

# Botnets and IoT Devices

Colby Hill - [h@email.sc.edu](mailto:h@email.sc.edu)

Nathanael Ellsworth - [ellswon@email.sc.edu](mailto:ellswon@email.sc.edu)

Caleb Conner - [cconner@email.sc.edu](mailto:cconner@email.sc.edu)

Jon Ramit - [jramit@email.sc.edu](mailto:jramit@email.sc.edu)

Matthew Venter - [mventer@email.sc.edu](mailto:mventer@email.sc.edu)

Michael Miranda - [mirandat@email.sc.edu](mailto:mirandat@email.sc.edu)

Samuel Nichols - [samueln@email.sc.edu](mailto:samueln@email.sc.edu)

# Botnets in IoT Devices

Using IoT devices as a Botnet is an easy way to create a powerful Botnet.

IoT devices are powerful in numbers.

The Mirai malware has already proven how powerful IoT botnets can be.

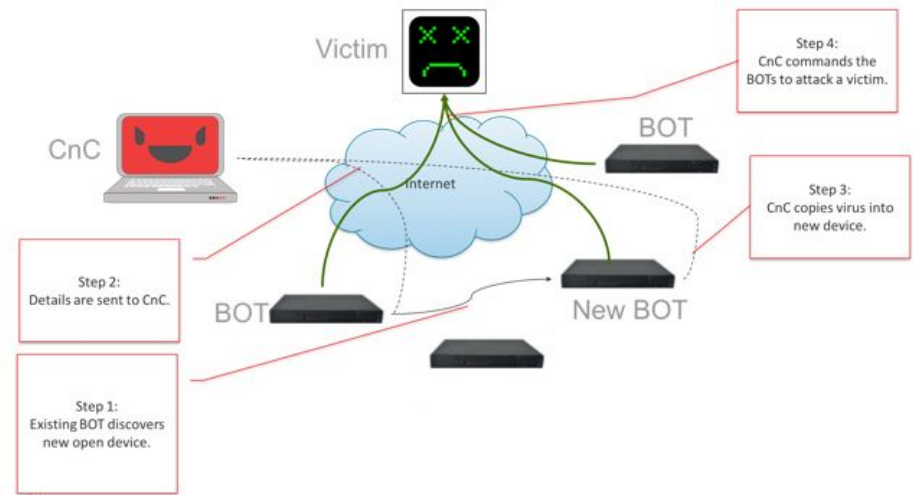
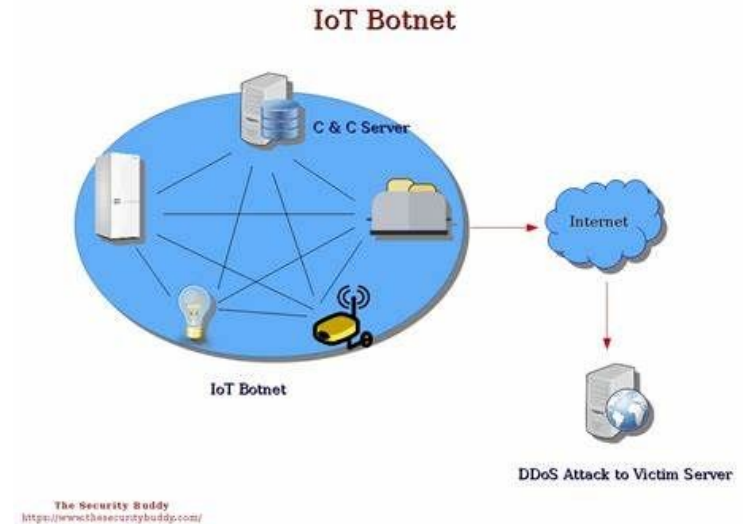


Figure 1 Mirai System



# Takeaway

- Securing IoT from the threat of BotNets is a challenge that does not have a simple solution
- Many solutions have been presented, all with benefits and drawbacks
  - Virtualized Networks
  - Centralized Management Devices
  - Standardized Firewalls
- The technologies exist, the greatest hurdle is the manufacturers
- Moving forward we can
  - find even better solutions / build upon those stated above
  - create incentive for companies to take the steps to better security of IoT devices