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.

Task 6.4

Tor is a software that provides anonymous communication through its own network. Therefore it uses the so called onion routing. When installing the software, it connects with a directory with all available addresses to the Tor-servers. These servers apply as nodes for the communication through the Tor-network. Therefore a random route is chosen by the client over the Tor-nodes to establish a communication. The directory also contains the public key of every Tor-node to encrypt the communication between every point of the route. Since the communication is passing mostly three Tor-nodes, it is encrypted several times (onion routing).[3][4]

My browser isn't able to open *3g2upl4pq6kufc4m.onion*, because .onion addresses are not part of DNS. We would need a special application that is able to connect with the Tor-network. .onion domains can just be reached through the tor-network. [5]

[1] heise online – Hydra der Moderne, https://www.heise.de/security/artikel/Fast-Flux-271526.html, date accessed: 05.07.2016
[2] Wikipedia-Lastverteilung per DNS, https://de.wikipedia.org/wiki/Lastverteilung_per_DNS, date accessed: 05.07.2016
[3] Wikipedia-Tor (Netzwerk), https://de.wikipedia.org/wiki/Tor_(Netzwerk)#Arbeitsweise, date accessed: 05.07.2016
[4] Wikipedia-Onion-Routing, https://de.wikipedia.org/wiki/Onion-Routing, date accessed: 05.07.2016
[5] Wikipedia-.onion, https://de.wikipedia.org/wiki/.onion, date accessed: 05.07.2016

Task 6.7

“Centralized botnets are easy targets for takedown efforts by computer security researchers and law enforcement.” However, there are also peer-to-peer botnets.[1]

The authors propose a graph model to capture the vulnerabilities of P2P botnets and apply it several malware families in order to assess their resilience against different attacks.[1]

[1] Sok:P2PWNED – Modeling and Evaluating the Resilience of Peer-to-Peer Botnets, http://christian-rossow.de/publications/p2pwned-ieee2013.pdf, date accessed: 03.07.2016

[1] heise online – Hydra der Moderne, https://www.heise.de/security/artikel/Fast-Flux-271526.html, date accessed: 05.07.2016
[2] Wikipedia-Lastverteilung per DNS, https://de.wikipedia.org/wiki/Lastverteilung_per_DNS, date accessed: 05.07.2016
[3] Wikipedia-Tor (Netzwerk), https://de.wikipedia.org/wiki/Tor_(Netzwerk)#Arbeitsweise, date accessed: 05.07.2016
[4] Wikipedia-Onion-Routing, https://de.wikipedia.org/wiki/Onion-Routing, date accessed: 05.07.2016
[5] Wikipedia-.onion, https://de.wikipedia.org/wiki/.onion, date accessed: 05.07.2016