Proactive Botnet Detection and Defense at Internet scale
A collaborative approach

Problem: Botnets enable various cyber-criminal activities\cite{1,2}.

Research Questions:

RQ 1: What do bots need to be deployed and to form a new or join an existing botnet?
RQ 2: How do bots interact with central internet services, like the domain name service (DNS)?
RQ 3: How can the interaction with central services be used for detection before botnets can evolve their full size and power?

Approach: Detection and mitigation of botnets before they evolve their full size and attack power.

References:

