Understanding the Mirai Botnet

Manos Antonakakis[†], Tim April[◆], Michael Bailey[★], Matthew Bernhard[ǂ], Elie Bursztein[✳]
Jaime Cochran[△], Zakir Durumeric[ǂ], J. Alex Halderman[ǂ], 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***, [ǂ] *University of Michigan*

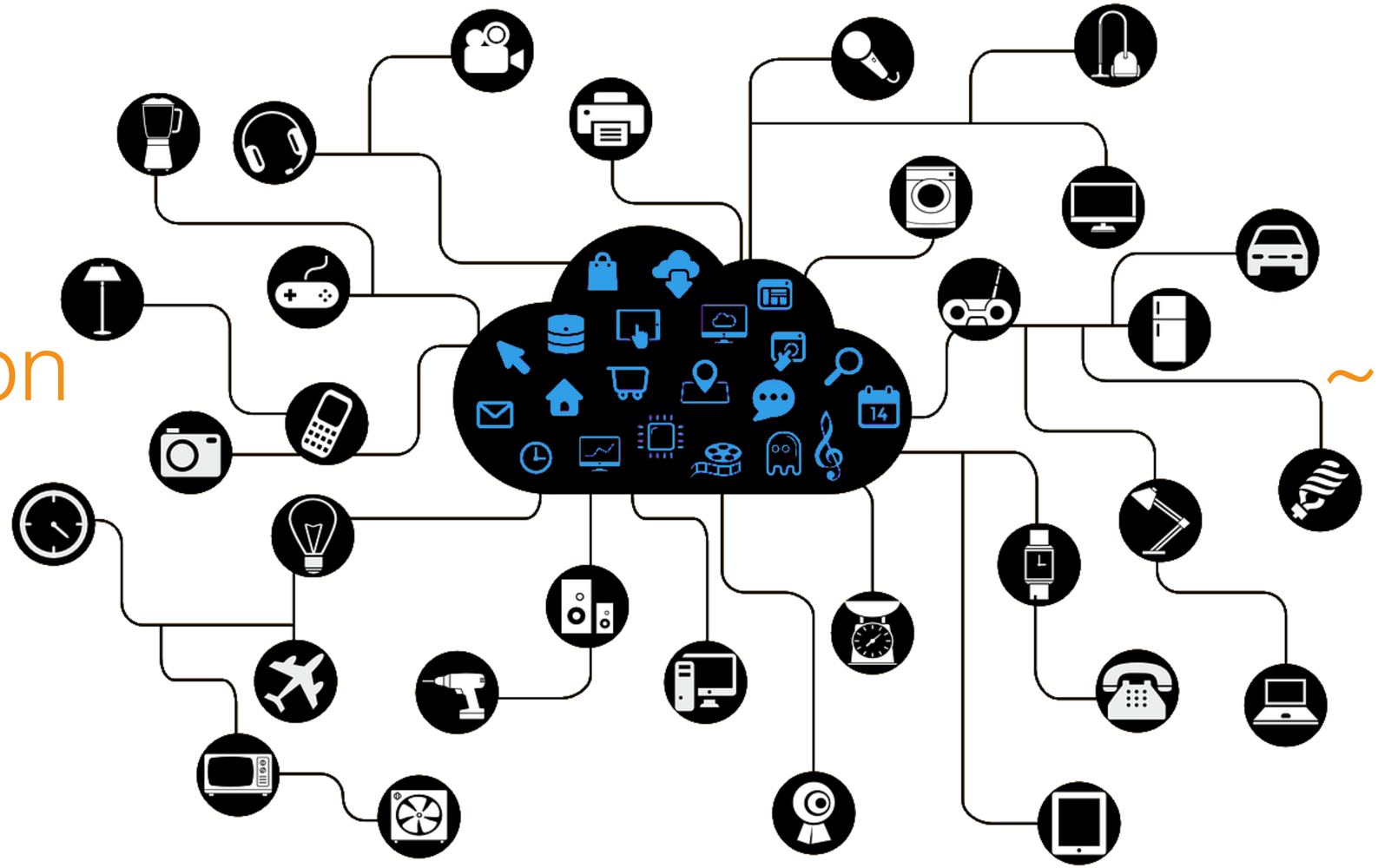
Mirai


THE WALL STREET JOURNAL.

Cyberattack Knocks Out Access to Websites

Growing IoT Threat

2016
6 - 9 Billion



2020
~30 Billion

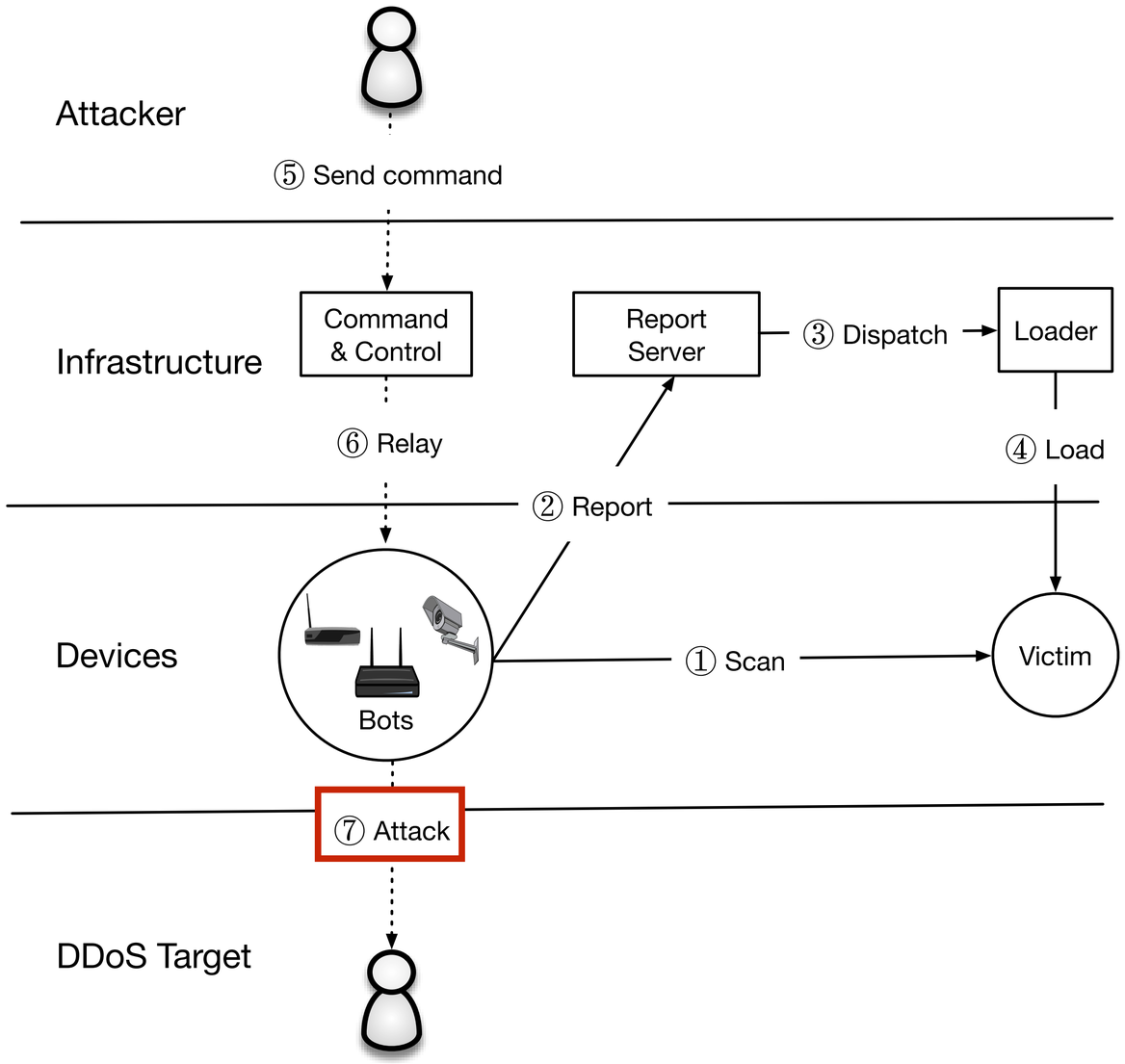
Research Goals

Snapshot the IoT botnet phenomenon

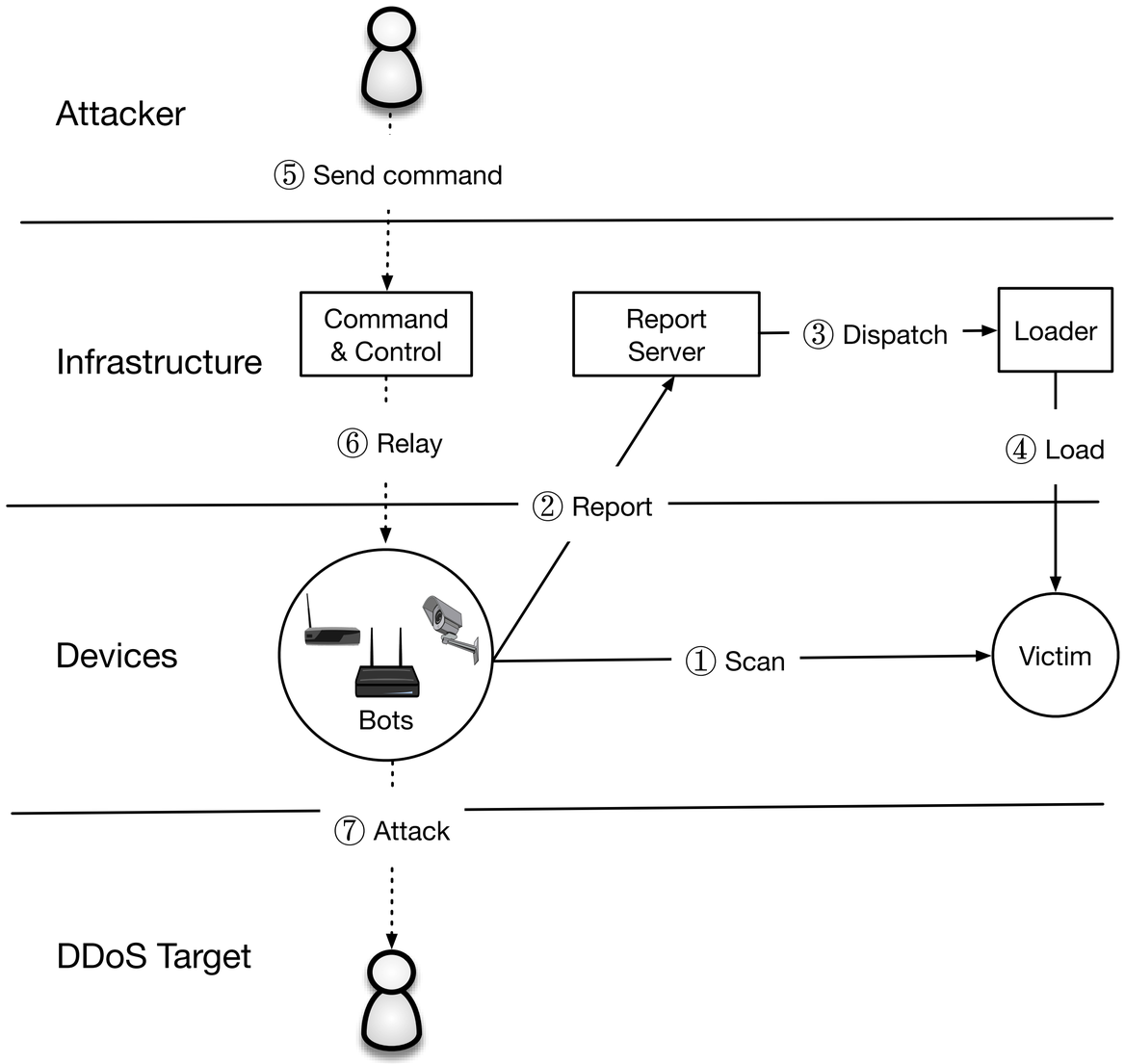
Reconcile a broad spectrum of botnet data perspectives

Understand Mirai's mechanisms and motives

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

Measurement

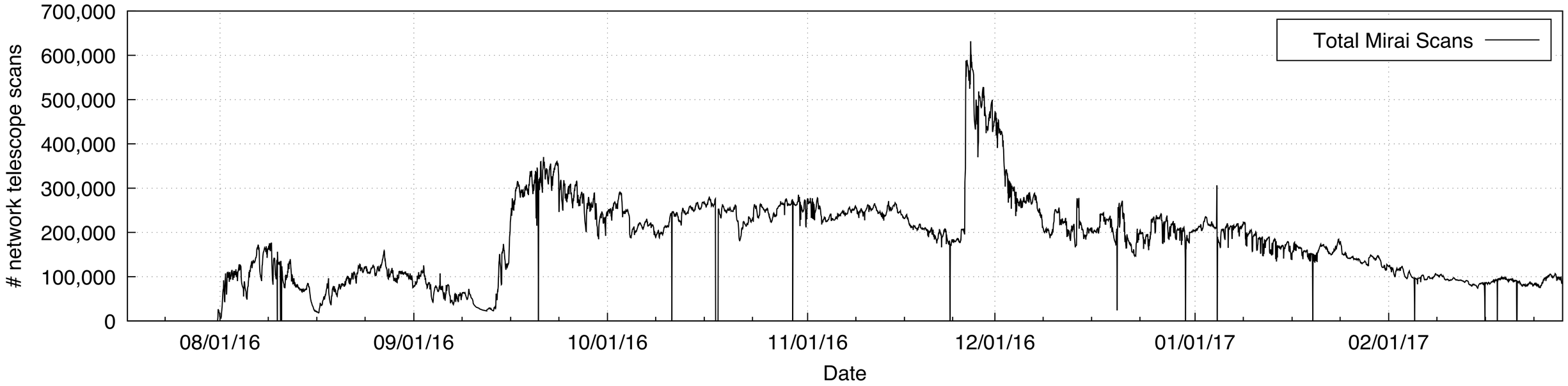


Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	594 binaries
Active/Passive DNS	499M daily RRs
C2 Milkers	64K issued attacks
Krebs DDoS Attack	170K attacker IPs
Dyn DDoS Attack	108K attacker IPS

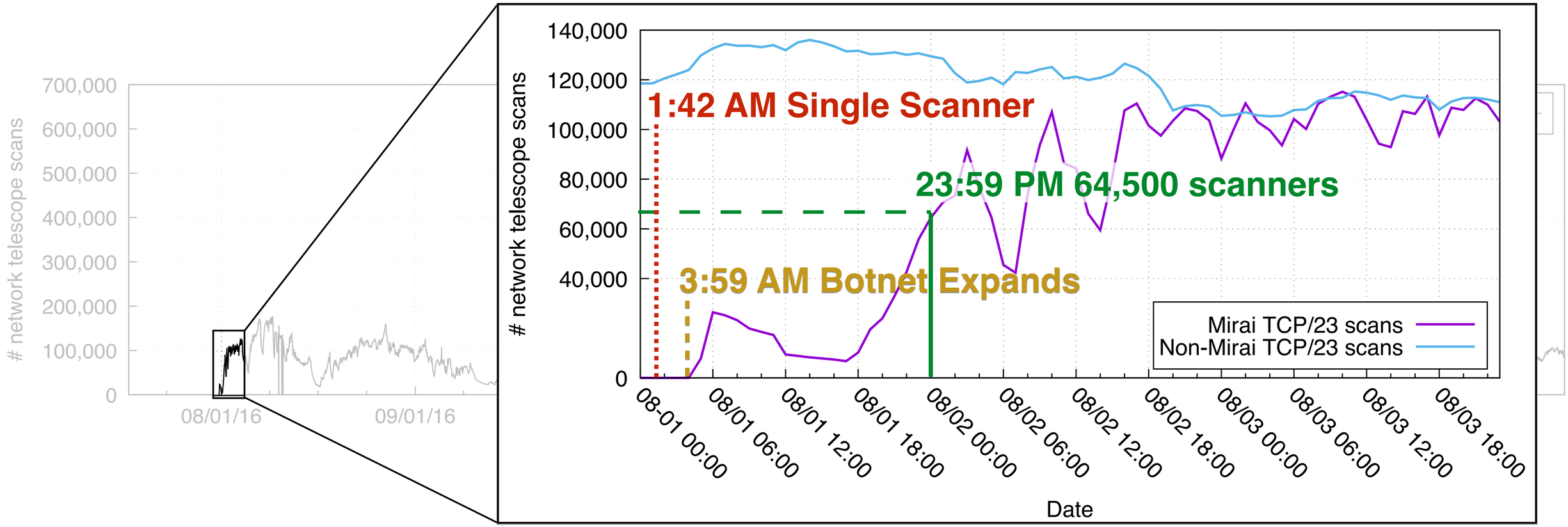
July 2016 - February 2017

What is the Mirai botnet?

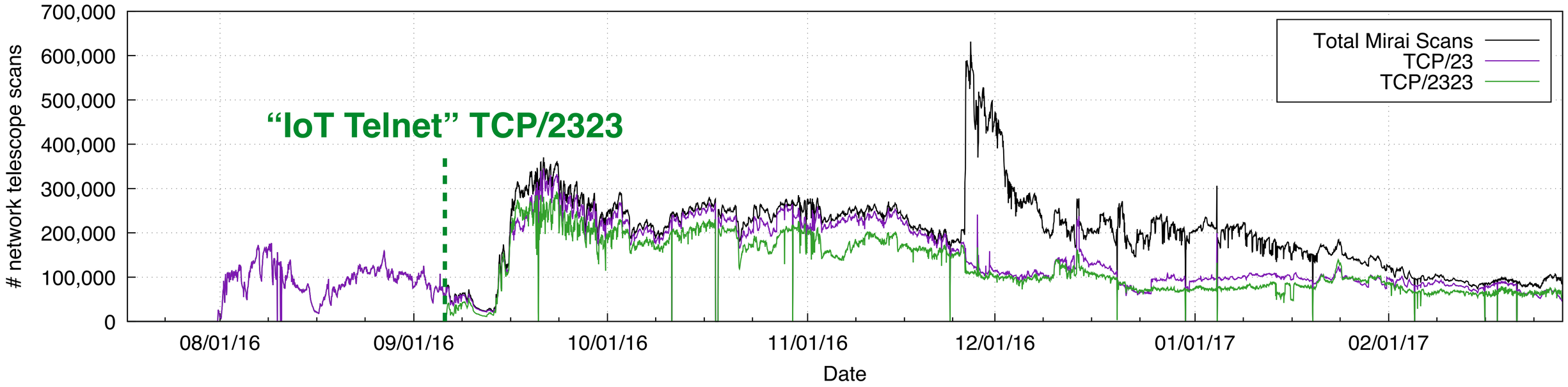
Population


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

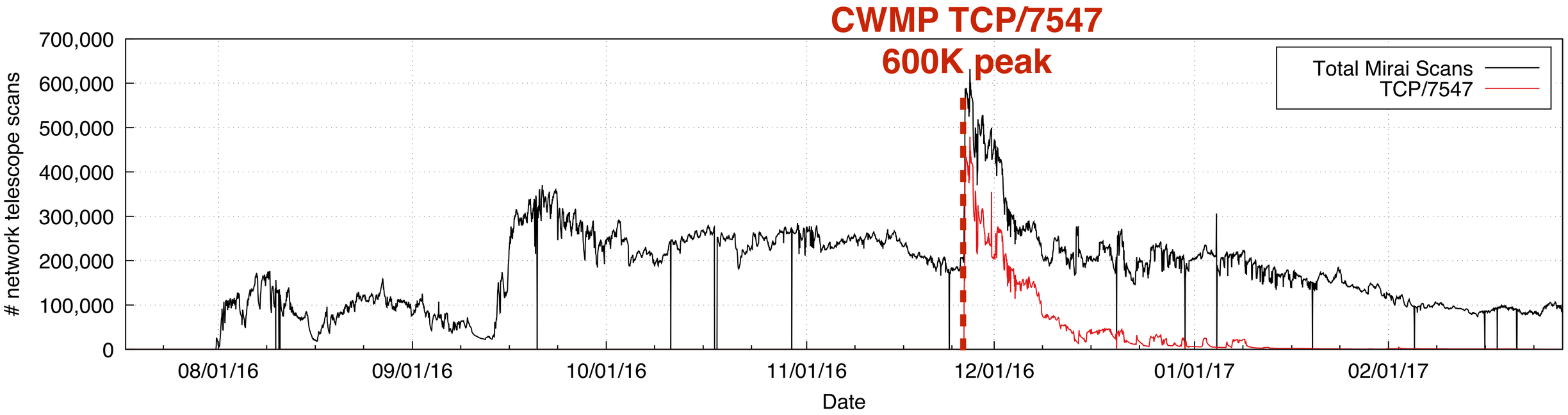
Rapid Emergence



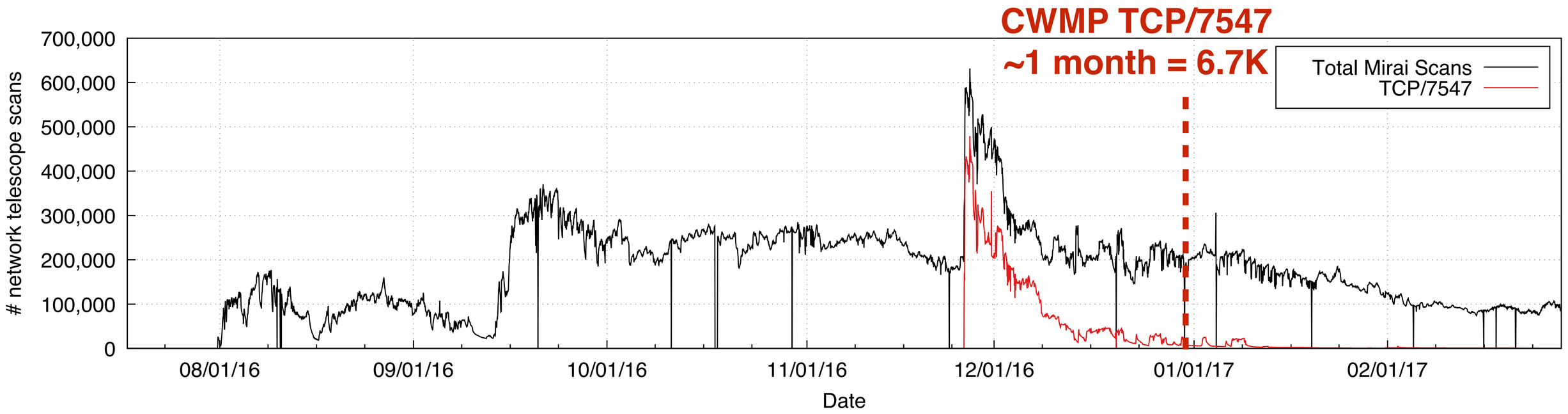
Many Ports of Entry



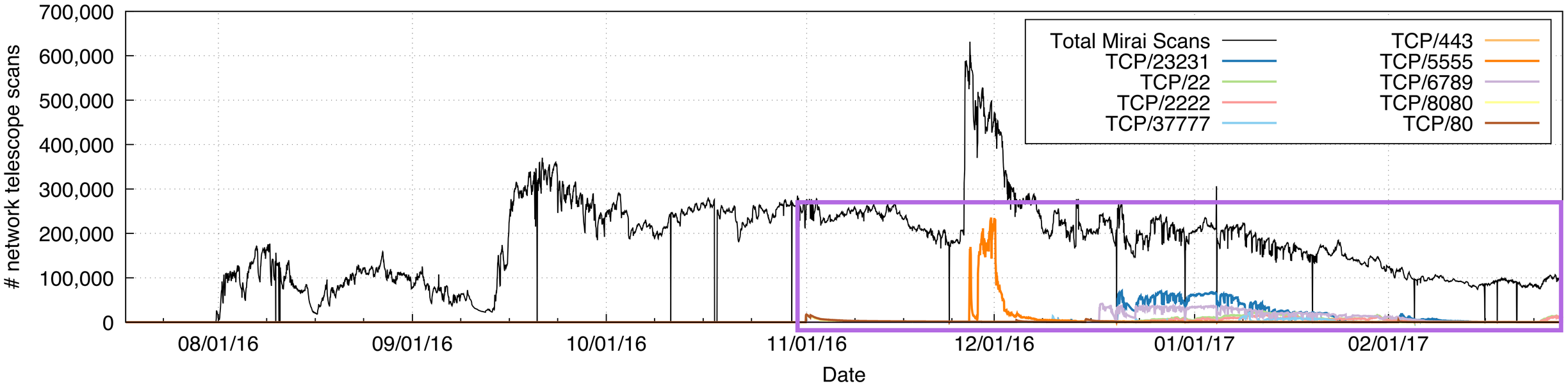
Many Ports of Entry



Many Ports of Entry

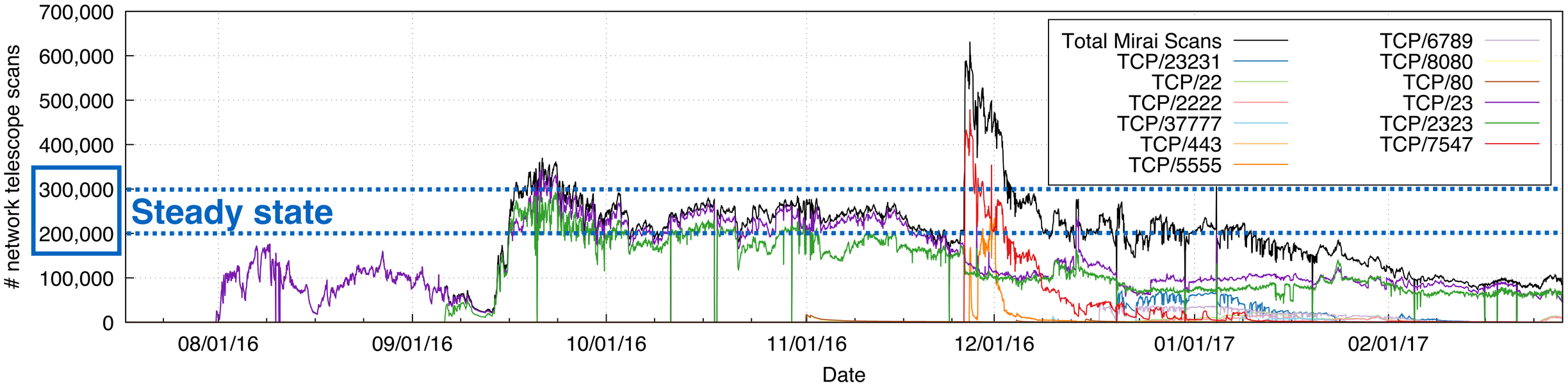


Many Ports of Entry

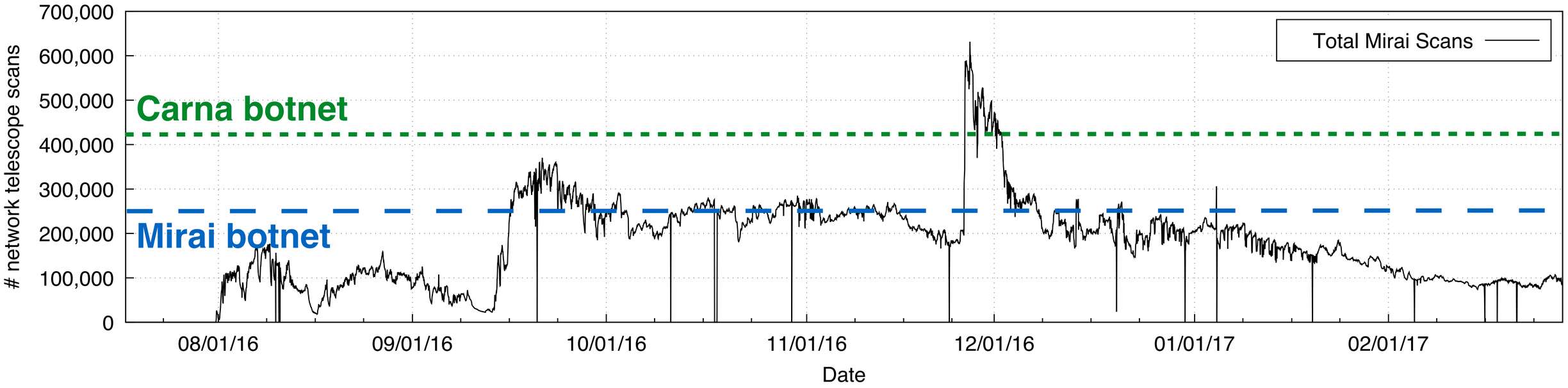


9 Additional Protocols

200K-300K Mirai Bots



Modest Mirai

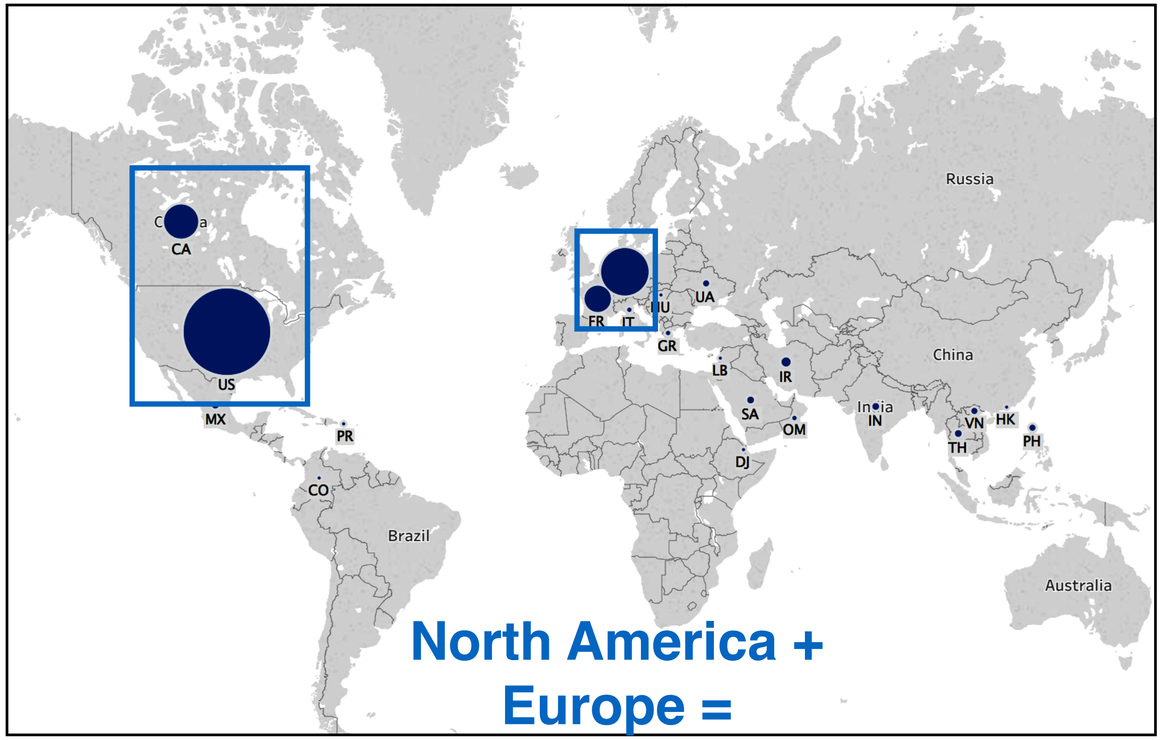


Global Mirai

Mirai

South America + Southeast Asia = 50% of Infections

TDSS/TDL4



North America + Europe = 94% of Infections

Cameras, DVRs, Routers

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

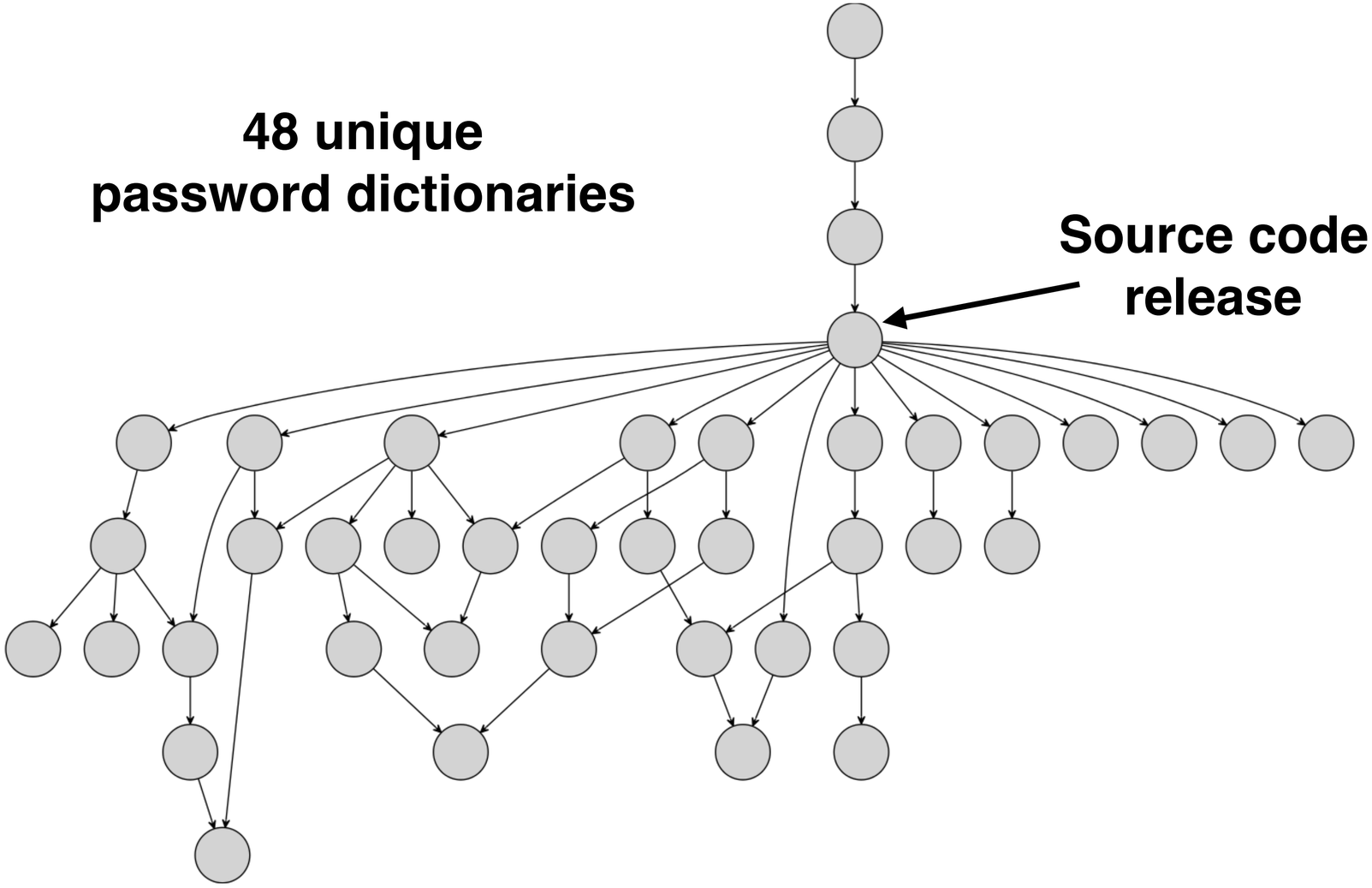
Infected Devices

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%

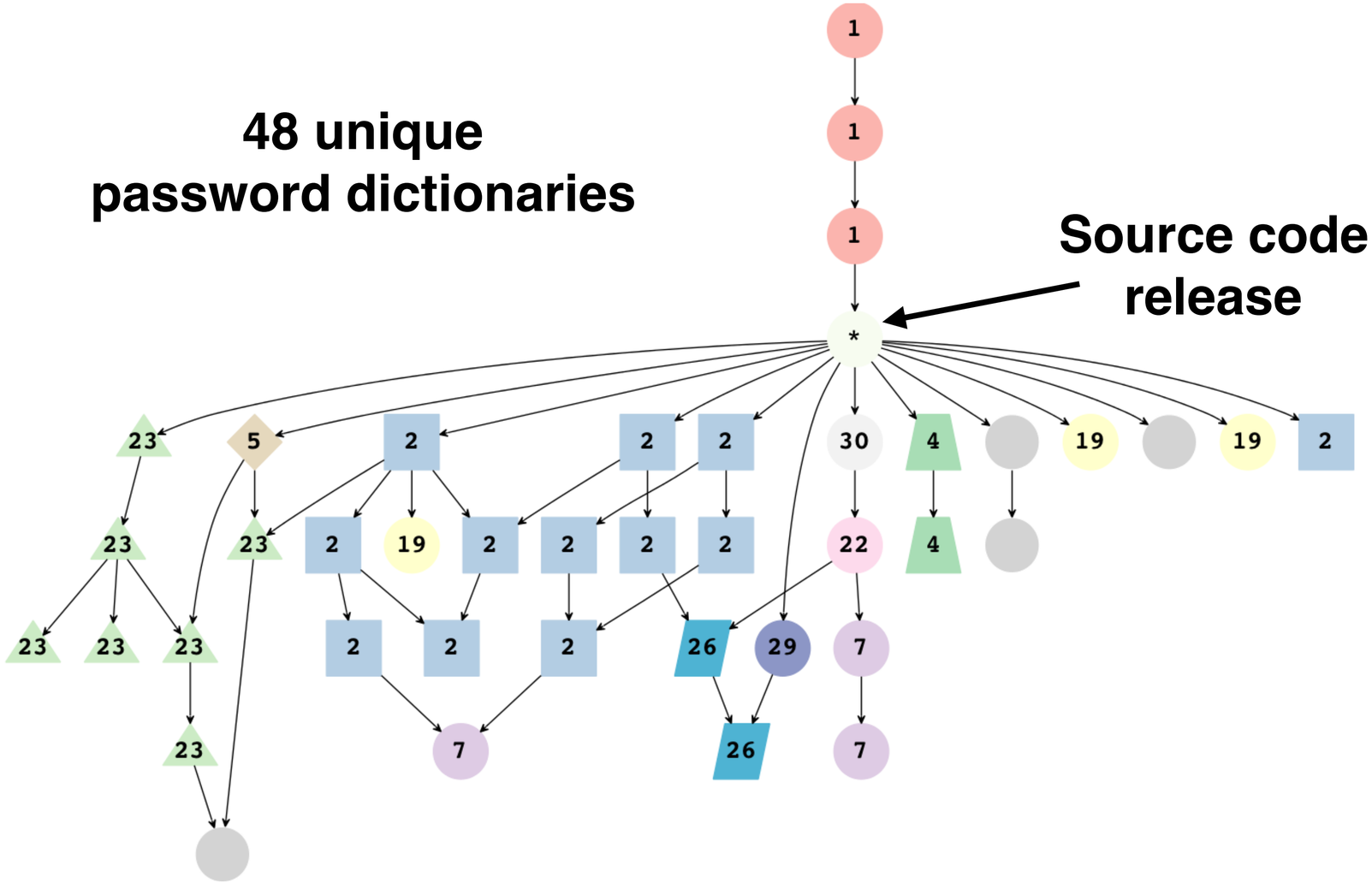
Who ran Mirai?

Divergent Evolution



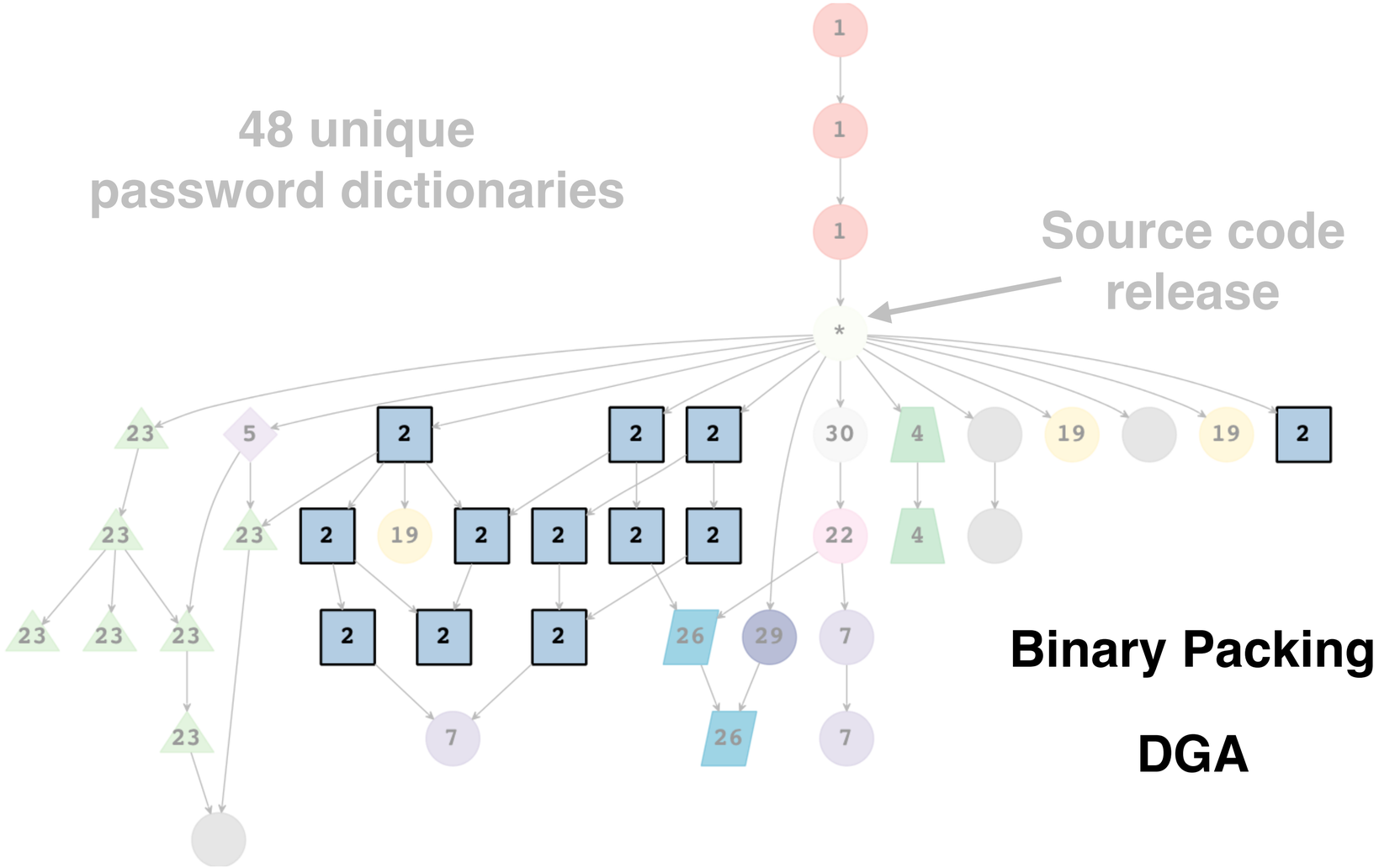
Divergent Evolution

48 unique password dictionaries



Source code release

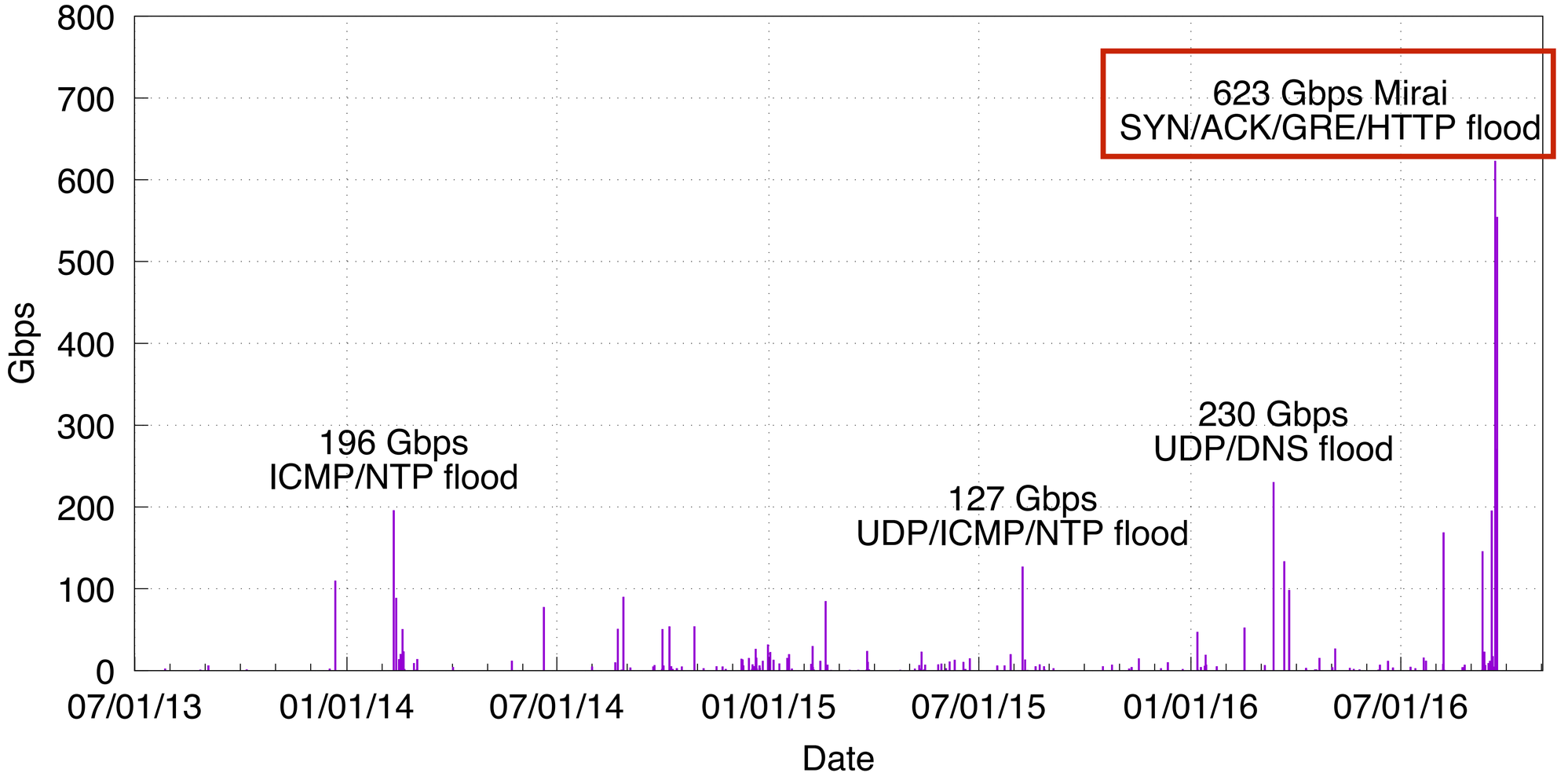
Divergent Evolution



How was Mirai used?

KrebsOnSecurity

Largest Reported DDoS



Dyn Attacker Motives

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 Attacker Motives

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

Booter-like Targets

Games: Minecraft, Runescape, game commerce site

Politics: Chinese political dissidents, regional Italian politician

Anti-DDoS: DDoS protection service

Misc: Russian cooking blog

Unconventional DDoS Behavior

Arbor Networks global DDoS report
65% volumetric, 18% TCP state, 18% application attacks

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

Valve Source Engine game server attack

Limited reflection/amplification
2.8% reflection attacks, compared to 74% for booters

Overview

200,000 - 300,000 globally distributed IoT devices compromised by default Telnet credentials

Evidence of **multiple operators** releasing new strains of Mirai

Mirai follows a **booter-like** pattern of behavior that is capable of launching some of the **largest attacks on record**

New Dog, Old Tricks

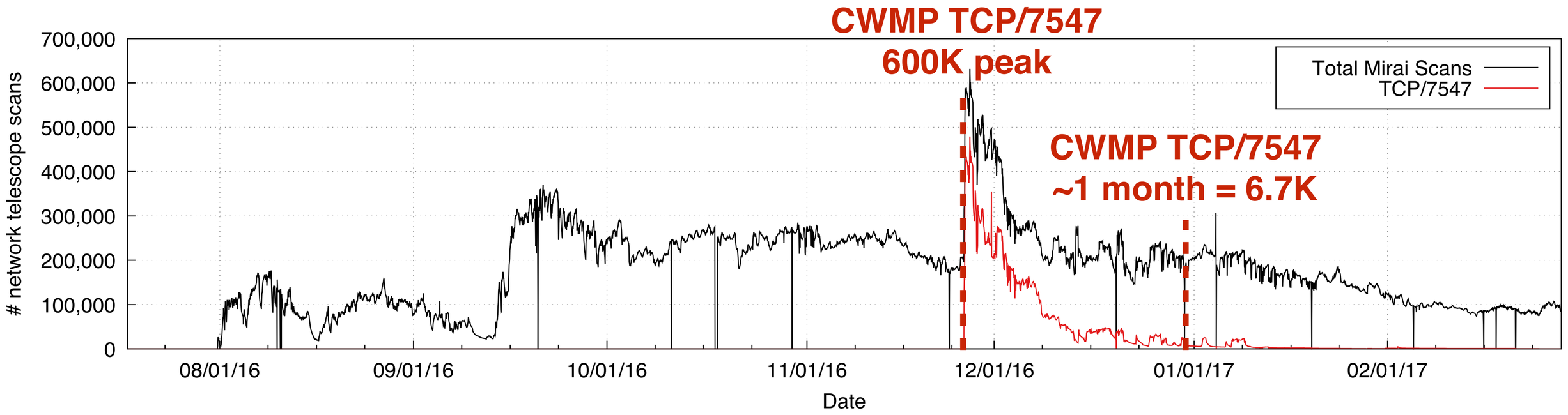
Security Hardening

Username	Password
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin

Username	Password
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko

Username	Password
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	0
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker

Automatic Updates



Device Attribution

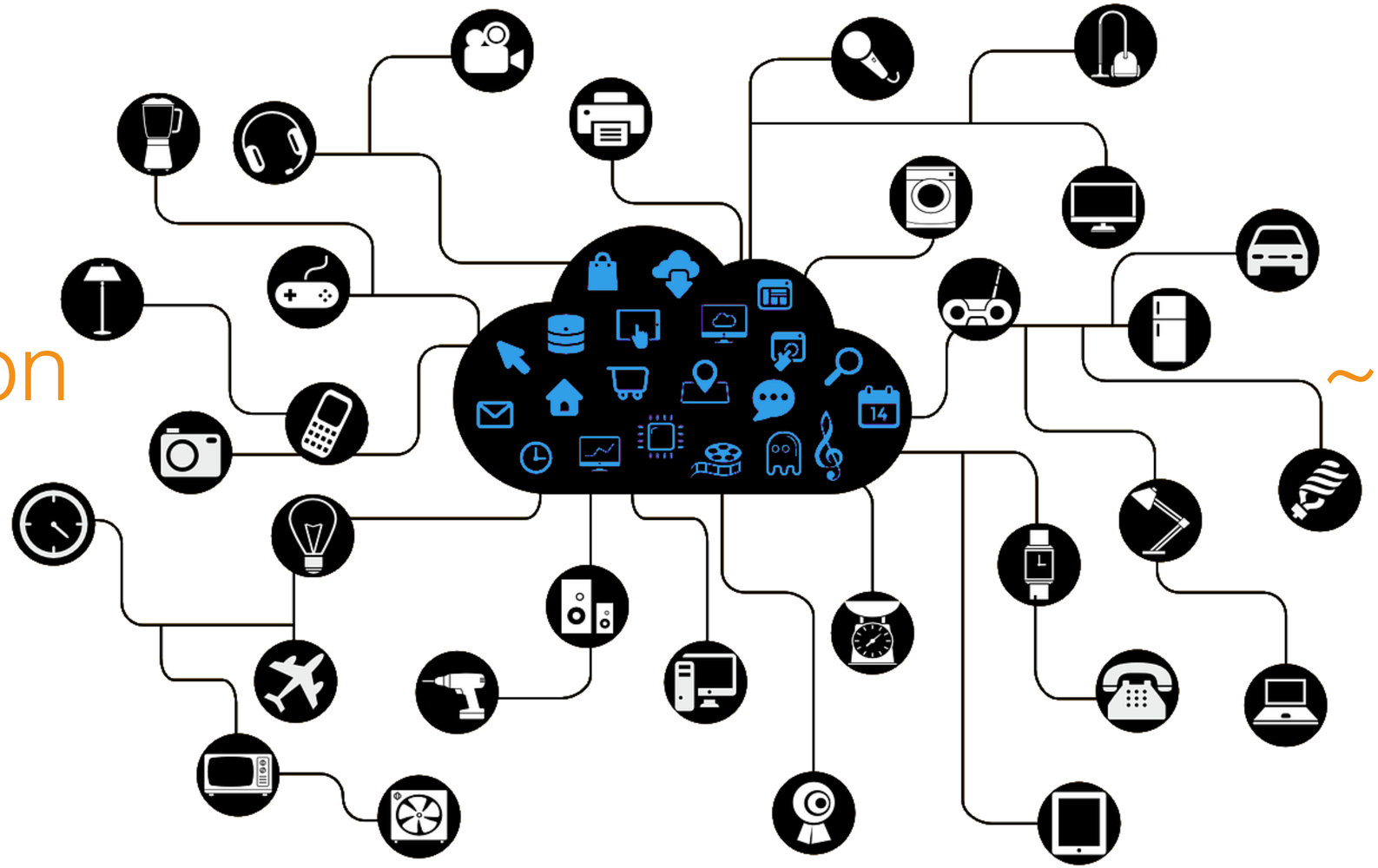
55.4M Scanning IP addresses

1.8M Protocol Banners

587K Identifying Labels

End-of-life

2016
6 - 9 Billion



2020
~30 Billion

Understanding the Mirai Botnet

Manos Antonakakis[†], Tim April[◆], Michael Bailey[★], Matthew Bernhard[ǂ], Elie Bursztein[✳]
Jaime Cochran[△], Zakir Durumeric[ǂ], J. Alex Halderman[ǂ], 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***, [ǂ] *University of Michigan*

zanema2@illinois.edu