Cryptography and Network Security Final Report

Ata Gürsel
Software Engineering
215060044

server.py Code Report

1. Overview:

This Python script represents a Remote Access Trojan (RAT) server. A RAT is a type of malicious software used to gain remote access to a computer system. This server can perform various operations on the target computer by receiving specific commands and processing their returns.

2. Code Structure and Modules:

- The code exhibits a modular structure and is organized within a class (RAT_SERVER).
- Python modules such as socket, os, random, and vidstream have been utilized.
- A try-except block checks for the existence of the vidstream module and provides notification in case of an error.

3. Connection and Communication:

- The build_connection method of the RAT_SERVER class creates a socket, listens for connections, and retrieves the IP address when a client connects.
- The execute method receives commands from the user and directs them to the corresponding functions for processing.

4. Commands and Functionality:

- The code can perform various operations on the target computer with a set of commands. Functionalities include file management, system control, audio control, screen management, keylogger control, and web browser usage.
- Each command processes the relevant results through the result method.

5. Error Handling:

Error handling is simplified, providing notification if the module is not found.

client.pyw Code Report:

1. Code Structure and Modules:

- The code exhibits a modular structure within a class (RAT_CLIENT).
- Various Python modules, including socket, os, threading, PIL, ctypes, comtypes, winreg, shutil, glob, ctypes, webbrowser, re, pyautogui, cv2, and pynput, are used.
- The ctypes module is employed for accessing Windows DLLs.

2. Connection and Communication:

- The build_connection method establishes a connection with the server and sends the IP address.
- The execute method continuously listens for commands from the server and directs them to the corresponding functions for processing.

3. Commands and Functionality:

- The code can perform various operations on the target computer using commands such as screen sharing, webcam capture, audio control, file operations, keyboard input, and system control.
- Each command invokes specific functions to execute the corresponding operations.
- Shutil and os modules are used for file operations.

4. Error Handling:

- The errorsend method encrypts and sends a "no output" message to the server in case of an error.
- Error situations are generally handled with try-except blocks, and error messages often contain general phrases like "Module is not founded."

THANK YOU!