Weaponizing IoT

Ted Harrington
Executive Partner
Independent Security Evaluators (ISE)
@ISESecurity
Weaponize

wep-uh-nahyz

1) To convert to use as a weapon
2) To supply or equip with weapons
Agenda

- Overview
- Common IoT exploits
- Case Study
- Victim Chain
- Prophecies
- Recommendations
Overview
IoT Security Trends

August 2015 – Present:

- 113 new 0-days
- 50 device types
- 39 manufacturers
Common IoT Security Flaws

2016
- Denial of Service
- Lack of Encryption
- Key Exposure
- Privilege Escalation
- Remote Code Execution
- Backdoors
- Runs as Root

2017
- All of the previous!! \textit{PLUS:}
  - Buffer Overflow
  - Command Injection
  - Session Management
  - Etc etc etc
Exploit Analysis
Key Exposure
Remote Code Execution
Command Injection
Case Study: Mirai Botnet
Mirai Botnet

21 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today.
Mirai Botnet
Mirai Botnet
WHO CARES?!
Victim Chain
Where do we go from here?
Recommendations

- Threat Modeling
- Secure Design Principles
- Adversarial Perspective
- Self-regulate
Prophecies

- It will get worse before it gets better
- The 10/16/16 event was covering something larger
- A person(s) will get hurt physically
Apply

- Consider motivation
- Think like the attacker
- Adhere to secure design principles
Thank You!

ted.harrington@securityevaluators.com