Our inspiration for our project came from your typical Hollywood movie attack where the secret agent is trying to infect the villain's computer to prevent them from being able to steal all the money from the richest person in the country before they flee to a different county. Or even the movie attack where the villain is trying to take over all of the systems in the world and the secret agent is trying to stop them. In both of those scenarios, it is an image that is being sent to everyone or just a specific target and once the image is opened then the attack is put into action, the ransomware or whatever malware is embedded in the image starts running, and the target loses their entire system or the villain gains control of every system in the world. Those types of movies are always interesting to watch but Hollywood movies always seem a little too far fetched to be real so we wanted to make it as simple as possible but still being super effective in encrypting the user's system. We wanted to make it a little more realistic by having the target be gullible enough to open the image and think that their pc is trying to give them steps for fixing the image but instead it is steps for running our ransomware on their pc. The process is actually very simple and it can actually be viewed as some sort of social engineering if the attack is executed properly. We aim to take advantage of someone’s trust in their computer. Most people typically just do whatever their computer says without questioning anything about it and in reality it could be something malicious and they will not know until it is far too late. The typical person sees a notification for an update and installs it instantly or schedules a time for it to install. Same with web pages not loading, people are quick to click the refresh button and they have no idea that whatever web page they are viewing could be made to look like it needs to be refreshed but in reality every single time they click refresh it is transferring $1,000,000 to the owner of the website without the target knowing. Yes $1,000,000 would be noticed by the typical user so maybe we say $1,000 or even $100. The amount doesn’t really matter for the point we are trying to make. The point is that people follow instructions blindly and have no idea why they are doing what they are doing and if it is even going to do what they want it to do. We are aiming to take advantage of that human instinct with our ransomware. If social engineering works over a phone call, through a text message, or through an email, why can it not work through a computer image explaining exactly “how to fix itself.” That is what we are trying to do. We want the target to receive an image that is embedded with our ransomware and instead of instantly encrypting everything, we want them to trust the computer and the process before the attack begins. We want the target to be unaware of what is actually happening and hide the magic behind a misdirection. Just like any magician performing their best trick, we plan to “misdirect” the target into starting the ransomware themselves. We have created an image that is just an ordinary image of instructions on how to “fix” the image but running some commands in the terminal. Like previously mentioned, the target thinks they are going to fix the image by running these commands but our ransomware is hidden behind them by being named “image” so it looks like the user is actually accessing the image. That is all there is to the villain’s side of the story when attacking everyone in the world. Now the secret agent’s side of the story is trying to stop the villain from attacking the world. Just like any good hero, a steakout has to take place to gain enough information to analyze the next moves of the villain. We created a monitoring bash file that will be constantly running to log any activity that is being conducted on the computer so we have enough information to detect the attack from the villian. Once enough information is collected it has to be analyzed to determine what is going to happen or if something is taking place at that very moment. We also wrote a detection python script that will continuously run and analyze the behavior that is taking place on the computer at that time. Once the next move has been observed and figured out, it is time to take action and attempt to stop the villain from taking over the world. Or at least stop the villain from taking over all the computers in the world. We wrote a mitigation bash file that has to be run while the attack is happening. The goal of it is to kill the ransomware process and stop it from causing any more harm. In the movies heroes like to help restore the community back to its previous state that way everyone is happy again. We wrote an added bonus into mitigation that will restore the system to its previous state from a backup that will be created moments before the attack happens. We took a lot of inspiration from the classic hero versus villain movies and wanted to do something to simulate that same action being taken in real life. It is scary to think that something like this can happen in real life but it happens every day and this project has taught us a lot.