Recitation 24: Mirai

MIT - 6.033

Spring 2022

Henry Corrigan-Gibbs

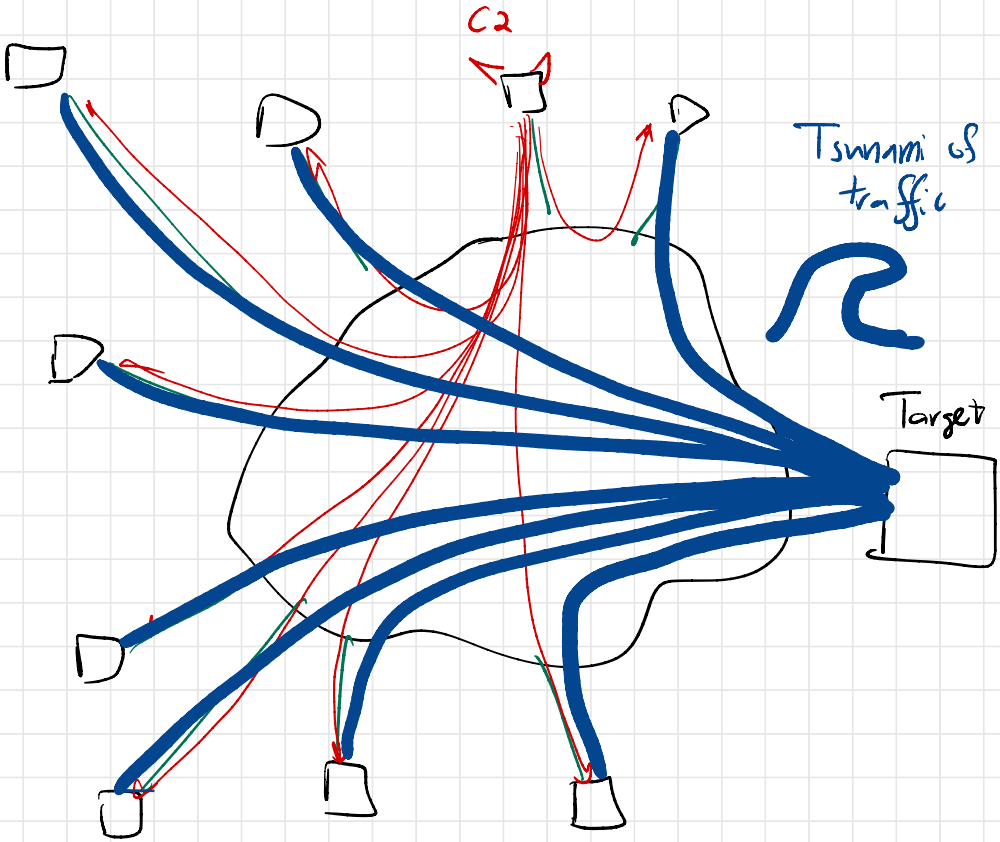
Plan

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

Logistics

* Check out the computer
* Exam 2 on 5/16 9-11am, Johnson Track
* Course evaluations open
  ↳ **Very important**
* Feedback form — post course notes?
* AMA / Chilling outside 5/12 10am-noon State Amphitheatre

What was the Mirai botnet?



Botnet = large fleet of hijacked machines that one entity controls.

Purpose: $$$! → Distributed DoS { political, business, gaming
→ Ad fraud
→ Spam mail

Technique:

1) Infected machines scan IPv4 space
2) Try common user/pass pairs
   ↳ Very common!?
3) Once logged in, infect machine

This attack is simple enough that any of us could do it.
↳ SHOW CODE

DO NOT TRY THIS AT HOME!?
↳ Bad karma and also illegal... many stories

Scanning like this is very common
↳ show market logs
↳ show country analysis
↳ show nmap

Be careful if you have a machine w/ a public IP (e.g. story at Stanford)

Things of note

* Different Mirai "flavors" often code leaked
* Mirai used to DDoS Mirai C2 servers
* Mirai competes against Mirai for hosts

Targets ....

Discuss in groups?

Why did it work?

- No one thought that these were security critical
  - ↳ Unsafe defaults
- Devices are not patched
  - ↳ How often do you update your TV / router / doorbell / toaster?
    - ↳ End-of-life problem
- Devices on open Internet — open by default

Also:

Incentive problem!

- ↳ Cost of security paid by you and toaster vendor
- ↳ benefit of security accrues to people getting DDoS'd.

#$#!

... Remember back to our first paper

"We did nothing wrong" ...

What do we do about it?

(Similar to preventing bank robberies?)

- Mandate safe defaults? (CA law)
  - "connected device" has to have unique pass or asked on 1st boot
- Mandate updates?
- Improve law enforcement / accountability?
- Eliminate payment channels?

For next time...

- Look at past papers, past exams
  - ↳ Bring your questions!
- Is there anything particular you'd like us to cover?
  - ↳ henrycg.com/feedback

Submit your subject evaluations, pleaw pleaze pleaze!