Team Name: Mermaid Man & Barnacle Boys

Team Members: Wayne Lin, Ning Wang, Jianqi Ma, Xingyu Liu, Yuhao He

"Oh magic conch shell, tell me the chrome passwords of the victim machine"

C2 Server & Client
- Operators can login via client interface and get an overview of the current state of server and implants
- Server interacts with implants on victim machines (send commands/DLL and get results)

Implant
- Get basic info of victim machine
- Get tasks from server and execute them
- Inject stealer DLL into remote processes
- Return results (chrome passwords) to Server

Technical Overview of the Application

C2 Server:
- Development = Flask
- CLient authentication: Flask-Login
- Database = MySQL+SQLALCHEMY
- Deployment = Heroku
- Encryption = AESGCM

Implant:
- Symmetric Encryption using AESGCM
- HTTPs Communication Between C2 and Implant
- Shell Command Execution by creating new process and communicating through named pipe
- Shellcode Injection using Donut to execute next stage payload
- Communicating with Steganography

Development Journey

C2 Outline
- Implant can register with server
- Operator can log into server
- Implant and server communication with json

Encryption
- HTTPs (TLS over HTTP)
- Symmetric encryption of communication using AESGCM

Stealer.dll
- Steals chrome passwords from victim machine

Shellcode/DLL Injection
- Transforms the implant into a loader that gets stealer DLL from server
- Injecting the stealer into a remote process