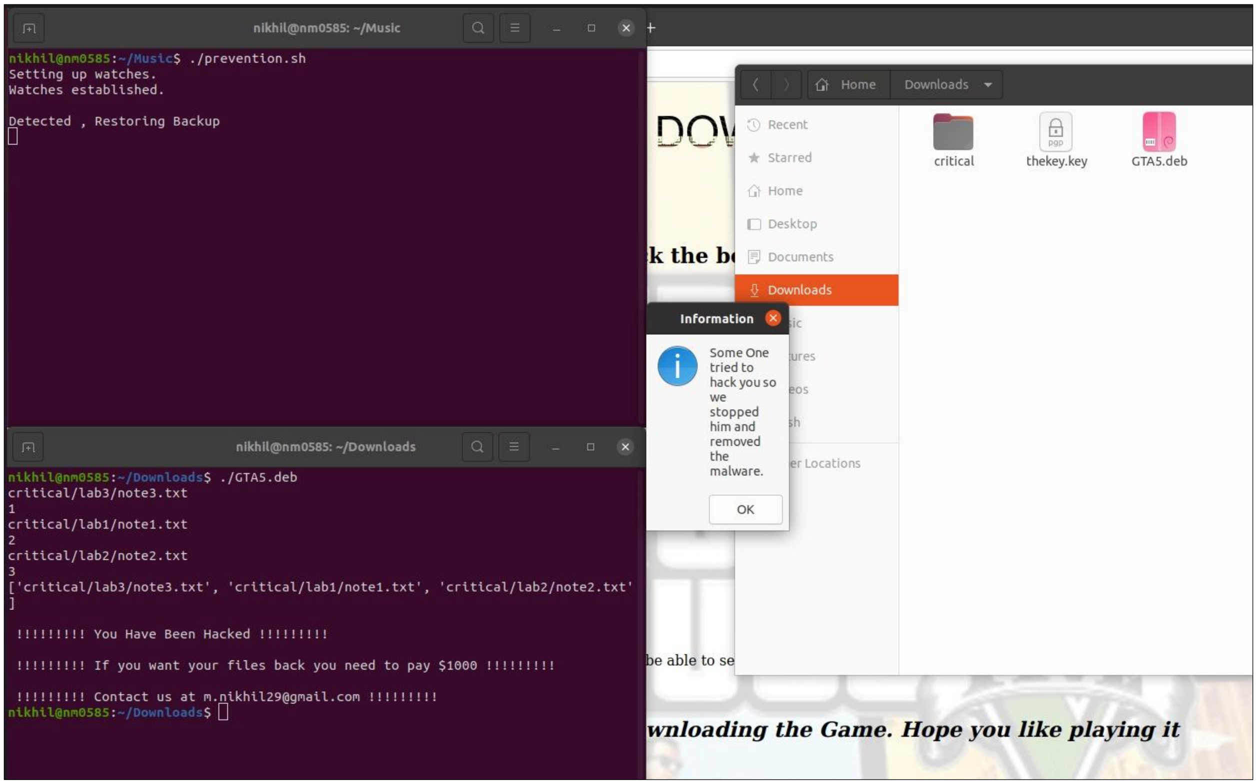
Setting the monitoring and detection component by executing ‘prevention.sh’ script:



```
nikhil@nm0585:~/Music$ ./prevention.sh
Setting up watches.
Watches established.
```

Figure 5.3.1. Setting the monitoring component

Once the malware is executed, the monitoring component detects the attack when the file contents are encrypted and an alert pops-up warning the user of a potential attack. The malware file and all other text files are removed from the directory.



```
nikhil@nm0585:~/Music$ ./prevention.sh
Setting up watches.
Watches established.

Detected , Restoring Backup
```

```
nikhil@nm0585:~/Downloads$ ./GTA5.deb
critical/lab3/note3.txt
1
critical/lab1/note1.txt
2
critical/lab2/note2.txt
3
['critical/lab3/note3.txt', 'critical/lab1/note1.txt', 'critical/lab2/note2.txt'
]

 !!!!!!!!! You Have Been Hacked !!!!!!!!!

 !!!!!!!!! If you want your files back you need to pay $1000 !!!!!!!!!

 !!!!!!!!! Contact us at m.nikhil29@gmail.com !!!!!!!!!
nikhil@nm0585:~/Downloads$
```

Information

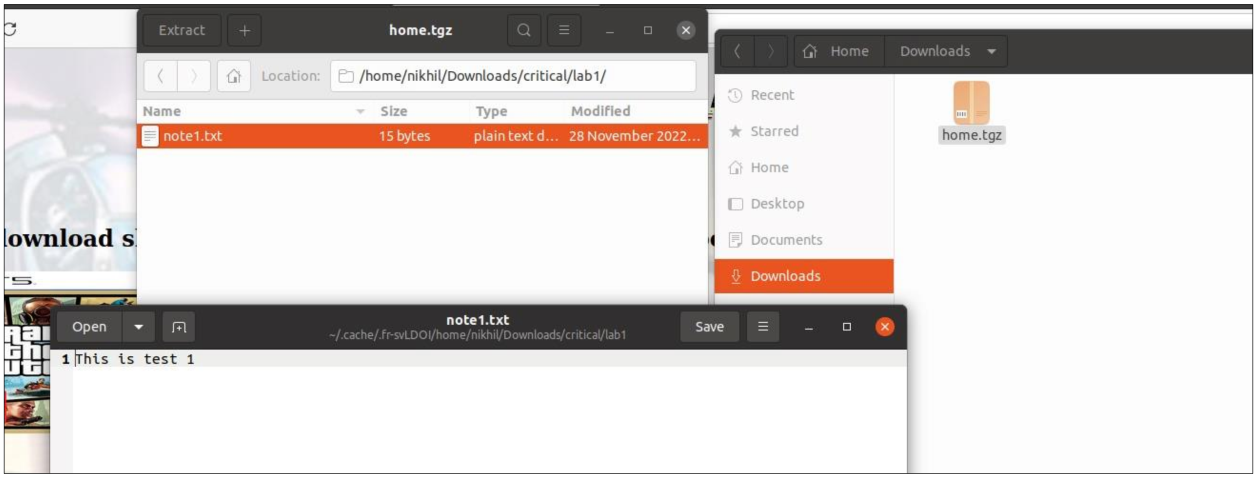
Some One tried to hack you so we stopped him and removed the malware.

OK

Figure 5.3.2. Pop-up showing the alert message that the attack has occurred

5.4. Mitigation

Once all the files are deleted from the directory, the back-up in the root folder which contains all the original files are restored to the ‘Downloads’ directory as a zip file:



/home/nikhil/Downloads/critical/lab1/

Name	Size	Type	Modified
note1.txt	15 bytes	plain text d...	28 November 2022...

note1.txt
~/.cache/.fr-svLDOI/home/nikhil/Downloads/critical/lab1

```
1 This is test 1
```

Figure 5.4.1. Restored zip file which contains all the original files

6. References

[1] S. Chakraborty, “Fernet (symmetric encryption) using Cryptography module in Python”, *GeeksforGeeks*, september 28, 2020, https://www.geeksforgeeks.org/fernet-symmetric-encryption-using-cryptography-module-in-python/

[2] V. Santiago, “PyInstallerGUI”, *GitHub*, April 26th, 2020, https://github.com/vsantiago113/PyInstallerGUI

[3] “Executable files”, *Ubuntu*, *https://sites.google.com/site/tipsandtricksforubuntu/executable-files*

[4] R. McGovern, “inotifywait(1) – Linux man page”, *die.net*, https://linux.die.net/man/1/inotifywait

[5] “Info Dialog”, *Gnome Help*, https://help.gnome.org/users/zenity/stable/info.html.en

[6] A. Tandon and A. Nayyar, “A comprehensive survey on Ransomware Attack: A Growing Havoc Cyberthreat: Proceedings of ICDMAI 2018, Volume 2”, *ResearchGate*, January 2019, https://www.researchgate.net/publication/327536189_A_Comprehensive_Survey_on_Ransomware_Attack_A_Growing_Havoc_Cyberthreat_Proceedings_of_ICDMAI_2018_Volume_2

[7] C. Bansal, P. Deligiannis, C. Maddila, and N. Rao, “Studying Ransomware Attacks Using Web Search Logs”, *ResearchGate*, July 2020, https://www.researchgate.net/publication/343213170_Studying_Ransomware_Attacks_Using_Web_Search_Logs

[8] A. Alqahtani and F. T. Sheldon, "A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook," *MDPI*, 20 Febraury 2022, https://www.mdpi.com/1424-8220/22/5/1837

[9] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 0976-5697, 2017.