Understanding Mirai Botnet

- Kunj Haria

Understanding the Mirai Botnet

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

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

Introduction - Mirai

Introduction - *cont'd*

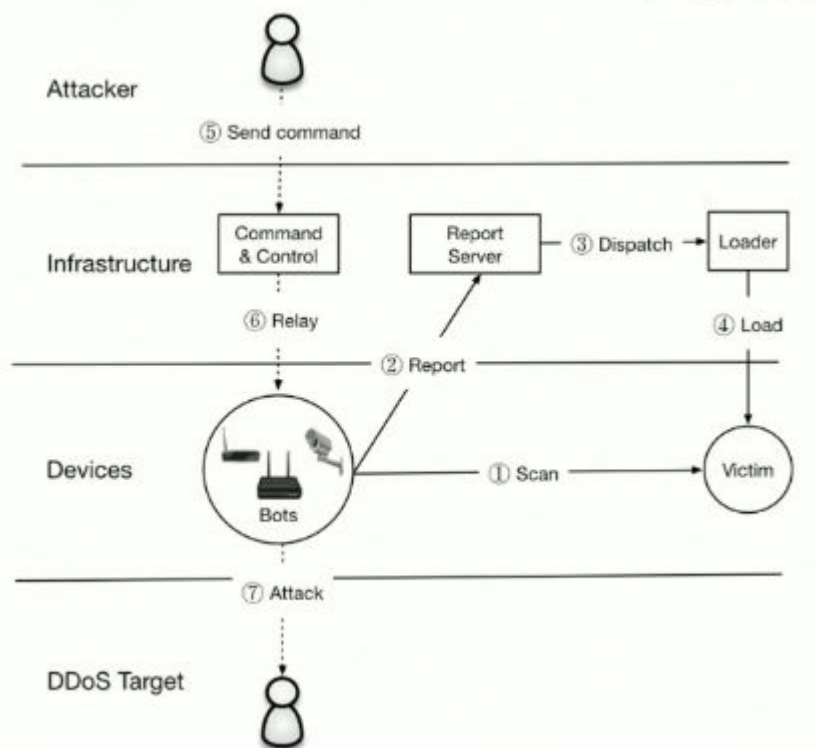
2020

20 Billion

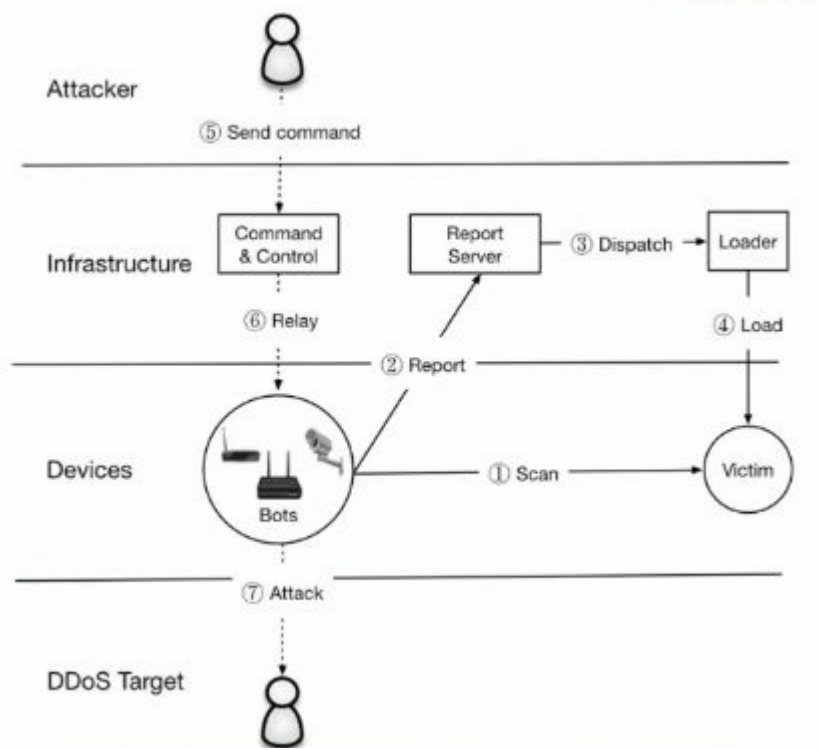
2025

25 Billion

Introduction - Mirai Lifecycle



Introduction - Mirai Lifecycle



Measurements

Network Telescope

Active Scanning

Telnet Honeypots

Malware Repositories

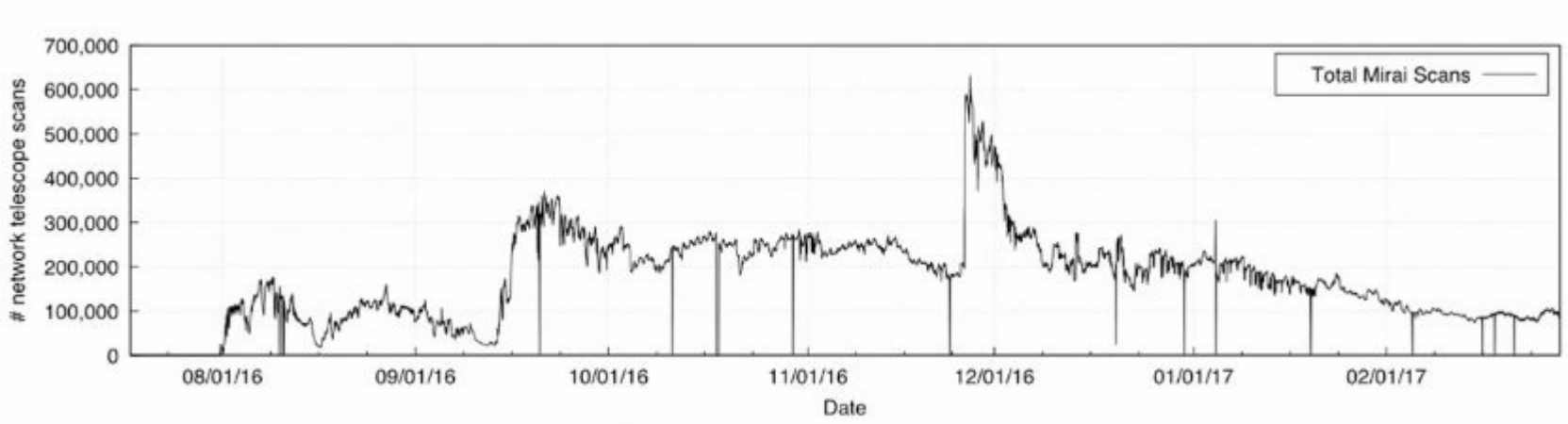
Active/Passive DNS

Krebs DDoS Attack & Dyn

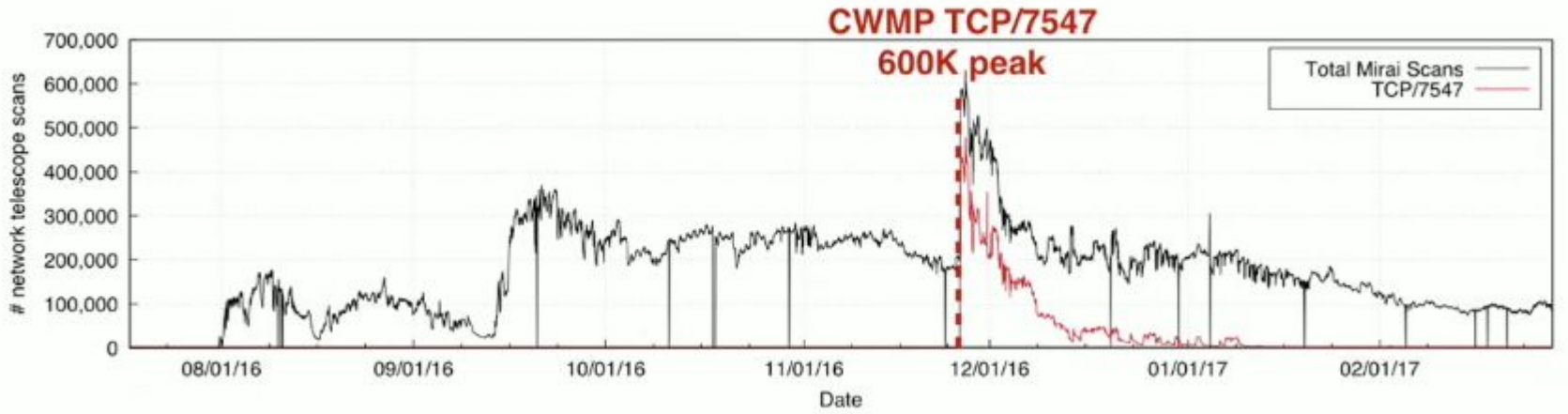
Motivation for study

- Reference point for future research
- Reconcile a broad spectrum of botnet data perspectives
- Studying the motives of IoT botnets so as to learn how to combat them

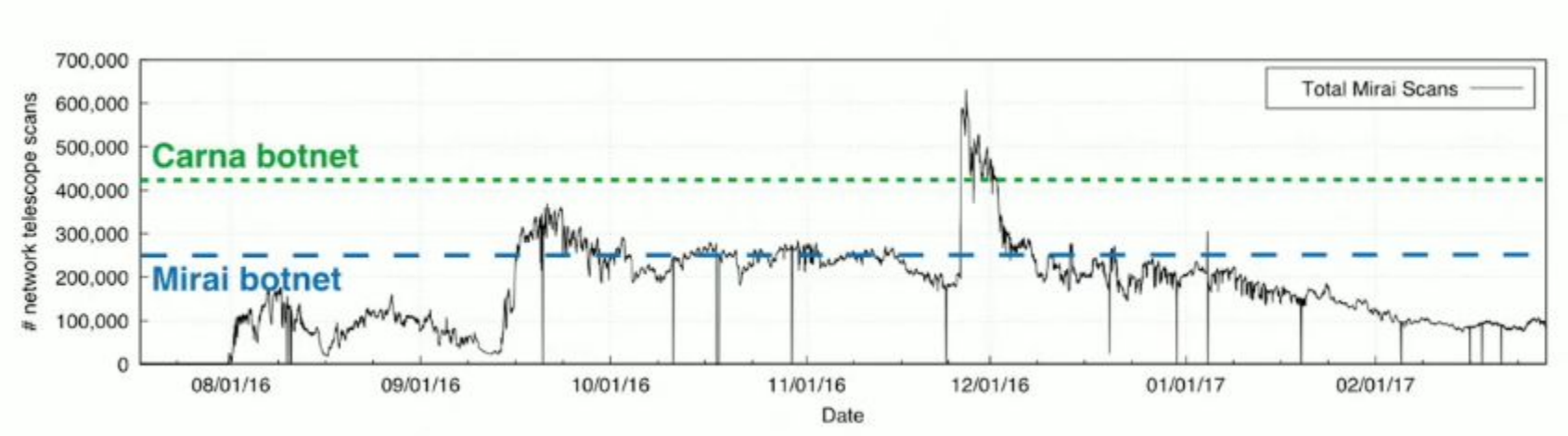
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
Total Mirai Scans
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date

Population


CWMP TCP/7547
600K peak
Total Mirai Scans
TCP/7547
network telescope scans
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date

Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
Carna botnet
Mirai botnet
Total Mirai Scans
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date

Targets

Targeted Devices

Source Code Password List

Device Type	# Targeted Passwords	Examples
Camera / DVR	**26 (57%)**	**dreambox, 666666**
Router	4 (9%)	smcadmin, zte521
Printer	2 (4%)	00000000, 1111
VOIP Phone	1 (2%)	54321
Unknown	13 (28%)	password, default

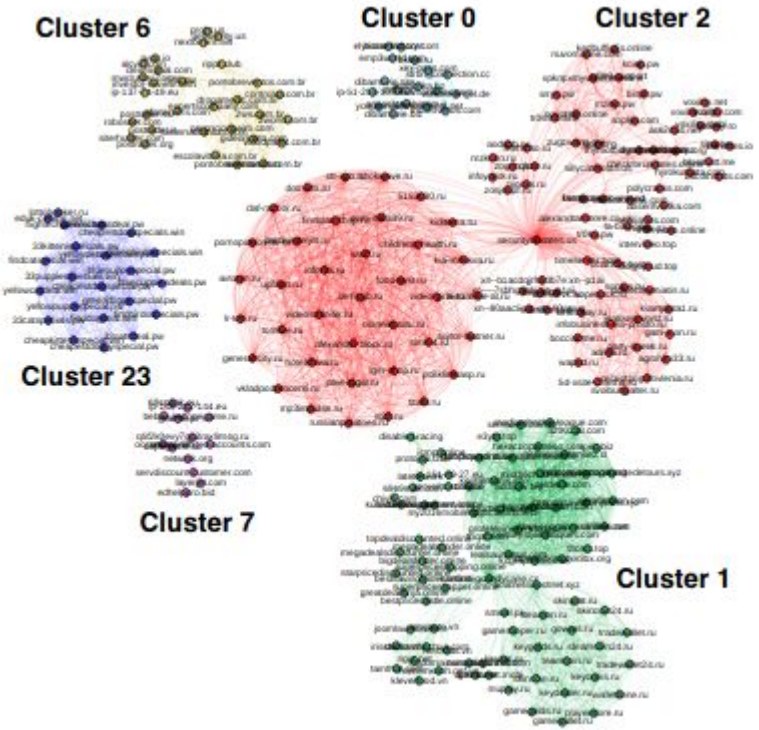
Infected Devices

HTTPS banners

Device Type	# HTTPS banners
Camera / DVR	**36.8%**
Router	6.3%
NAS	0.2%
Firewall	0.1%
Other	0.2%
Unknown	56.4%

Who ran it

- Extracted from C2 binaries



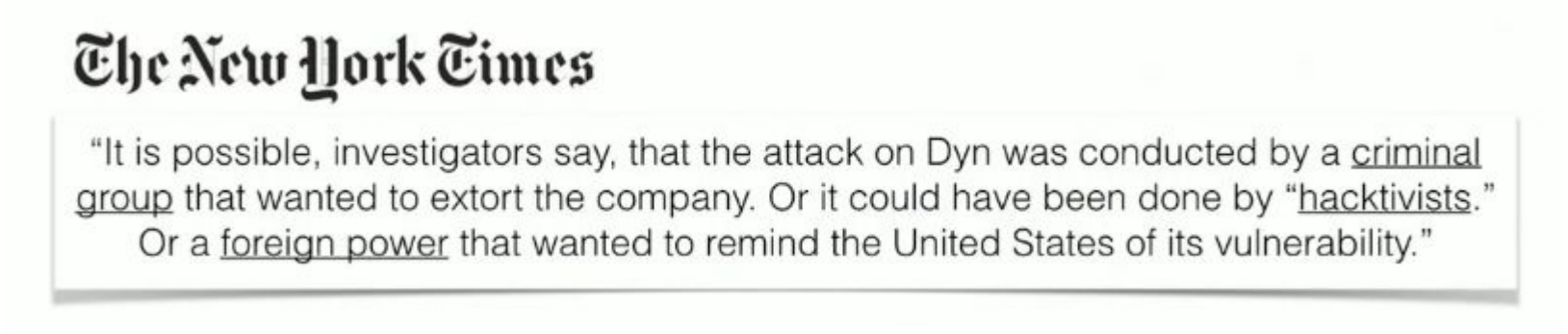
1 - Original botnet

1 - attacked Krebs

2 - Scan CWMP

6 - Attacked Dyn

DDos Targets



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

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
208.78.70.5
204.13.250.5
208.78.71.5
204.13.251.5
198.107.156.219
216.115.91.57

Dyn

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

The New York Times

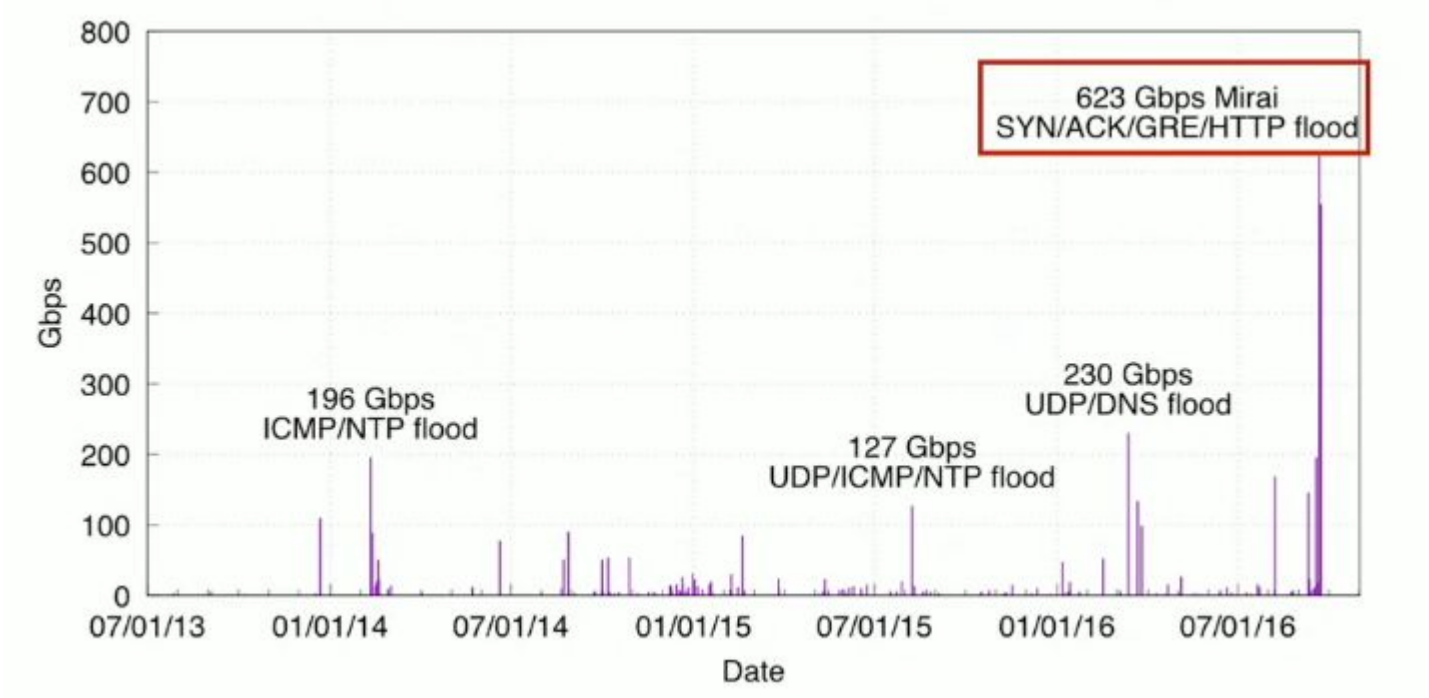
"It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability."

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

DDos Targets

Largest Reports DDoS



Overview

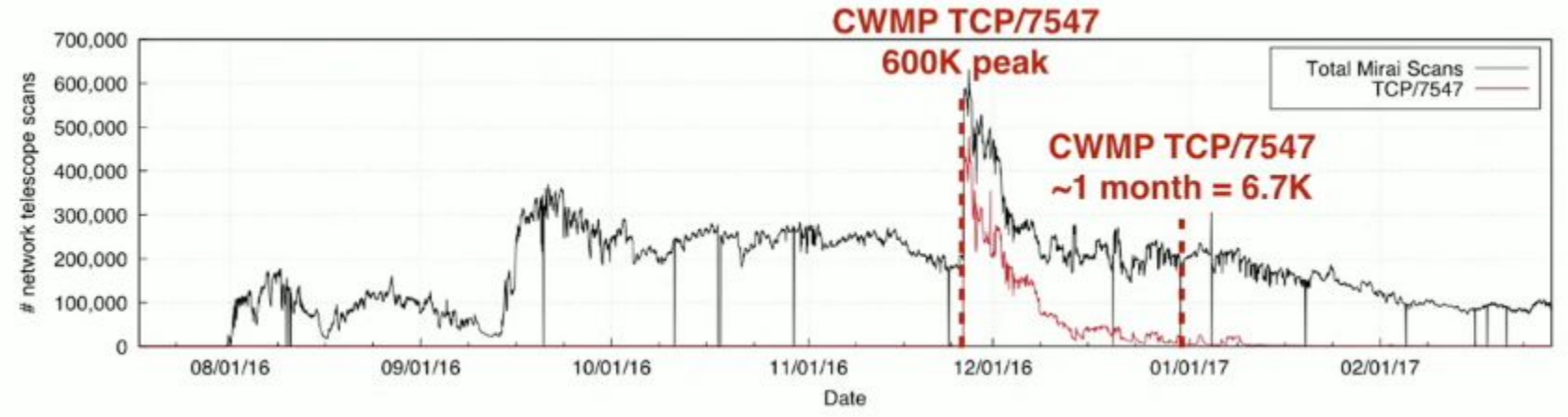
- 200,000 - 300,000 IoT Devices Compromised
- Evidence of multiple operators releasing new strains of Mirai
- Largest known attack on record (of that time)

Currently,

1. The Google Attack, 2020 - Peak 2.5Tbps (4 times of Mirai)
2. The AWS DDos - Peak 2.3Tbps

Mirai Taught Lesson

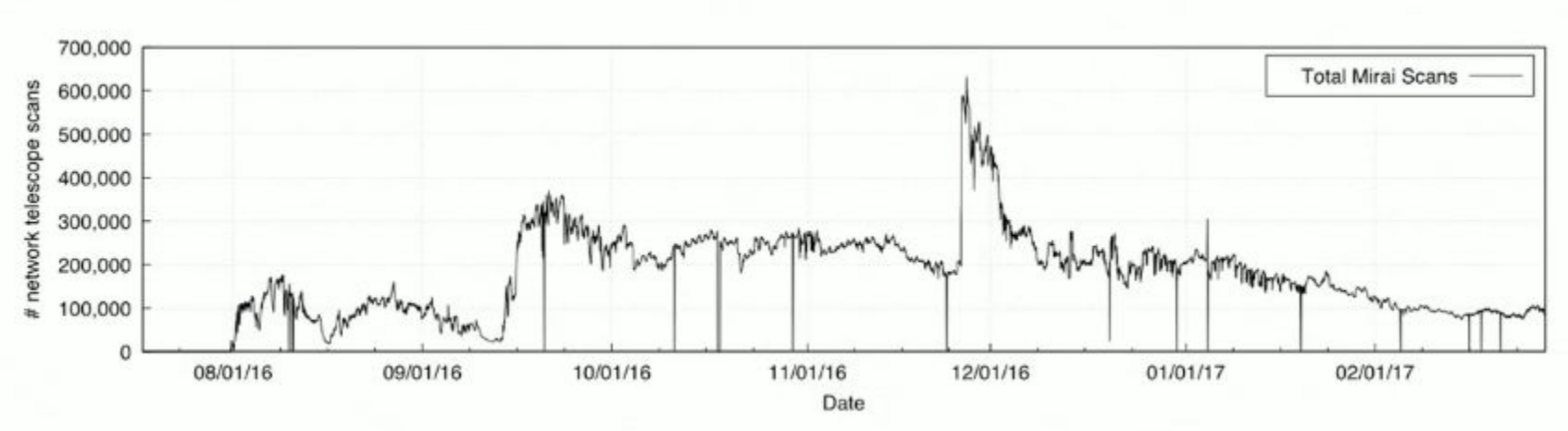
- Security Hardening
- Automatic Updates



What about the future ?

Future

- Improved Security in IoT since 2016



Questions