TPR Ransomware

Pedro Almeida 89205
Pedro Valente 88858

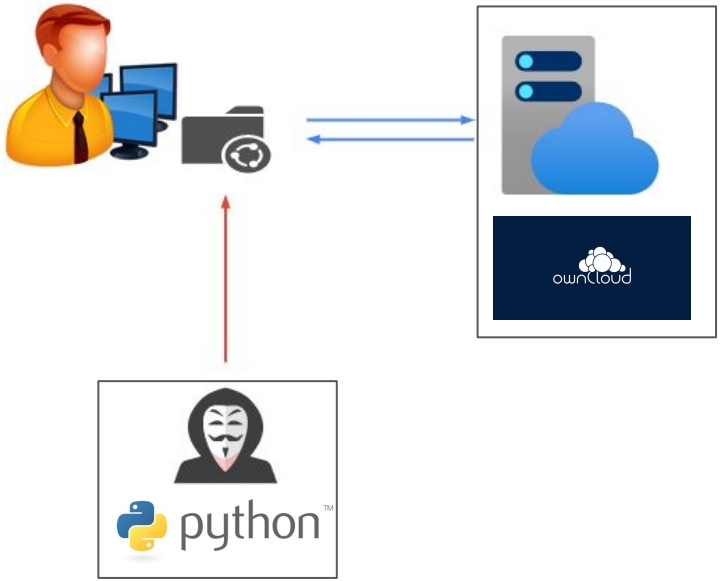
Problem identification

Ransomware is a public affair. It’s a type of malicious software that encrypts a user’s computer or device, sending the user a blatant message telling them their system has been compromised.

The inspiration for this project came from an attack made against the company Garmin in July 2020 in which the hackers seized control of all the files on the system and demanded to be paid a ransom of $10 million to decrypt the compromised data.

Link to the news: https://www.mitnicksecurity.com/blog/2020-garmin-ransomware-attack

In order to simulate the attack, we will use a local cloud service named owncloud and then develop some *python* scripts to create, delete and cipher some files and directories.



Observation

- Time Independent Features
  - Metrics
    - Download and Upload
    - number of packets and bytes
  - Features
    - Minimum and Maximum
    - Standart deviation
- Time Dependent Features
  - Length of activity and Periodicity
  - Silence Periods

Retrieval of data

- Retrieval

Normal use of *owncloud's* service and retrieval of its generated traffic by listening to its port with wireshark

Solution

Block the IP address;

Develop a system of users that gives ownage of a file to a user and only that user can edit/delete that file.