AN ARCHITECTURE FOR COLLABORATIVE SECURITY AND PROACTIVE DEFENSE AGAINST IOT BOTNETS

SYED MUHAMMAD SAJJAD

Problems

- DDoS mitigation is at destination end rather than source end.
- Higher Cost of DDoS destination end mitigation solutions
- DDoS mitigation is in Reactive mode.
- Device owner didn’t have the knowledge that his/her device is being compromised as bot and acting as source of DDoS
  - like in mirai the owners of the IP Cameras and Home routers have not information's that their devices are compromised

Objective

- DDoS detection at its source end at IoT bot propagation Stage
- Inform the device owner about the abnormal behavior of the device
- Mitigation steps against IoT Botnets during its propagation stage
- Collaboration and Incident Sharing between manufacturers for safeguarding their devices from becoming bots

Architecture