CSE363 Final Project

Covert C&C and Exfiltration

Haoyu Tan, Hsin Ying Lin

Goal:

This project’s goal is to control infected client(s)’s shell, executing remote commands, and send/receive files to/from client(s).

Used tool / approach:

Python

Main Functionalities:

Connect – search and connect to all clients that have the same host and port

List – list all clients that are captured through connection in order

Shell <id> - preceding command before sending commands to a specific client connection

Quit – close all client connections listed in list

Exit – end program and end all connections in the connection list

Extra functionalities after shell <id> command:

Retrieve <filename> – file transfer from server to client

Send <filename> - file transfer from client to server

Back – return to main control without closing the current client connection

Close – close the current client connection

Exit – end program and close all client connections in the connection list

\*\*\*For normal commands like ls, pwd, etc. after printing, use ^C before entering next command \*\*\*

Communication hiding:

port is set to 443 (HTTPS) to fake the communication as a HTTPS communication. Furthermore, command communications are encode using steganography, hiding important information in image form.