


---

---

---

---

---



# Plan

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

## Logistics

\* This is your

LAST  
RECITATION!

\* Course evals open

↳ Very important!

\* Feedback form... post course notes?

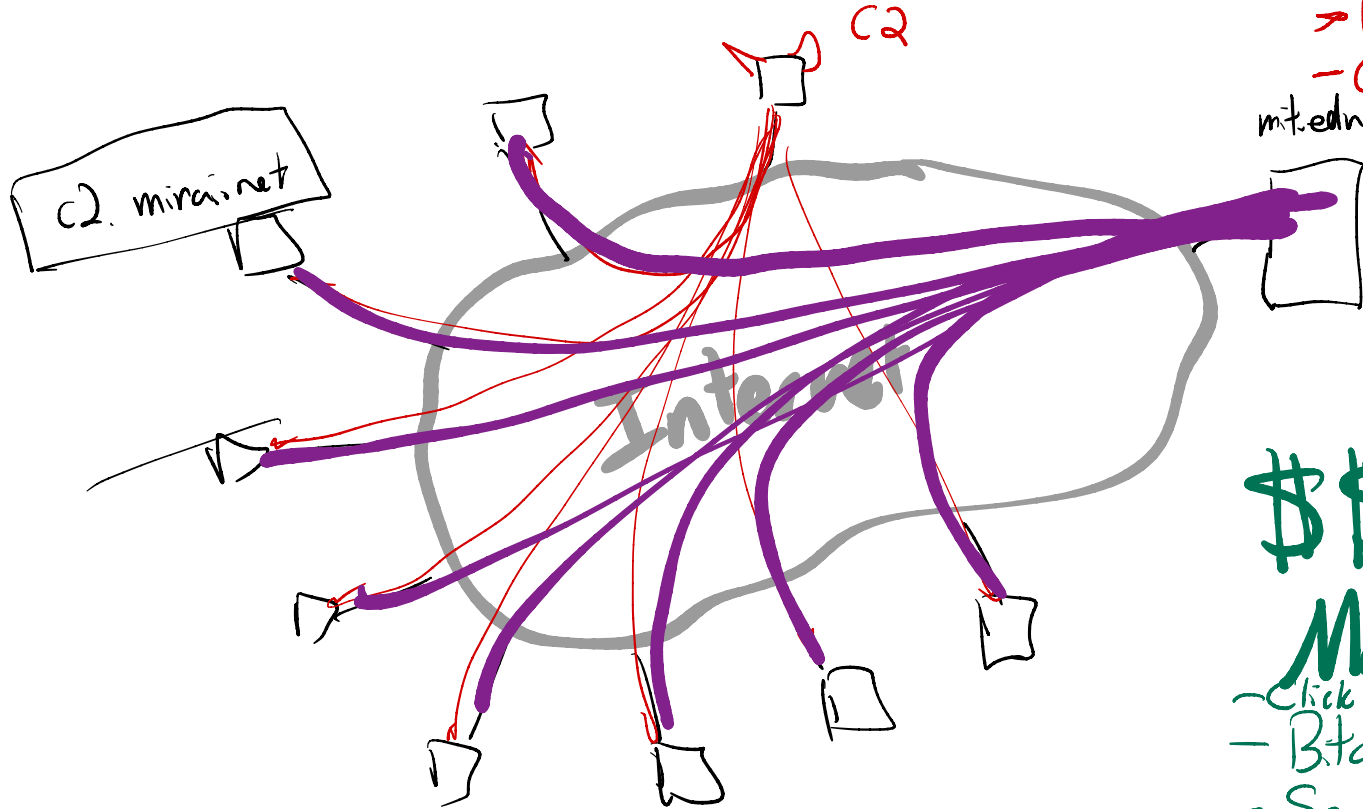
[henrycg.com/feedback](https://henrycg.com/feedback)

\* Office hrs /AMA w/ me & Amir  
5/20

↳ Sign up on  
Google doc

9:30-10:30  
am

# What was the Mirai botnet?



- Mess up the competition  
→ Political

- Gaming

mit.edu

\$\$\$

Make green!

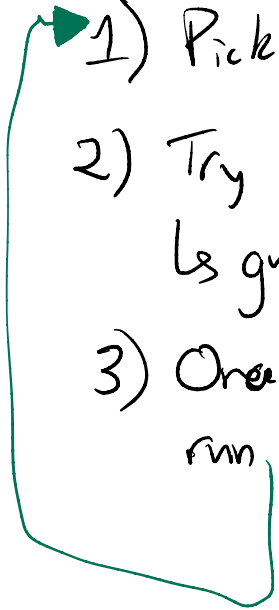
- Click Fraud

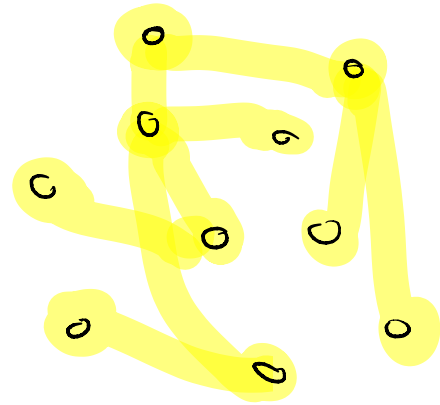
- Bitcoin

- Spam email

- DDoS

# Technique

- 1) Pick random IP addrs.
  - 2) Try to connect to them using telnet  
↳ guess user/pass
  - 3) Once logged in, copy attack code to target,  
run attack on target
- 



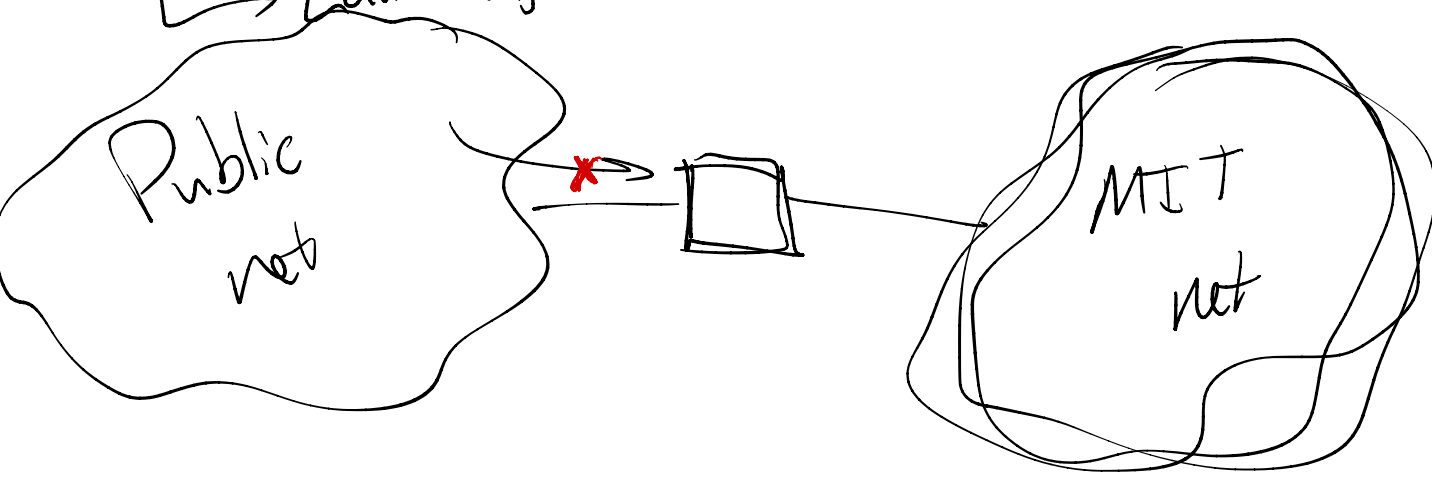
What can you do to prevent this?

↳ Better passwords — safe defaults

↳ DNS analysis (ISP)

↳ Closed by default ("firewalls")

↳ Law enforcement



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](https://henrycg.com/feedback)

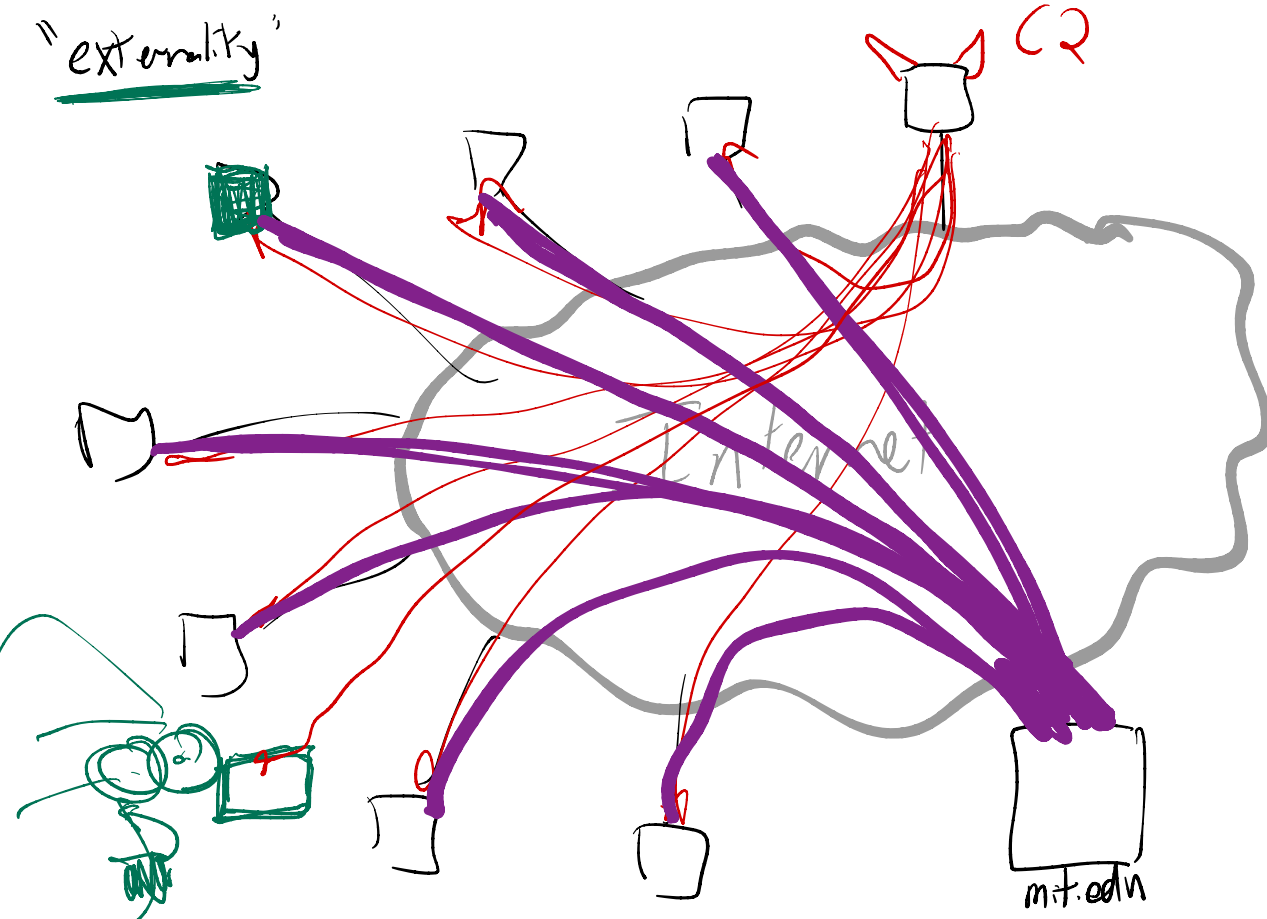
\* Office hrs /AMA w/ me & Amir  
5/20

↳ Sign up on  
Google doc

9:30-10:30  
am

# What was the Mirai botnet?

"externality"



What do you do with a botnet?



(political ends)

↳ DDoS

↳ Send spam

↳ Make a bigger botnet

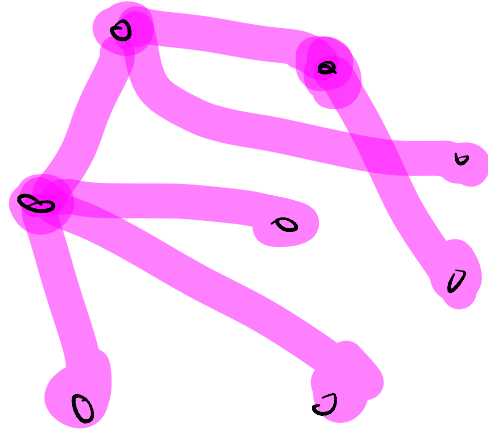
↳ Mine bitcoin

↳ Ad Fraud

- political
- retaliation  
banks  
govt
- gaming

# Technique

- 1) Pick some random IP address
- 2) Try to login to them over telnet  
w/ 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.

