Understanding the Mirai Botnet - USENIX '17

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*

Presented by - Deepak Gouda
30 Aug, 2023

Mirai

DDoS attack that disrupted internet was largest of its kind in history, experts say

The Botnet That Broke the Internet Isn't Going Away

It's going to take years to move past Mirai, the botnet that's causing havoc online.

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/
Zane Ma, USENIX 2017

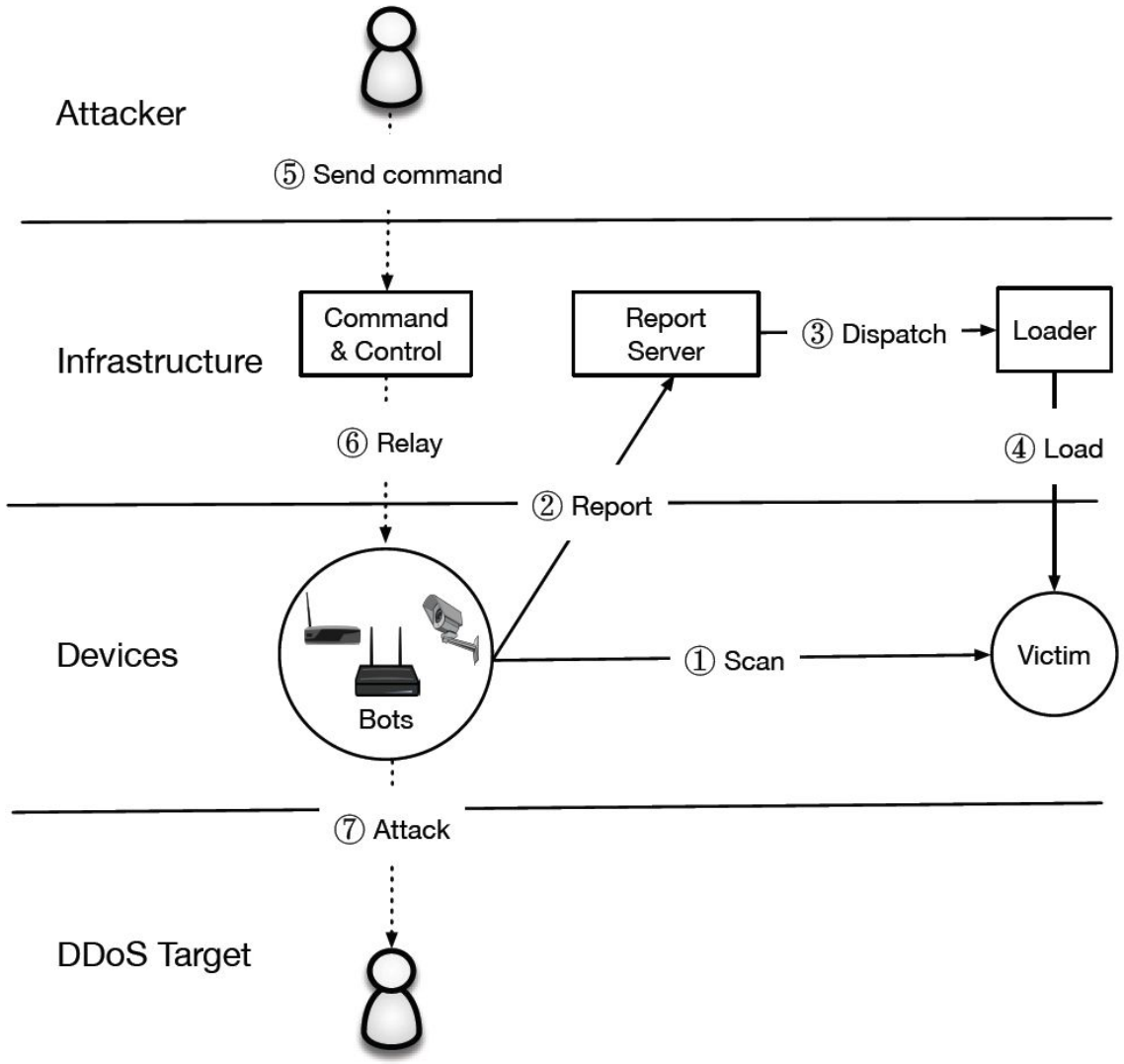
Georgia Tech

Goals

- Architecture, Growth and Evolution
- Mechanism
- Motive
- How to secure IoT ecosystem

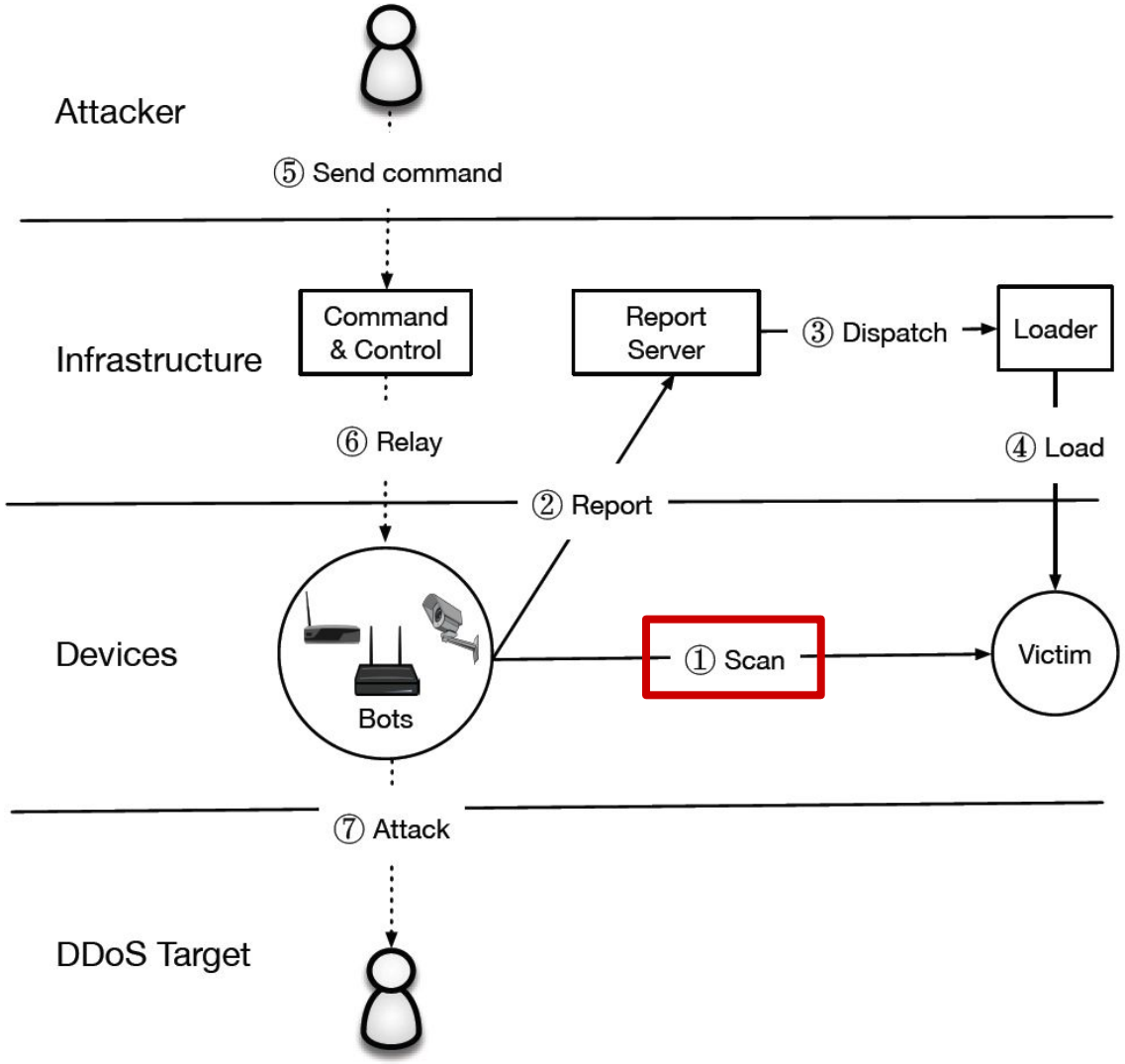
How Mirai worked?

Architecture



Georgia Tech

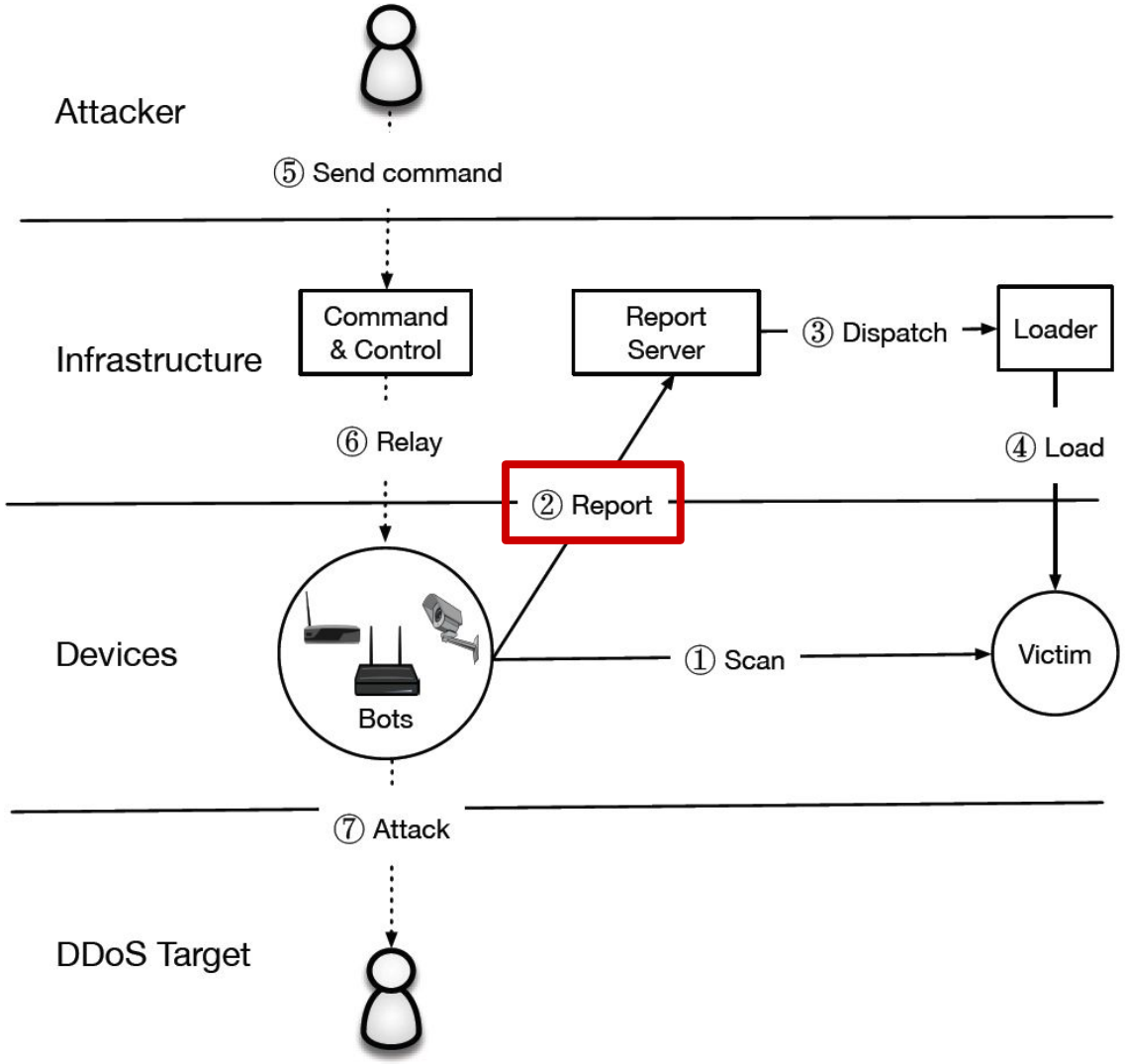
Architecture



Rapid Scanning Phase

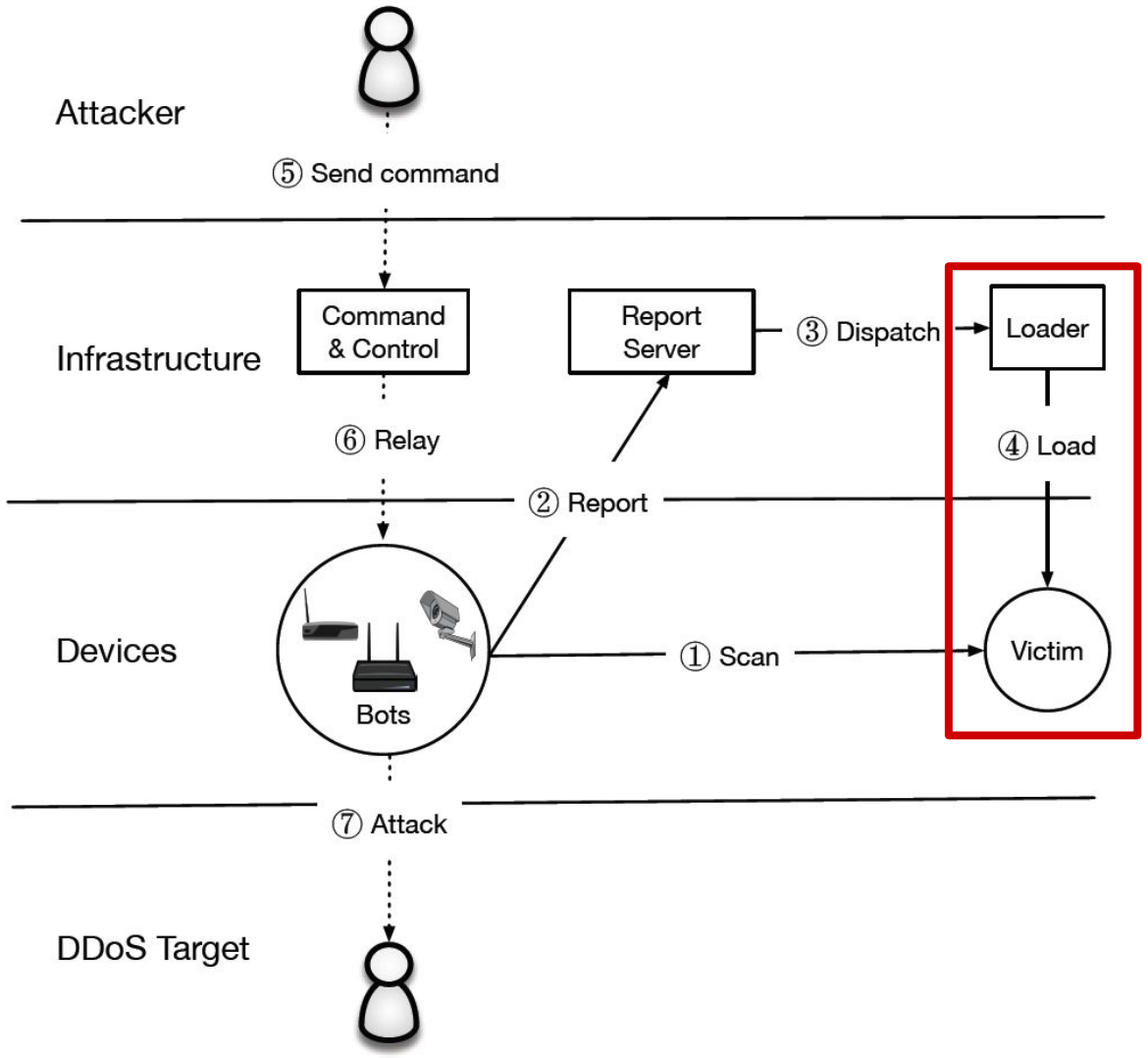
Georgia Tech

Architecture



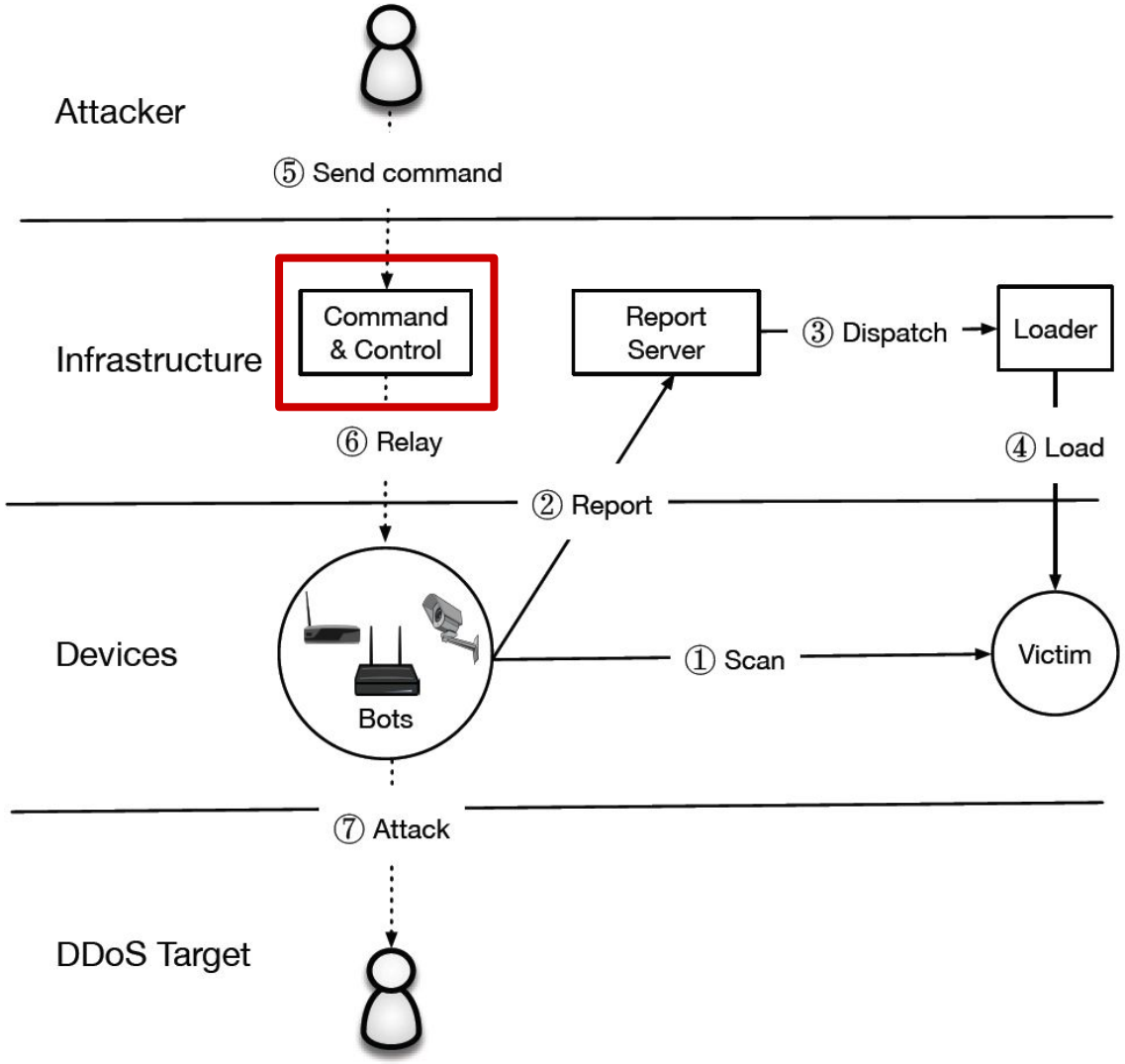
Georgia Tech

Architecture



Delete binary and obfuscate process name

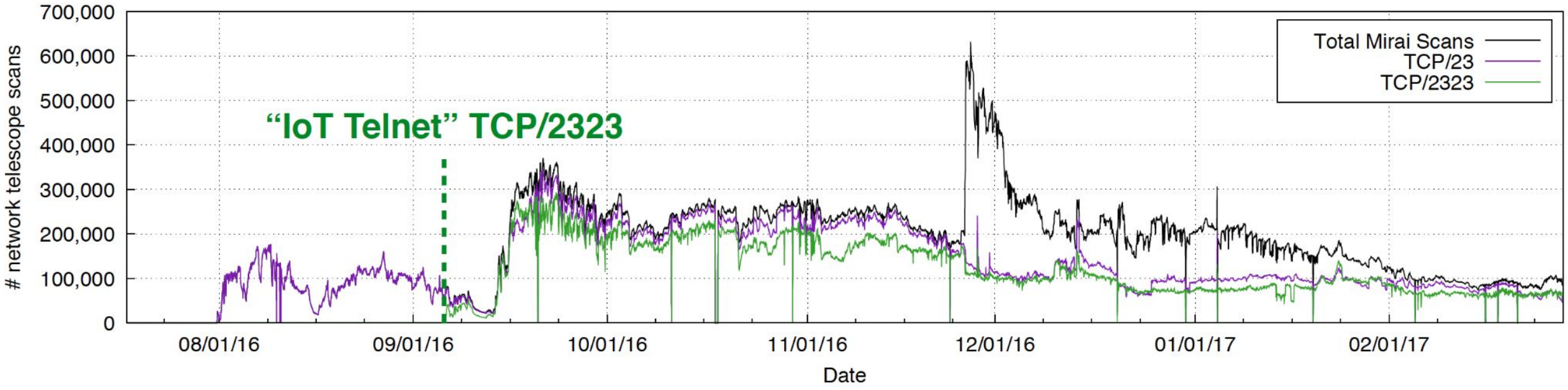
Architecture



Scan new victims and listen to C2

Georgia Tech

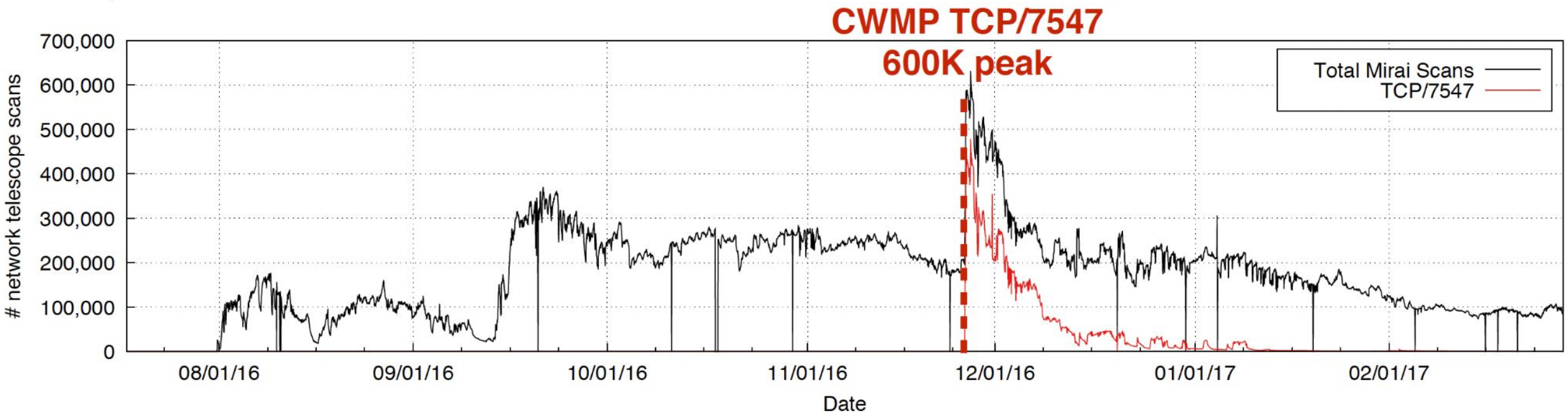
Timeline



Georgia Tech

Timeline

Different variants!



Georgia Tech

Geographic Distribution

Georgia Tech

Data Sources

	Data Source	Size	
Merit Network	Network Telescope	4.7M unused IPs	Scan attempts
Censys	Active Scanning	136 IPv4 scans	Device fingerprinting
Self + Akamai	Telnet Honeypots	434 binaries	Malware
VirusTotal	Malware Repository	594 binaries	Malware
US ISP + Thales	Active/Passive DNS	499M daily RRs	C2 infrastructure
Akamai	C2 Milkers	64K issued attacks	C2 commands
	Krebs DDoS Attack	170K attacker IPs	
	Dyn DDoS Attack	108K attacker IPS	

July 2016 - February 2017

Device Composition

Inferred using :

- Password dictionary
- Device fingerprints

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%

Evolution of the Bot

- IP-based C2 to Domain-based C2
- Deletion of binary + process obfuscation
- Growth of password dictionary - targeting more devices
- Close scan ports + kill competing malware
- Releasing source code
- Hardened binaries
- Application level attacks + other protocols

Questions

- Why didn’t the variants increase the dictionary size?

Questions

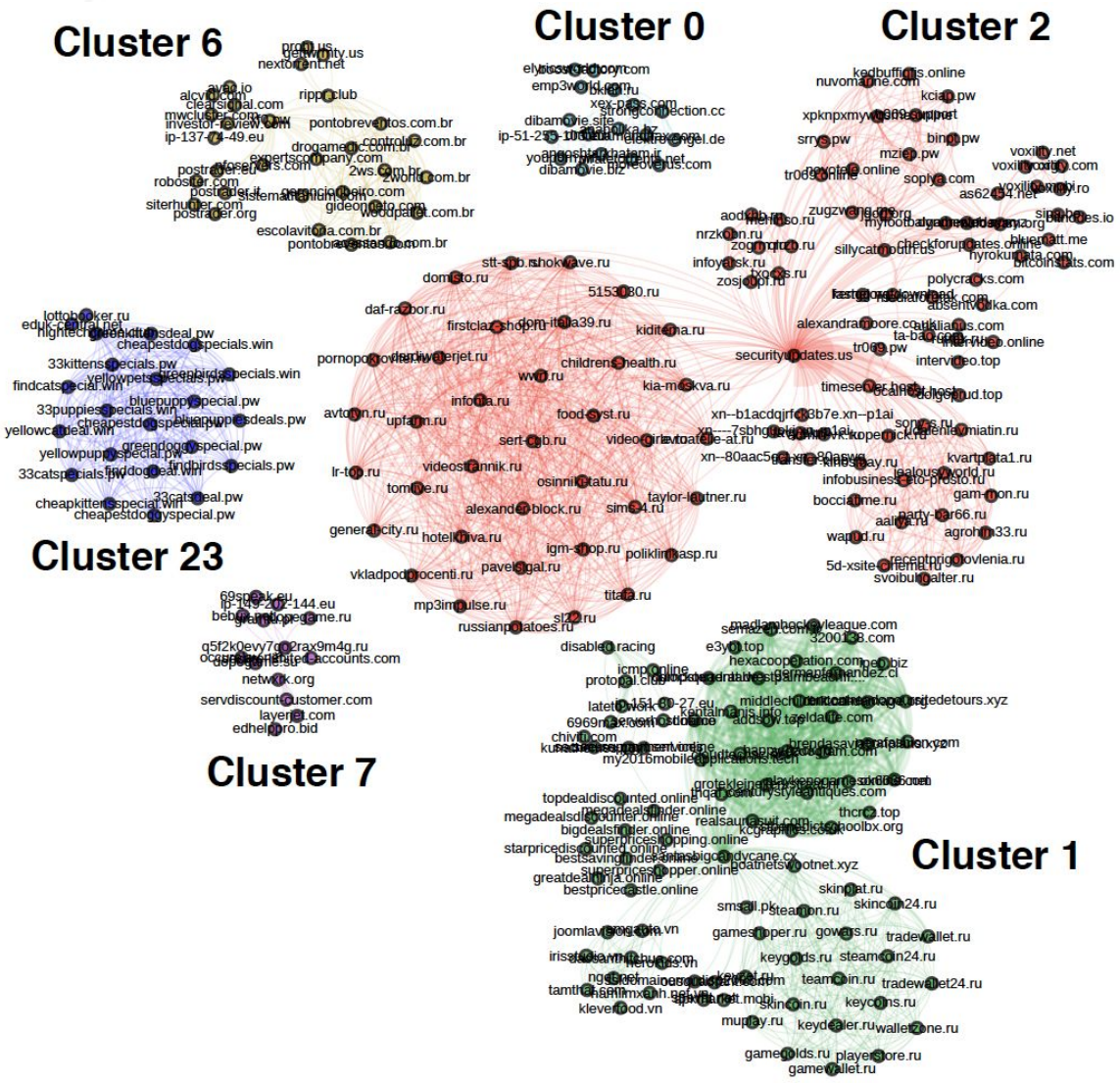
- Why didn’t the variants increase the dictionary size?
- Why did Mirai shut down scan ports?

Questions

- Why didn’t the variants increase the dictionary size?
- Why did Mirai shut down scan ports?
- Why it doesn’t care for persistence?

Who ran Mirai?

C2 Infrastructure



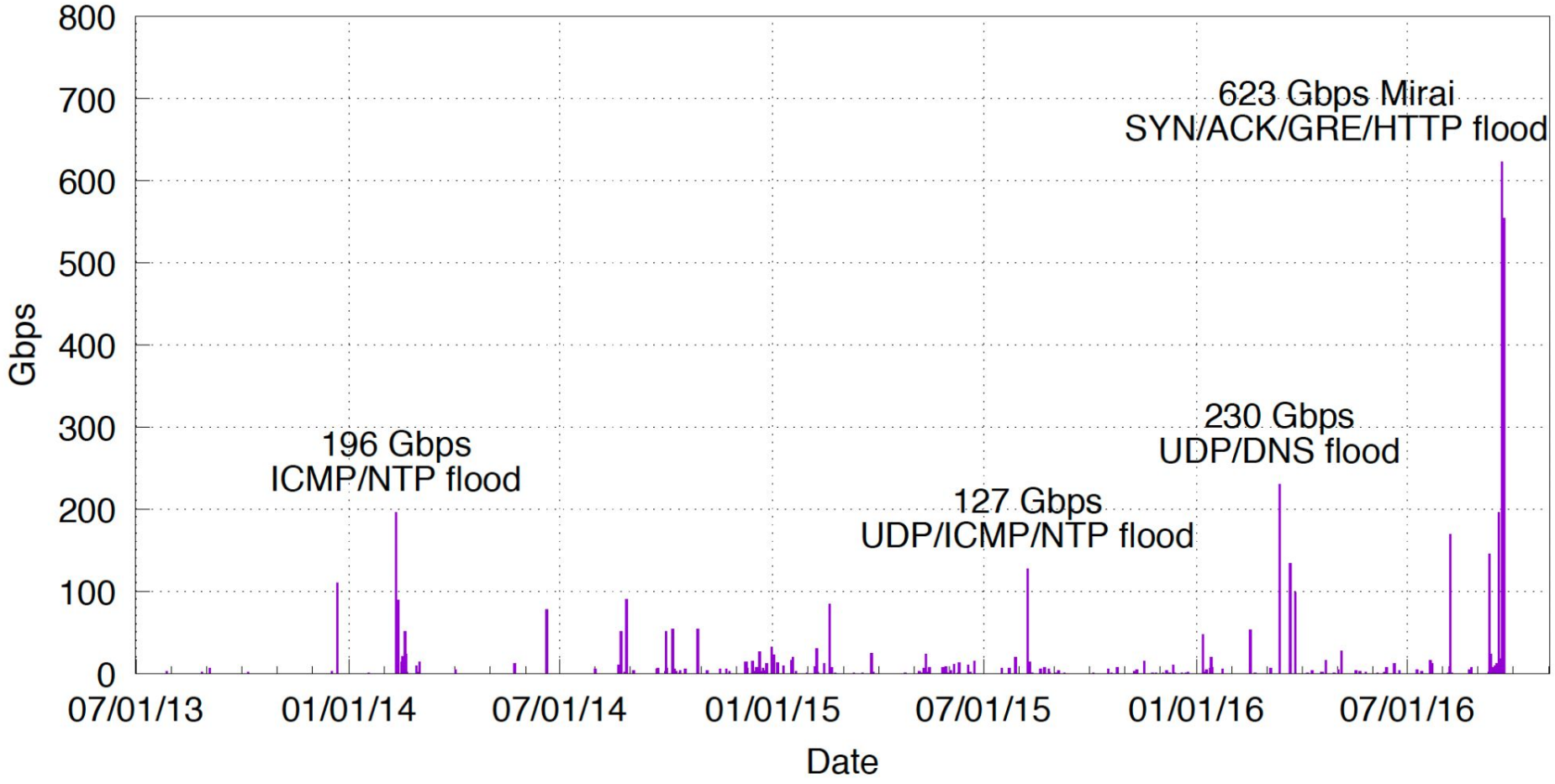
- Extract C2 domains
- DNS expansion
- Cluster by shared DNS infrastructure

Cluster	Notes
Cluster 1	Original, Krebs attack
Cluster 2	Complex, CWMP scan
Cluster 6	Largest, Dyn attack

Georgia Tech

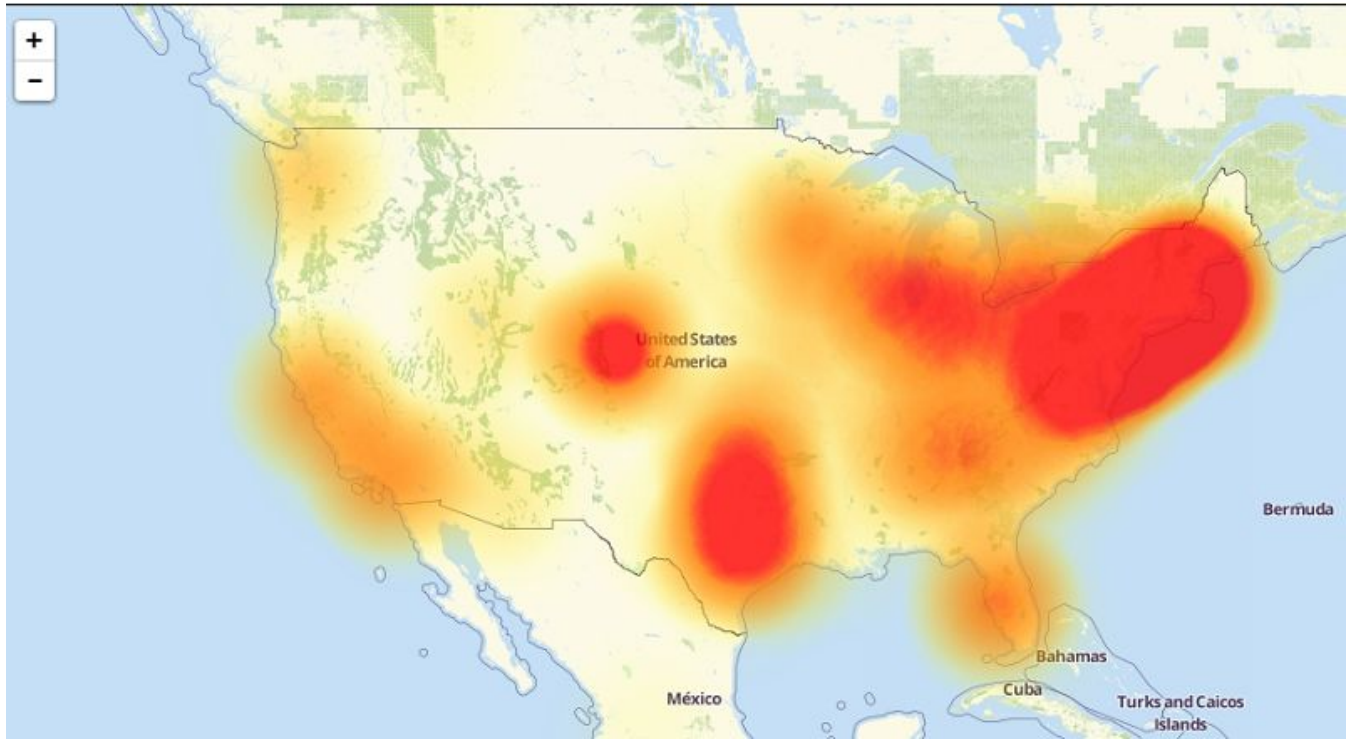
How was Mirai used?

Largest DDoS Attack (by 2017)



Georgia Tech

Dyn Attack



reddit amazon web services NETFLIX Spotify

twitter GitHub PayPal

Georgia Tech

Dyn Attack

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**

IP list obtained
from C2 Milkers

DDoS-as-a-Service

Games: Minecraft, Runescape, game commerce sites

Politics: Chinese political dissidents

Telecom: Lonestar Cell

Misc: Individual sites (93.7%)!

Other C2s!

Countries

US: 50.3%

France: 6.6%

UK: 6.1%

Discussion

Discussion

Securing a fragmented ecosystem of heterogeneous devices with low bandwidth and less frequent updates is difficult

Recommendations :

- Ports - default closed
- Limit remote address access to devices
- Compliance and certifications for security practices
- Bug-bounties for vulnerability disclosure and patches
- Manual alerts and announcements

Questions?