Task 6.1

Global source: [1]

Fast- or double-flux are methods used by botnets to hide the location of a server. The communication between the bots is centralized with a command & control server, which gives the commands for an attack to the associated bots. Since this communication is centralized it is quite easy to interrupt the communication by just taking out the command & control server.

Fast-flux is used to hide the location of this server. Therefore the so called Round robin DNS is used, which allows that several ip addresses can assigned to one domain name, normally used for load balancing[2]. When a bot tries to connect to his master server, he gets different ip addresses and can choose one. But these ip addresse aren’t leading to the master, but an also infected system, which just deals as a deliverer of communication between a bot and the master. Additionally the DNS-entries of the ip addresses have a short time to live and are changed regularly.

Double-flux describes a structure of several nodes that a continuously changing their DNS-list. This accomplishes another layer in the communication from a bot to its master.