James Howard (jhoward6)

Dhyaanesh Mullagur (mullagu2)

James Zhen (jzhen4)

Botnet Proposal

For our group project we decided to design a botnet. Botnets are ubiquitous in cybercrime, used for everything from DDoS attacks, to spamming, to identity theft, to bitcoin mining.

For our botnet, we would like to employ a P2P architecture to make it less susceptible to server takedown. In our design, there will be two types of infected machines: nodes, and workers. A node would be any machine that is able to accept incoming connections. These nodes would act as the “servers” in our botnet. Workers would be machines that cannot accept incoming connections, such as machines behind a firewall or NAT. Each node would have a collection of workers that report to that node. By isolating the workers into different groups, the botnet only loses part of its capabilities if a node is taken down. When we want to send out commands to the bot, we would send our commands out to the nodes, which would then distribute those commands out to the workers. Since the nodes can’t directly send commands to the workers, the workers will check in with their respective nodes to download commands at regular intervals.

In terms of capabilities, we had a few ideas that could be implemented. Some ideas we had were a keylogging feature, and DDoS capabilities. The modular nature of the botnet would allow us to implement or remove features as we see fit.