Plan

What was Mirai?

How did it work?

Why did it work?

Course evals open very important?

This is your LAST RECITATION?

What do we do about it?

Feedback form. henrycg.com/feedback

Office hrs / AMA w/ Amir 5/20 9:30-12:30

Very important!
What was the Mirai botnet?

- Mess up the competition
- Political
- Gaming

Make green!

C2

Inter

C2.mirai.net

$\$\$

- Click fraud
- Bitcoin
- Spam email
- DDoS
**Technique**

1) Pick random IP address.
2) Try to connect to them using telnet.
   - guess user/pass
3) Once logged in, copy attack code to target.
   - run attack on target
What can you do to prevent this?

- Better passwords — safe defaults
- DNS analysis (ISP)
- Closed by default ("firewalls")
- Law enforcement

Public net → MIT net
Plan

* What was Mirai?
* How did it work?
* Why did it work & what do we do about it?

THE END!

Logistics

* This is your LAST RECITATION?
* Course evals open
  * Very important!
* Feedback form... post course notes?
  henrycg.com/Feedback

Office hrs / AMA w/ me & Amir
5/20 9:30-12:30 am

Sign up on Google doc
What was the Mirai botnet?

 externality

What do you do with a botnet?

- DDoS
- Send spam
- Make a bigger botnet
- Mine bitcoin
- Ad Scamd
Technique

1) Pick some random IP address
2) Try to login to them over telnet with common user/pass pair.
3) Once in, infect the machine.
What to do?

- Make it hard to make $ off attacks
- Stop using bad passwords
  - Default pass randomized
  - Force user to pick pass on first boot
- Decommission old devices
- Law enforcement (?)
- Block access to devices from pub internet by default
- Barrier to entry