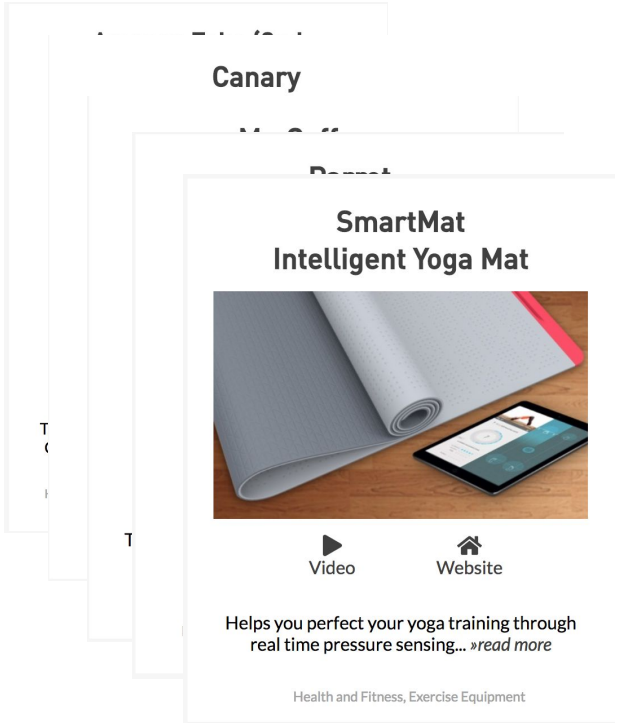
The Mirai Botnet

Ehimare Okoyomon
CS261

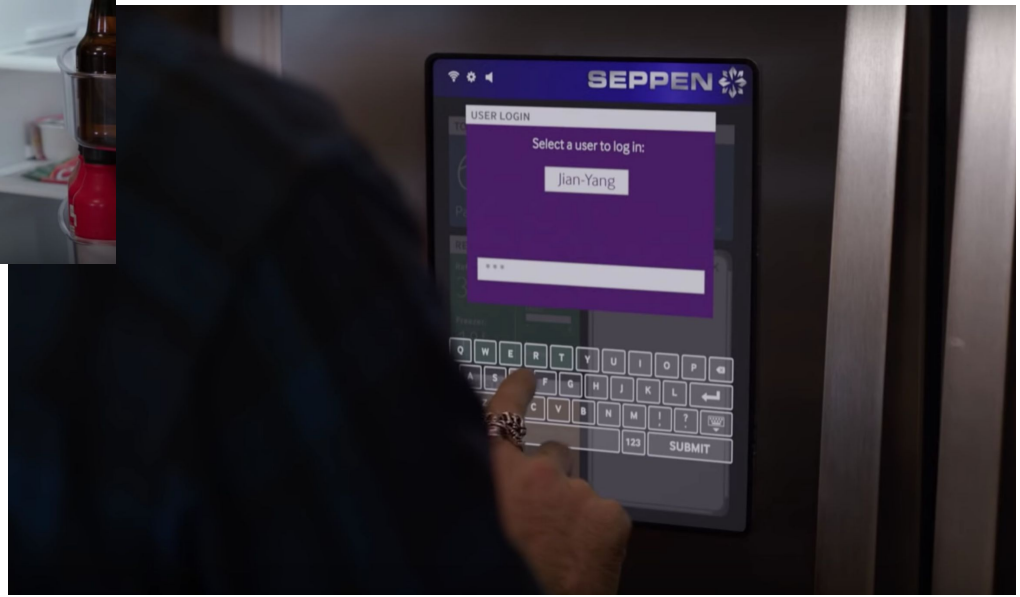
IoT Devices

- Nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data

- Usually some form of user interaction
  - Through application
  - Gestures
  - Speech



Security?



What can you do with default passwords?

Cyberattack Knocks Out Access to Websites

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

Mirai botnet adds three new attacks to target IoT devices

21 OCT 16 **Hacked Cameras, DVRs Powered Today's Massive Internet Outage**

Mirai botnet hacker ordered to pay $8.6 million in damages

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

4 NOV 16 **Did the Mirai Botnet Really Take Liberia Offline?**

How to not break the Internet

October 26, 2016

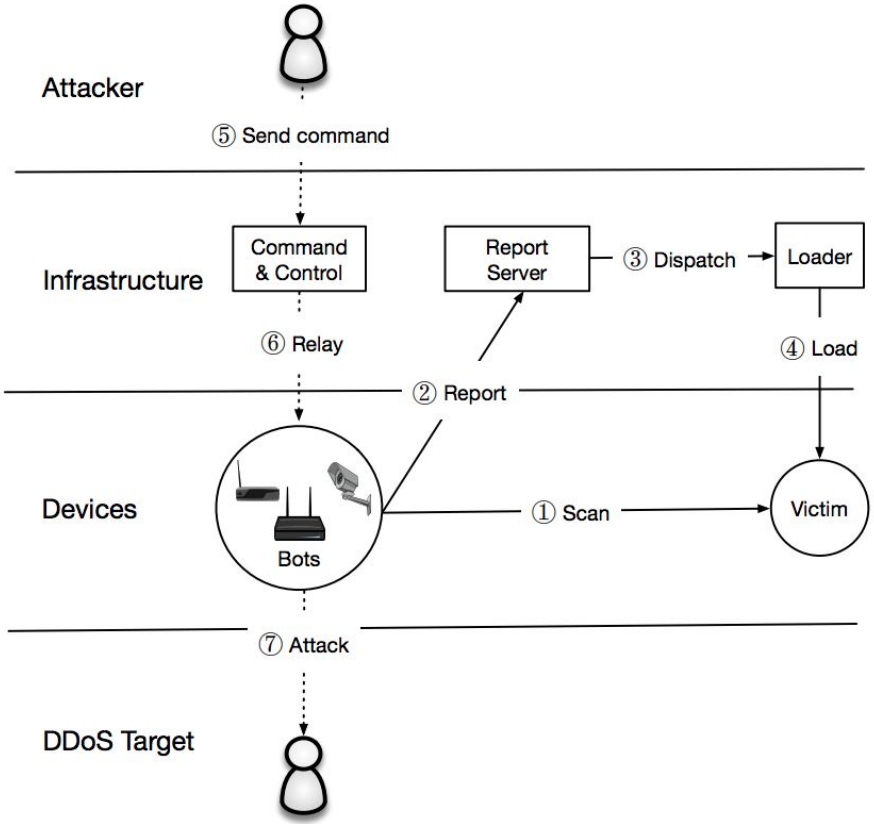
Perhaps the most striking point about last week's huge DDoS attack, which took down more than 80 big websites and online services, is that the criminals behind the attack accomplished it not by particularly sophisticated or cutting-edge means, but by creating a veritable army of consumer connected devices — what we call the Internet of Things (IoT). In this post we explain the critical

Mirai Botnet: What is it?

The Original

- Worm-like family of malware that infected IoT devices
- Corralled them into a DDoS botnet
- Port scanning and brute force dictionary attack
  - Used a dictionary of 62 username/password pairs

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                    // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                         // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                         // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                     // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                     // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                 // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                 // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);             // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                     // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                         // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);     // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                             // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);         // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                             // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                         // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                             // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                         // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                             // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);     // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                             // root     1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);         // admin    smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                         // admin    1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                     // root     666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);             // root     password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                             // root     1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                     // root     klv123
...
```


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

Mirai Botnet: What did it do?

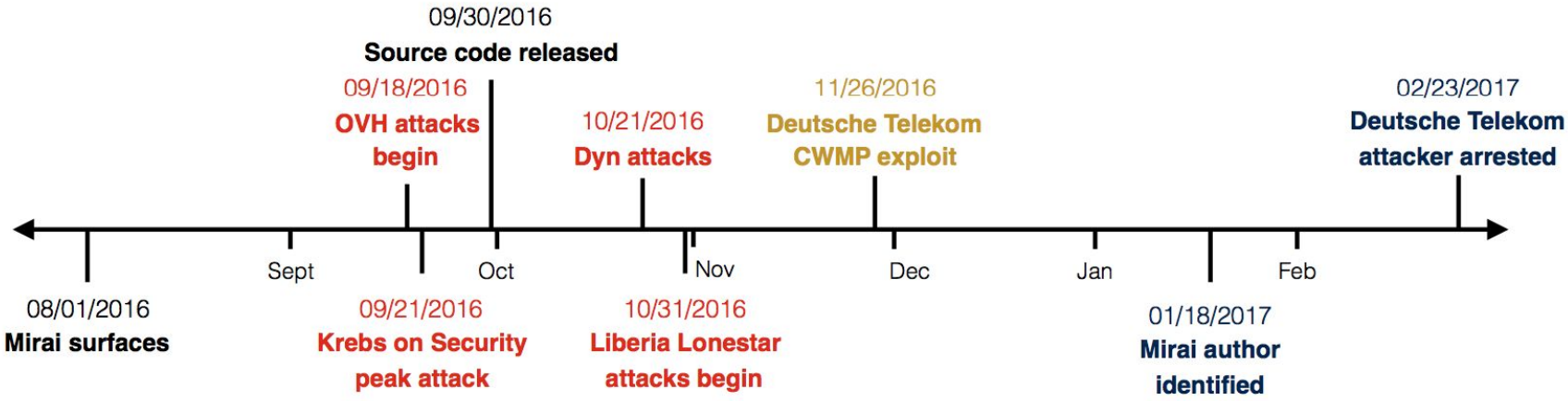


Figure 1: **Mirai Timeline**—Major attacks (red), exploits (yellow), and events (black) related to the Mirai botnet.

Attacks

Krebs on Security (Blog):

- 623 Gbps DDoS attack (largest publicly disclosed)

Dyn (DNS Provider):

- Disrupted name resolution for clients including Amazon, Github, Netflix, Paypal, Reddit.
- 21 short lived (25s) attacks then two sustained 1 and 5 hour long

Lonestar (Telecom Operator):

- 341 attacks - most targeted victim by attack account
- claims that Mirai substantially deteriorated Liberia's overall Internet connectivity

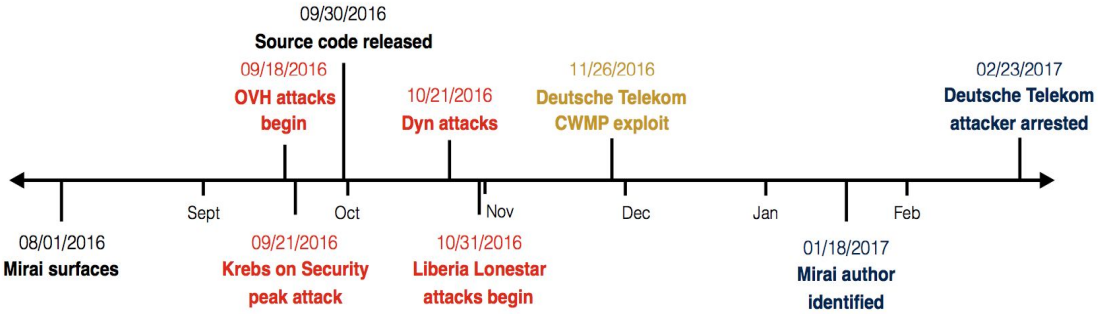


Figure 1: **Mirai Timeline**—Major attacks (red), exploits (yellow), and events (black) related to the Mirai botnet.

Unconventional DDos

(From Arbor Networks global DDoS report) DDoS attacks usually:

65% volumetric, 18% TCP state, 18% application attacks

Mirai:

33% volumetric, 32% TCP state, 34% application attacks

Limited reflection/amplification attacks

2.8% reflection attacks, mostly just SYN along with a few ACK and GRE IP attacks.

Mirai Botnet: How did it do this?

Understanding the Mirai Botnet

Manos Antonakakis[†], Tim April[◆], Michael Bailey[★], Matthew Bernhard[‡], Elie Bursztein[✳]
Jaime Cochran[△], Zakir Durumeric[‡], J. Alex Halderman[‡], Luca Invernizzi[✳]
Michalis Kallitsis[•], Deepak Kumar[★], Chaz Lever[†], **Zane Ma**[★], Joshua Mason[★]
Damian Menscher[✳], Chad Seaman[◆], Nick Sullivan[△], Kurt Thomas[✳], Yi Zhou[★]

[◆]*Akamai Technologies,* [△]*Cloudflare,* [†]*Georgia Institute of Technology,* [✳]*Google,* [•]*Merit Network*
[★]***University of Illinois Urbana-Champaign,*** [‡] *University of Michigan*

Research Setup

Network Telescope (Distributed Monitoring Infrastructure)

- Monitored all requests to a network telescope from July 18, 2016 - February 28, 2017
- Composed of 4.7 million IP addresses operated by Merit Network
- **Uniquely fingerprinted Mirai probes** based on how Mirai does stateless scanning
- **Observed 116.2 billion Mirai probes from 55.4 million IP addresses**

Active Scanning

- Used Censys, a public search engine backed by data collected from ongoing Internet-wide scans
  - Actively scans IPv4 space and aggregates application layer data about hosts
- Focused analysis on scans of HTTPS, FTP, SSH, TELNET, and CWMP **to identify devices by model**

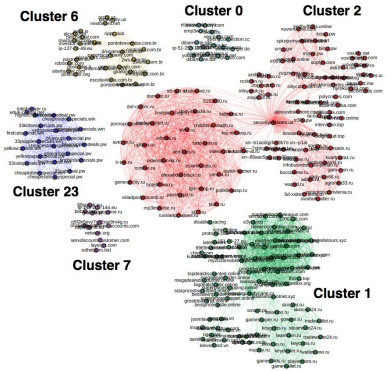
Research Setup

Telnet Honeypots

- **Collected binaries** installed on honeypots pretending to be vulnerable IoT devices
  - Logged all incoming traffic and downloaded binaries being installed via wget or tftp
- 141 Mirai binaries collected from this method, and 1028 in total from all sources
- **Extracted logins and passwords, IP blacklists, and Command and Control (C2) domains**

Active and Passive DNS

- Mapped IP addresses in attack commands to victim names
- **Created graph reflecting shared infrastructure used by Mirai variants**



Research Setup

Attack Commands

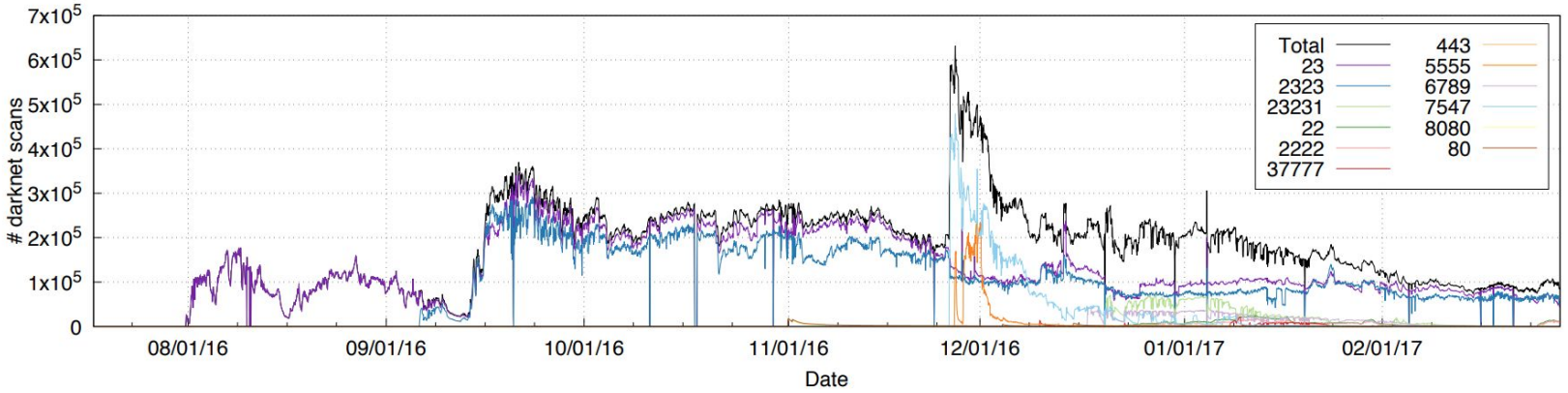
- Simulated Mirai-infected device listened for commands from C2 servers
- Akamai **observed 64K attack commands issued by 484 unique C2 servers** (by IP address)

DDos Attack Traces

- Compared network traces and statistics from Akamai, Google Shield and Dyn to those found scanning their passive network telescope
- Were **able to attribute the Krebs, Dyn and Lonestar attacks to Mirai**

Botnet Size

- Initial 2-hour bootstrapping scan
- Botnet emerges with 834 scanning devices
- **11K hosts infected within 10 minutes**
- 65K devices within 20 hours
- **75 minute doubling time**
- Initial steady state of **200-300K devices**



Mirai Adaptation/Variants

- Updated from IP-based to domain-based
- **Deletion of executing binary** and **obfuscation of process ID**
- **More username/password pairs**
- Closing of infection ports TCP/23 and TCP/2323
- Aggressive killing of competitive malware
- **Attacks on CPE WAN Management Protocol (CWMP)**
    - scans for TCP/7547 and TCP/5555
    - an HTTP-based protocol that enables auto-configuration and remote management of home routers

Device Bandwidth

- Half of the Mirai bots that scanned the network telescope sent **fewer than 10,000 scan packets**
- Majority scanned at a **rate below 250 bytes per second**
- In contrast, SQL Slammer scanned at 1.5 MBps (about 6000 times faster), and the Witty worm scanned even faster at 3 MBps
- Devices with limited computational capacity and/or located in regions with low bandwidth?

Device Composition

- Analyzed credentials hardcoded into binaries
  - Observed 371 unique passwords
- Identified 84 devices and/or vendors associated with these passwords
- **Security Cameras, DVRs, and consumer routers made up majority**
  - Also printers and tv receivers
  - Manufacturers responsible were **Dahua, Huawei, ZTE, Cisco, ZyXEL, and MikroTik.**

Global Distribution

- Disproportionate number of devices concentrated in South America and Southeast Asia at the time of Krebs attack

- CWMP exploit were concentrated in Europe, but prompt patching returned Mirai back to its original concentration in South America and Southeast Asia

Country	Mirai Infections	Mirai Prevalence	Telnet Prevalence
Brazil	49,340	15.0%	7.9%
Colombia	45,796	14.0%	1.7%
Vietnam	40,927	12.5%	1.8%
China	21,364	6.5%	22.5%
S. Korea	19,817	6.0%	7.9%
Russia	15,405	4.7%	2.7%
Turkey	13,780	4.2%	1.1%
India	13,357	4.1%	2.9%
Taiwan	11,432	3.5%	2.4%
Argentina	7,164	2.2%	0.2%

Mirai Botnet: How do we fix this?

Author Suggestions

- Basic security practices like NOT using default passwords and limiting remote access
- Automatic Updates
- Out-of-band notifications
- Device Attribution
- Mechanisms for End-of-life of devices

Takeaways and Discussion

Do we need to enforce these policies in a way similar to GDPR?

This botnet was not the biggest in device size or in power of devices - why was it so impactful?

Weakest link - adversaries will continue to abuse the most fragile hosts.

How much overhead would security add to these devices?

Questions?