Introduction to Computer Security
Ransomware: Step 3 Infection

Team Members:

JyothishSaiTalagadadeevi - 11790777

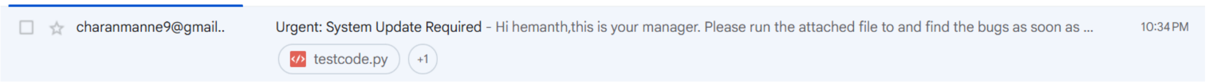
Hemanth Chowdary Vallabhaneni - 11809252

Manne Sree charan sai - 11790768

Gopi Krishna muppineni - 11790826

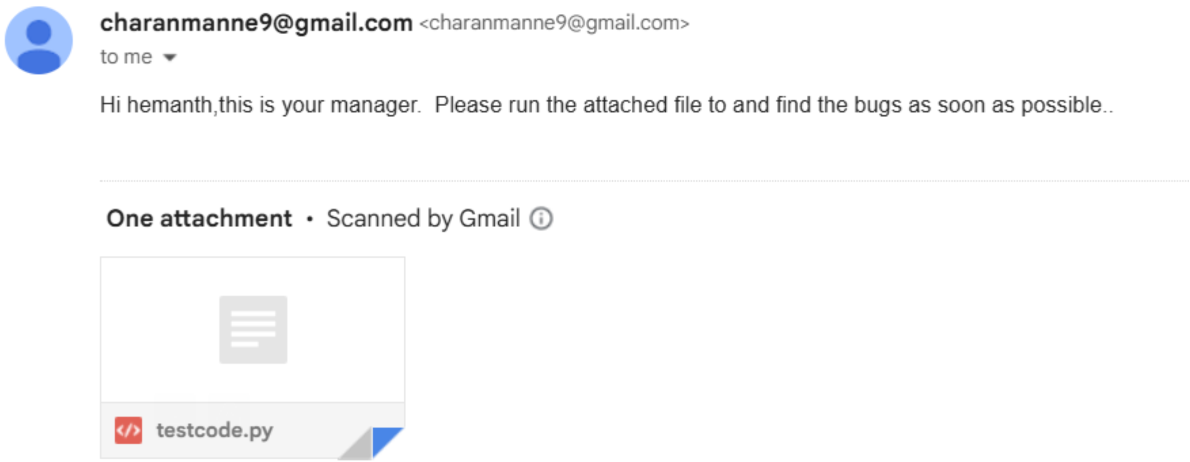
Steps performed:

1. The target user is sent a mail that contains the malicious code.



charanmanne9@gmail.. Urgent: System Update Required - Hi hemanth,this is your manager. Please run the attached file to and find the bugs as soon as ... 10:34 PM

The mail has a simple fake message from a manager asking to run the file.



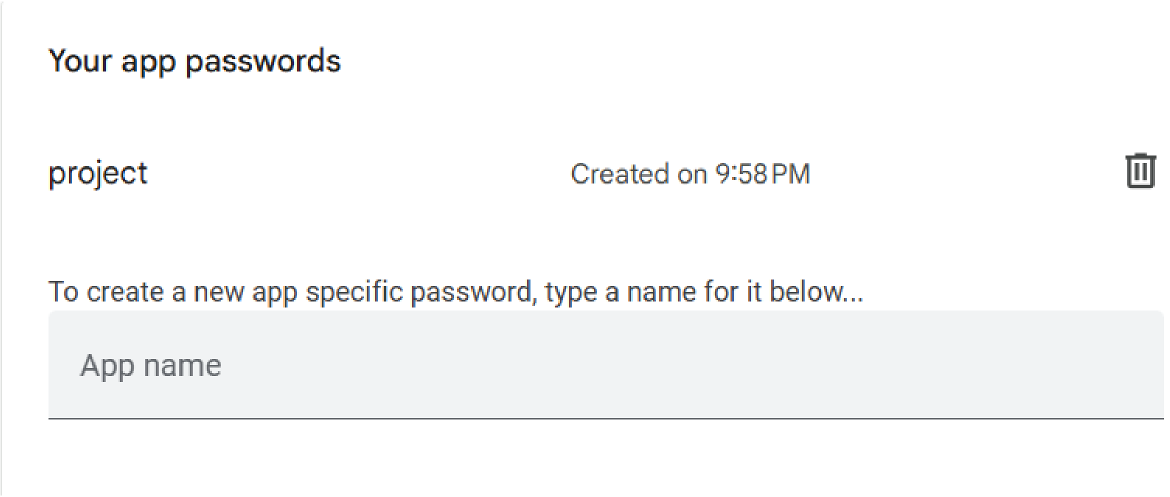
charanmanne9@gmail.com <charanmanne9@gmail.com>
to me

Hi hemanth,this is your manager. Please run the attached file to and find the bugs as soon as possible..

Here the mail contains a testcode.py which has a malicious python code, when executed will encrypt the folder and all the files in the folder.

2. In this infection we are using a inbuilt library called sendmail that is used to send a phishing mail to the victim.

For this we need a mail id of the attacker and the victim. And also we need to create an app password for the attacker inorder to send the mail to the victims mail id.



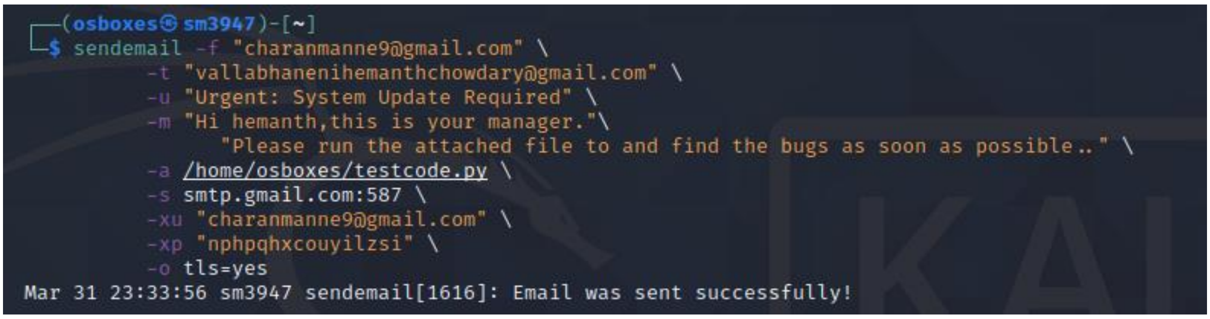
Your app passwords

project Created on 9:58 PM

To create a new app specific password, type a name for it below...

Using this password and email id’s of both the victim and the attacker we can send a mail.

The following screenshot will show the code for the sendmail.



```
┌──(osboxes㉿sm3947)-[~]
└─$ sendemail -f "charanmanne9@gmail.com" \
          -t "vallabhanenihemanthchowdary@gmail.com" \
          -u "Urgent: System Update Required" \
          -m "Hi hemanth,this is your manager."\
             "Please run the attached file to and find the bugs as soon as possible.." \
          -a /home/osboxes/testcode.py \
          -s smtp.gmail.com:587 \
          -xu "charanmanne9@gmail.com" \
          -xp "nphpqhxcouyilzsi" \
          -o tls=yes
Mar 31 23:33:56 sm3947 sendemail[1616]: Email was sent successfully!
```

Here we can see the code which has the following parameters,

-f from address

-t to address

-u subject

-m message

- attachment

-s server

-xu attacker mail app id

-xp app password

Here we can see that there is an attachmet of the file testcode.py which is created and has the encryption and decryption code in it. And the screenshot also shows that the mail has been sent successfully.