

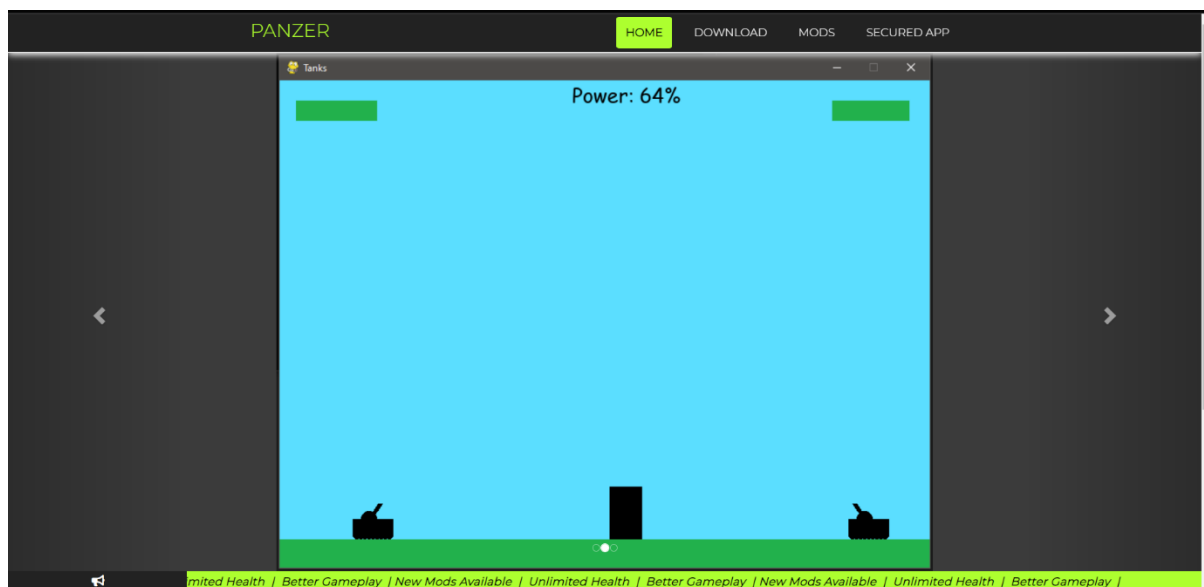
Abstract

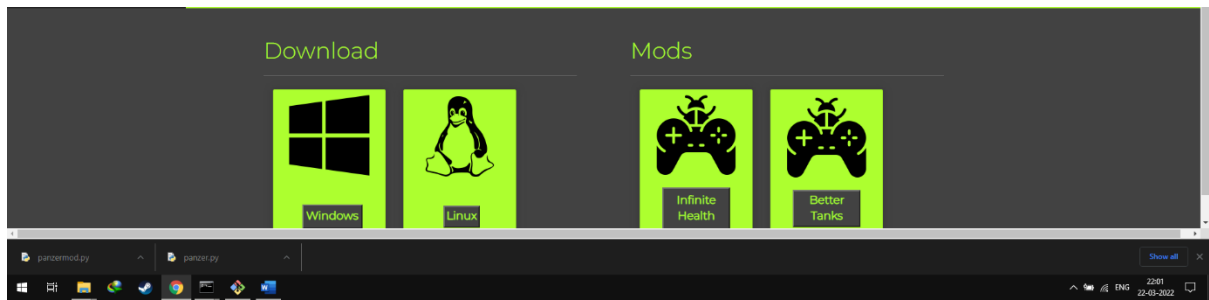
The project uses a video game to deploy the malware, the original code shared by the developer is fine and does not contain any malicious code.

The attacker offers lucrative mods like unlimited health or free in game currency, the user when runs the mod, the game code is modified such that it injects a backdoor inside the code.

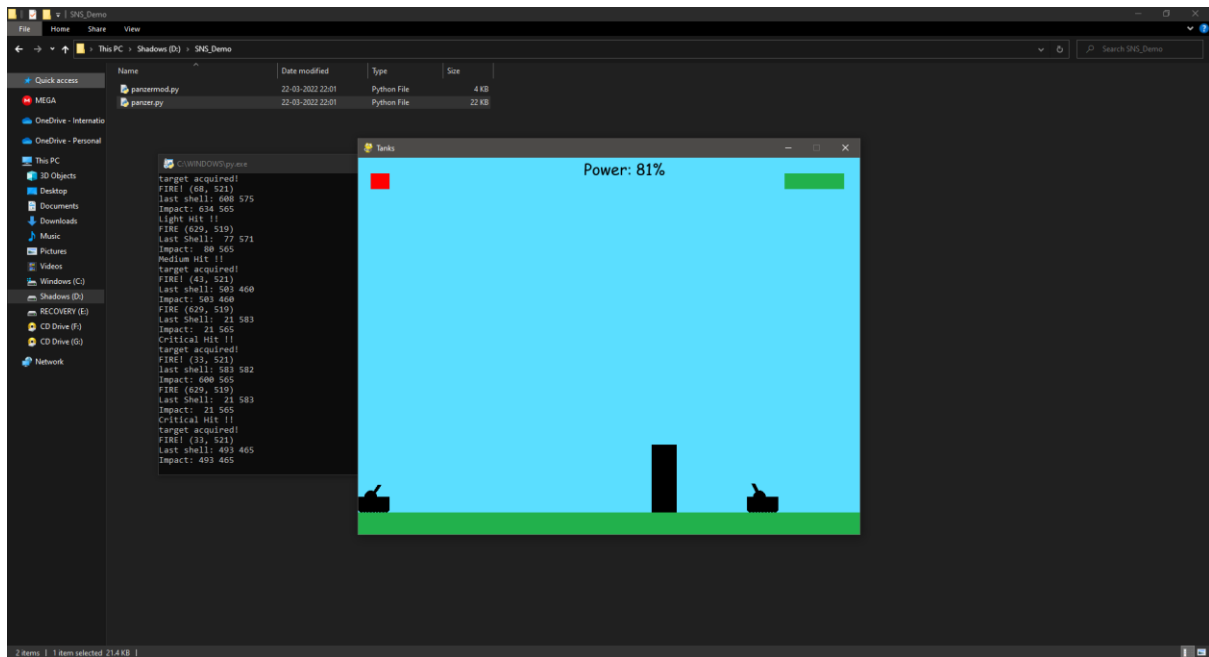
This backdoor can then be used to perform all sorts of malicious actions on the victim's machine.

1. The user can download the game from the website. <https://pois-proj.github.io/>

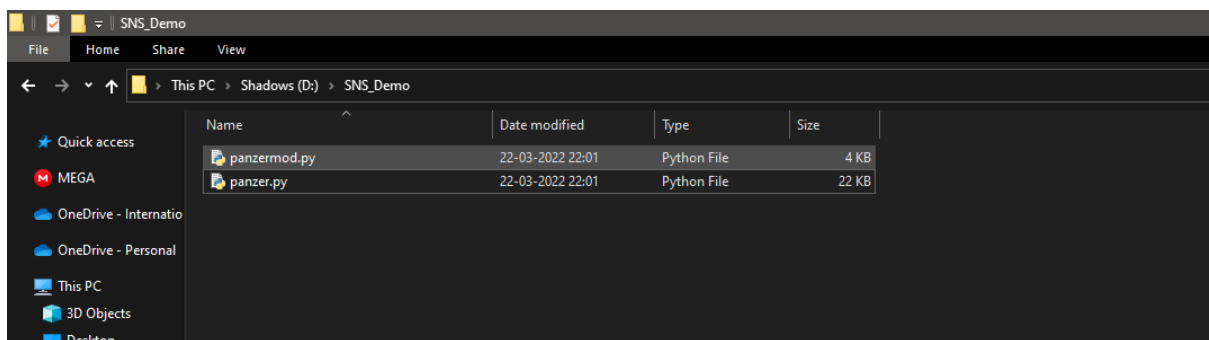




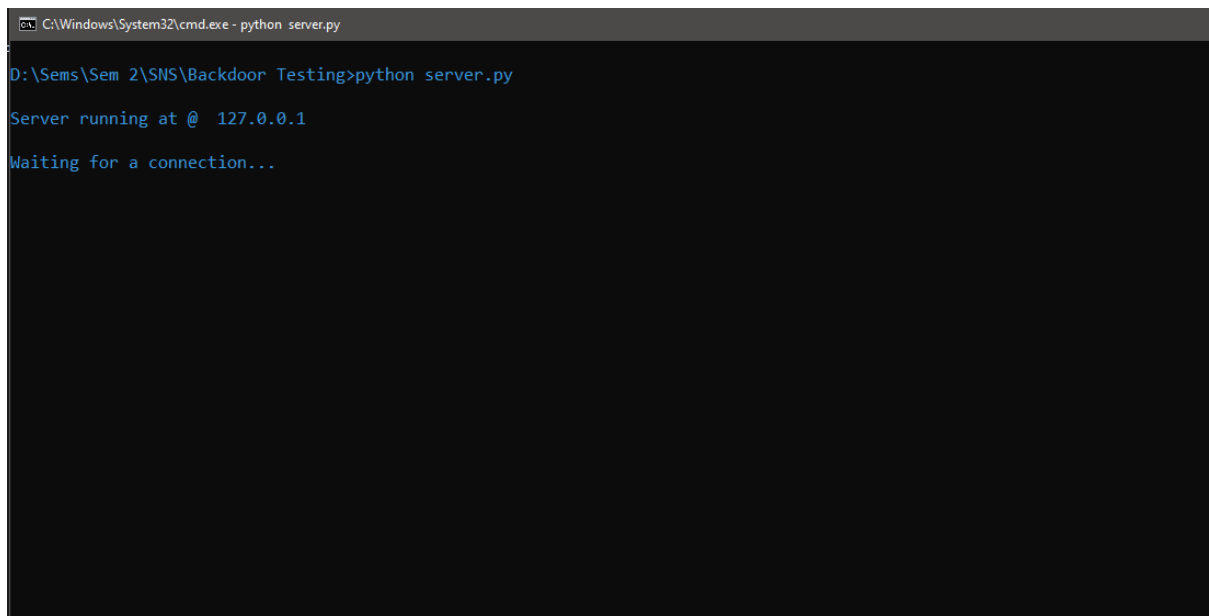
2. User can run and enjoy the game just fine.



3. User then runs the mod file.



4. Meanwhile attacker runs the listening server for the backdoor.

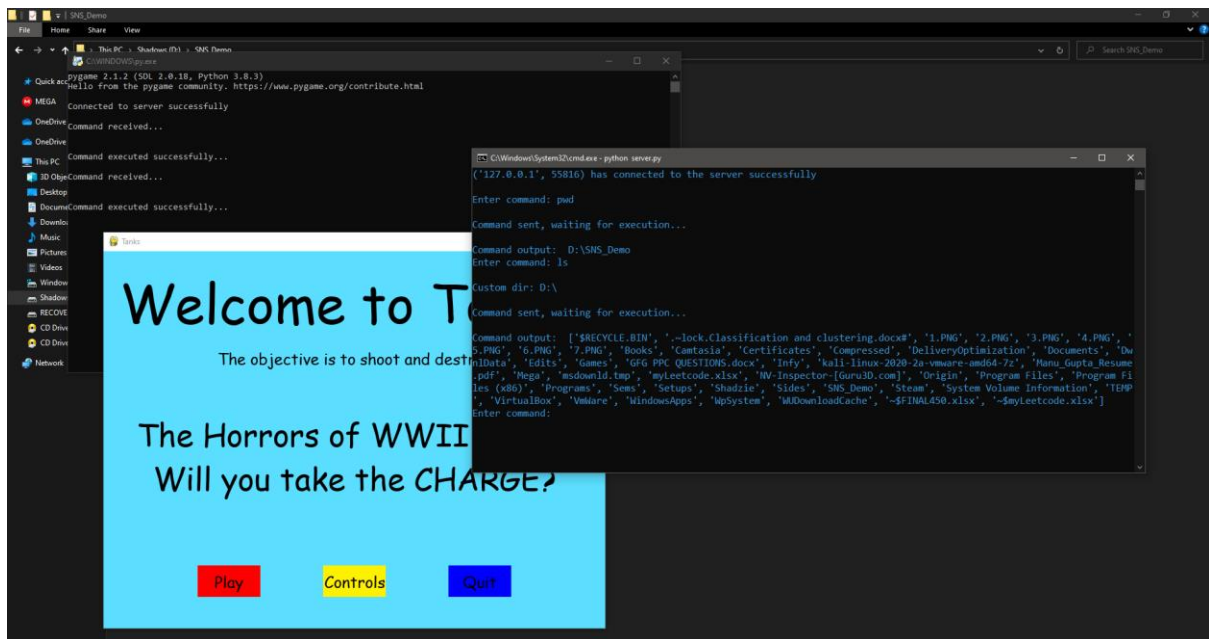


A screenshot of a Windows command prompt window. The title bar reads "C:\Windows\System32\cmd.exe - python server.py". The command prompt shows the following text:
D:\Sems\Sem 2\SNS\Backdoor Testing>python server.py
Server running at @ 127.0.0.1
Waiting for a connection...

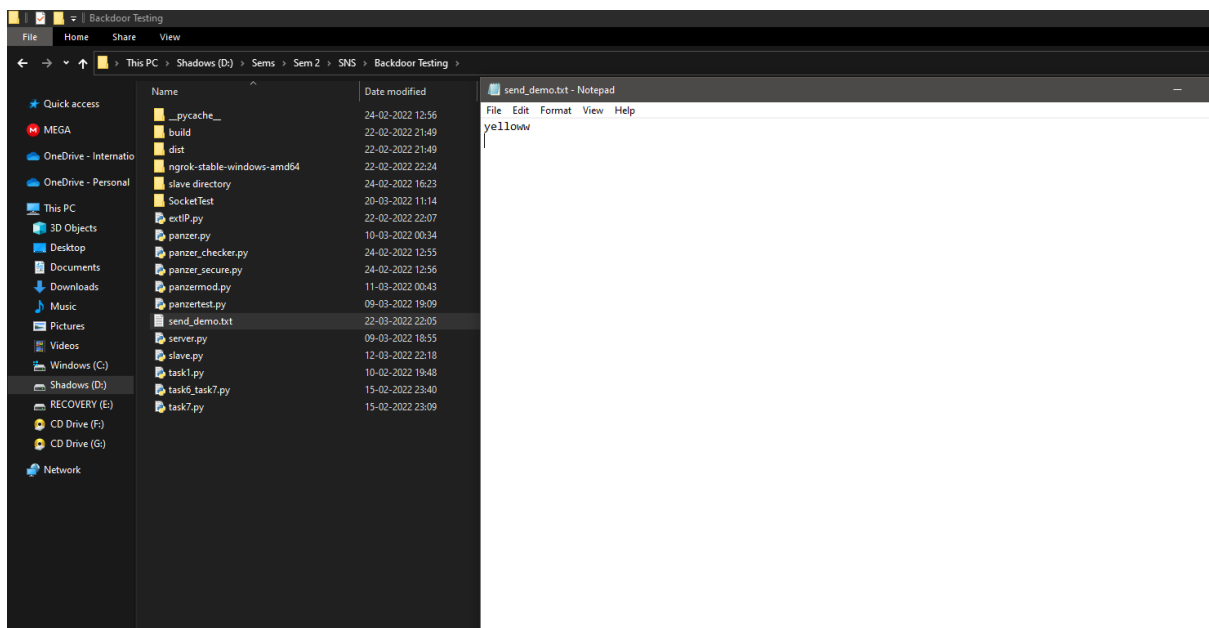
5. This time when user runs the game, one of the threads in the backdoor code connects to the attacker's server in the background.

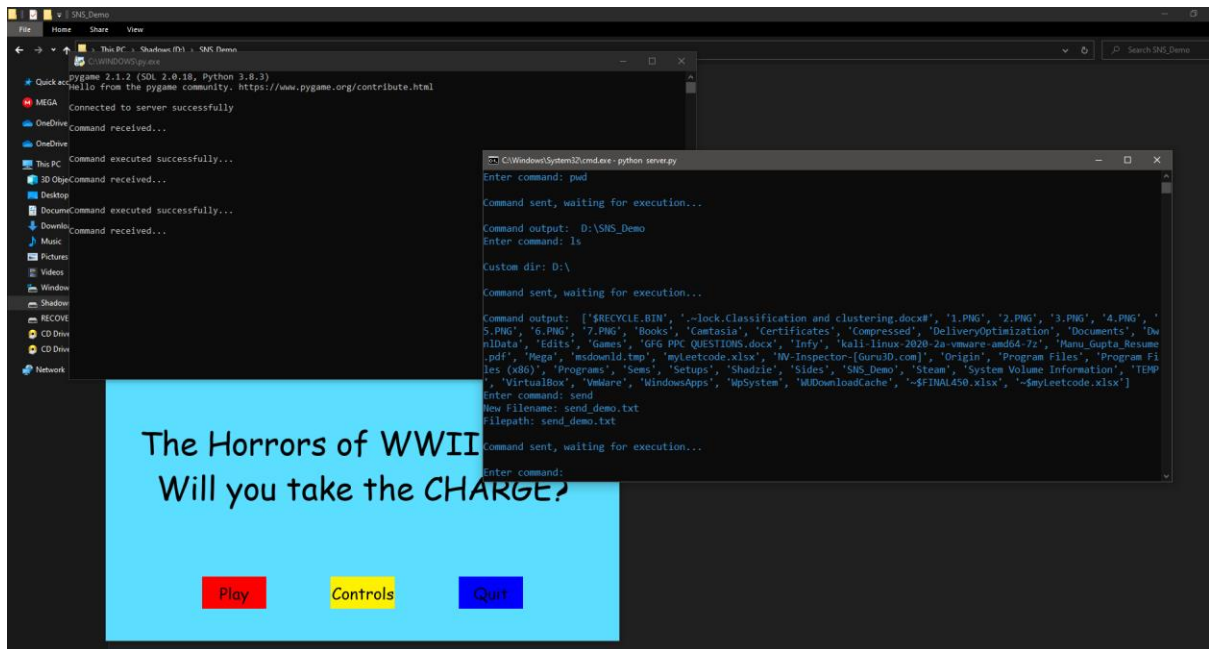


- Once connected attacker can investigate the victim's computer, like checking all the files present in the directory, downloading a file, sending a file, removing a file etc.

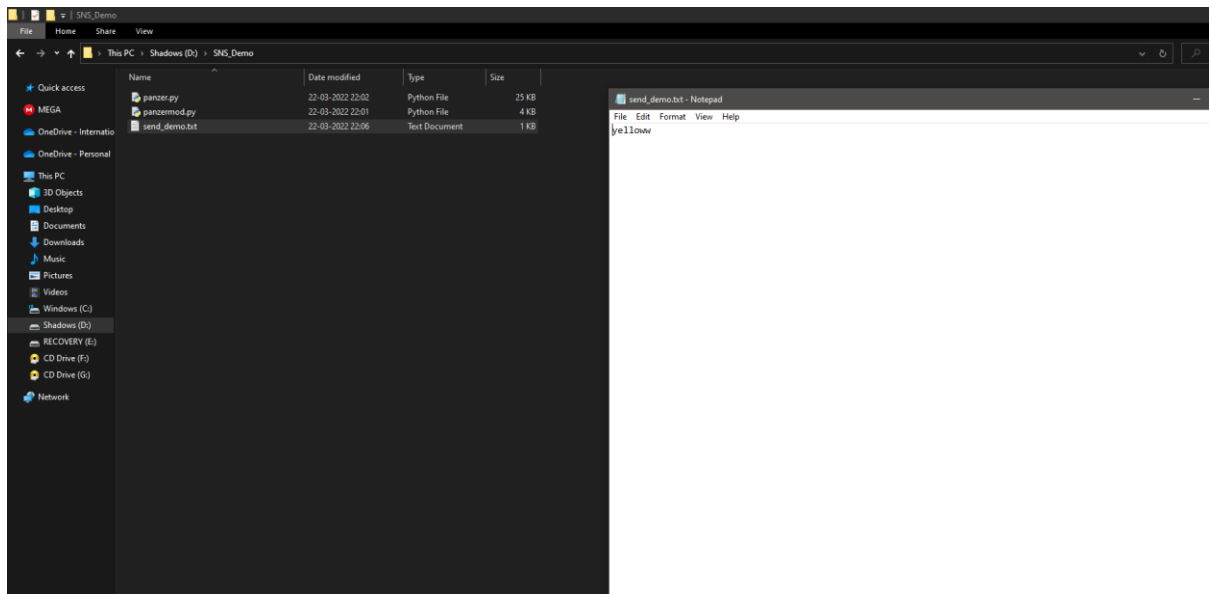


- Initially we try to send this demo file to the victim's system.

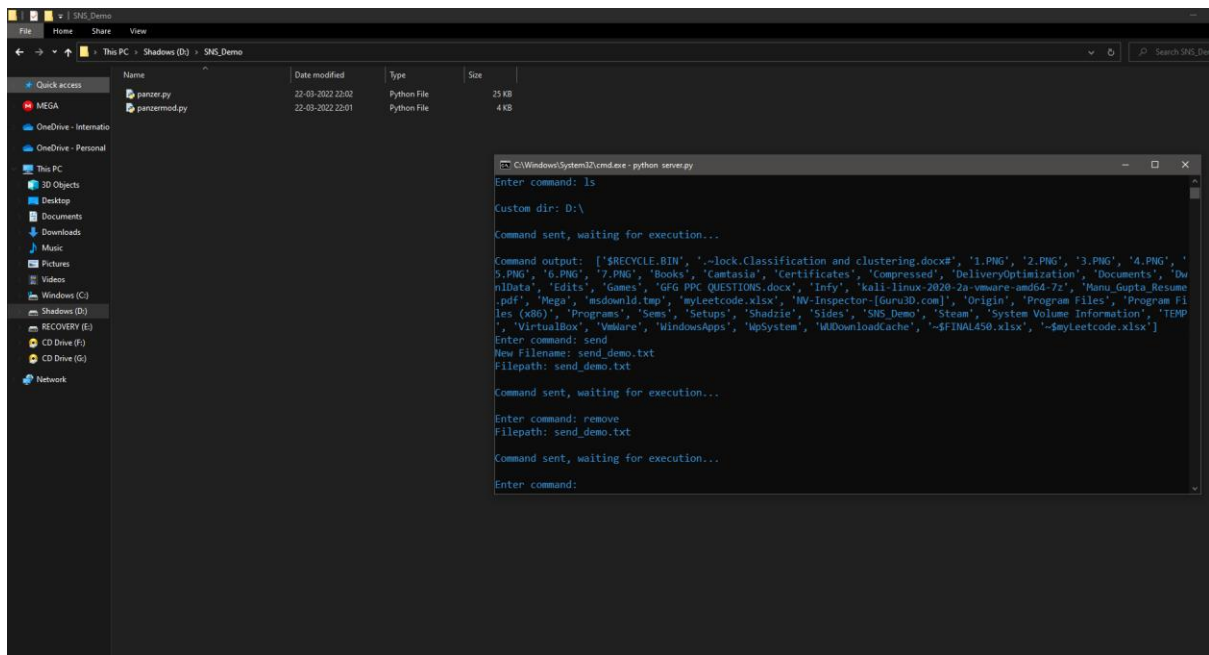




8. Here, we can see that the file has been received by the victim.



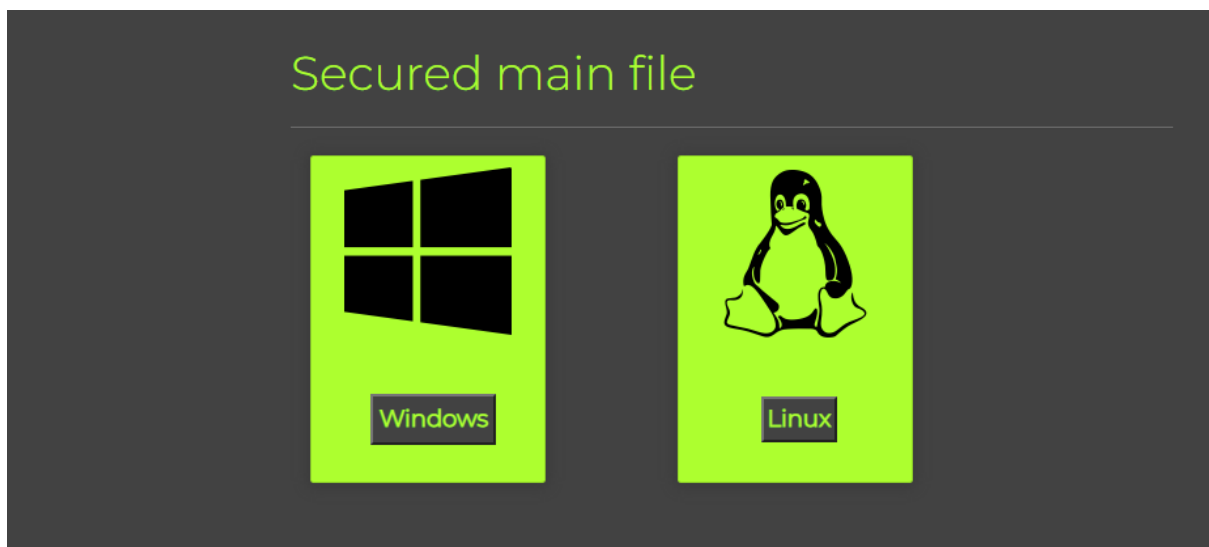
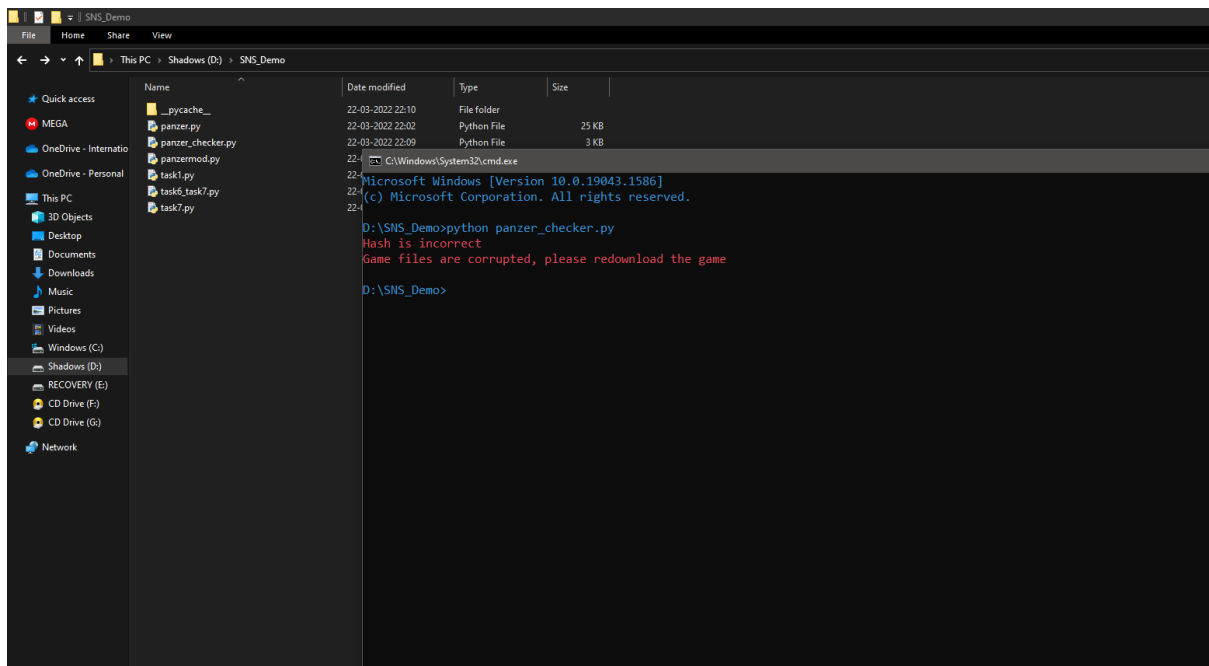
9. Here, we can see that attacker can easily remove a file from victim's system as well.



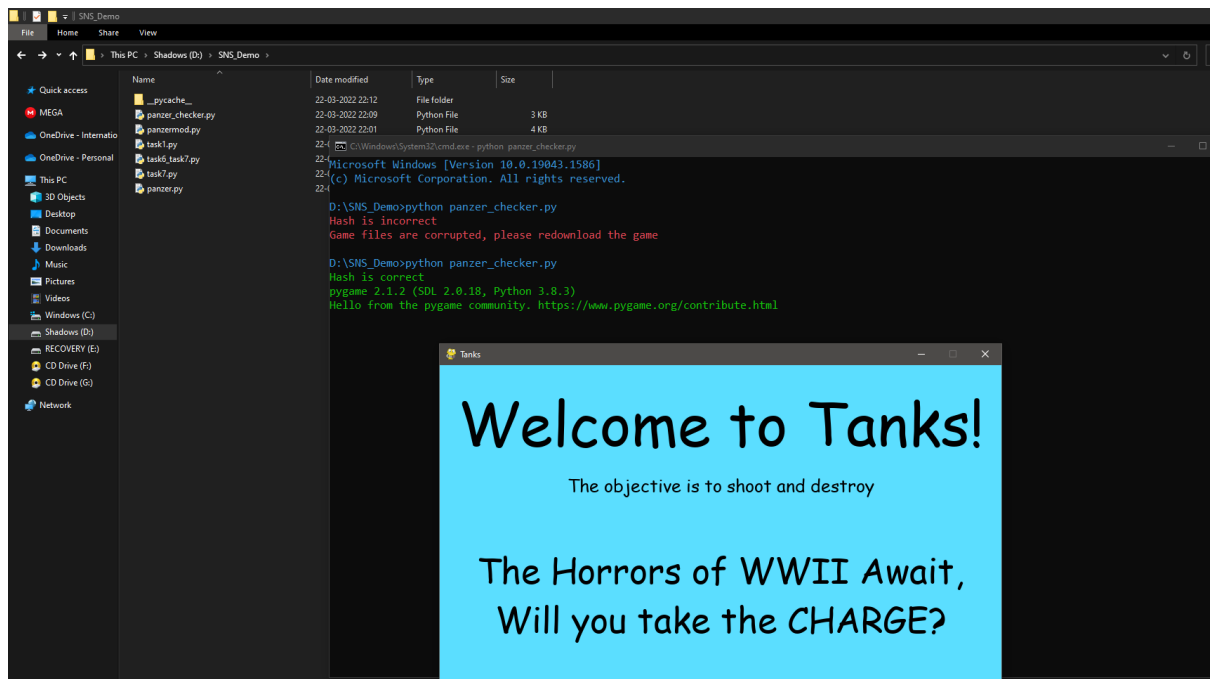
10. Now we look at how we can thwart this attack. Move over to the secured app section of the website.



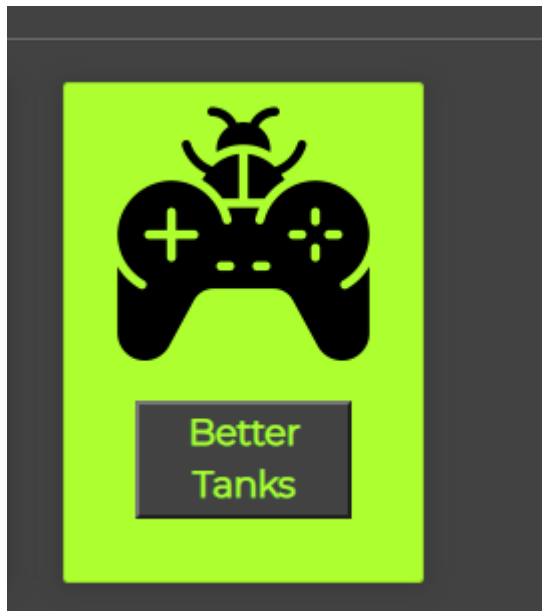
11. Download the panzer_checker files, we can either download all the 4 python files or if you are on windows, you can simply download the windows exe file that does the same thing. Here, as we can see that if the game code doesn't match the original code provided by the developer the checker throws an error and won't let the user execute the program.



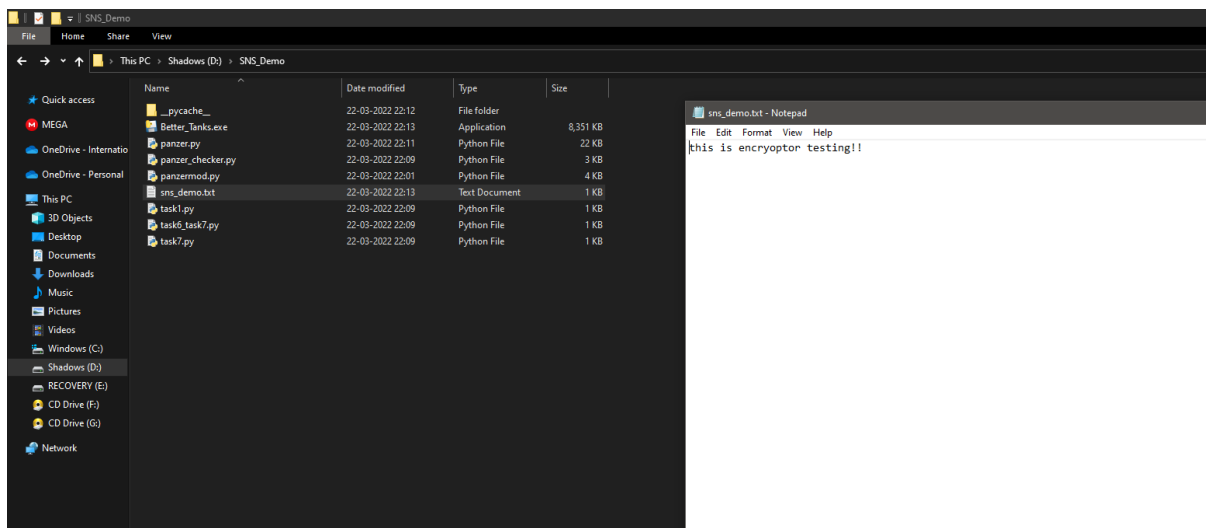
12. To play the game user then downloads a fresh copy of the game from the website and again tries to run it, as we can see the checker allows it to pass and the game then runs fine.



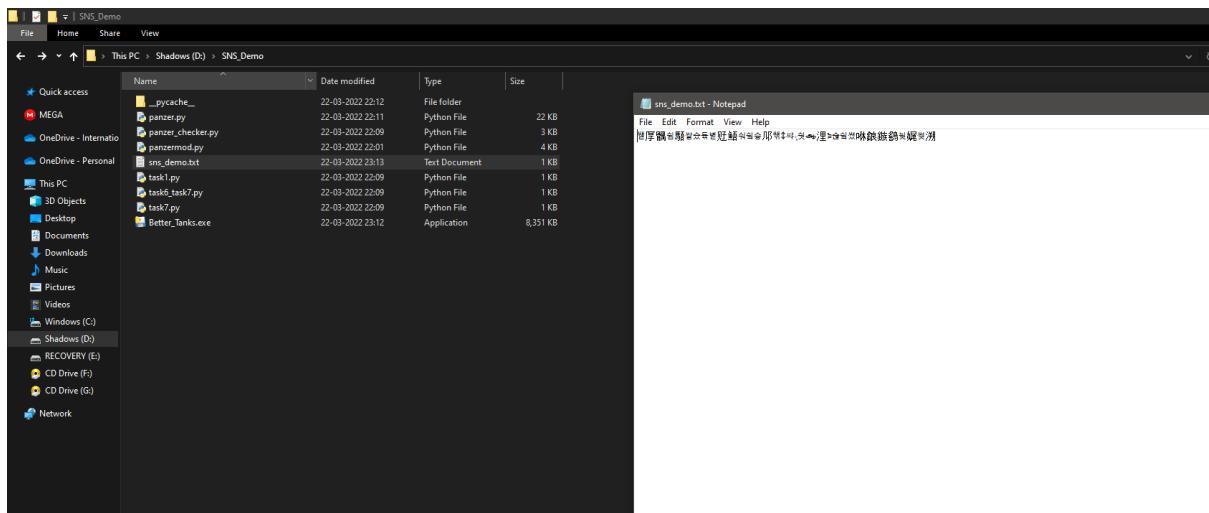
1. Another exploit we made is an encryptor, a sort of initial version of a ransomware. If the user downloads this better_tanks.exe file and runs it. All the .txt files present in that folder will be encrypted and a copy of the original file will be sent to the attacker via mail. We can encrypt all types of files easily but since the encryption algorithm takes a fair bit of time we are using just .txt files for now.



2. Here is the sample .txt file we will use as a demo.



- Once the user runs the .exe file, the txt file is encrypted and the original file is sent to the attacker.



- Here, we can see the attacker's email as they receive the actual file.

