Team: Kill A Byte

Malware + C2 project that was built by BU students in BU's CS501 Class (Introduction to Malware, Threat Hunting, and Offensive Capabilities Development).

Members: Luke Staib (ljstaib@bu.edu), Dalen Witthoft (jynbu@bu.edu), Shirene Cao (xcao19@bu.edu), Harshit Agrawal harshit@bu.edu), and Annette Hong (ahong12@bu.edu)

Task: To create malware that could be ran on a victim machine which can connect to a C2 (Command and Control) server. Agents should then be able to communicate with malware on a specific victim's computer using this C2 server.

Malware Capabilities:

- Loot
- Persistence
- Execution of commands
- Situational awareness
- File I/O
- Defense evasion

Technical Overview of the Application

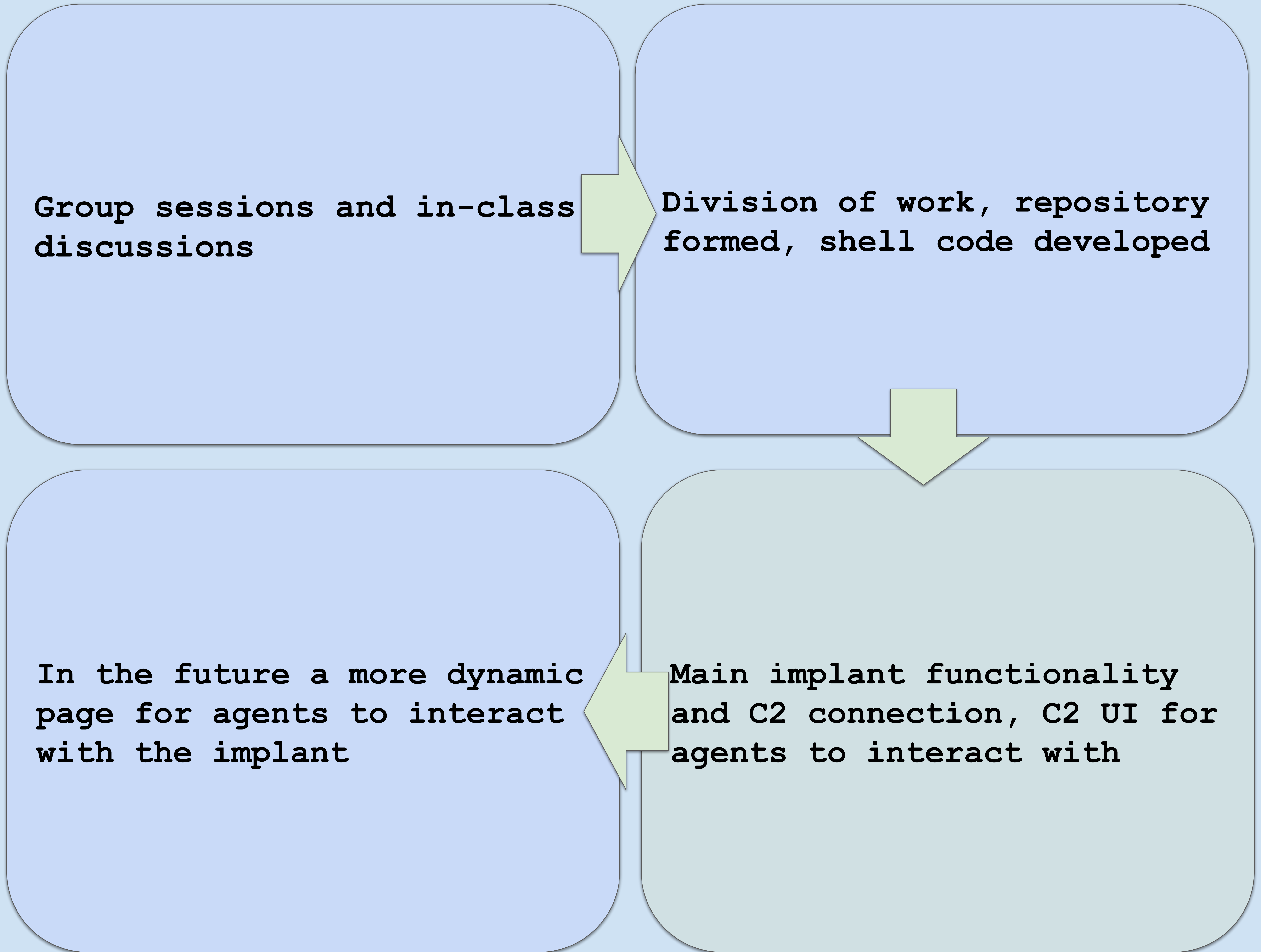
Malware

- C++, MinGW
- Windows API
  - WinHTTP
  - BCrypt, WinCrypt

C2

- Flask
- SQLAlchemy
- HTML/CSS/Bootstrap

Innovation Journey: Pivots and Future Work



Group sessions and in-class discussions

Division of work, repository formed, shell code developed

Main implant functionality and C2 connection, C2 UI for agents to interact with

In the future a more dynamic page for agents to interact with the implant