– Social Media Posting Allowed –

Tweeter, Facebook, LinkedIn, other social media posts are welcomed in this session if you:

- Only post comments made by the speakers or panelists
- Do not post comments or questions from the audience (but you can share the speakers' responses to questions)
- Do not post the name, position or company of other meeting attendees
- Do not post conversations with attendees
- M³AAWG is not a deliverability conference; we are:
  - An industry working group meeting
  - An anti-abuse conference, or
  - A gathering of security experts
- All of the M³AAWG Membership, Trademarks and Logo guidelines apply (https://www.m3aawg.org/members/how-promote-m3aawg#TrademarkGuidelines)
- Appreciate a shout out to @maawg and #m3aawg42

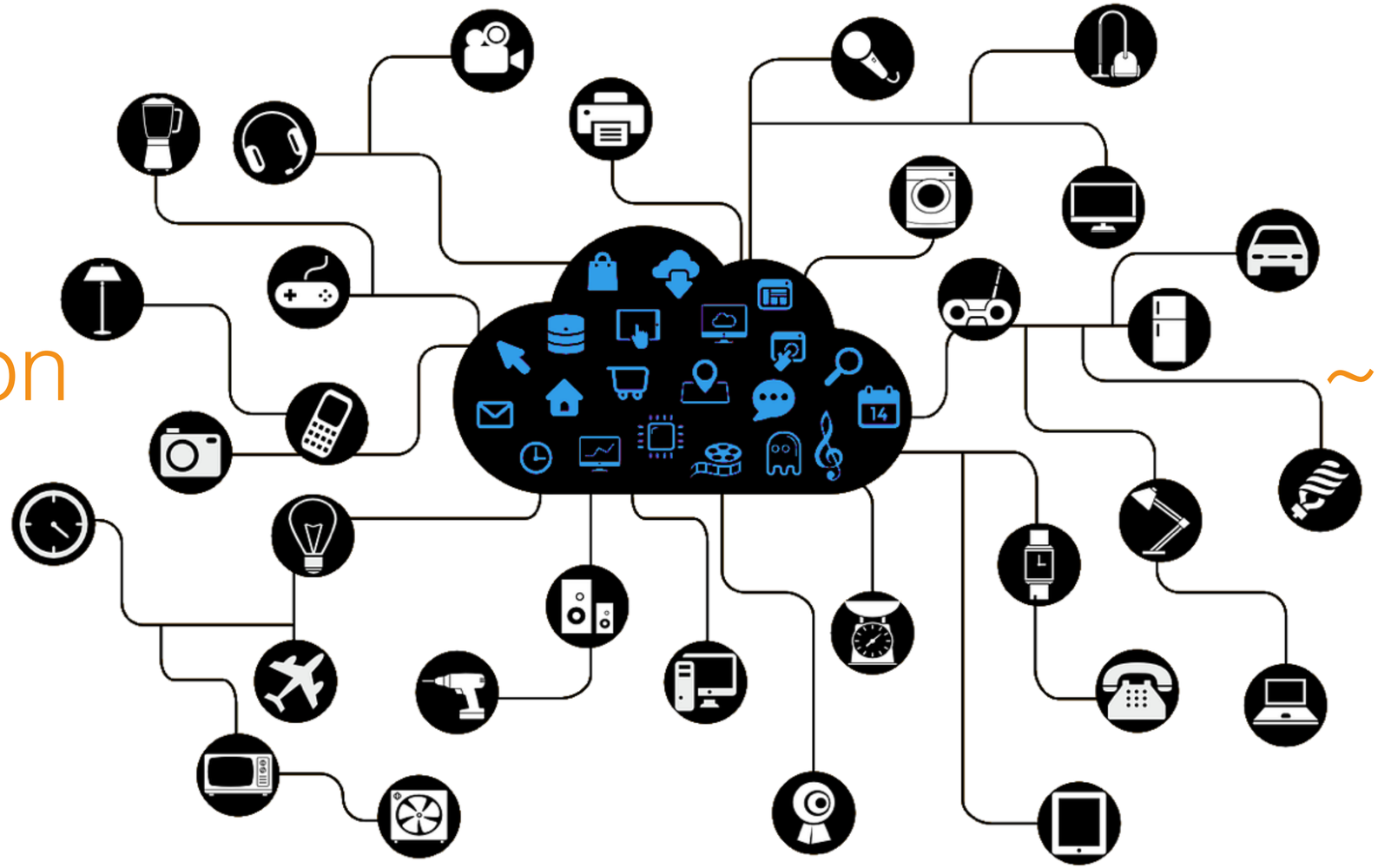
Understanding the Mirai Botnet

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*

Internet of Things

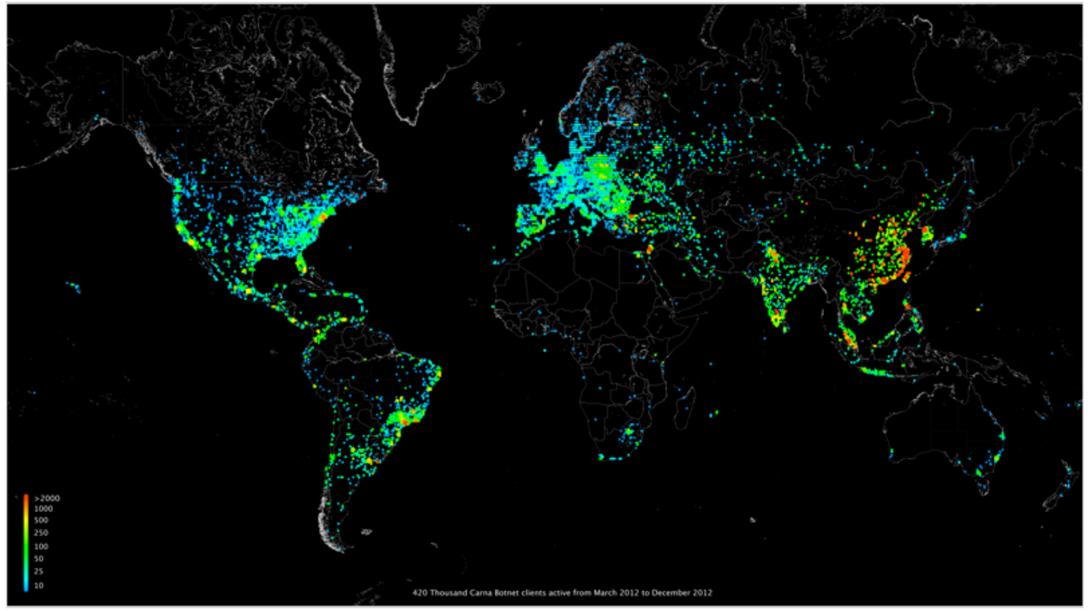
2016
6 - 9 Billion



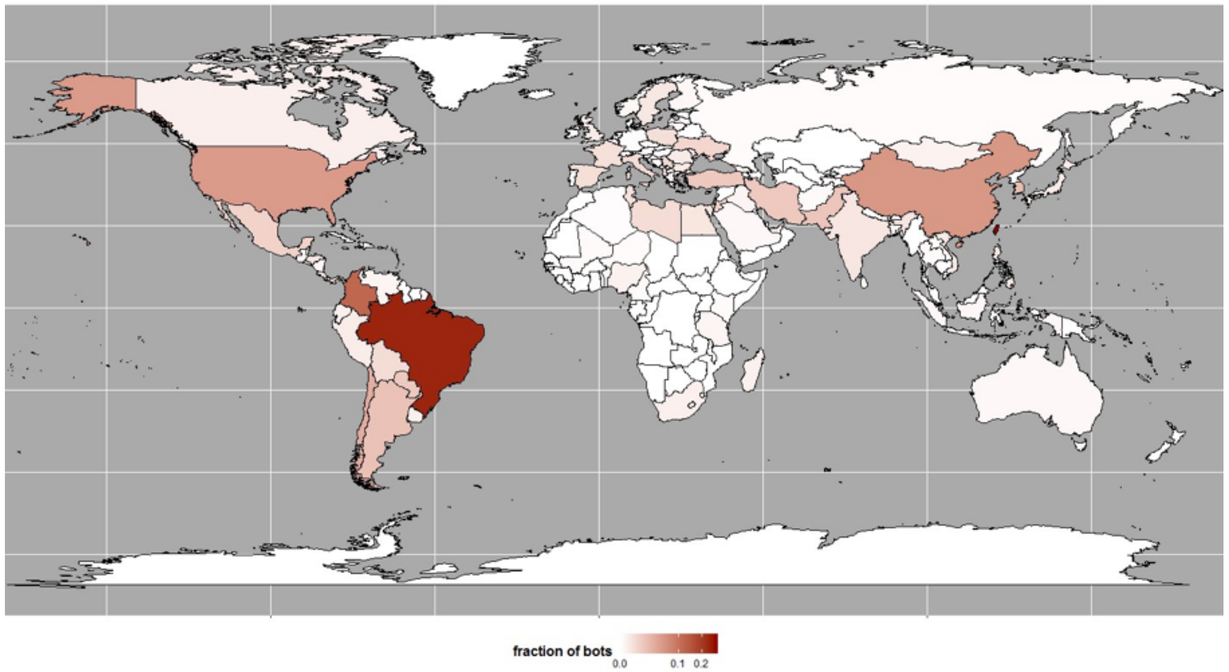
2020
~30 Billion

IoT Botnets

2012 Carna Botnet
420,000 devices



2015 BASHLITE / gafgyt
1,000,000 devices



Mirai

THE WALL STREET JOURNAL.

Cyberattack Knocks Out Access to Websites

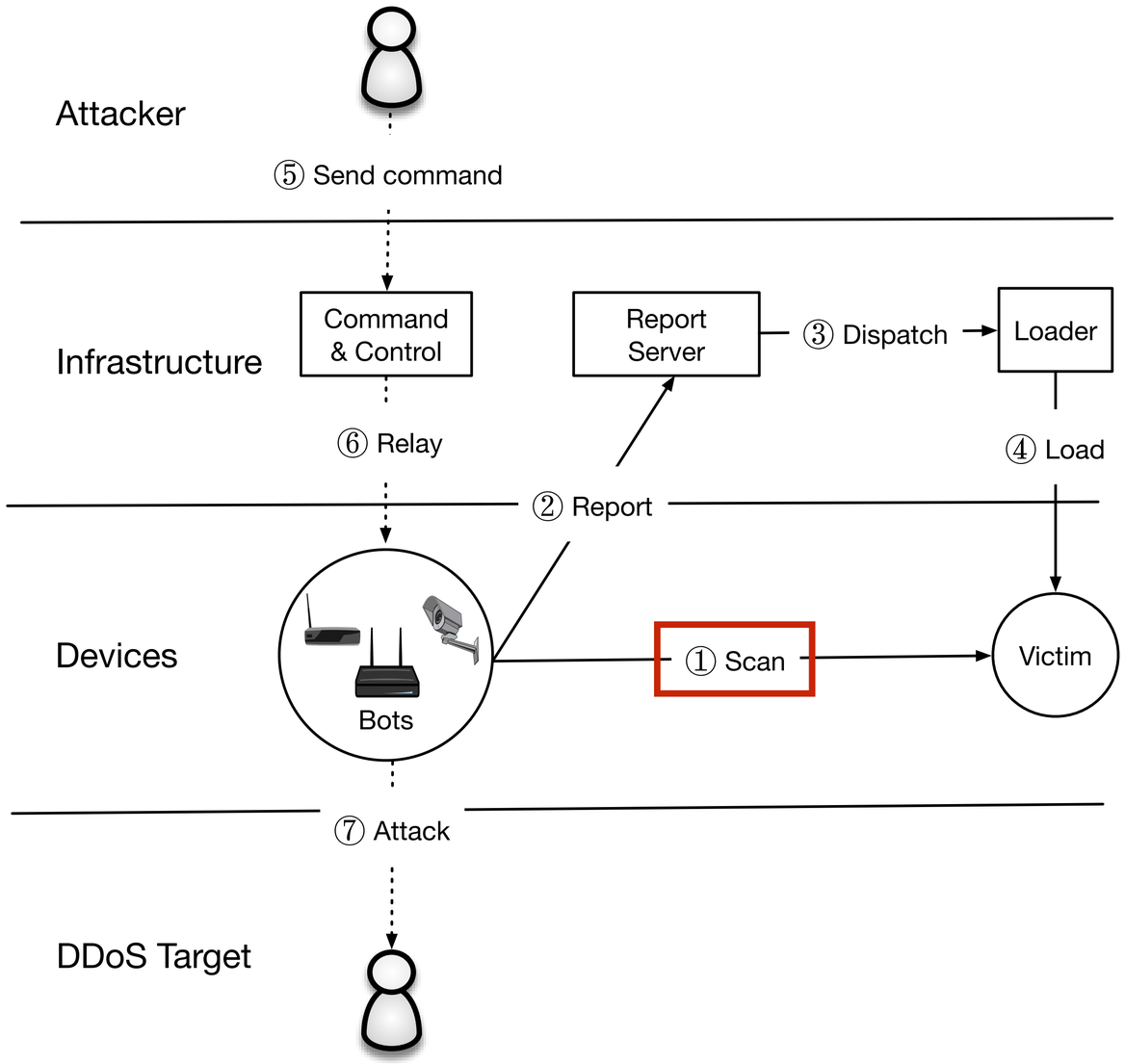
Popular sites such as Twitter, Netflix and PayPal were unreachable for part of the day

21 KrebsOnSecurity Hit With Record DDoS
SEP 16

KrebsonSecurity
In-depth security news and investigation

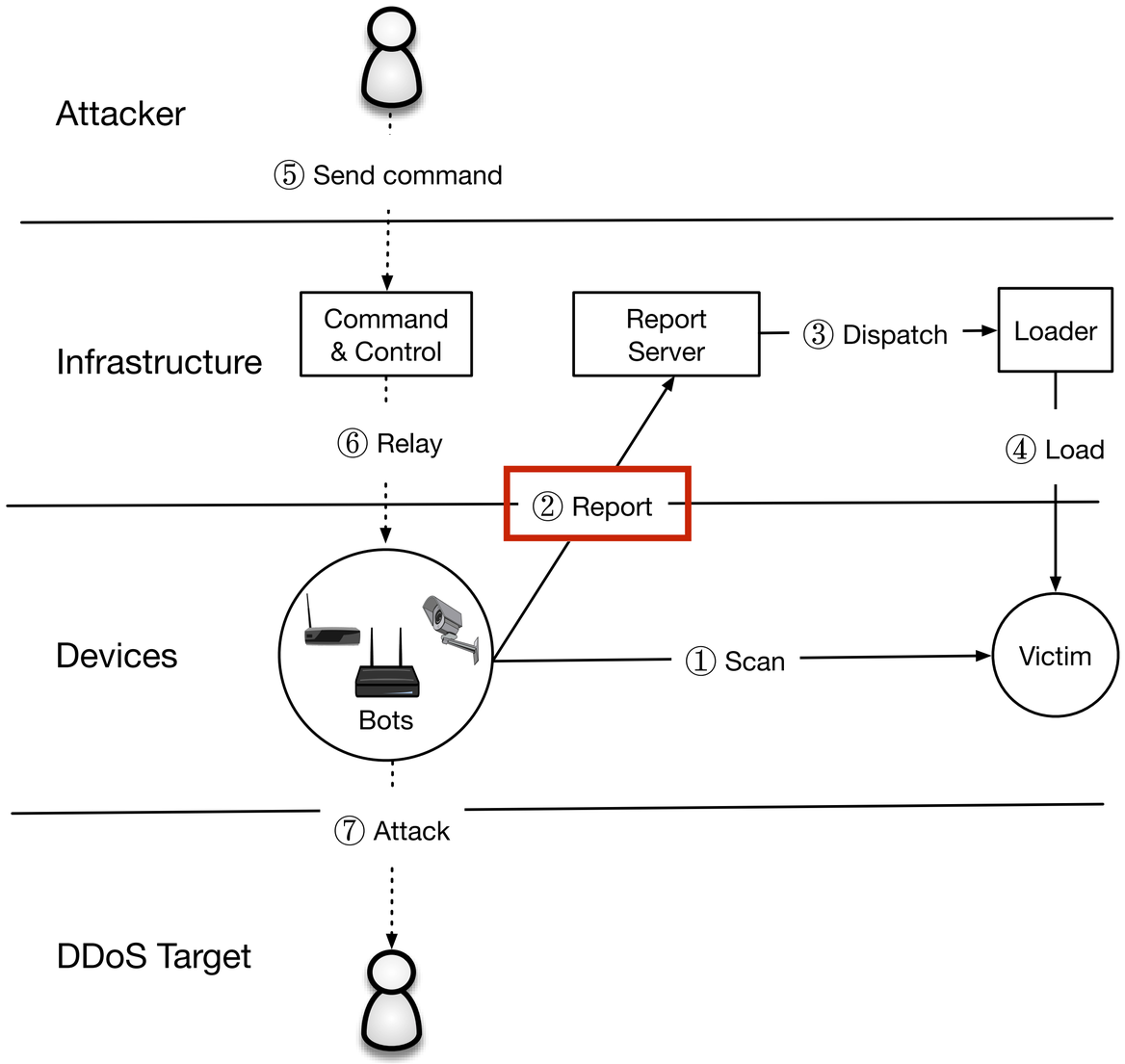
01 Source Code for IoT Botnet 'Mirai' Released
OCT 16

Lifecycle



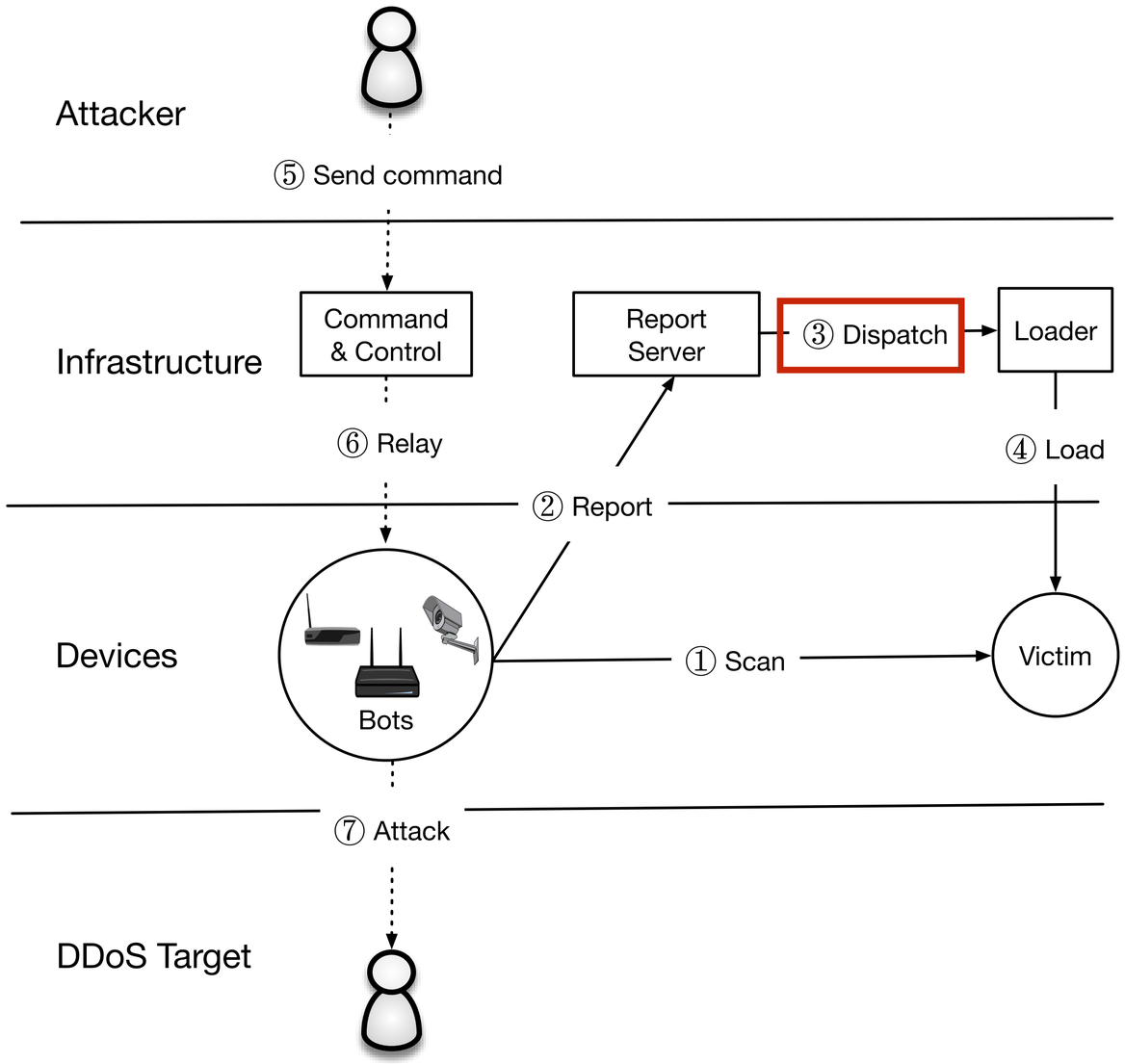
- Fast, stateless port-scanning: SYN w/ *TCP seq # = dest IP*
- Check for SYN-ACKs where *TCP seq # = src IP + 1*
- Raw socket, requires root
- If port open, brute force telnet login credentials

Lifecycle



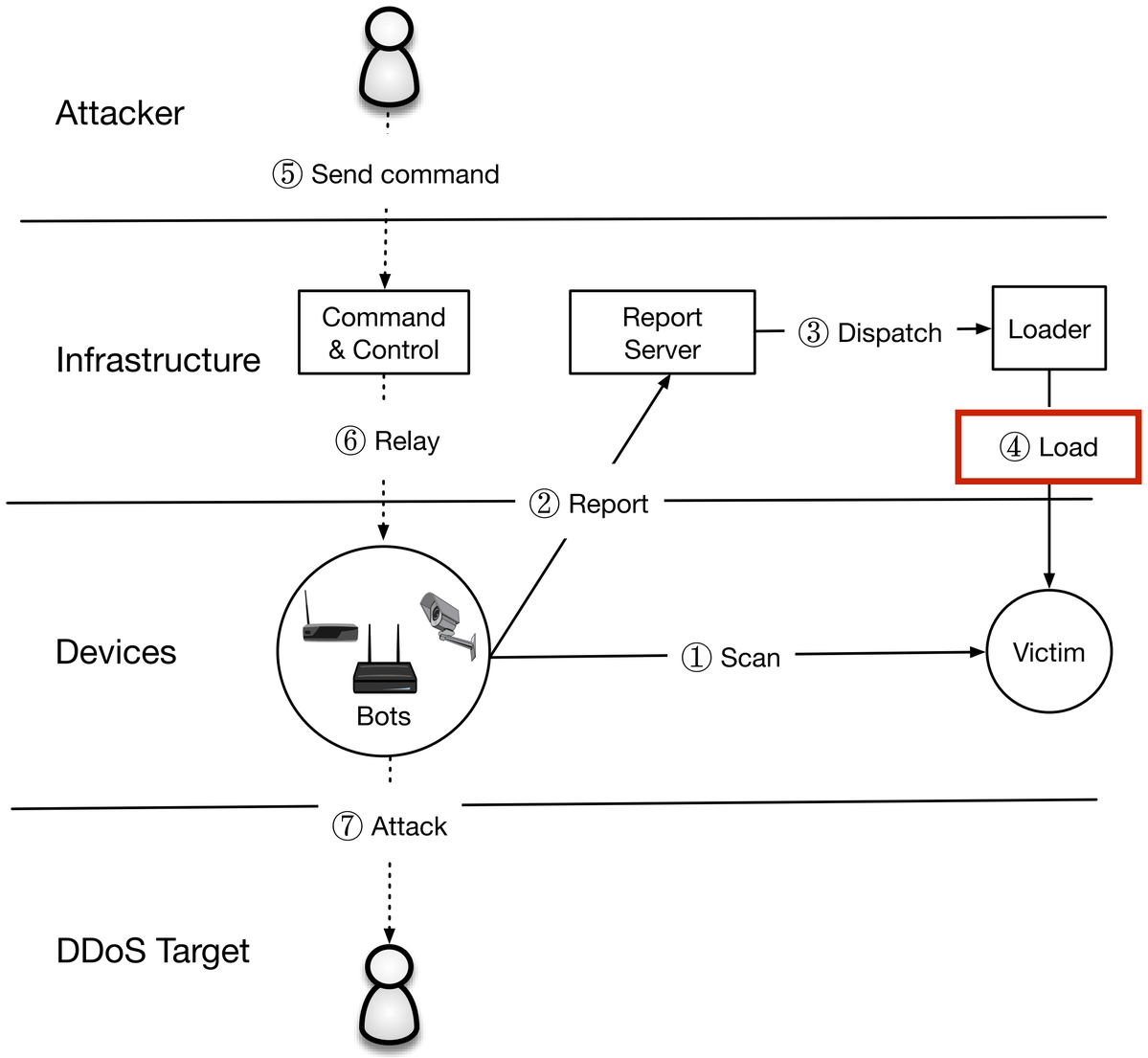
- Reports successful IP:port, username:password
- Report server aggregates results

Lifecycle



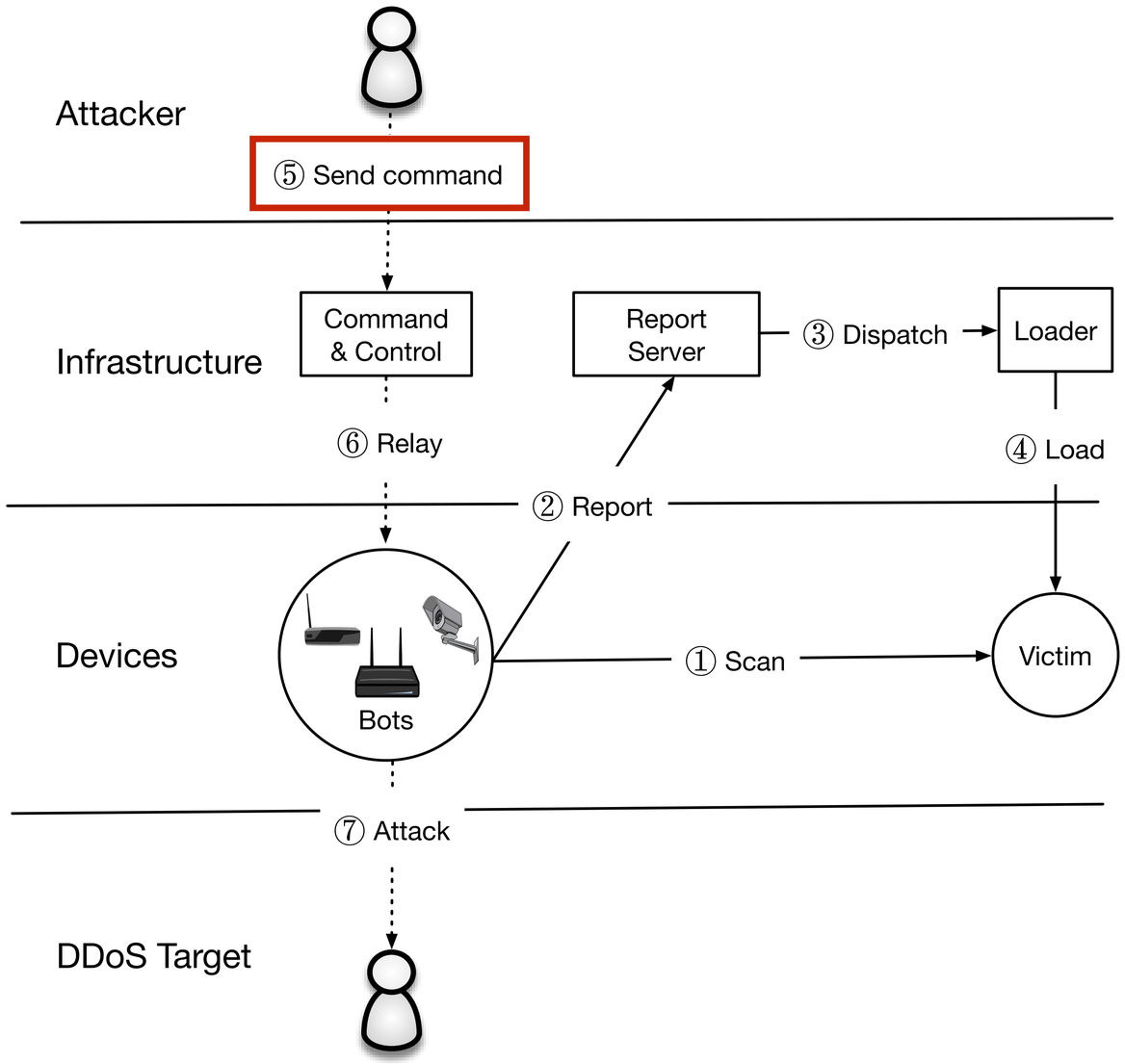
- Asynchronous from scanning + reporting
- Supports building up potential “hit list”

Lifecycle



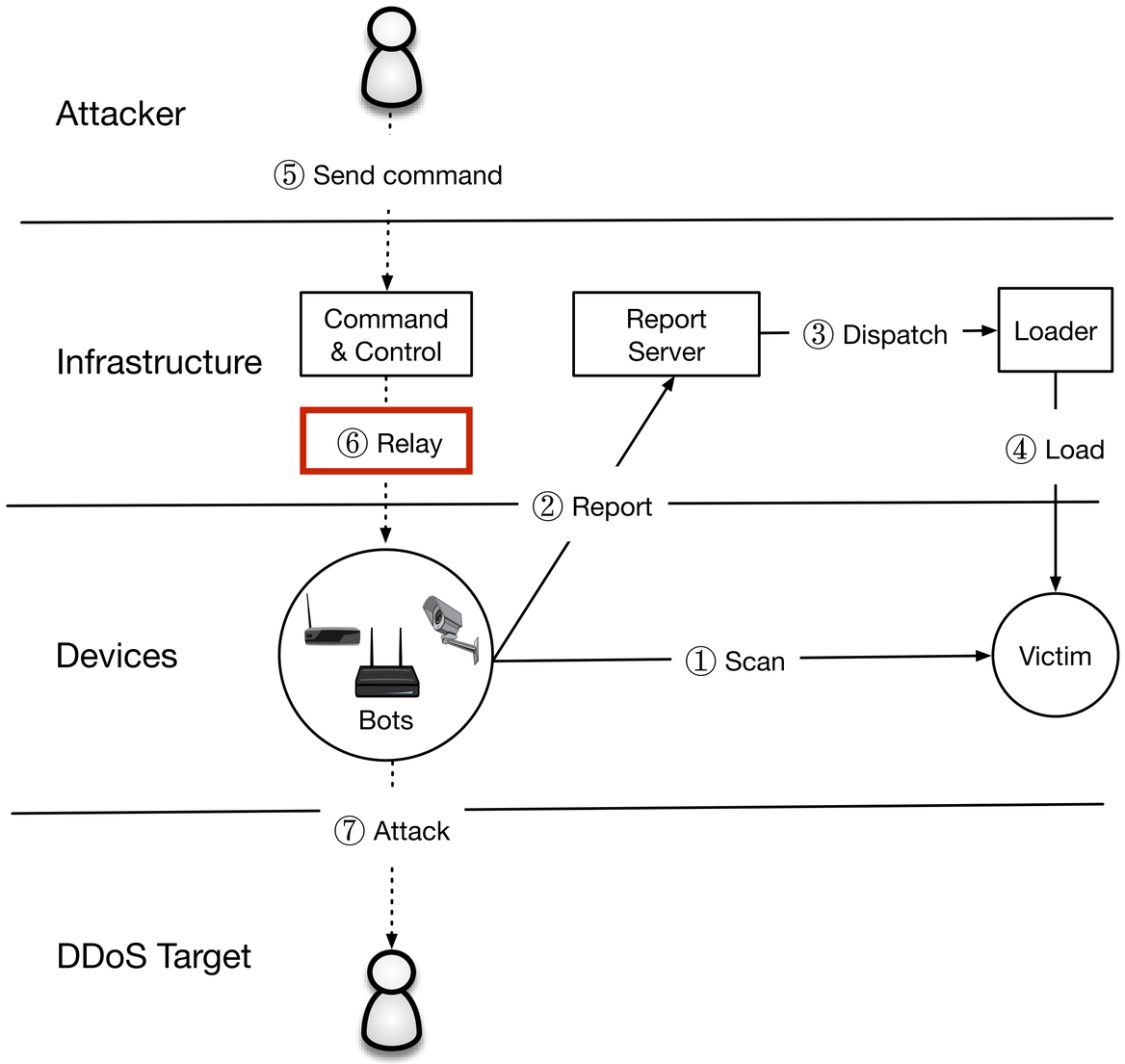
- Determines architecture, wget/tftp 1 out of 9 archs.
- Defensive - kills competing Mirai, and any processes listening on HTTP/Telnet/SSH
- Obfuscates process name and removes executable - <u>does not survive reboots</u>

Lifecycle



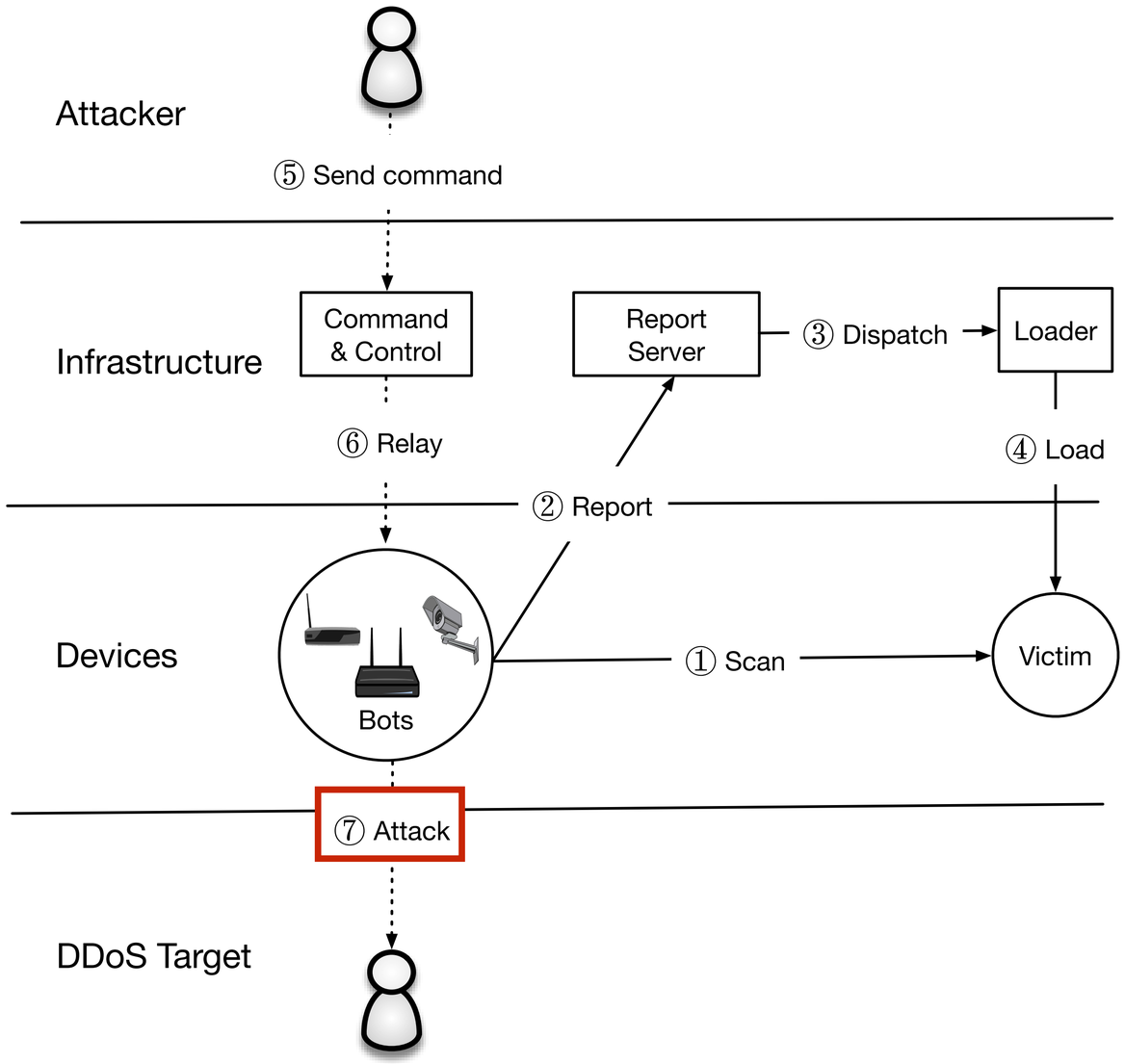
- Simple attack API - configurable duration, attack size (# bots), IP spoofing
- Supports 10 attack types, volumetric/TCP/application

Lifecycle



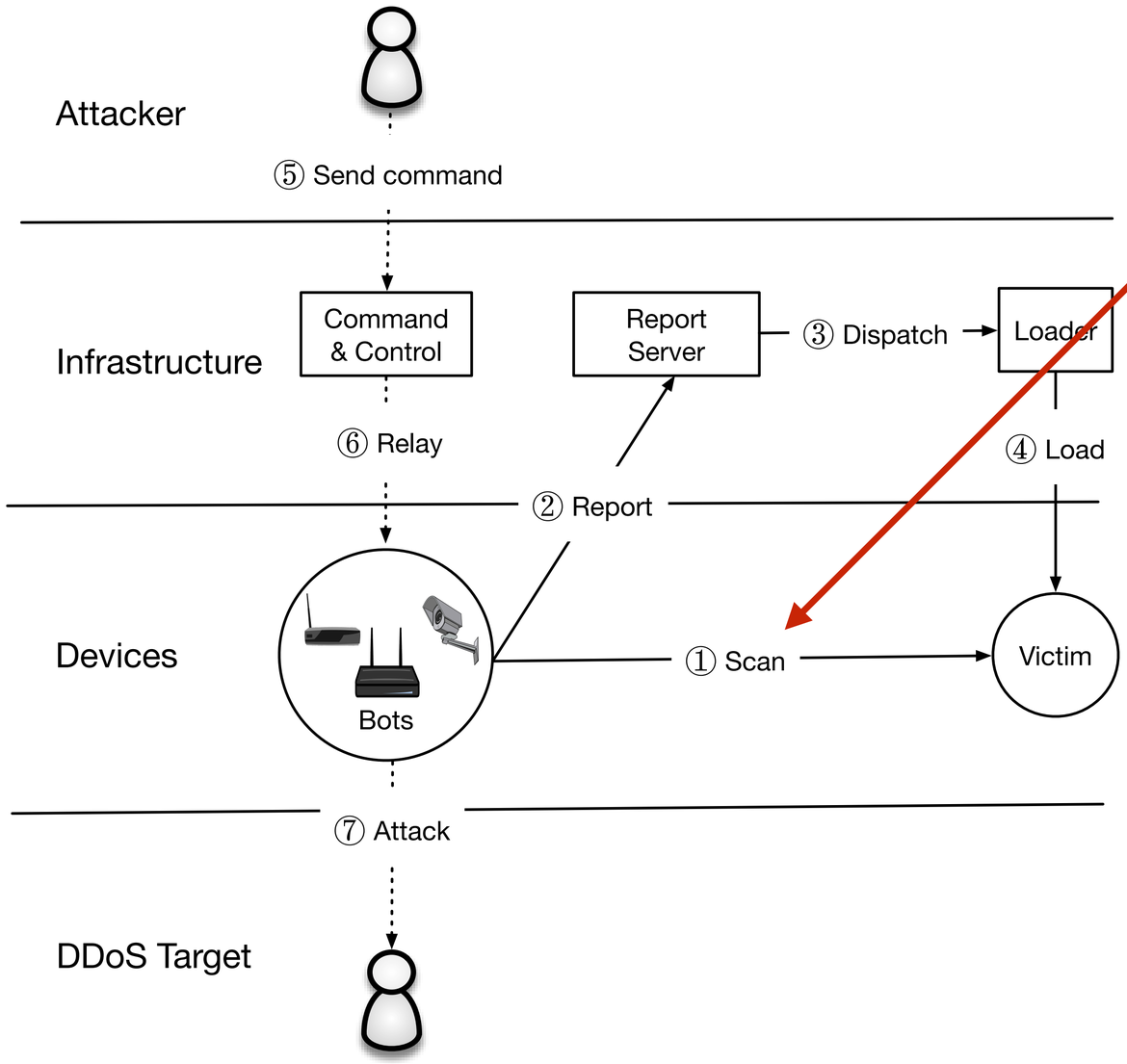
- C&C resolves domains, issues attacks on IPs

Lifecycle



- Attacks do not interrupt scanning
- Fingerprintable application level packets
- Configurable reflection / amplification attacks

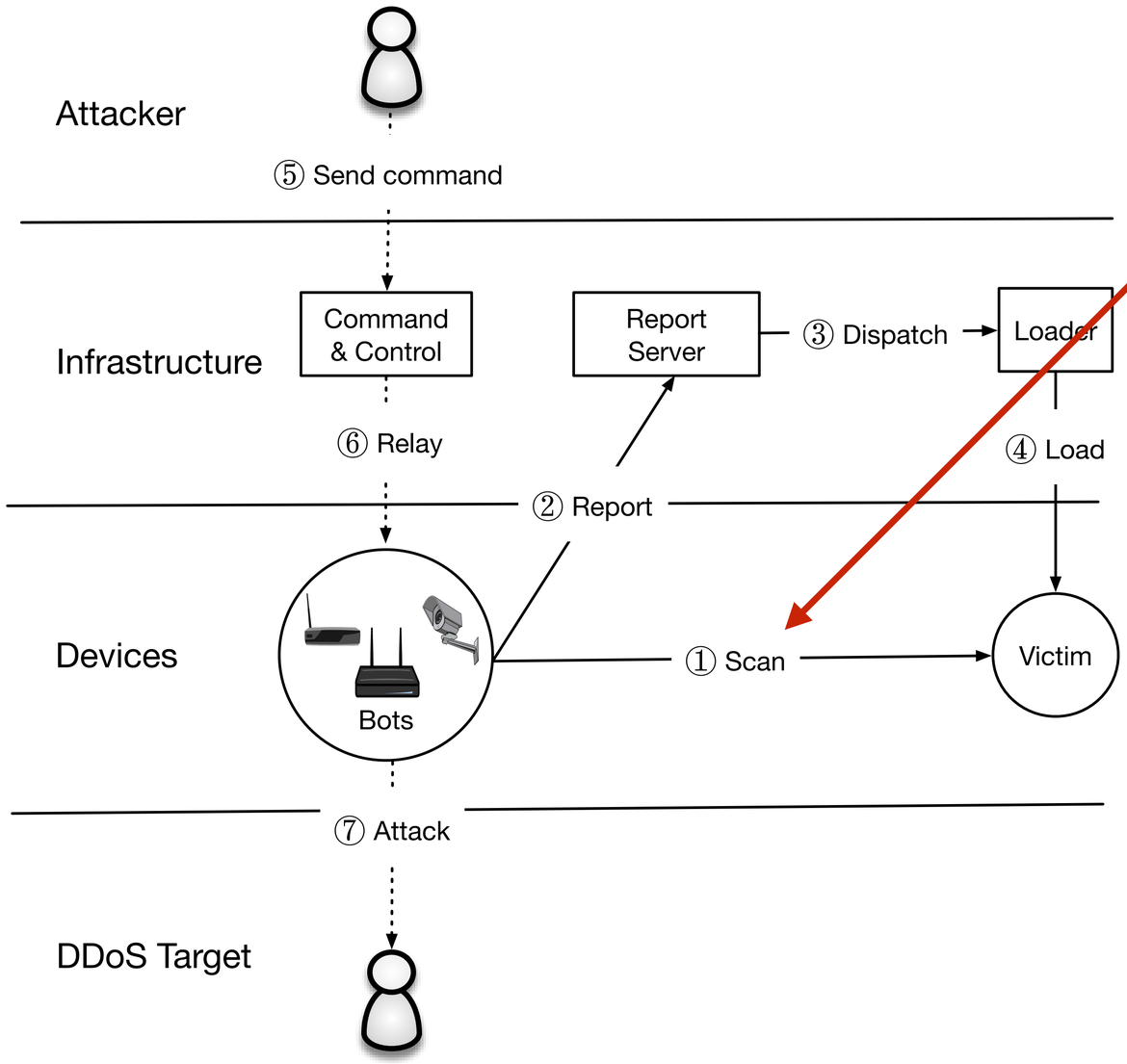
Measurement



Data Source	Size
Network Telescope	**4.7M unused IPs**

- 0.1% of IPv4 address space
- 1.1M packets / min
- Look for Mirai fingerprint

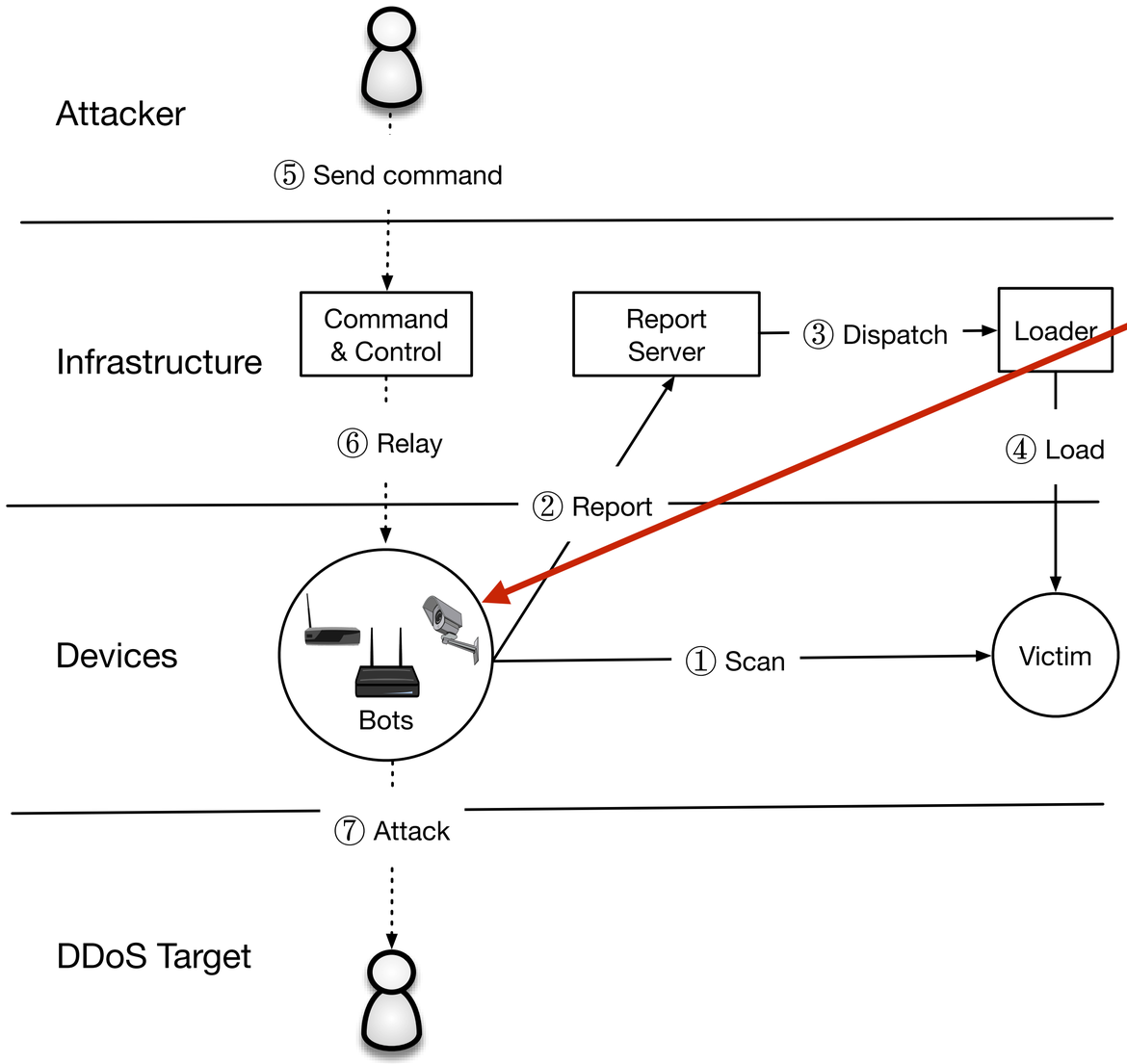
Measurement



Data Source	Size
Network Telescope	**4.7M unused IPs**

- 0.1% of IPv4 address space
- 1.1M packets / min
- Look for Mirai fingerprint
- Handling IP churn: look for active concurrent scans

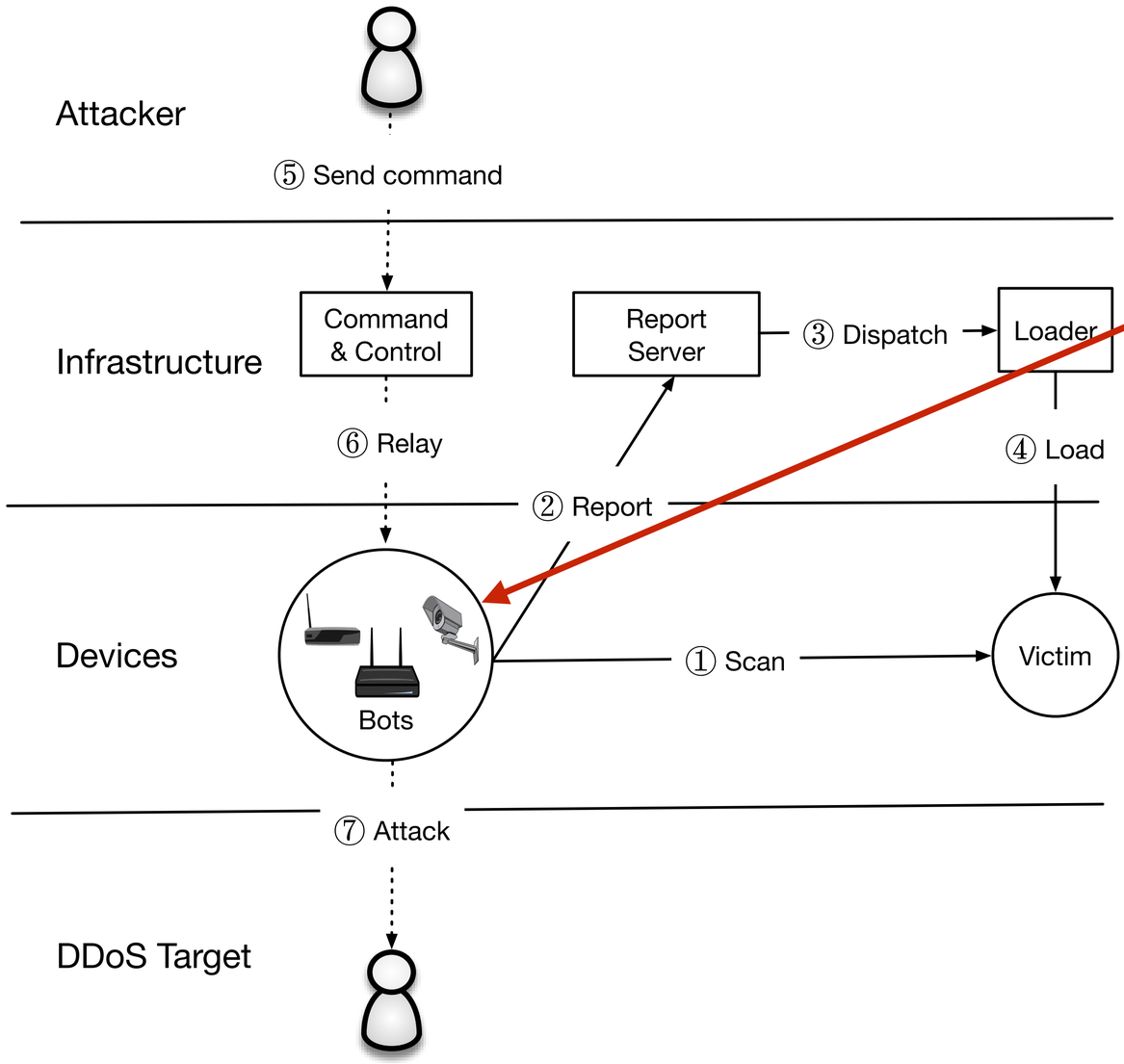
Measurement



Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	**136 IPv4 scans**

- Application protocol banners (telnet, FTP, HTTP, etc.)
- Device attribution: NMap service probes, manual labeling

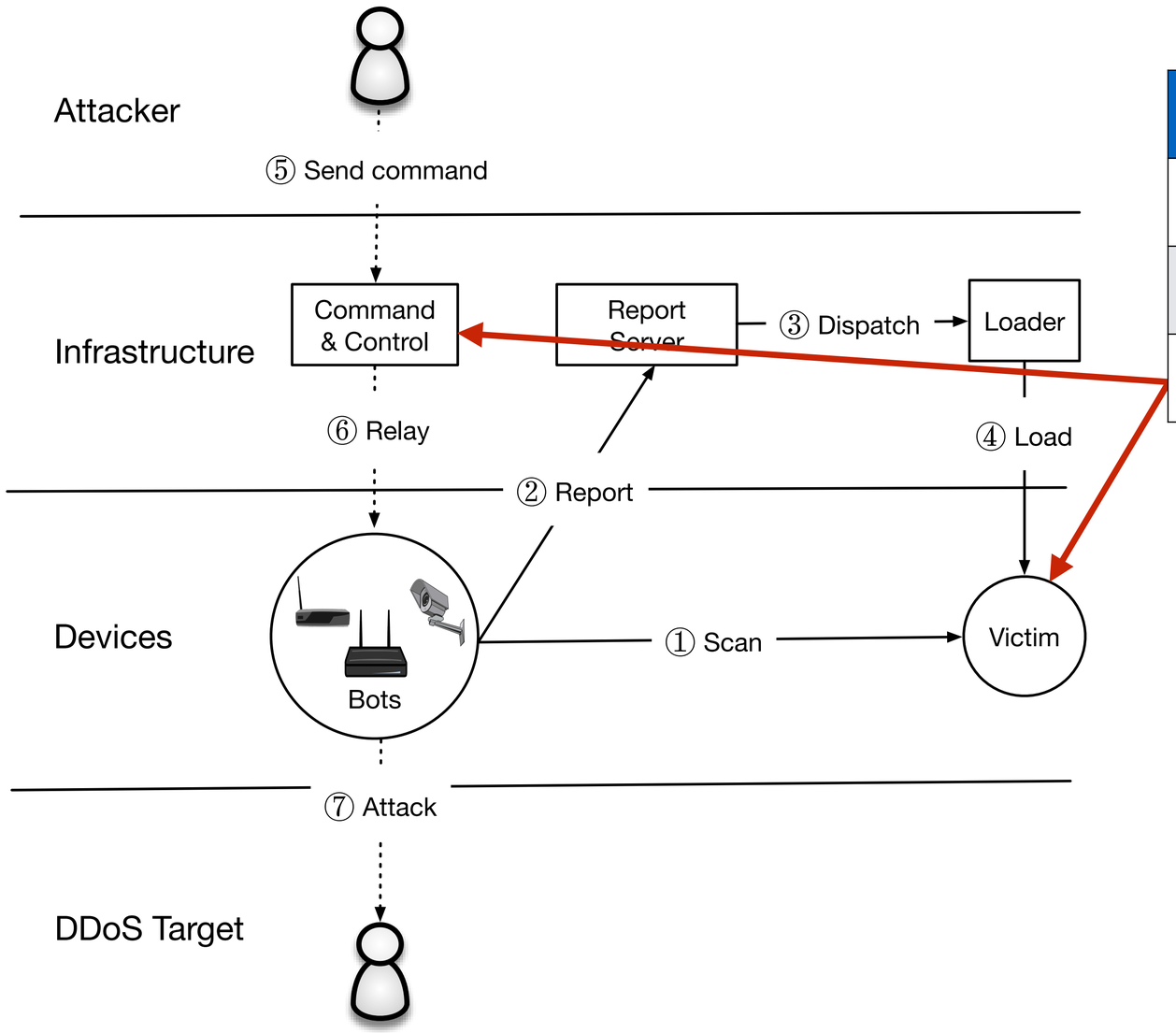
Measurement



Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	**136 IPv4 scans**

- Application protocol banners (telnet, FTP, HTTP, etc.)
- Device attribution: NMap service probes, manual labeling
- Future work: Individual device fingerprinting

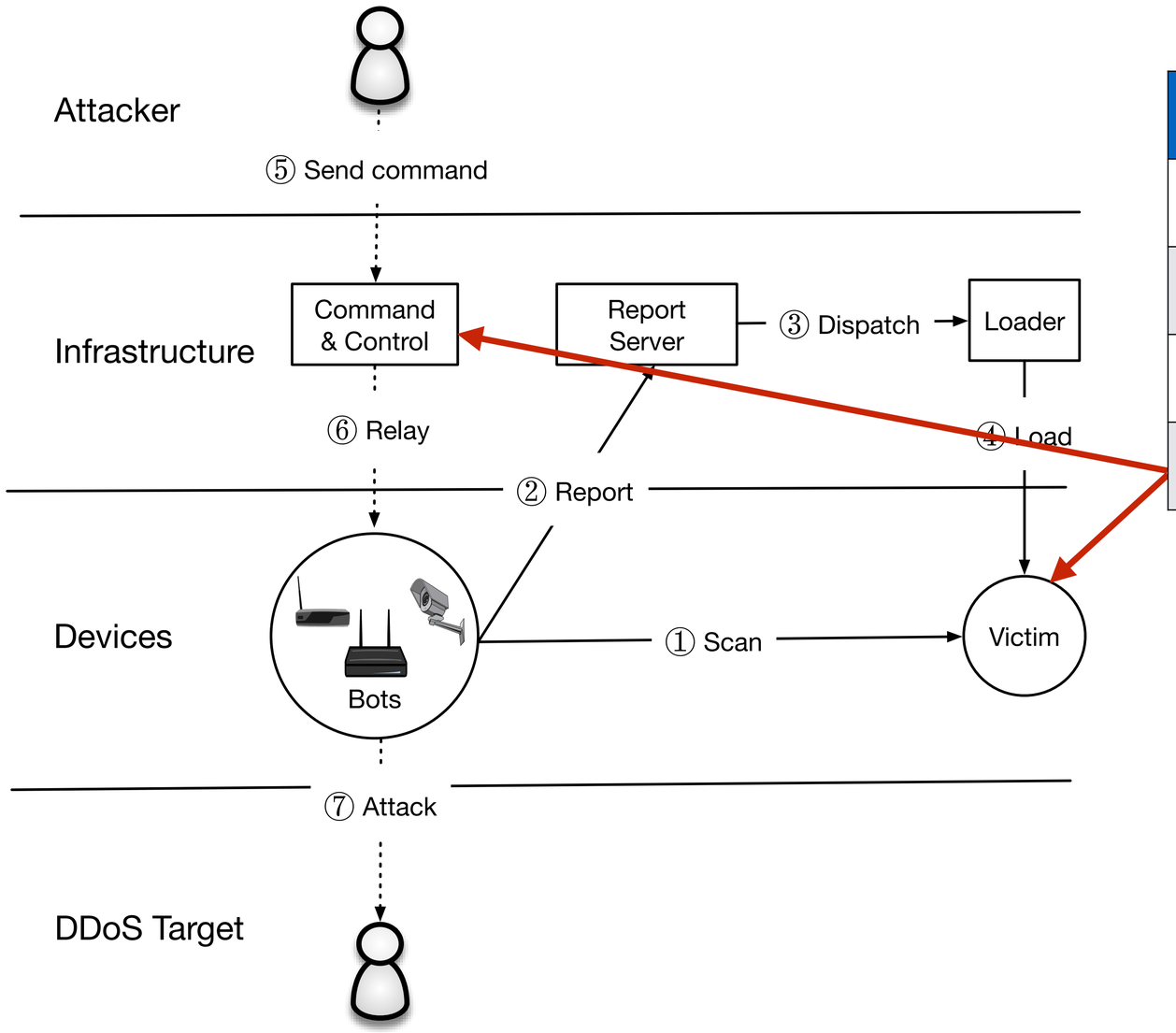
Measurement



Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	**434 binaries**

- Busybox shell that accepts any telnet login credentials
- Used collected binaries to generate YARA rules

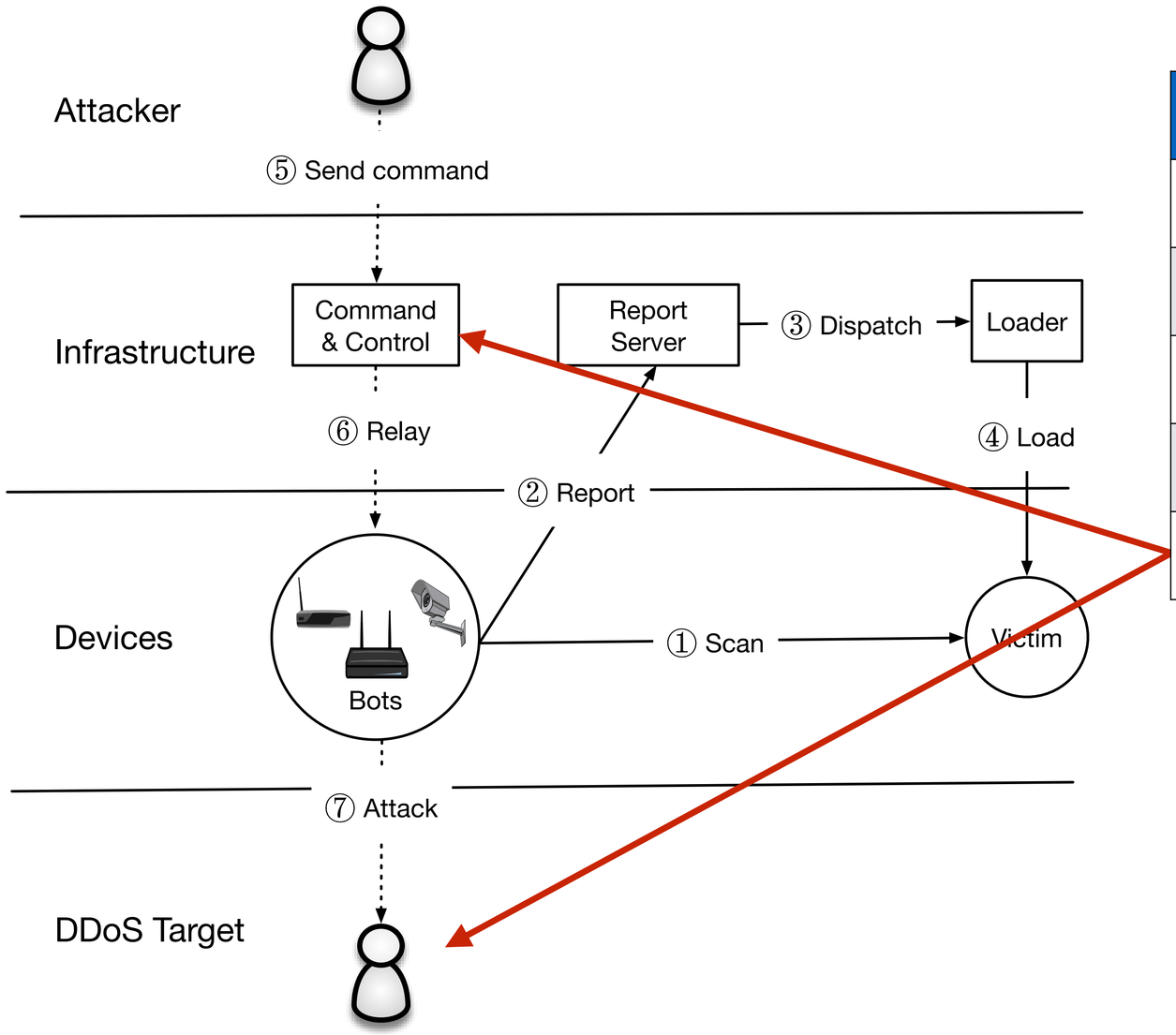
Measurement



Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	**594 binaries**

- Found VirusTotal binaries matching YARA rules

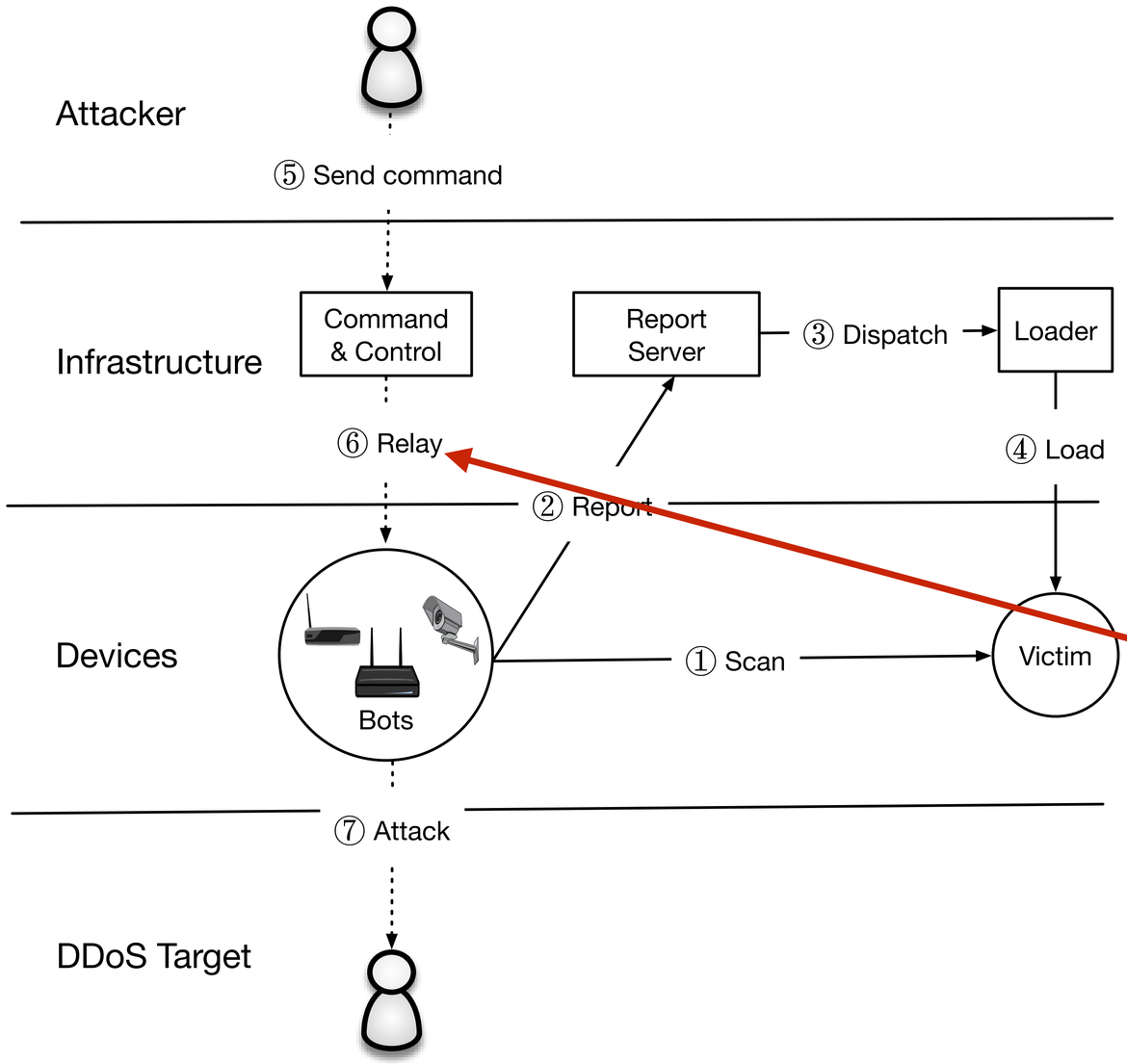
Measurement



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**

- Active = Thales DNS monitoring system, using zone files, domain lists
- Passive = Resource Records from large US ISP

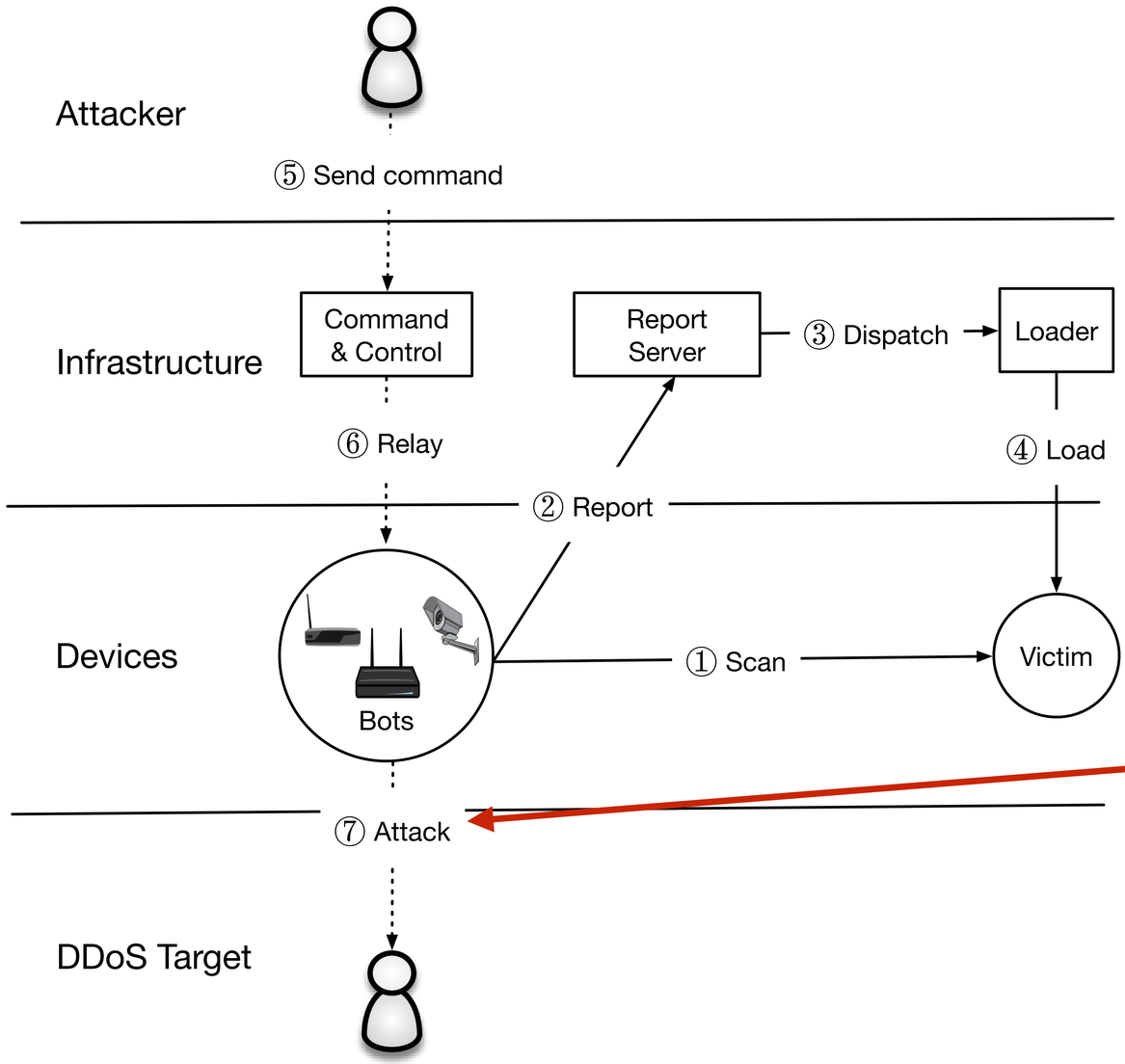
Measurement



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**

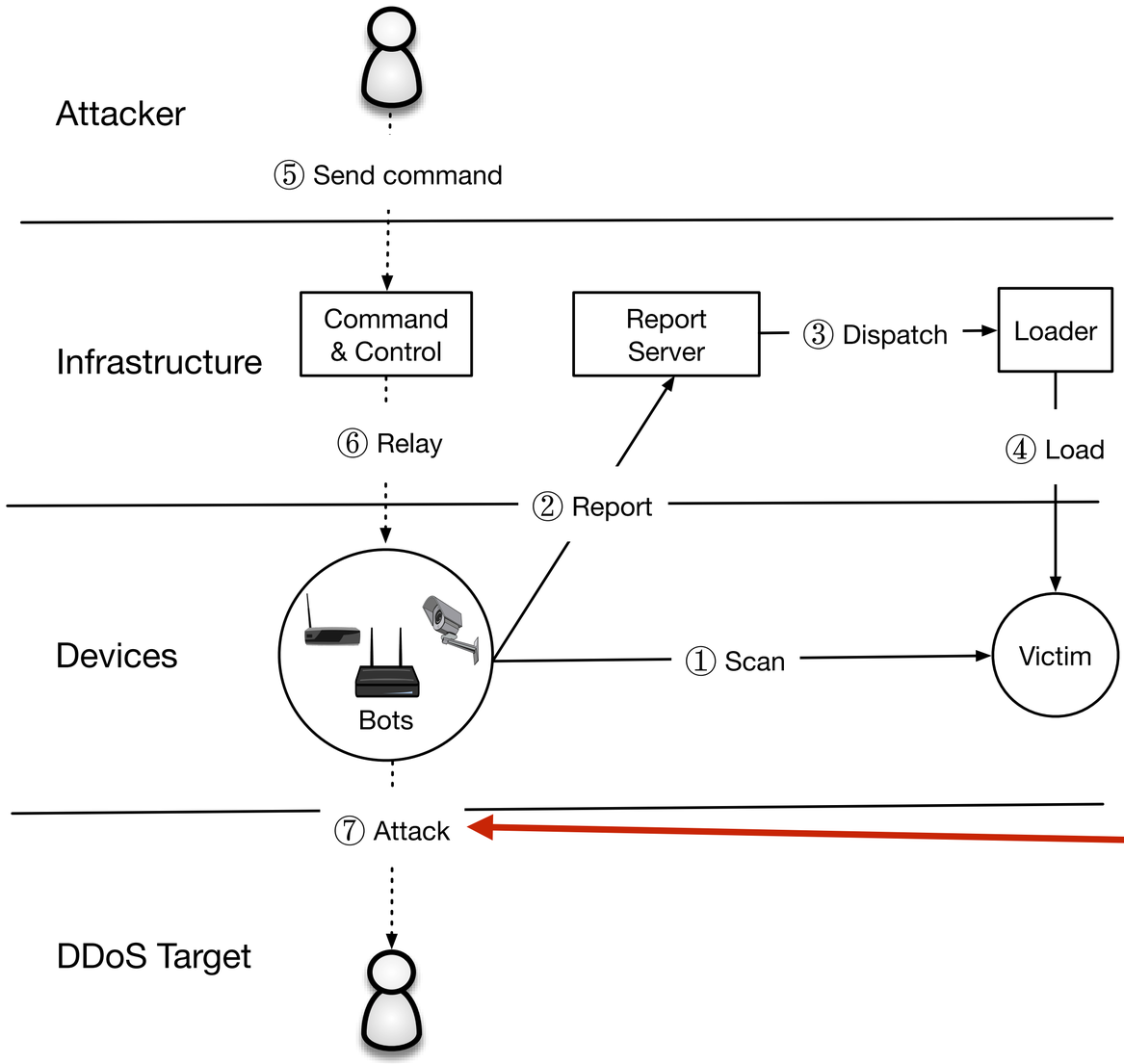
- C&C doesn't authenticate / validate connecting bots

Measurement



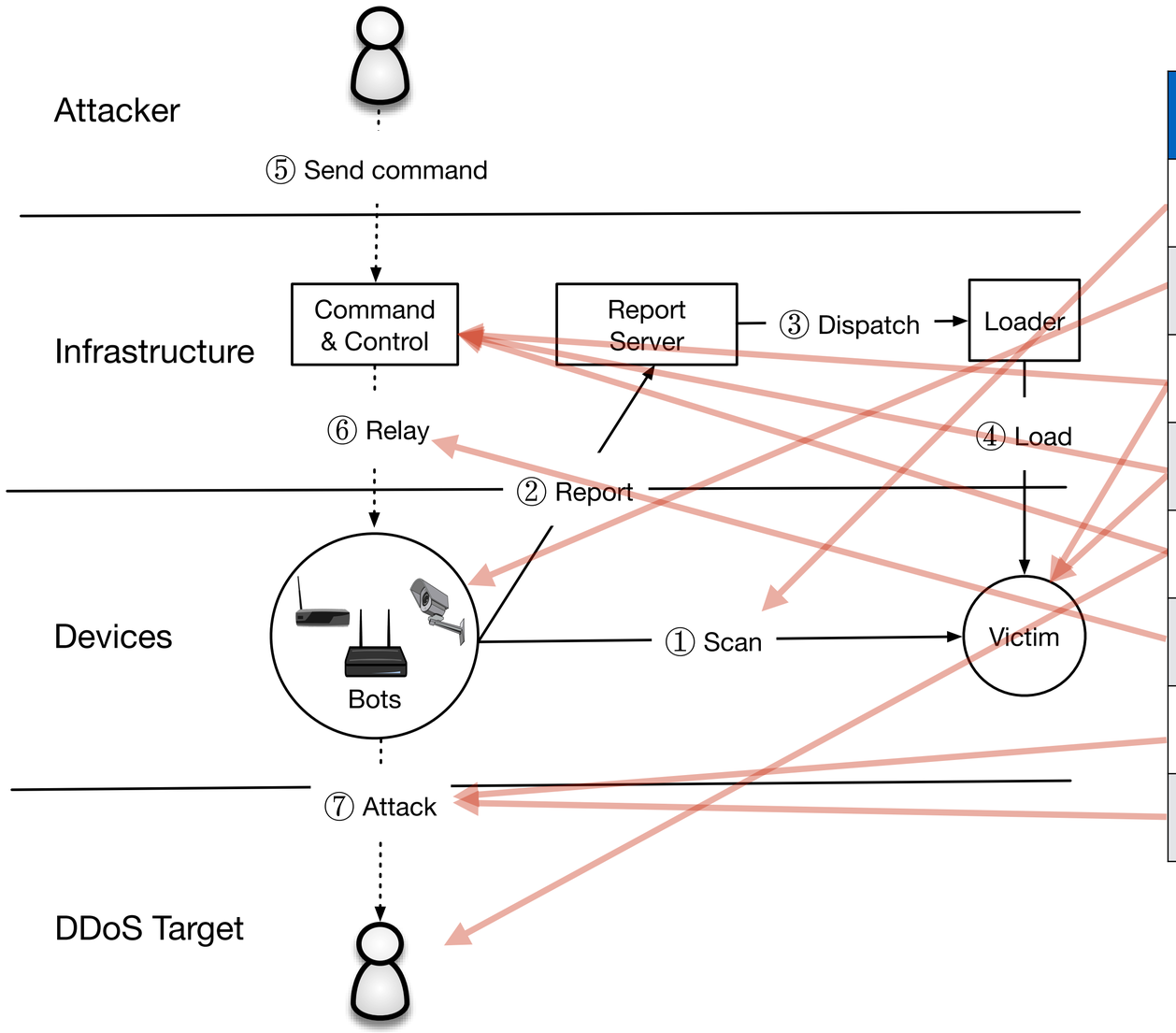
Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	594 binaries
Active/Passive DNS	499M daily RRs
C2 Milkers	64K issued attacks
Krebs DDoS Attack	**170K attacker IPs**

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**

Measurement



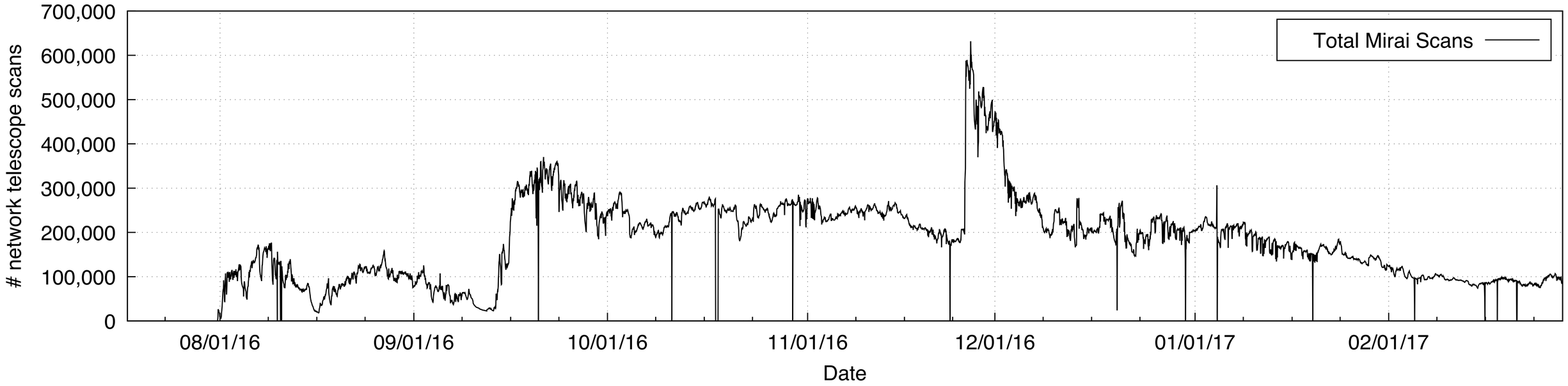
Data Source	Size
Network Telescope	4.7M unused IPs
Active Scanning	136 IPv4 scans
Telnet Honeypots	434 binaries
Malware Repository	594 binaries
Active/Passive DNS	499M daily RRs
C2 Milkers	64K issued attacks
Krebs DDoS Attack	170K attacker IPs
Dyn DDoS Attack	108K attacker IPS

July 2016 - February 2017

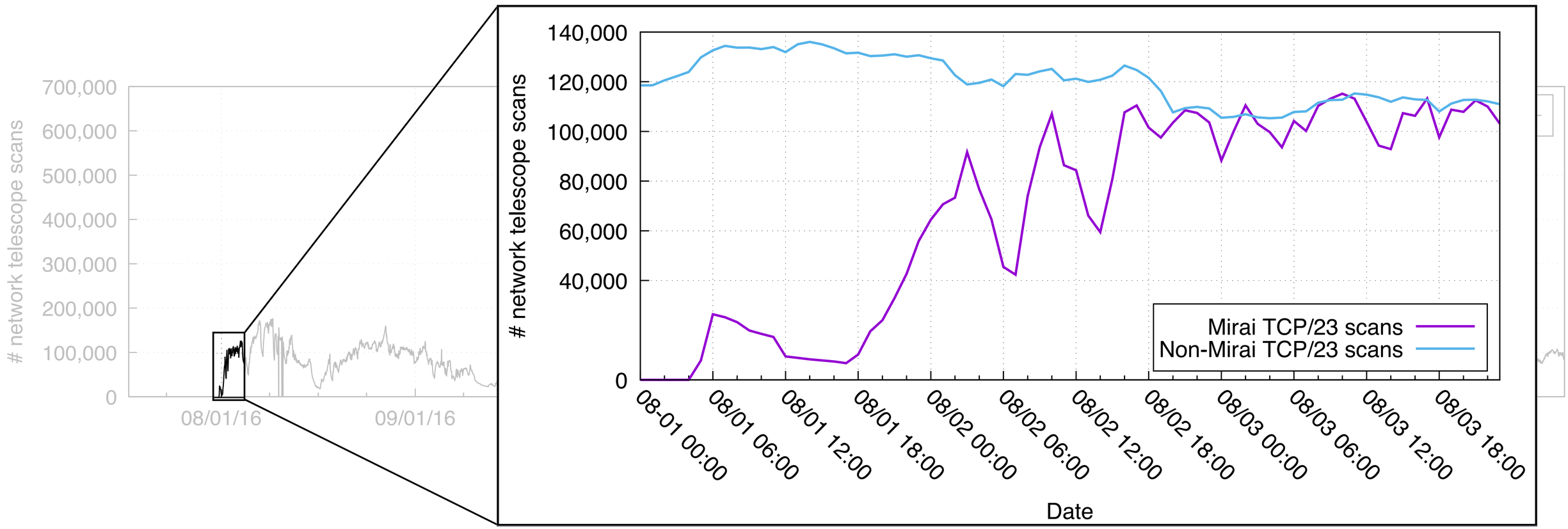
Roadmap

1. **Growth & Composition**
2. Ownership & Evolution
3. Attacks
4. Post-Mirai
5. Lessons Learned

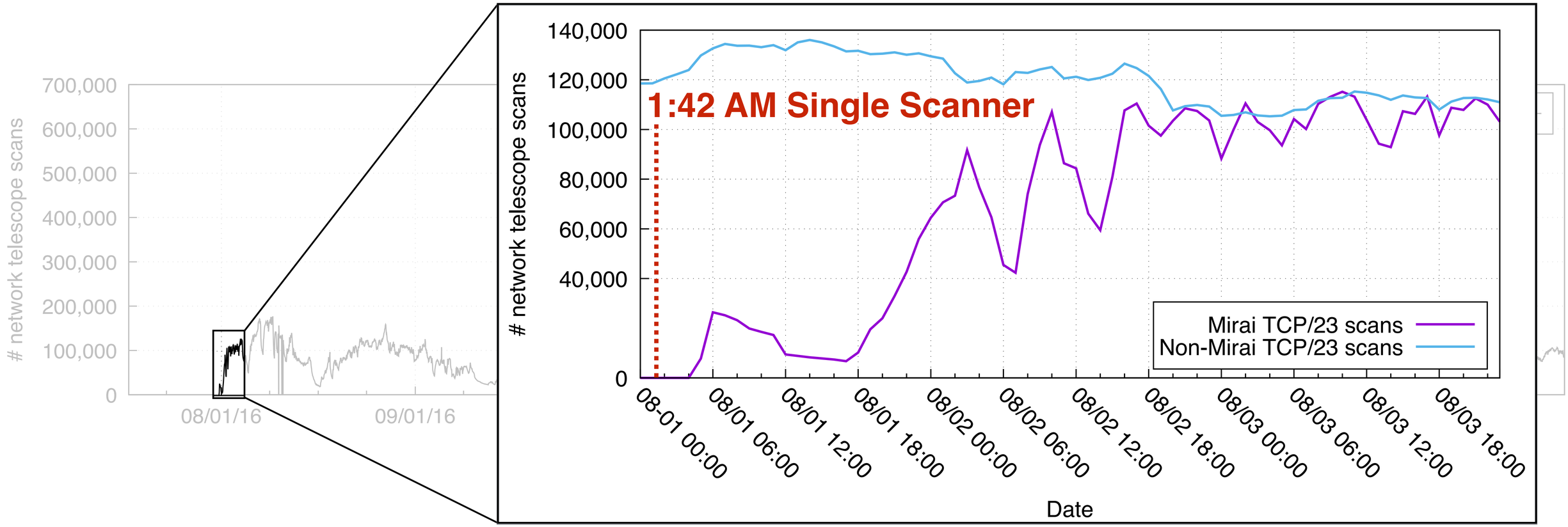
Population


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

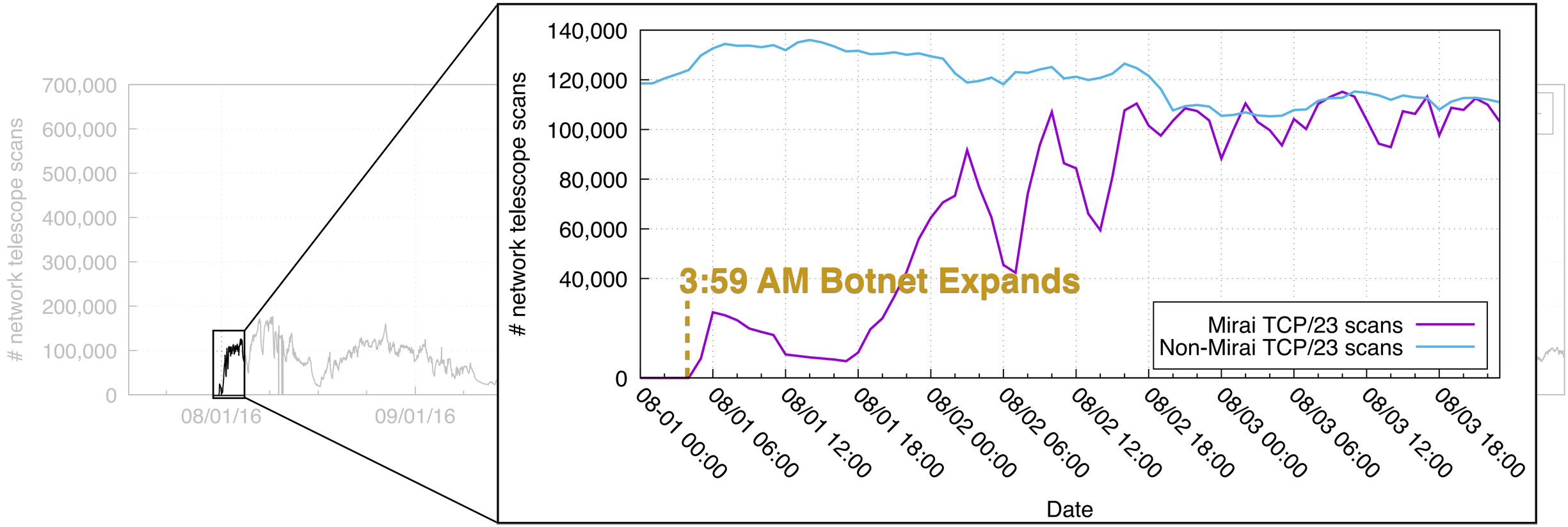
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
08/01/16
09/01/16
140,000
120,000
100,000
80,000
60,000
40,000
0
network telescope scans
Mirai TCP/23 scans
Non-Mirai TCP/23 scans
08-01 00:00
08/01 06:00
08/01 12:00
08/01 18:00
08/02 00:00
08/02 06:00
08/02 12:00
08/02 18:00
08/03 00:00
08/03 06:00
08/03 12:00
08/03 18:00
Date

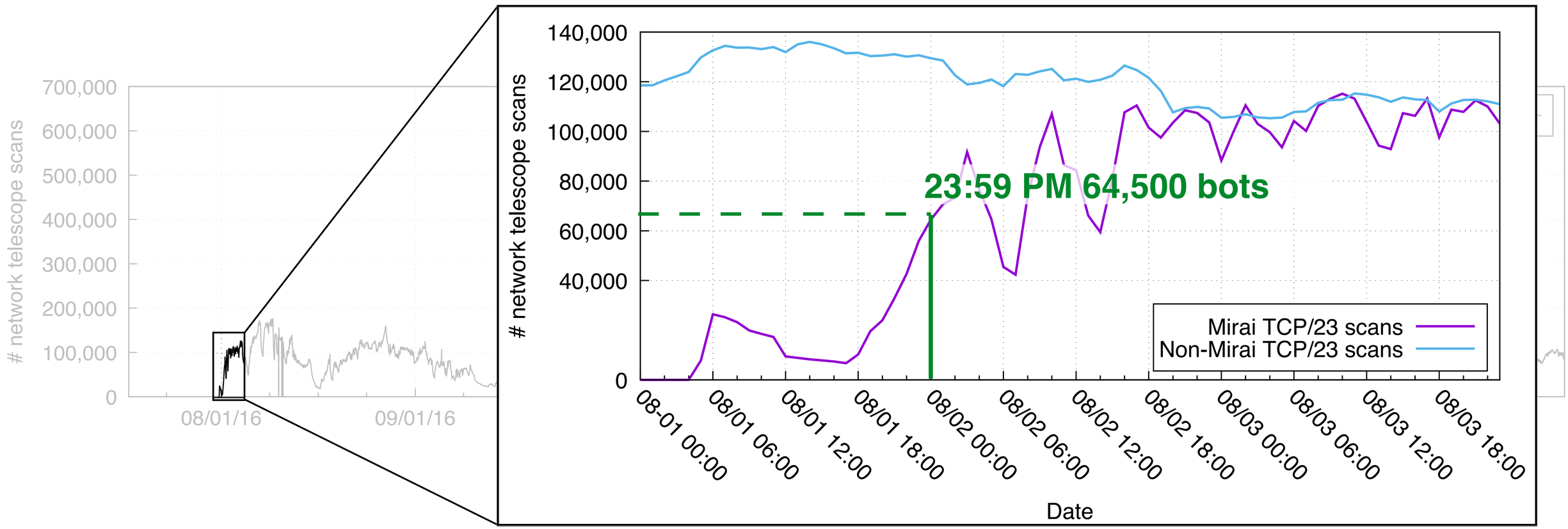
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
08/01/16
09/01/16
140,000
120,000
100,000
80,000
60,000
40,000
0
network telescope scans
1:42 AM Single Scanner
Mirai TCP/23 scans
Non-Mirai TCP/23 scans
08-01 00:00
08/01 06:00
08/01 12:00
08/01 18:00
08/02 00:00
08/02 06:00
08/02 12:00
08/02 18:00
08/03 00:00
08/03 06:00
08/03 12:00
08/03 18:00
Date

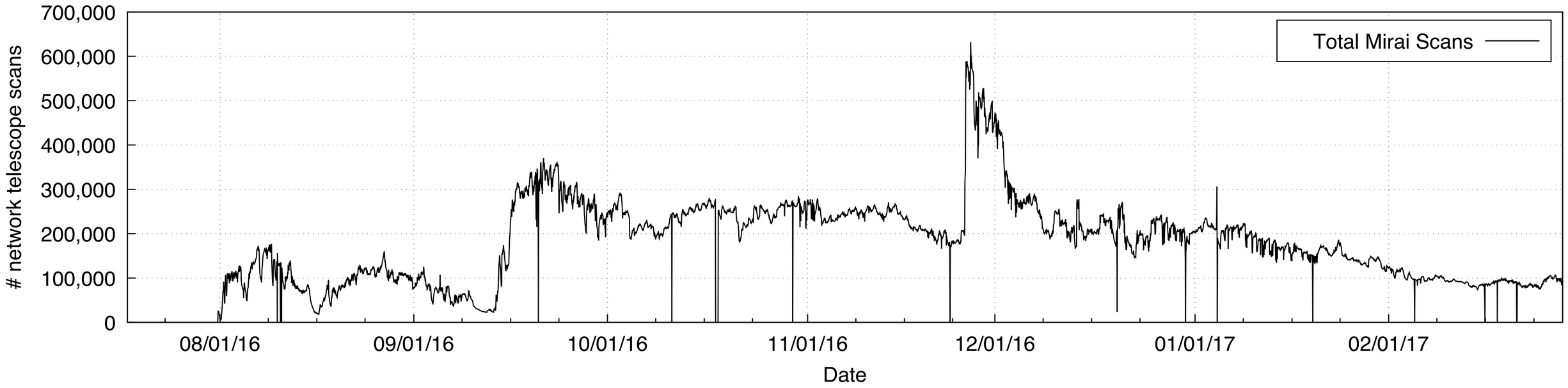
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
08/01/16
09/01/16
140,000
120,000
100,000
80,000
60,000
40,000
0
network telescope scans
3:59 AM Botnet Expands
Mirai TCP/23 scans
Non-Mirai TCP/23 scans
08-01 00:00
08/01 06:00
08/01 12:00
08/01 18:00
08/02 00:00
08/02 06:00
08/02 12:00
08/02 18:00
08/03 00:00
08/03 06:00
08/03 12:00
08/03 18:00
Date

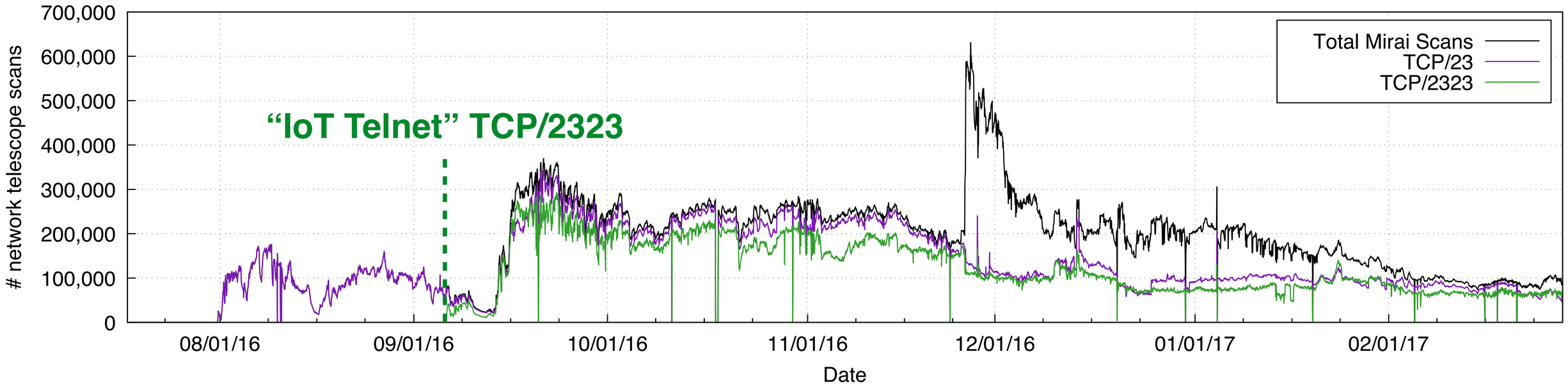
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
08/01/16
09/01/16
140,000
120,000
100,000
80,000
60,000
40,000
0
network telescope scans
23:59 PM 64,500 bots
Mirai TCP/23 scans
Non-Mirai TCP/23 scans
08-01 00:00
08/01 06:00
08/01 12:00
08/01 18:00
08/02 00:00
08/02 06:00
08/02 12:00
08/02 18:00
08/03 00:00
08/03 06:00
08/03 12:00
08/03 18:00
Date

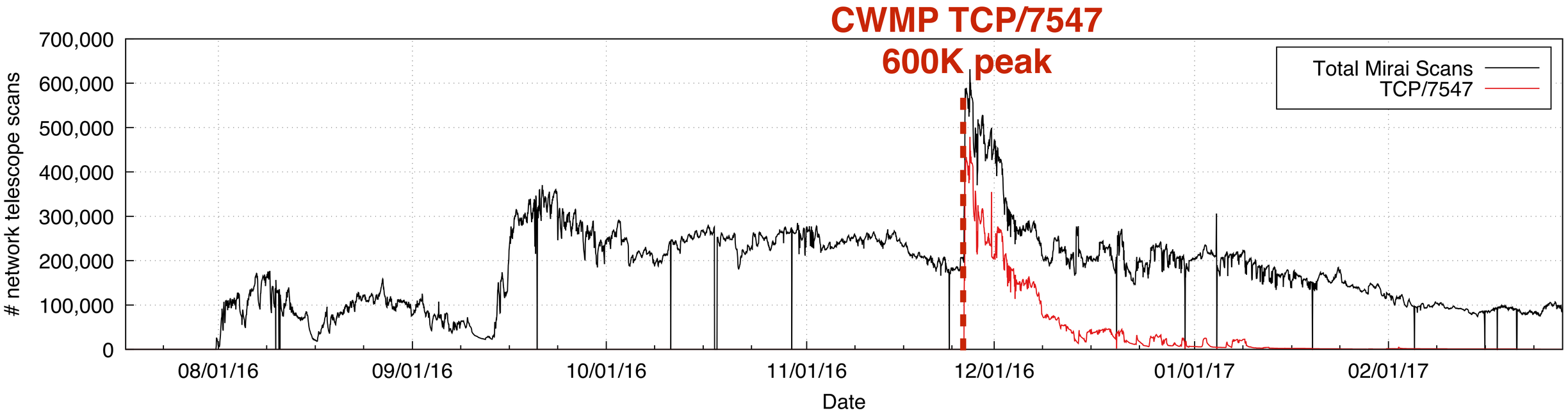
Population


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

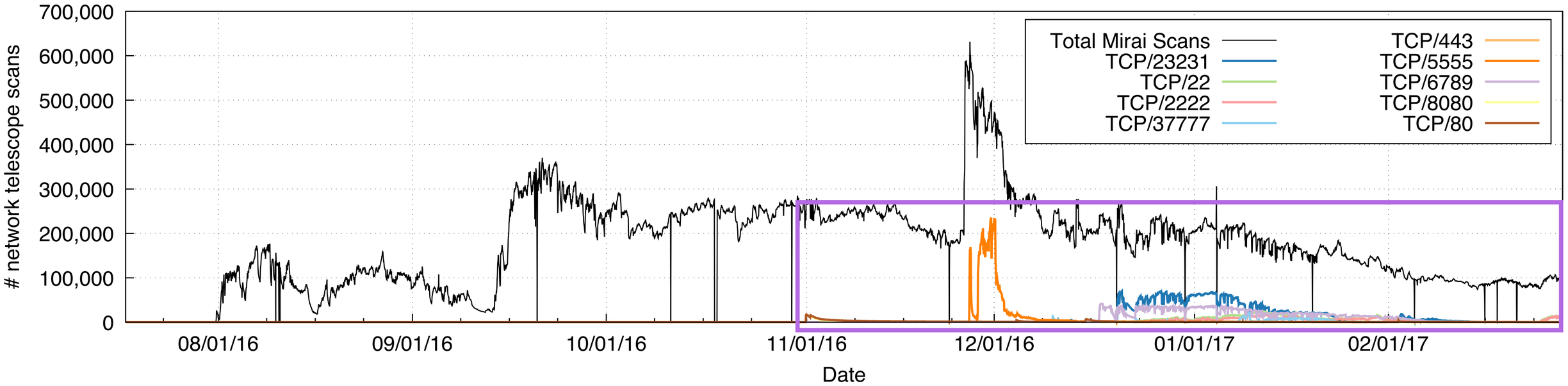
Population


700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
“IoT Telnet” TCP/2323
Total Mirai Scans
TCP/23
TCP/2323
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date

Population

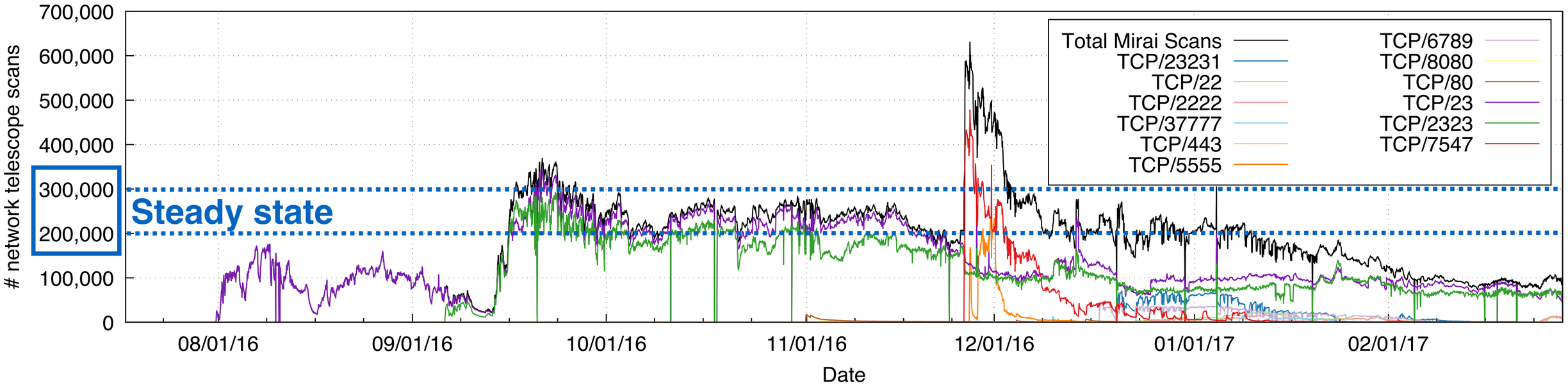

CWMP TCP/7547
600K peak
Total Mirai Scans
TCP/7547
network telescope scans
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date

Population



9 Additional Protocols

Population

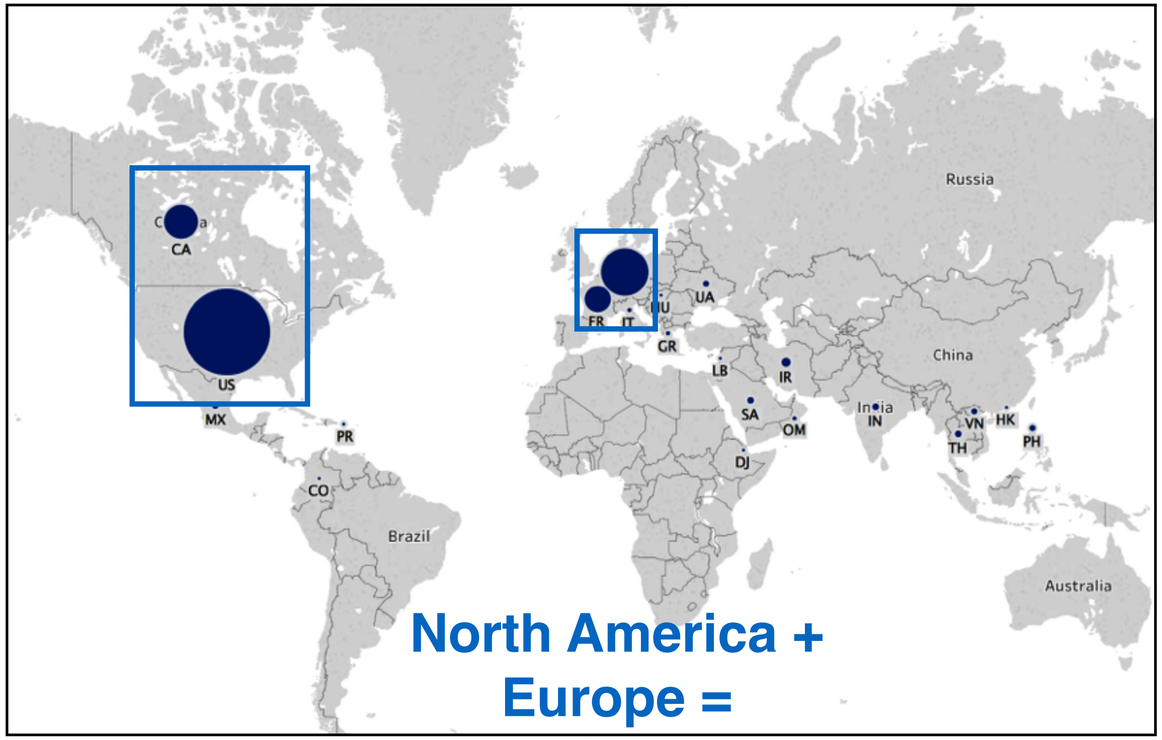

700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
network telescope scans
Steady state
08/01/16
09/01/16
10/01/16
11/01/16
12/01/16
01/01/17
02/01/17
Date
Total Mirai Scans
TCP/23231
TCP/22
TCP/2222
TCP/37777
TCP/443
TCP/5555
TCP/6789
TCP/8080
TCP/80
TCP/23
TCP/2323
TCP/7547

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

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

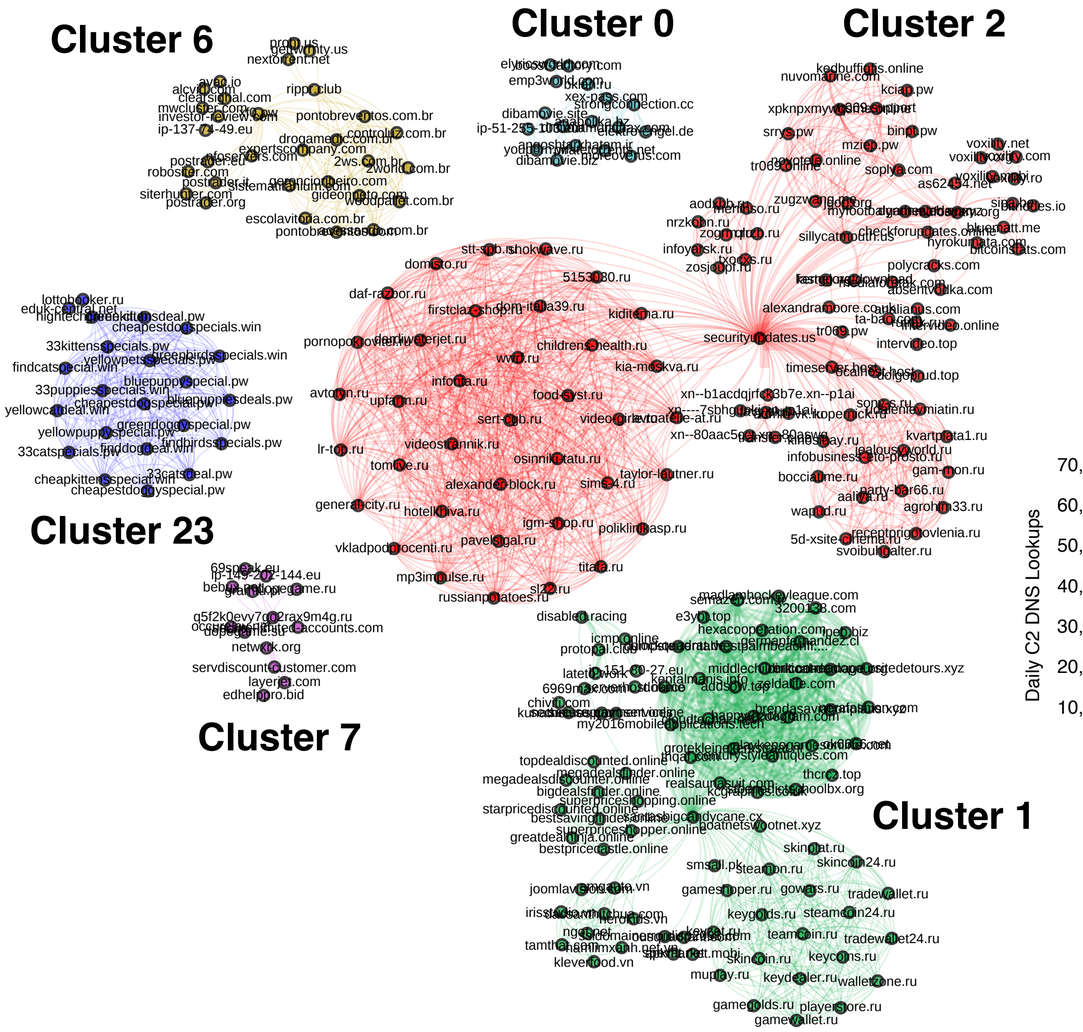
CWMP (28.30%)		Telnet (26.44%)		HTTPS (19.13%)		FTP (17.82%)		SSH (8.31%)	
Router	4.7%	Router	17.4%	Camera/DVR	36.8%	Router	49.5%	Router	4.0%
		Camera/DVR	9.4%	Router	6.3%	Storage	1.0%	Storage	0.2%
				Storage	0.2%	Camera/DVR	0.4%	Firewall	0.2%
				Firewall	0.1%	Media	0.1%	Security	0.1%
Other	0.0%	Other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

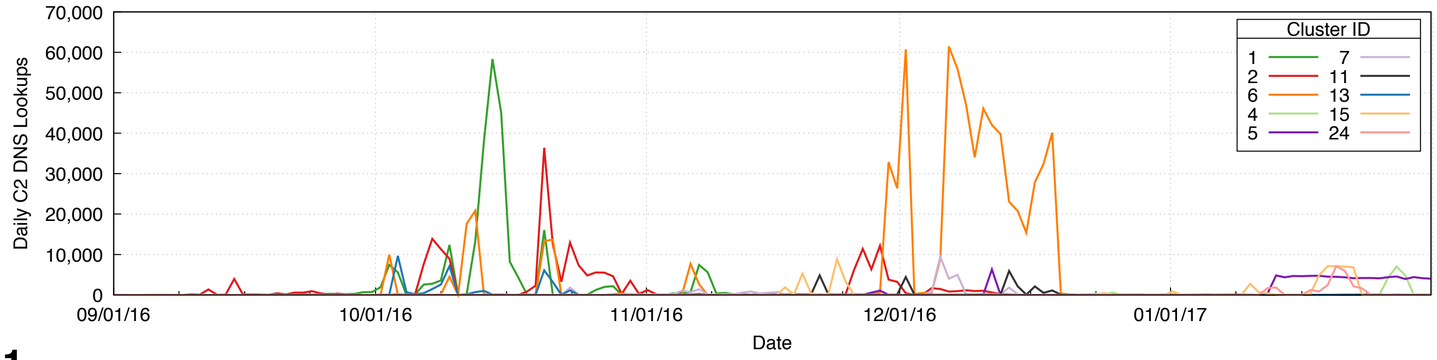
Roadmap

1. Growth & Composition
2. **Ownership & Evolution**
3. Attacks
4. Post-Mirai
5. Lessons Learned

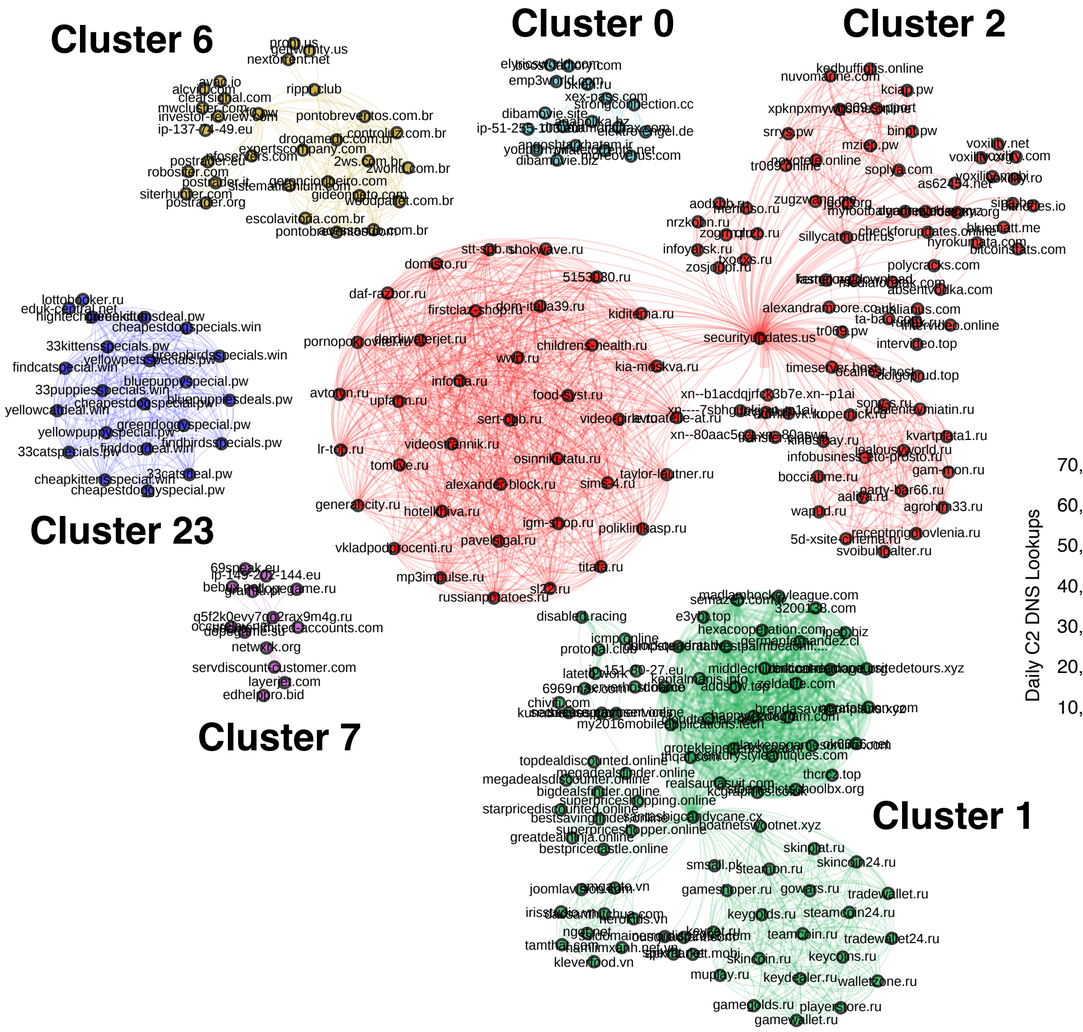
Ownership



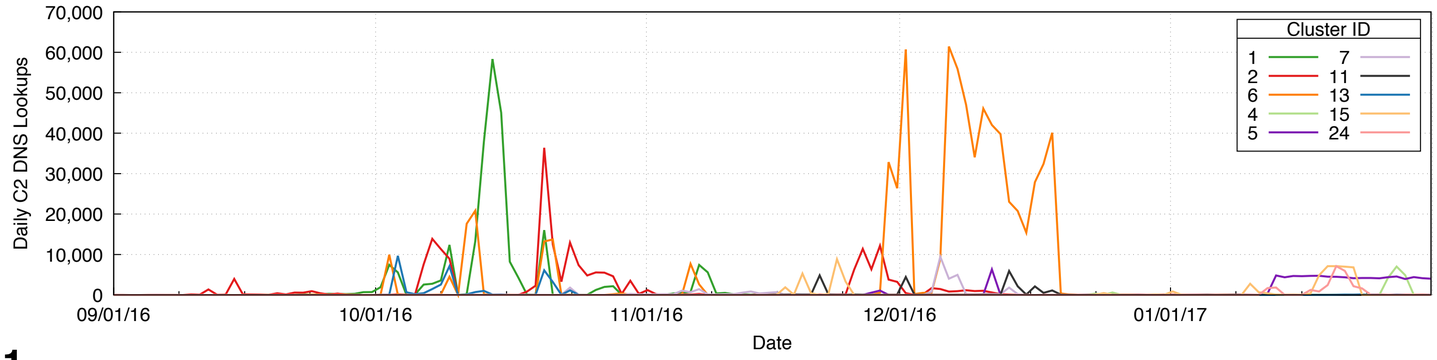
- Extract C2 domains from binaries
- Find coinciding C2s through active and passive DNS data



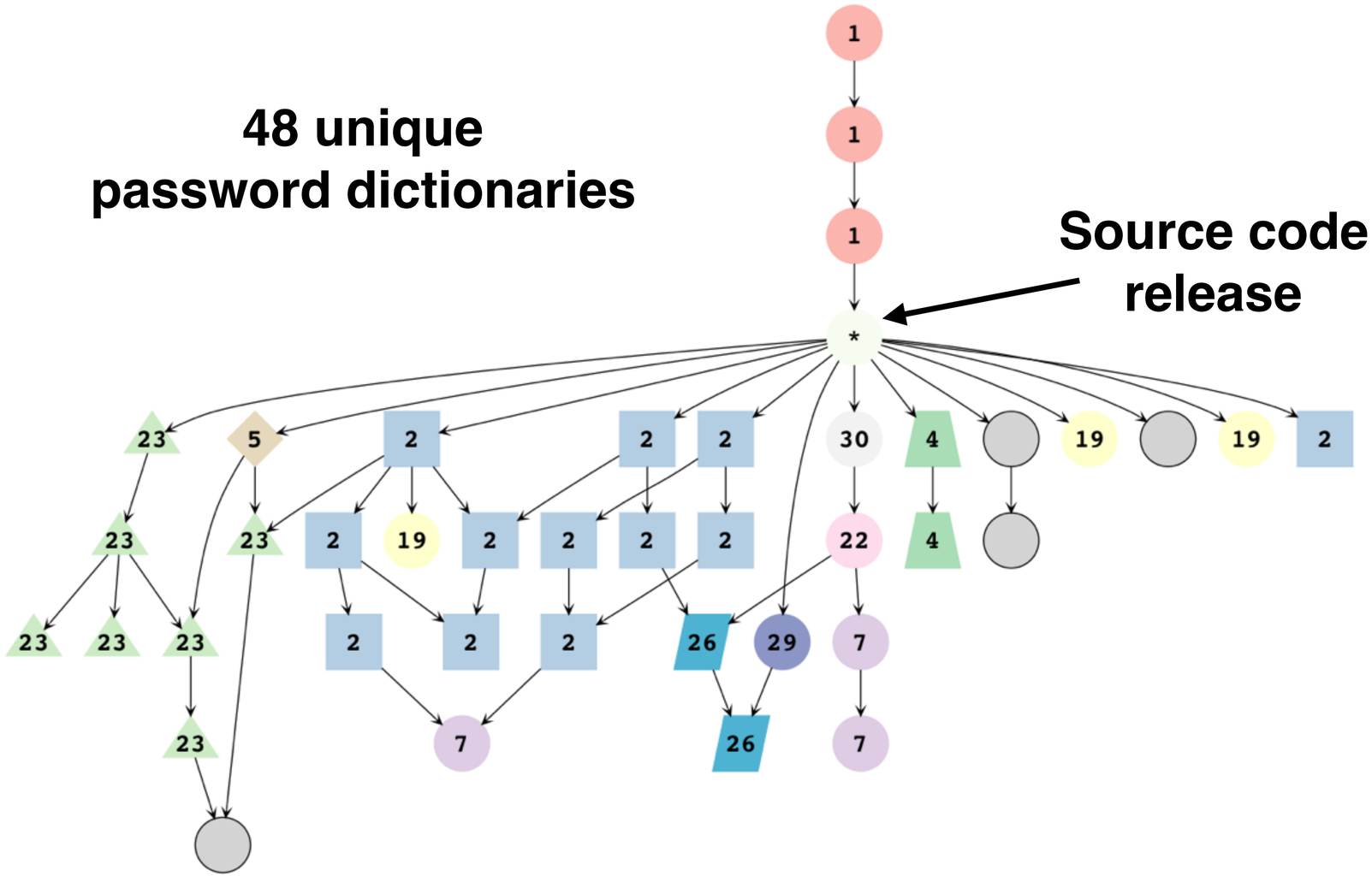
Ownership



Cluster	Notes
1	Original botnet, attacked Krebs, OVH
2	Scans CWMP, adds DGA
6	Attacked Dyn, gaming related sites



Evolution


48 unique
password dictionaries
Source code
release
1
1
1
*
23
5
2
2
2
30
4
19
19
2
23
23
2
19
2
2
2
2
22
4
23
23
23
2
2
2
26
29
7
23
7
26
7

Evolution

DGA

Packing

New protocols

Roadmap

1. Growth & Composition
2. Ownership & Evolution
3. **Attacks**
4. Post-Mirai
5. Lessons Learned

Attacks

Attack	Count	%	Class
HTTP	2,736	18.0%	Application
UDP-PLAIN	2,542	16.7%	Volumetric
UDP	2,440	16.1%	Volumetric
ACK	2,173	14.3%	TCP State
SYN	1,935	12.7%	TCP State
GRE-IP	994	6.5%	Application
ACK-STOMP	830	5.5%	TCP State
VSE	809	5.3%	Application
DNS	417	2.7%	Application
GRE-ETH	318	2.1%	Application

- Broad distribution across attack types, compared to Arbor report 65% volumetric, 18% TCP state, 18% app
- VSE = Valve Source Engine, popular game server
- Little reflection/amplification: 2.8% reflection attacks, compared to 74% for booters

Attacks

Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.

Attacks

Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.

Attacks

Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.

Attacks

Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.

Attacks

Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.

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	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

Roadmap

1. Growth & Composition
2. Ownership & Evolution
3. Attacks
4. **Post-Mirai**
5. Lessons Learned

Post-Mirai

1. “Reaper” - vendor specific RCEs, 10-20K infections [1]
   - integrated LUA execution environment, 100+ DNS open resolvers
2. “Satori” - Huawei HG532 routers vulnerable to SOAP exploits [2]
   - 100K infections
3. “Okiru” - ARC processors [3]
4. “Masuta” - Home Network Administration Protocol [4]

[1] https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/
[2] https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/
[3] http://securityaffairs.co/wordpress/67742/malware/mirai-okiru-botnet.html
[4] https://threatpost.com/satori-author-linked-to-new-mirai-variant-masuta/129640/

Roadmap

1. Growth & Composition
2. Ownership & Evolution
3. Attacks
4. Post-Mirai
5. **Lessons Learned**

New Dog, Old Tricks

1. **Security Hardening**
2. Automatic Updates
3. Device Attribution
4. Defragmentation
5. End-of-life

- Enforce strong passwords
- Default open —> default closed ports
- Limit network access
- ASLR, isolation boundaries, least privilege

New Dog, Old Tricks

1. Security Hardening
2. **Automatic Updates**
3. Device Attribution
4. Defragmentation
5. End-of-life

- Established practice in desktop and mobile OSes
- Requires cryptographic capabilities and infrastructure
- Active policing: bug bounties have proven to be effective
- Deutsche Telekom case study is encouraging

New Dog, Old Tricks

1. Security Hardening
2. Automatic Updates
3. **Device Attribution**
4. Defragmentation
5. End-of-life

- Required for attack diagnosis, notification, and response
- Need a standardized mechanism for identifying model/firmware
- Perhaps MAC address encoding?

New Dog, Old Tricks

1. Security Hardening
2. Automatic Updates
3. Device Attribution
4. **Defragmentation**
5. End-of-life

- Found many implementations of different protocols: FTP/HTTP/telnet
- New implementations yield old bugs
- Some convergence towards Android Thing, RIOT OS, Tock, Windows for IoT

New Dog, Old Tricks

1. Security Hardening
2. Automatic Updates
3. Device Attribution
4. Defragmentation
5. **End-of-life**

- Huge volume of IoT devices / manufacturers
- What happens when companies dissolve? Or devices become outdated?

Aftermath

- Arrest of perpetrators
  - Mirai authors / Deutsche Telekom attackers / vDOS “attack for hire” company

Aftermath

- Arrest of perpetrators
  - Mirai authors / Deutsche Telekom attackers / vDOS “attack for hire” company
- Limited actions regarding manufacturers
  - FTC complaint against D-Link

Aftermath

- Arrest of perpetrators
  - Mirai authors / Deutsche Telekom attackers / vDOS “attack for hire” company
- Limited actions regarding manufacturers
  - FTC complaint against D-Link
- Need to facilitate / incentivize white hats
  - Internet of Things (IoT) Cybersecurity Improvement Act of 2017
  - Bounty programs

Understanding the Mirai Botnet

1. Growth & Composition
2. Ownership & Evolution
3. Attacks
4. Post-Mirai
5. Lessons Learned
6. **Questions? zanema2@illinois.edu**