Ransomware

Description

Ransomware causes a lot of headache and money each year. Your task is to experiment with ransomware.

You are allowed to work in groups of two on this assignment. In the end you will need one windows machine to compile the ransomware payload on and another one to execute the payload on. To tell the truth, I used the same machine as the compiler and as the victim. I tried within a single subnet, but it could probably work if they were on different subnets (unless some firewall blocks it).

Here is an example demo of the ransomware.

Begin by viewing the github link here.

Essentially, on the machine that you will compile this on you will:

- Download and install python. I TESTED WITH PYTHON 3.7.8. I know that the most current version WILL NOT WORK. You may have to google fu to find this download. My link was hereMake sure to check the box to add python to your PATH in the installer wizard.
- Download the github files. (I just grabbed the zip version). Extract. (I couldn't download with edge, but could with chrome)
- Open a command prompt in windows, navigate to newly extracted directory. Follow instructions on github webpage. Something like `pip install -r requirements.txt` followed by `python RAASNet.py`.
- Create a payload, change the settings to what you would like. Make a note of the directories and filetypes it is going to encrypt
- Create a few sample files on the victim machine that match the settings you identified in the wizard.
- Build the payload
- Compile the payload
- Copy the payload to the other machine
- Start the server
- Execute the payload
- See if it actually encrypted some files. Probably screenshot this

Optional and untested

- See if you access the website identified in the instructions. May have to use tor browser?? **I couldn't get this to work, but I didn't spend much time on it**
- See if the decrypt executable works. Screenshot.

TO pass off

Prove that you can do this.