# U-Pick-Em!

# Internet of Things Security

# Goals for Today

Learning Objectives:

Define Internet of Things and recognize its place in computing today

Understand IoT security challenges and the state of current security research

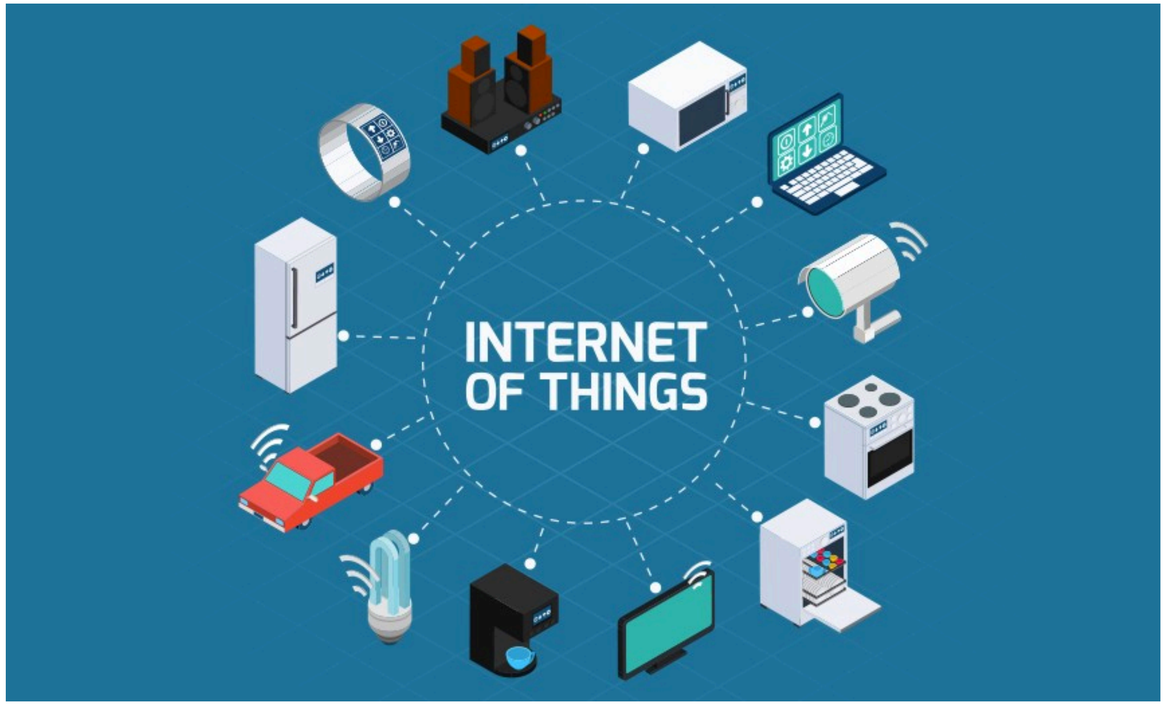
Announcements, etc:

Final Exam is on Dec 13 at 7pm

Forensics CP2 due Friday, Dec 6th at 6PM

# What is the Internet of Things?

# Internet of Things

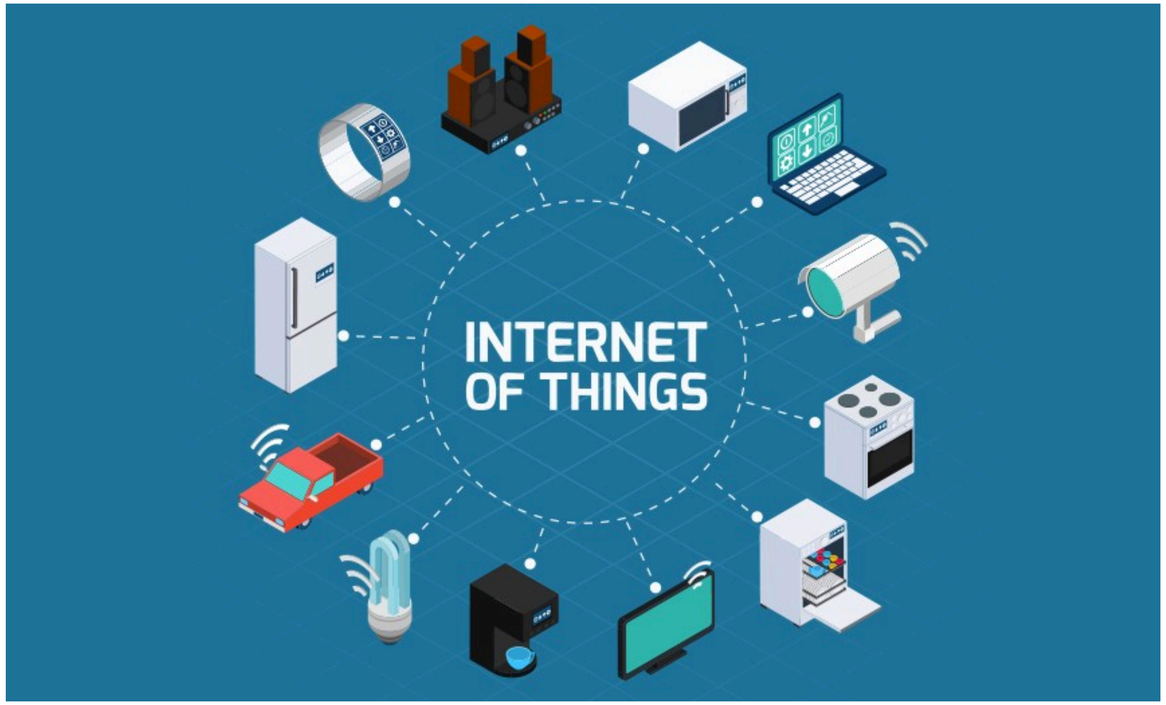



https://towardsdatascience.com/iot-in-action-a8b7fac83619

From Wikipedia:

> "The **Internet of Things** (**IoT**) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

# Internet of Things

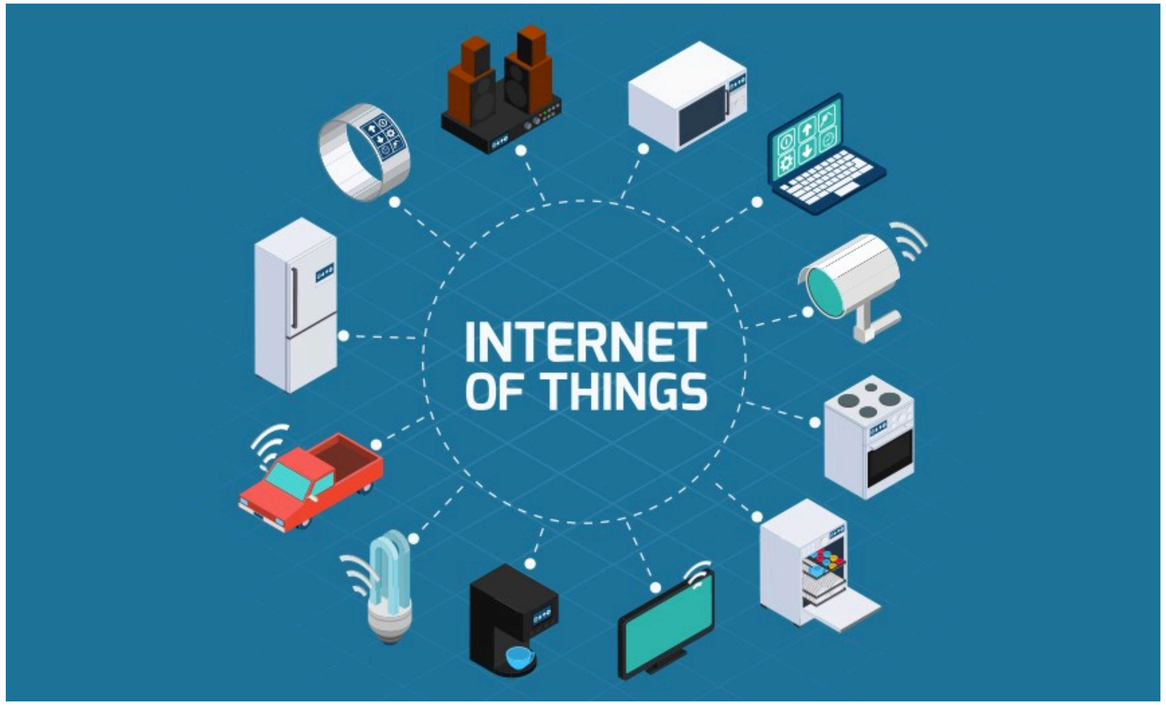



https://towardsdatascience.com/iot-in-action-a8b7fac83619

From Google:

> "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."

# Internet of Things




https://towardsdatascience.com/iot-in-action-a8b7fac83619

From me:

> “An IoT device is one that combines sensing and networked control to actuate in the real world.”

# IoT Examples




https://www.theverge.com/2019/5/29/18644973/ecobee-smart-thermostat-premium-glass-leak-lowes

# More IoT Examples

## Rethink the refrigerator

From creating shopping lists to coordinating schedules to playing your favorite song and mirroring your TV shows, the Family Hub™ keeps your life more connected than ever.

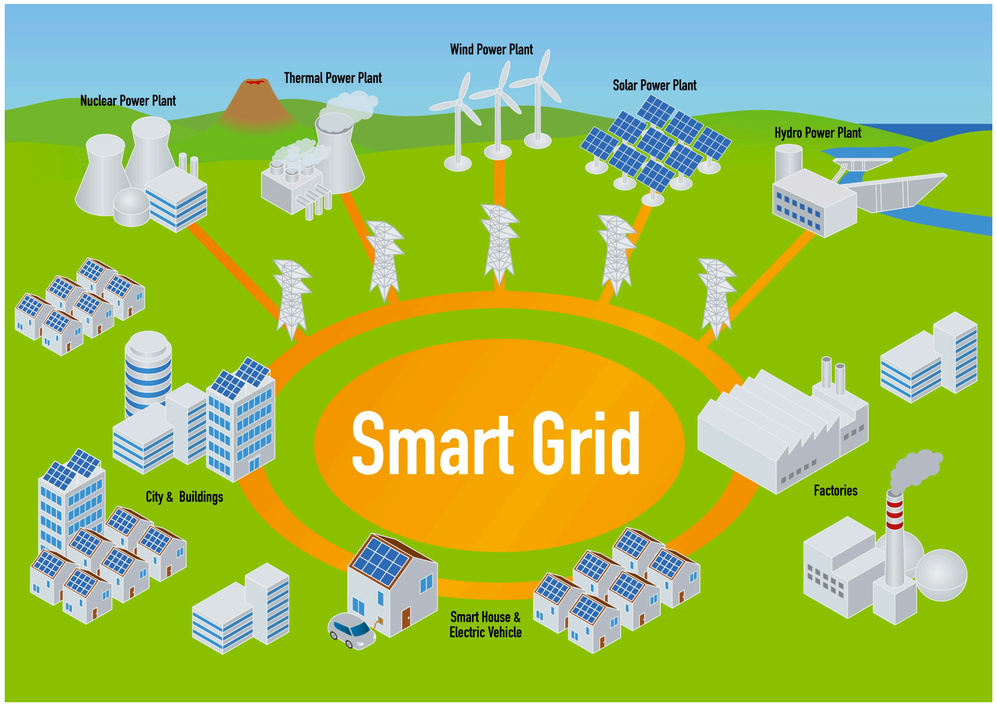

## Smart toasters are here

## What Are Smart Clothes?

Discover how your clothes can improve your life

https://www.designnews.com/automation-motion-control/10-weirdest-iot-applications

# Even More IoT Examples





https://blog.westmonroepartners.com/the-utility-iot-can-the-smart-grid-make-our-homes-businesses-cities-smarter/

**IoT is much more than just the home – it expands to our critical infrastructure, to our cities, and our everyday lives**

**Smart home devices attract hackers in their first five minutes online**

**‘World’s first Bluetooth hair straighteners’ can be easily hacked**

Researchers demonstrate new ways to hack your stupidly complex smart home

**'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices**

**How one lightbulb could allow hackers to burgle your home**

**Security flaws in a popular smart home hub let hackers unlock front doors**

# What makes IoT so hard to secure?

# What makes IoT so hard to secure?

Heterogenous ecosystem

- Devices are running on a diverse set of hardware, running bespoke (often vulnerable!) software, and are globally distributed

Wider Attack Surface

- Could attack sensor, the device itself, the software controlling the device, the cloud backend

Lack of realistic security measurements

- Devices are sitting behind NATs or private networks, making it challenging to diagnose security problems at scale

# Mirai

THE WALL STREET JOURNAL.

## Cyberattack Knocks Out Access to Websites

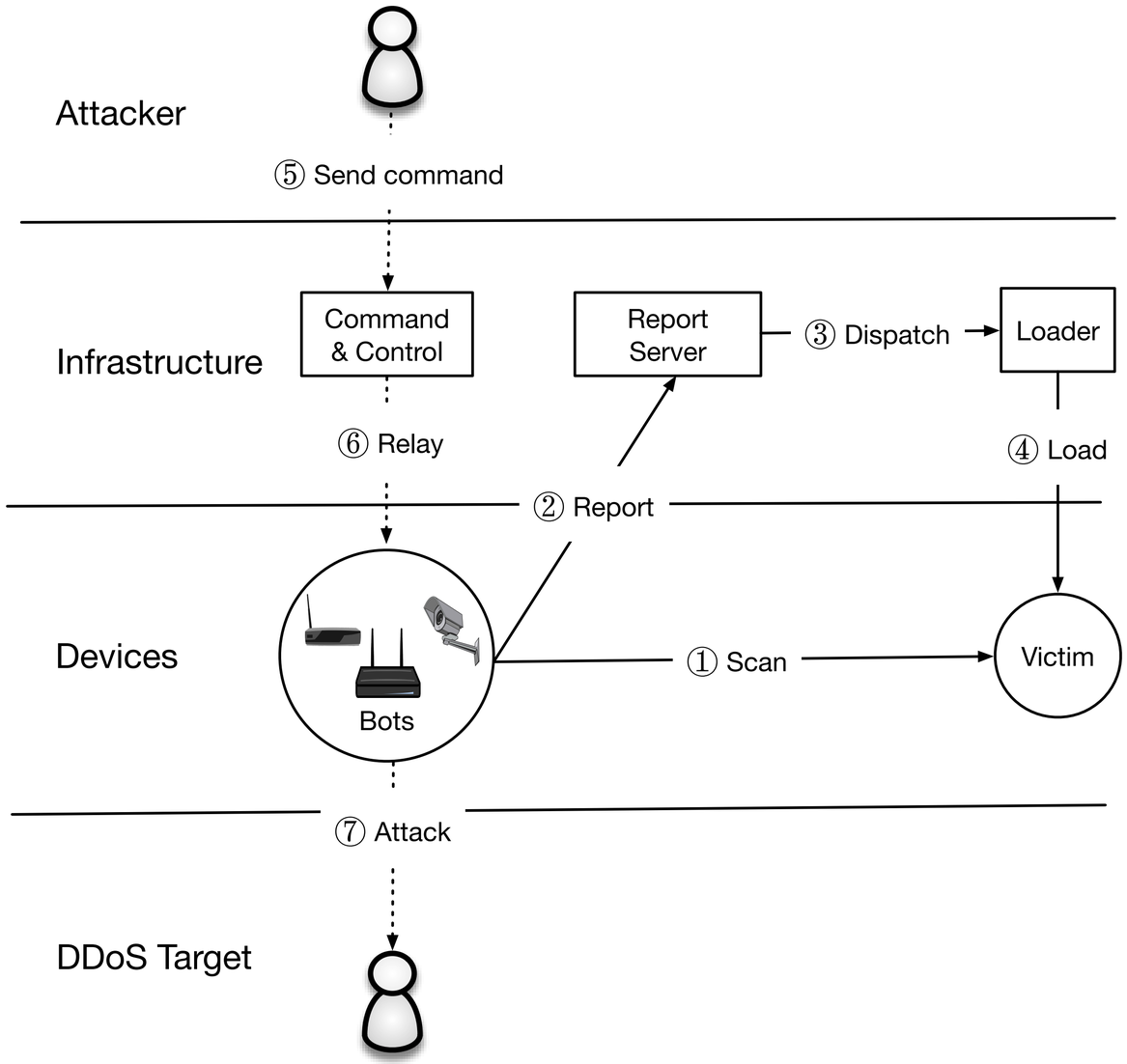
Popular sites such as Twitter, Netflix and PayPal were unreachable for part of the day

**21 KrebsOnSecurity Hit With Record DDoS**
SEP 16

KrebsonSecurity
In-depth security news and investigation

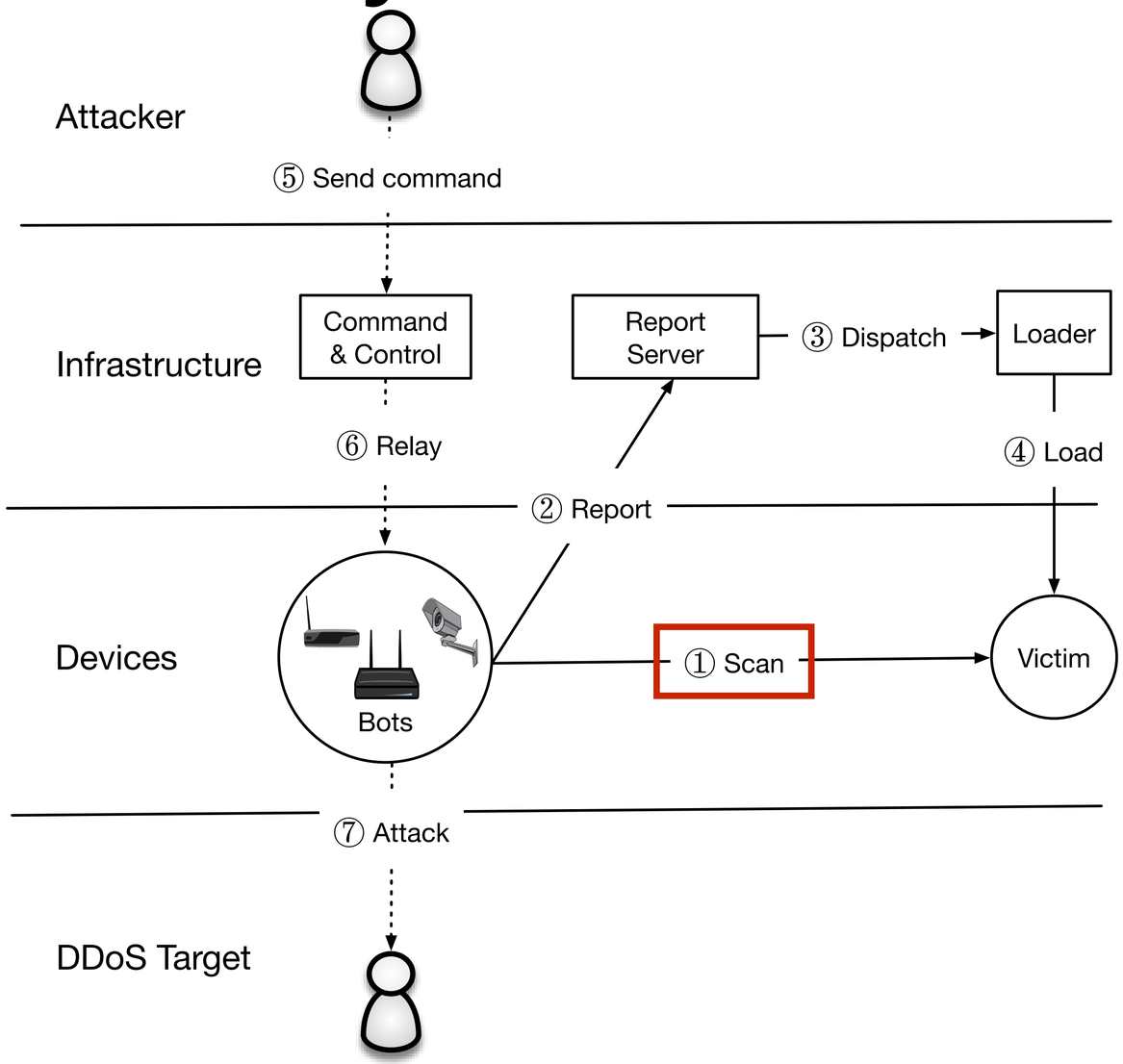
**01 Source Code for IoT Botnet 'Mirai' Released**
OCT 16

# How Did Mirai Work?

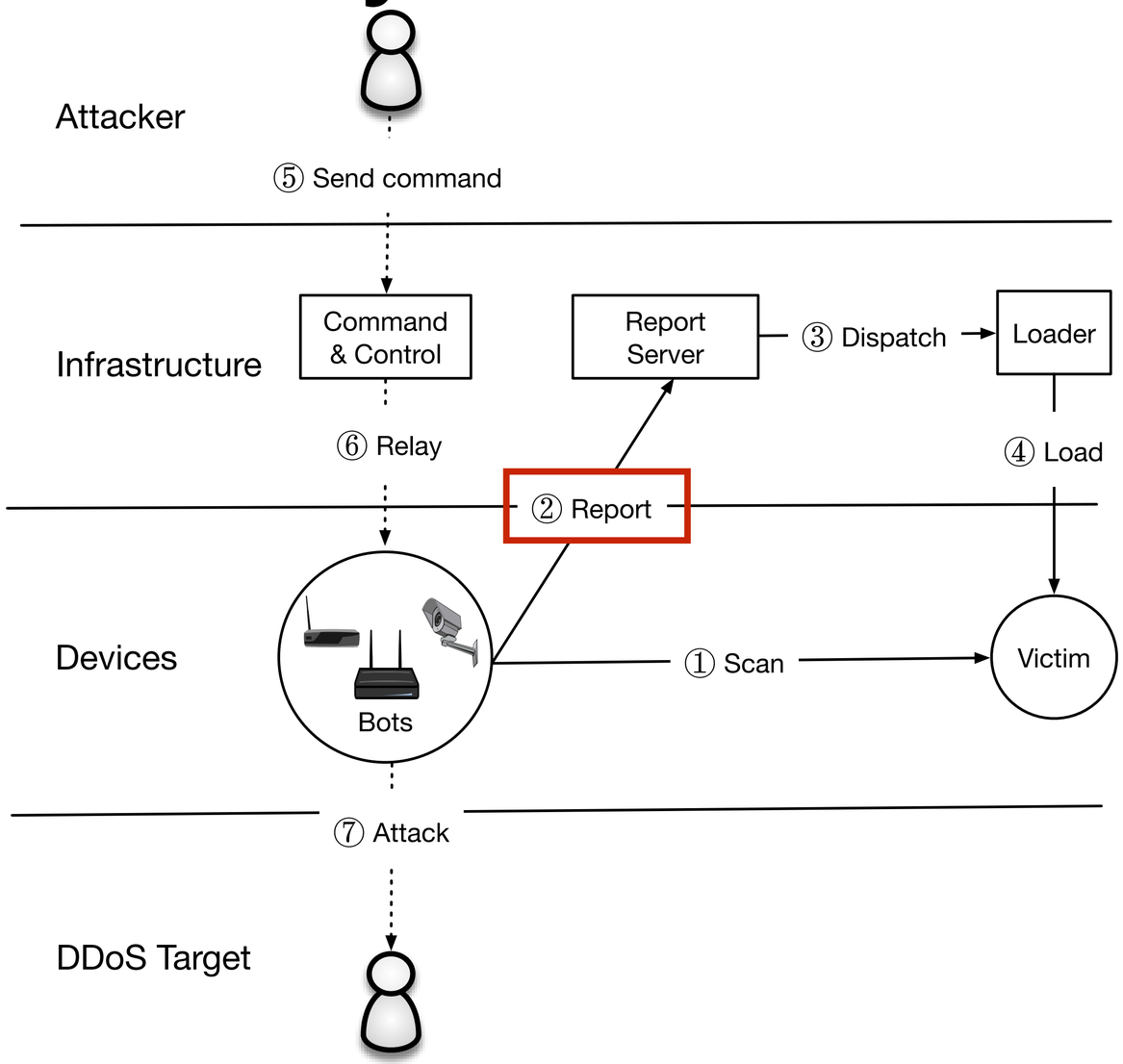



**Mirai infected IoT devices with weak, default credentials**

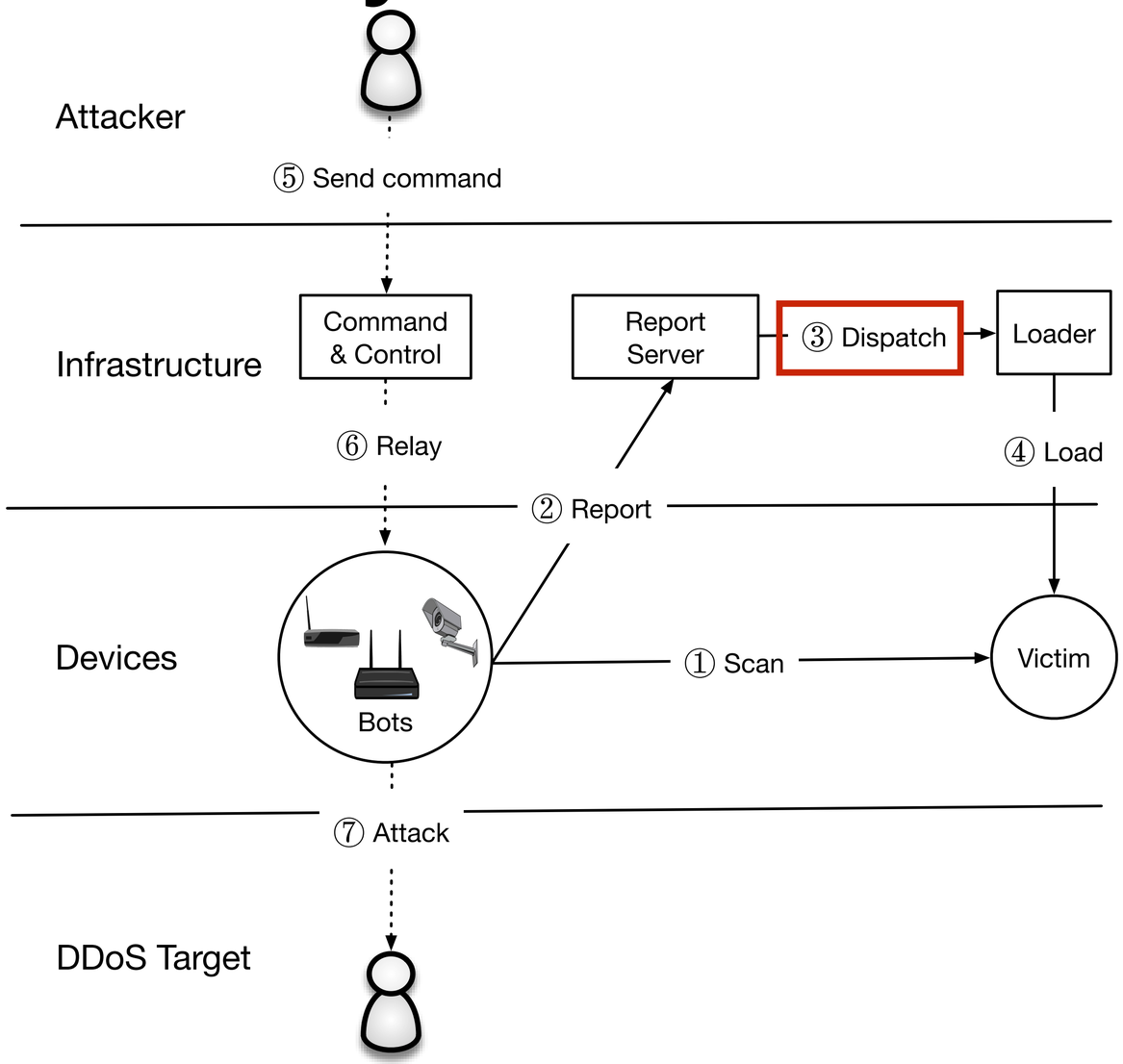
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

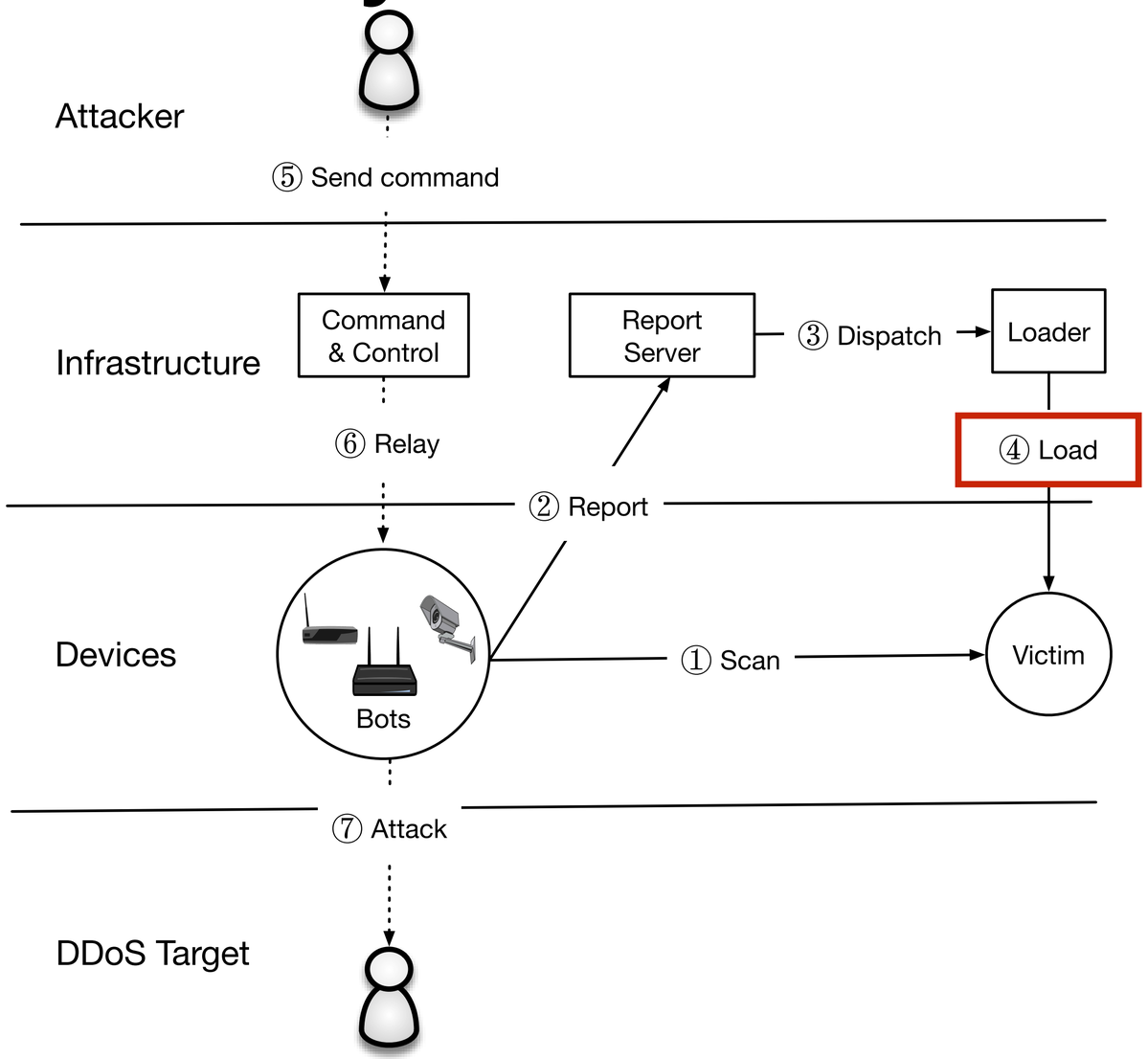
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

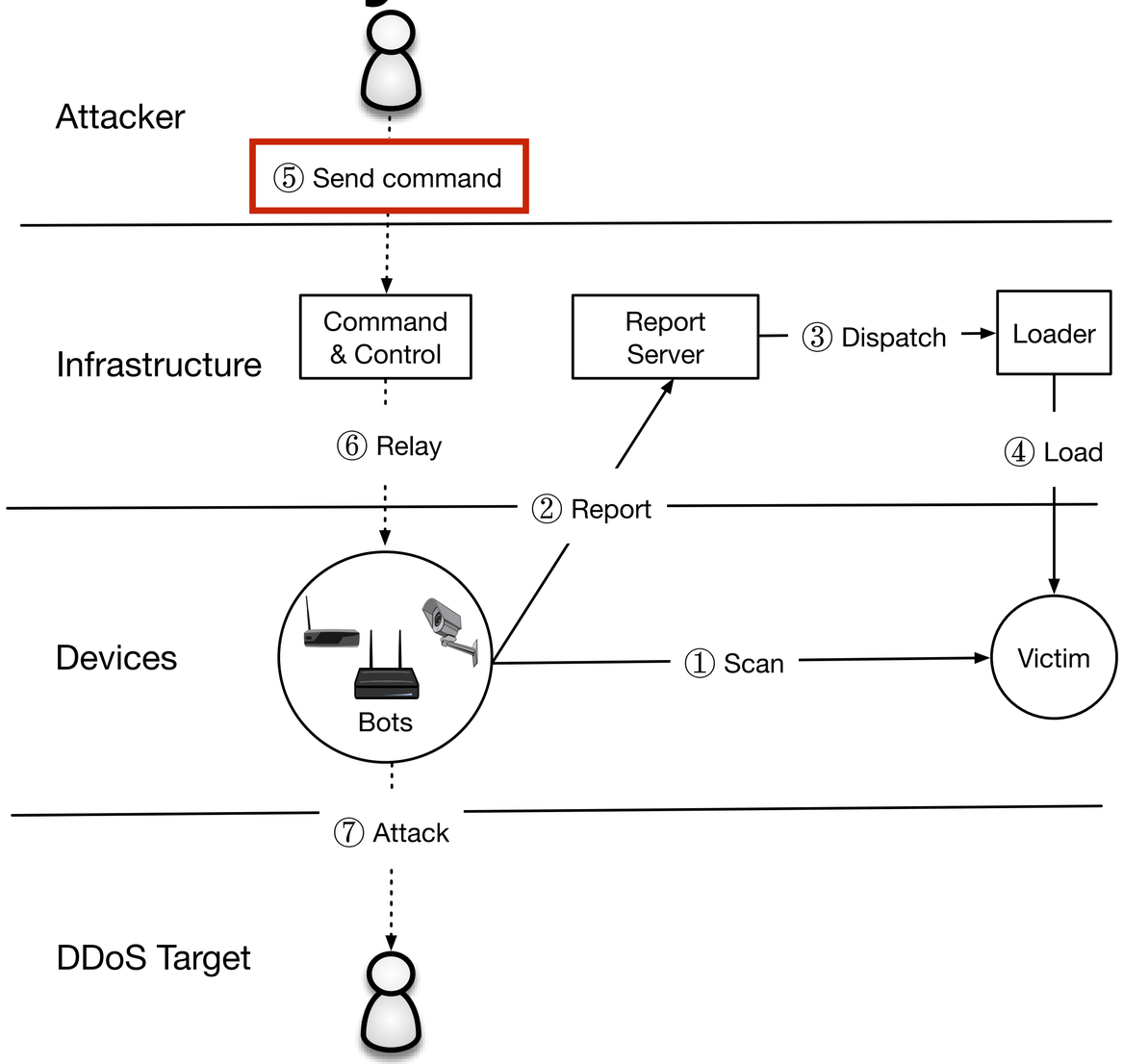
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

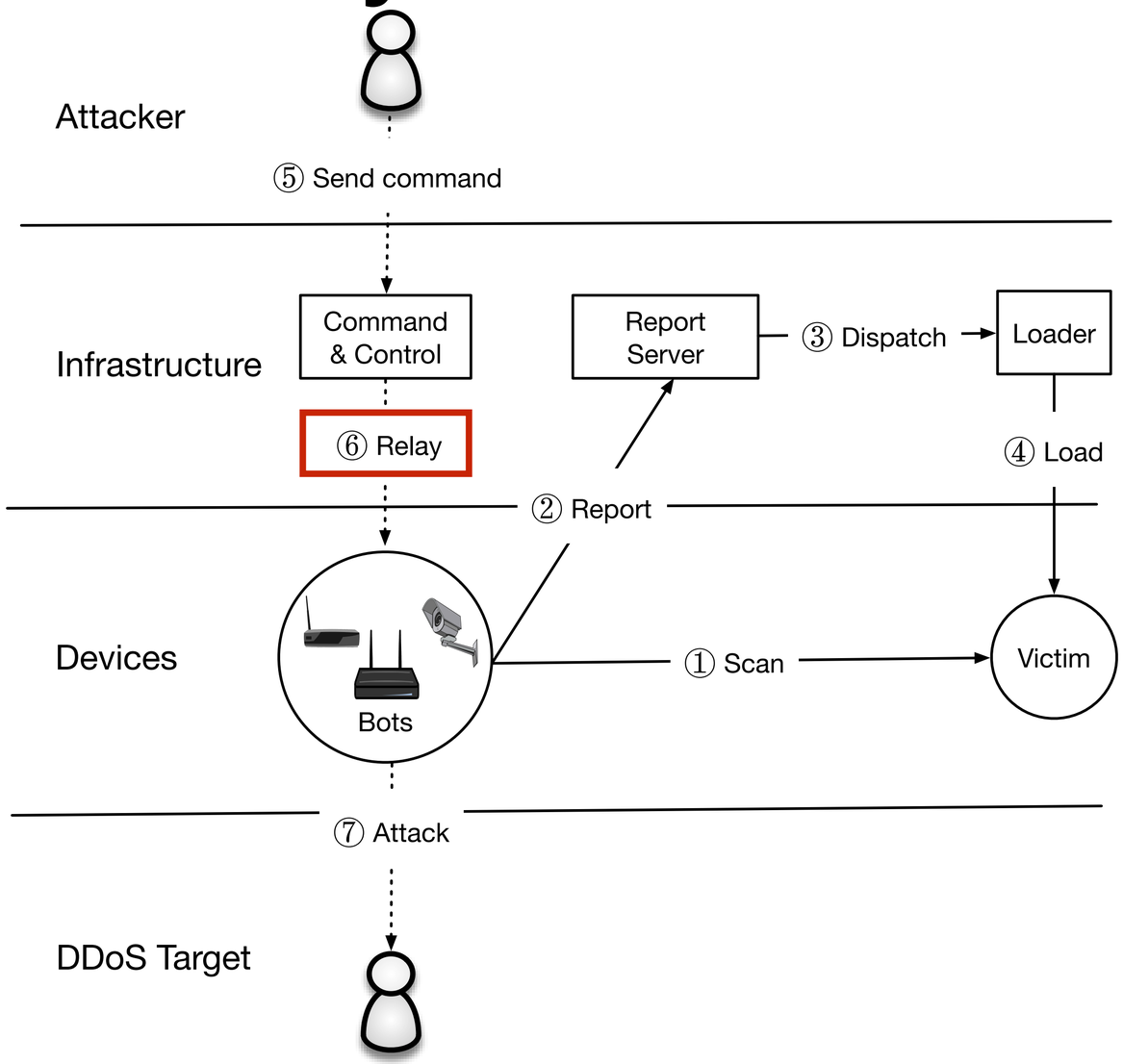
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

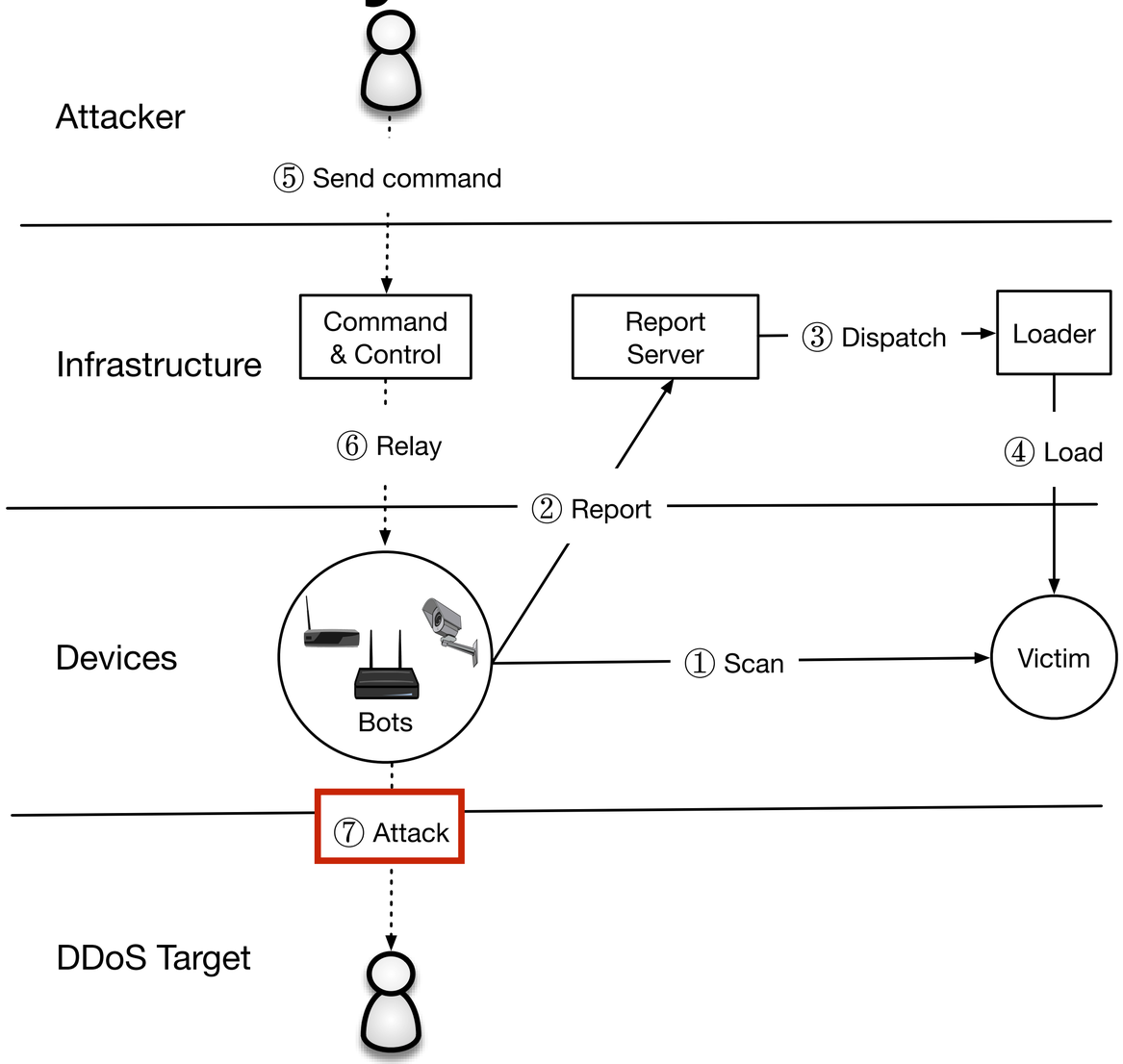
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

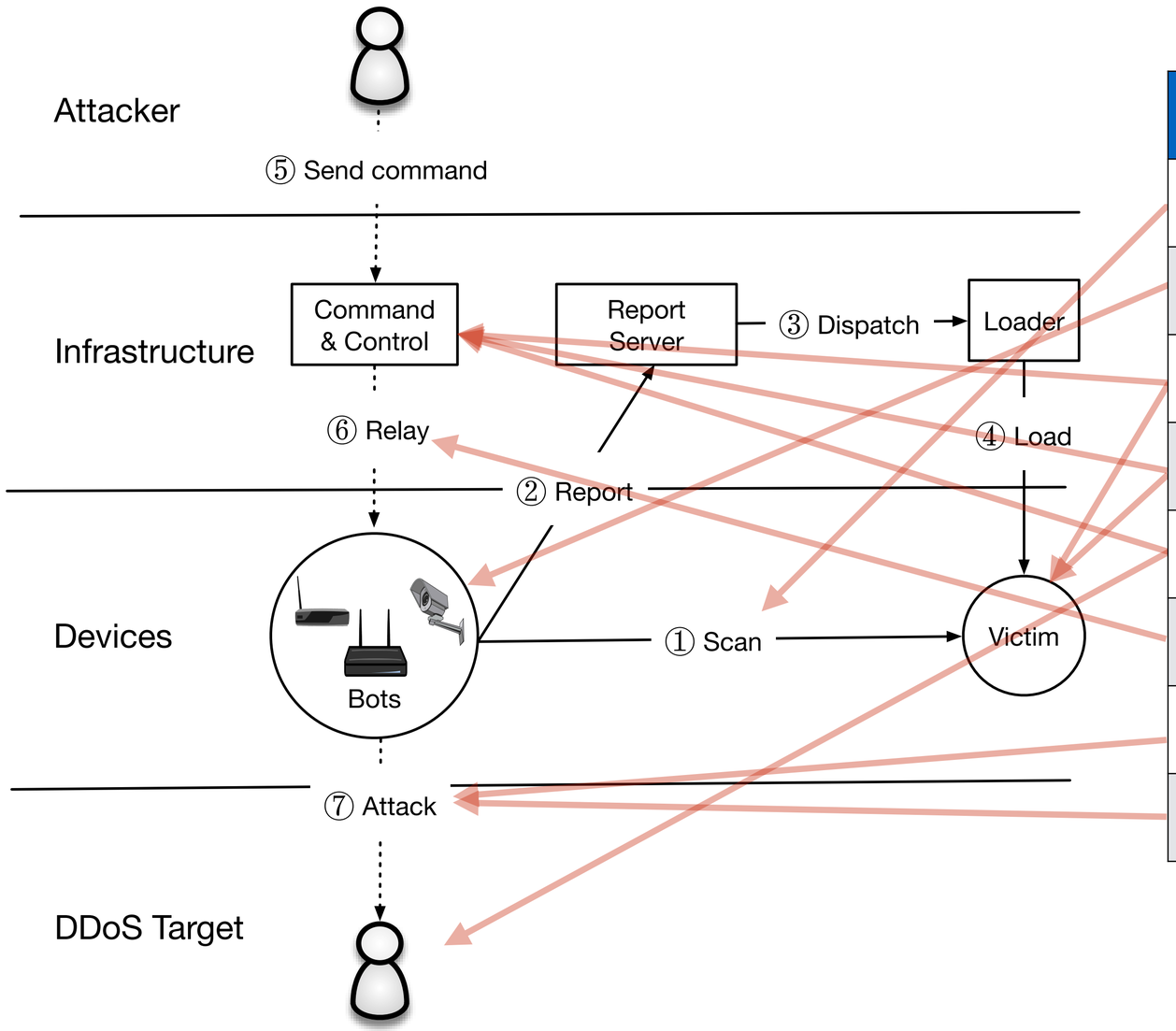
# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

# Lifecycle


Attacker
⑤ Send command
Infrastructure
Command & Control
Report Server
③ Dispatch
Loader
⑥ Relay
④ Load
② Report
Devices
Bots
① Scan
Victim
⑦ Attack
DDoS Target

# Measurements




| Data Source | Size |
|---|---|
| Network Telescope | 4.7M unused IPs |
| Active Scanning | 136 IPv4 scans |
| Telnet Honeypots | 434 binaries |
| Malware Repository | 594 binaries |
| Active/Passive DNS | 499M daily RRs |
| C2 Milkers | 64K issued attacks |
| Krebs DDoS Attack | 170K attacker IPs |
| Dyn DDoS Attack | 108K attacker IPS |

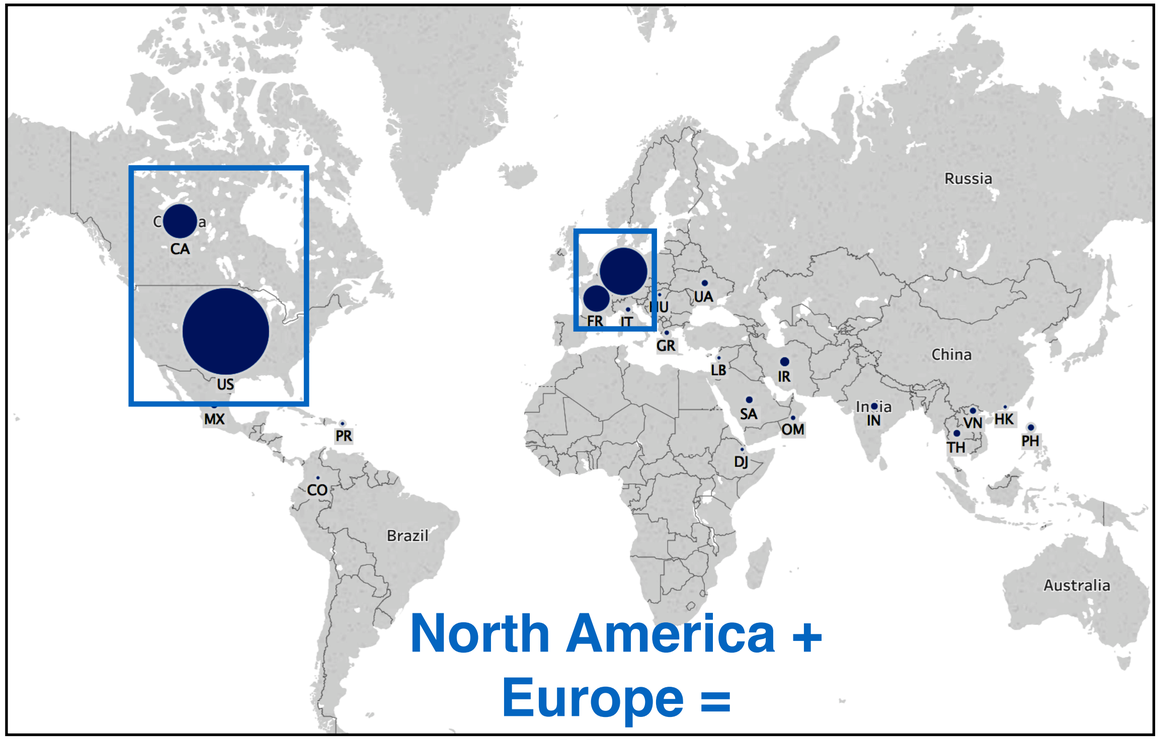
**July 2016 - February 2017**

# Geography

## Mirai


South America + Southeast Asia = 50% of Infections

## TDSS/TDL4




North America + Europe = 94% of Infections

# Composition

## Targeted Default Passwords

| Password | Device Type | Password | Device Type | Password | Device Type |
|---|---|---|---|---|---|
| 123456 | ACTi IP Camera | klv1234 | HiSilicon IP Camera | 1111 | Xerox Printer |
| anko | ANKO Products DVR | jvbzd | HiSilicon IP Camera | Zte521 | ZTE Router |
| pass | Axis IP Camera | admin | IPX-DDK Network Camera | 1234 | Unknown |
| 888888 | Dahua DVR | system | IQinVision Cameras | 12345 | Unknown |
| 666666 | Dahua DVR | meinsm | Mobotix Network Camera | admin1234 | Unknown |
| vizxv | Dahua IP Camera | 54321 | Packet8 VOIP Phone | default | Unknown |
| 7ujMko0vizxv | Dahua IP Camera | 00000000 | Panasonic Printer | fucker | Unknown |
| 7ujMko0admin | Dahua IP Camera | realtek | RealTek Routers | guest | Unknown |
| 666666 | Dahua IP Camera | 1111111 | Samsung IP Camera | password | Unknown |
| dreambox | Dreambox TV Receiver | xmhdipc | Shenzhen Anran Camera | root | Unknown |
| juantech | Guangzhou Juan Optical | smcadmin | SMC Routers | service | Unknown |
| xc3511 | H.264 Chinese DVR | ikwb | Toshiba Network Camera | support | Unknown |
| OxhlwSG8 | HiSilicon IP Camera | ubnt | Ubiquiti AirOS Router | tech | Unknown |
| cat1029 | HiSilicon IP Camera | supervisor | VideoIQ | user | Unknown |
| hi3518 | HiSilicon IP Camera | <none> | Vivotek IP Camera | zlxx. | Unknown |
| klv123 | HiSilicon IP Camera | | | | |

# Composition

## Targeted Default Passwords

| Password | Device Type | Password | Device Type | Password | Device Type |
|---|---|---|---|---|---|
| 123456 | ACTi IP Camera | klv1234 | HiSilicon IP Camera | 1111 | Xerox Printer |
| anko | ANKO Products DVR | jvbzd | HiSilicon IP Camera | Zte521 | ZTE Router |
| pass | Axis IP Camera | admin | IPX-DDK Network Camera | 1234 | Unknown |
| 888888 | Dahua DVR | system | IQinVision Cameras | 12345 | Unknown |
| 666666 | Dahua DVR | meinsm | Mobotix Network Camera | admin1234 | Unknown |
| vizxv | Dahua IP Camera | 54321 | Packet8 VOIP Phone | default | Unknown |
| 7ujMko0vizxv | Dahua IP Camera | 00000000 | Panasonic Printer | fucker | Unknown |
| 7ujMko0admin | Dahua IP Camera | realtek | RealTek Routers | guest | Unknown |
| 666666 | Dahua IP Camera | 1111111 | Samsung IP Camera | password | Unknown |
| dreambox | Dreambox TV Receiver | xmhdipc | Shenzhen Anran Camera | root | Unknown |
| juantech | Guangzhou Juan Optical | smcadmin | SMC Routers | service | Unknown |
| xc3511 | H.264 Chinese DVR | ikwb | Toshiba Network Camera | support | Unknown |
| OxhlwSG8 | HiSilicon IP Camera | ubnt | Ubiquiti AirOS Router | tech | Unknown |
| cat1029 | HiSilicon IP Camera | supervisor | VideoIQ | user | Unknown |
| hi3518 | HiSilicon IP Camera | <none> | Vivotek IP Camera | zlxx. | Unknown |
| klv123 | HiSilicon IP Camera | | | | |

# Composition

## Infected Devices

| CWMP (28.30%) | | Telnet (26.44%) | | HTTPS (19.13%) | | FTP (17.82%) | | SSH (8.31%) | |
|---|---|---|---|---|---|---|---|---|---|
| Router | 4.7% | Router | 17.4% | Camera/DVR | 36.8% | Router | 49.5% | Router | 4.0% |
| | | Camera/DVR | 9.4% | Router | 6.3% | Storage | 1.0% | Storage | 0.2% |
| | | | | Storage | 0.2% | Camera/DVR | 0.4% | Firewall | 0.2% |
| | | | | Firewall | 0.1% | Media | 0.1% | Security | 0.1% |
| Other | 0.0% | Other | 0.1% | Other | 0.2% | Other | 0.0% | Other | 0.0% |
| Unknown | 95.3% | Unknown | 73.1% | Unknown | 56.4% | Unknown | 49.0% | Unknown | 95.6% |

| CWMP (28.30%) | | Telnet (26.44%) | | HTTPS (19.13%) | | FTP (17.82%) | | SSH (8.31%) | |
|---|---|---|---|---|---|---|---|---|---|
| Huawei | 3.6% | Dahua | 9.1% | Dahua | 36.4% | D-Link | 37.9% | MikroTik | 3.4% |
| ZTE | 1.0% | ZTE | 6.7% | MultiTech | 26.8% | MikroTik | 2.5% | | |
| | | Phicomm | 1.2% | ZTE | 4.3% | ipTIME | 1.3% | | |
| | | | | ZyXEL | 2.9% | | | | |
| | | | | Huawei | 1.6% | | | | |
| Other | 2.3% | Other | 3.3% | Other | 7.3% | Other | 3.8% | Other | 1.8% |
| Unknown | 93.1% | Unknown | 79.6% | Unknown | 20.6% | Unknown | 54.8% | Unknown | 94.8% |

# Composition

## Infected Devices

| CWMP (28.30%) | | Telnet (26.44%) | | HTTPS (19.13%) | | FTP (17.82%) | | SSH (8.31%) | |
|---|---|---|---|---|---|---|---|---|---|
| Router | 4.7% | Router | 17.4% | Camera/DVR | 36.8% | Router | 49.5% | Router | 4.0% |
| | | Camera/DVR | 9.4% | Router | 6.3% | Storage | 1.0% | Storage | 0.2% |
| | | | | Storage | 0.2% | Camera/DVR | 0.4% | Firewall | 0.2% |
| | | | | Firewall | 0.1% | Media | 0.1% | Security | 0.1% |
| Other | 0.0% | Other | 0.1% | Other | 0.2% | Other | 0.0% | Other | 0.0% |
| Unknown | 95.3% | Unknown | 73.1% | Unknown | 56.4% | Unknown | 49.0% | Unknown | 95.6% |

| CWMP (28.30%) | | Telnet (26.44%) | | HTTPS (19.13%) | | FTP (17.82%) | | SSH (8.31%) | |
|---|---|---|---|---|---|---|---|---|---|
| Huawei | 3.6% | Dahua | 9.1% | Dahua | 36.4% | D-Link | 37.9% | MikroTik | 3.4% |
| ZTE | 1.0% | ZTE | 6.7% | MultiTech | 26.8% | MikroTik | 2.5% | | |
| | | Phicomm | 1.2% | ZTE | 4.3% | ipTIME | 1.3% | | |
| | | | | ZyXEL | 2.9% | | | | |
| | | | | Huawei | 1.6% | | | | |
| Other | 2.3% | Other | 3.3% | Other | 7.3% | Other | 3.8% | Other | 1.8% |
| Unknown | 93.1% | Unknown | 79.6% | Unknown | 20.6% | Unknown | 54.8% | Unknown | 94.8% |

# Dyn Attack

The New York Times

"It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability."







# Dyn Attack

The New York Times

> "It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability."

| Targeted IP | rDNS |
|---|---|
| 208.78.70.5 | ns1.p05.dynect.net |
| 204.13.250.5 | ns2.p05.dynect.net |
| 208.78.71.5 | ns3.p05.dynect.net |
| 204.13.251.5 | ns4.p05.dynect.net |
| 198.107.156.219 | service.playstation.net |
| 216.115.91.57 | service.playstation.net |

# Dyn Attack

The New York Times

"It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability."

| Targeted IP | rDNS | Passive DNS |
|---|---|---|
| 208.78.70.5 | ns1.p05.dynect.net | **ns00.playstation.net** |
| 204.13.250.5 | ns2.p05.dynect.net | **ns01.playstation.net** |
| 208.78.71.5 | ns3.p05.dynect.net | **ns02.playstation.net** |
| 204.13.251.5 | ns4.p05.dynect.net | **ns03.playstation.net** |
| 198.107.156.219 | service.playstation.net | **ns05.playstation.net** |
| 216.115.91.57 | service.playstation.net | **ns06.playstation.net** |

- Top targets are linked to Sony PlayStation
- Attacks on Dyn interspersed among attacks on other game services

# How a Dorm Room *Minecraft* Scam Brought Down the Internet

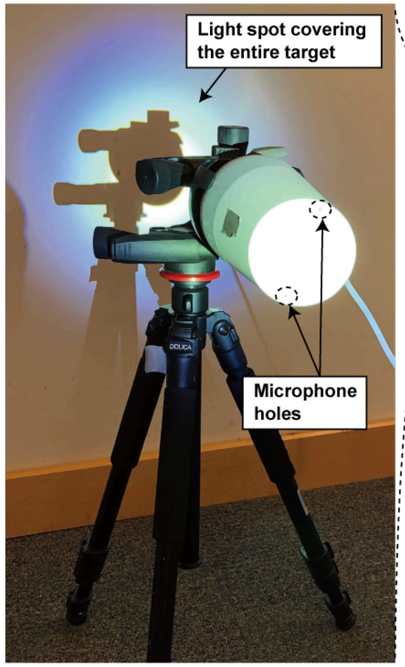
The DDoS attack that crippled the internet last fall wasn't the work of a nation-state. It was three college kids working a *Minecraft* hustle.

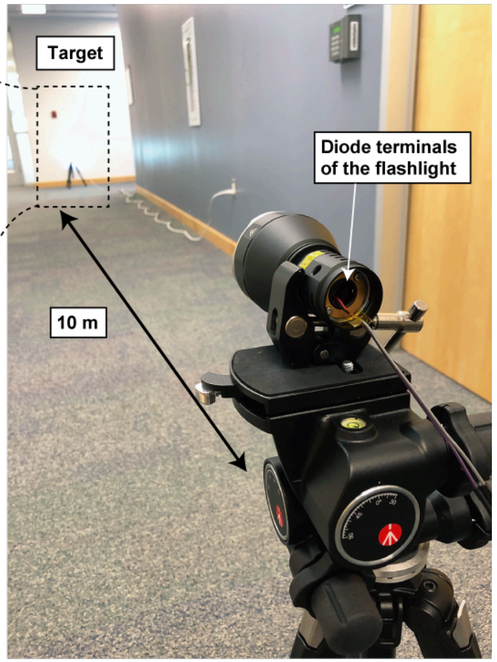
# Where else could IoT go wrong?

# Attacking the Sensors

## LIGHT COMMANDS

### Laser-Based Audio Injection on Voice-Controllable Systems




https://lightcommands.com/

# Attacking the Mobile App

# Attacking the Mobile App

TABLE I: Summary of IoT Devices under Testing

| Device Type | Vendor | Device Model | Firmware Version | Official Mobile App (Android[1]) | Protocol and Format (Encrypted: Yes/No) |
|---|---|---|---|---|---|
| **IP Camera** | D-Link | DCS-5010L | 1.13 | com.dlink.mydlinkmyhome | HTTP, K-V Pairs (N) |
| **Smart Bulb** | TP-Link | LB100 | 1.1.2 | com.tplink.kasa_android | UDP, JSON (Y) |
| | KONKE | KK-Light | 1.1.0 | com.kankunitus.smartplugcronus | UDP, String (Y) |
| **Smart Plug** | Belkin | Wemo Switch | 2.00 | com.belkin.wemoandroid | HTTP, XML (N) |
| | TP-Link | HS110 | v1_151016 | com.tplink.kasa_android | TCP, JSON (Y) |
| | D-Link | DSP-W215 | 1.02 | com.dlink.mydlinkmyhome | HNAP, XML (N) |
| **Printer** | Brother | HL-L5100DN | Ver. E | com.brother.mfc.brprint | LPD & HTTP, URI (N) |
| **NAS** | Western Digital | My Passport Pro | 1.01.08 | com.wdc.wd2go | HTTP, JSON (N) |
| | | My Cloud | 2.21.126 | com.wdc.wd2go | HTTP, JSON (N) |
| | QNAP | TS-212P | 4.2.2 | com.qnap.qmanager | HTTP, K-V Pairs (N) |
| **IoT Hub** | Philips | Hue Bridge | 01036659 | com.philips.lighting.hue | HTTP, JSON (N) |
| **Home Router** | NETGEAR | N300 | 1.0.0.34 | com.dragonflow | HTTP, XML (N) |
| | Linksys | E1200 | 2.0.7 | com.cisco.connect.cloud | HNAP, XML (N) |
| | Xiaomi | Xiaomi Router | 2.19.32 | com.xiaomi.router | HTTP, K-V Pairs (N) |
| **Story Teller** | Xiaomi | C-1 | 1.2.4_89 | com.xiaomi.smarthome | UDP, JSON (Y) |
| **Extension Socket** | KONKE | Mini-K Socket | sva.1.4 | com.kankunitus.smartplugcronus | UDP, String (Y) |
| **Humidifier** | POVOS | PW103 | v2.0.1 | com.benteng.smartplugcronus | UDP, String (Y) |

Remarks: All IoT apps mentioned in this table could be obtained from Google Play.

IoTFuzzer: Discovering Memory Corruptions in IoT Through App-based Fuzzing

Jiongyi Chen1 , Wenrui Diao2 , Qingchuan Zhao3 , Chaoshun Zuo3 , Zhiqiang Lin3,4, XiaoFeng Wang5 , Wing Cheong Lau1 , Menghan Sun1 , Ronghai Yang1 , Kehuan Zhang1

# Attacking the Mobile App

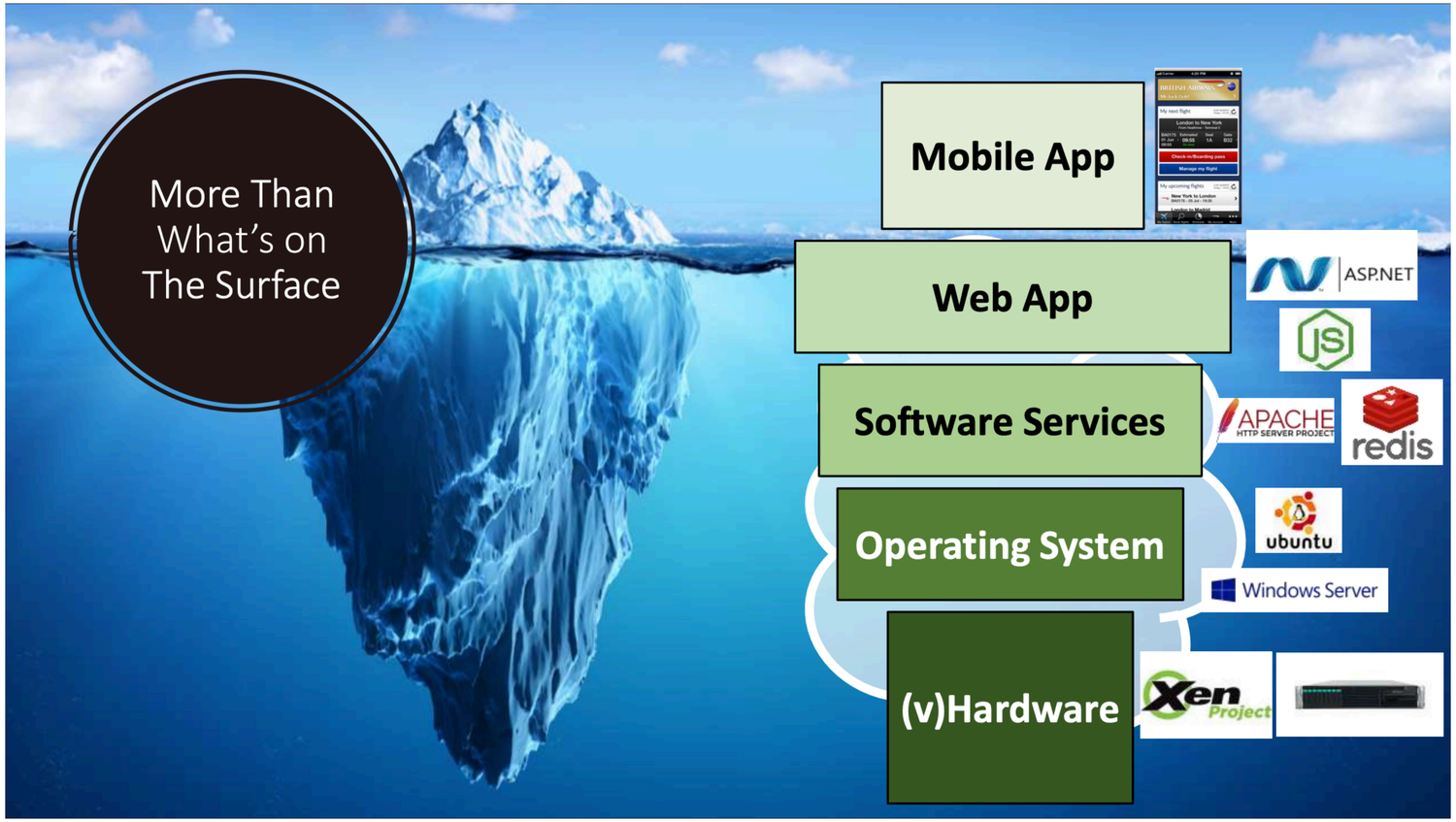
TABLE II: Summary of Discovered Vulnerabilities

| Device | Vulnerability Type | # of Issues | Remotely Exploitable? |
|---|---|---|---|
| Belkin WeMo (Switch) | Null Pointer Dereference | 1 | No |
| TP-Link HS110 (Plug) | Null Pointer Dereference | 3 | No |
| D-Link DSP-W215 (Plug) | Buffer Overflow (Stack-based) | 4 | Yes |
| WD My Cloud (NAS) | Buffer Overflow (Stack-based) | 1 | Yes |
| QNAP TS-212P (NAS) | Buffer Overflow (Heap-based) | 2 | Yes |
| Brother HL-L5100DN (Printer) | Unknown Crash | 1 | Not determined |
| Philips Hue Bridge (Hub) | Unknown Crash | 1 | Not determined |
| WD My Passport Pro (NAS) | Unknown Crash | 1 | Not determined |
| POVOS PW103 (Humidifier) | Unknown Crash | 1 | Not determined |

IoTFuzzer: Discovering Memory Corruptions in IoT Through App-based Fuzzing

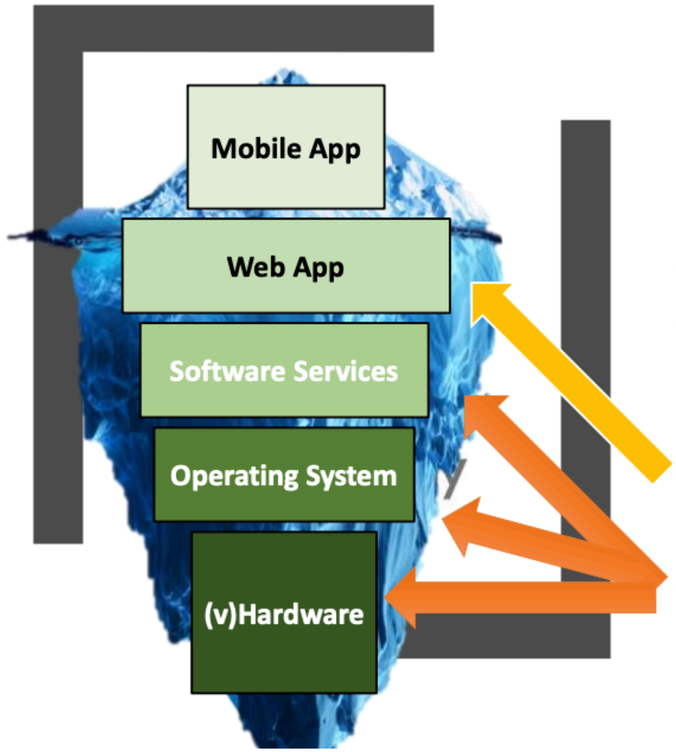
Jiongyi Chen1 , Wenrui Diao2 , Qingchuan Zhao3 , Chaoshun Zuo3 , Zhiqiang Lin3,4, XiaoFeng Wang5 , Wing Cheong Lau1 , Menghan Sun1 , Ronghai Yang1 , Kehuan Zhang1

# Attacking the Cloud Backend




[The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends]
**Omar Alrawi***, Chaoshun Zuo*, Ruian Duan, Ranjita Kasturi, Zhiqiang Lin, Brendan Saltaformaggio

# Attacking the Cloud Backend




## Google Play Store

- Top 5,000 apps from August 2018
- We found
  - Over **600 0-DAY**
  - Over **900 N-DAY**
- 0-day vulnerabilities affect web apps
- N-day affects software below the web apps

The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends
**Omar Alrawi***, Chaoshun Zuo*, Ruian Duan, Ranjita Kasturi, Zhiqiang Lin, Brendan Saltaformaggio

# Attacking the Cloud Backend

| Category | # Mob. Apps | Vulnerabilties | | | | | Labels | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | # *OS* | # *SS* | # *AS* | # *CS* | **Total** | # $B_{1st}$ | # $B_{3rd}$ | # $B_{hyb}$ | # $B_{ukn}$ | **Total** |
| Books & Reference | 332 | 15 | 49 | 55 | 71 | 190 | 365 | 653 | 501 | 354 | 1,873 |
| Business | 145 | 5 | 22 | 10 | 37 | 74 | 93 | 258 | 150 | 113 | 614 |
| Entertainment | 1,177 | 36 | 108 | 158 | 170 | 472 | 746 | 913 | 942 | 783 | 3,384 |
| Games | 1,283 | 34 | 81 | 147 | 106 | 368 | 290 | 804 | 651 | 444 | 2,189 |
| Lifestyle | 363 | 20 | 50 | 79 | 72 | 221 | 262 | 665 | 311 | 237 | 1,475 |
| Misc | 199 | 6 | 21 | 45 | 46 | 118 | 76 | 422 | 163 | 105 | 766 |
| Tools | 792 | 19 | 84 | 184 | 115 | 402 | 729 | 796 | 812 | 464 | 2,801 |
| Video & Audio | 689 | 24 | 46 | 89 | 98 | 257 | 267 | 648 | 434 | 357 | 1,706 |
| **Total** | 4,980 | 121 | 356 | 655 | 506 | 1,638 | 2,492 | 1,089 | 3,336 | 2,506 | 9,423 |

The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends

**Omar Alrawi***, Chaoshun Zuo*, Ruian Duan, Ranjita Kasturi, Zhiqiang Lin, Brendan Saltaformaggio

# Attacking the Cloud Backend

| Category | # Mob. Apps | Vulnerabilties | | | | | Labels | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | # *OS* | # *SS* | # *AS* | # *CS* | Total | # $B_{1st}$ | # $B_{3rd}$ | # $B_{hyb}$ | # $B_{ukn}$ | Total |
| Books & Reference | 332 | 15 | 49 | 55 | 71 | 190 | 365 | 653 | 501 | 354 | 1,873 |
| Business | 145 | 5 | 22 | 10 | 37 | 74 | 93 | 258 | 150 | 113 | 614 |
| Entertainment | 1,177 | 36 | 108 | 158 | 170 | 472 | 746 | 913 | 942 | 783 | 3,384 |
| Games | 1,283 | 34 | 81 | 147 | 106 | 368 | 290 | 804 | 651 | 444 | 2,189 |
| Lifestyle | 363 | 20 | 50 | 79 | 72 | 221 | 262 | 665 | 311 | 237 | 1,475 |
| Misc | 199 | 6 | 21 | 45 | 46 | 118 | 76 | 422 | 163 | 105 | 766 |
| Tools | 792 | 19 | 84 | 184 | 115 | 402 | 729 | 796 | 812 | 464 | 2,801 |
| Video & Audio | 689 | 24 | 46 | 89 | 98 | 257 | 267 | 648 | 434 | 357 | 1,706 |
| **Total** | 4,980 | 121 | 356 | 655 | 506 | 1,638 | 2,492 | 1,089 | 3,336 | 2,506 | 9,423 |

The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends

**Omar Alrawi***, Chaoshun Zuo*, Ruian Duan, Ranjita Kasturi, Zhiqiang Lin, Brendan Saltaformaggio

# What can we do about it?

# Future Directions

Security Hardening

Automatic Updates

Device Attribution + Provenance

Defragmentation

End-of-life

# Future Directions

Security Hardening

Automatic Updates

Device Attribution + Provenance

Defragmentation

End-of-life

….and more research!

# Future Directions

Security Hardening

Automatic Updates

Device Attribution + Provenance

Defragmentation

End-of-life

….and more research!

**Questions?**
**dkumar11@illinois.edu**
**@_kumarde**