AN ARCHITECTURE FOR COLLABORATIVE SECURITY AND PROACTIVE DEFENSE AGAINST IOT BOTNETS

SYED MUHAMMAD SAJJAD
1. Attacker attacks customer IoTs Devices

2. MUD Manager identifies the abnormal behavior based on MUD Profile

3. MUD Manager reports abnormality to the owner of the device

4. MUD Manager exchanges abnormal behavior with Manufacturer (e.g., CACAO)

5a. CACAO Response (Mitigation Actions)

5b. Mitigation actions to MUD Manager on all its devices

6. Share Attacker Info With the manufacturer

7. Issue patch/software update to software supplier

8. Mitigation actions to MUD Manager on all its devices

Software Supplier