Demystifying the Mirai Botnet

Zakir Durumeric
Stanford University / Censys

Stanford | ENGINEERING
Computer Science

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

twitter

amazon web services™

PayPal

NETFLIX

SOUNDCLOUD

Spotify

GitHub

reddit

New York Times

“SpainSquad, Anonymous, and New World Hackers claimed responsibility for the attack in retaliation for Ecuador's rescinding Internet access to WikiLeaks founder Julian Assange.”

“Dyn said it has not yet attributed the attack to any group or country, and that the DDoS traffic has been coming from tens of millions of discrete IP addresses around the globe.”

gathering. It's not normal for companies to do that. Furthermore, the size and scale of these probes—and especially their persistence—points to state actors. It feels like a nation's military cybercommand trying to calibrate its weaponry in the case of cyberwar. It reminds me of the

Dyn

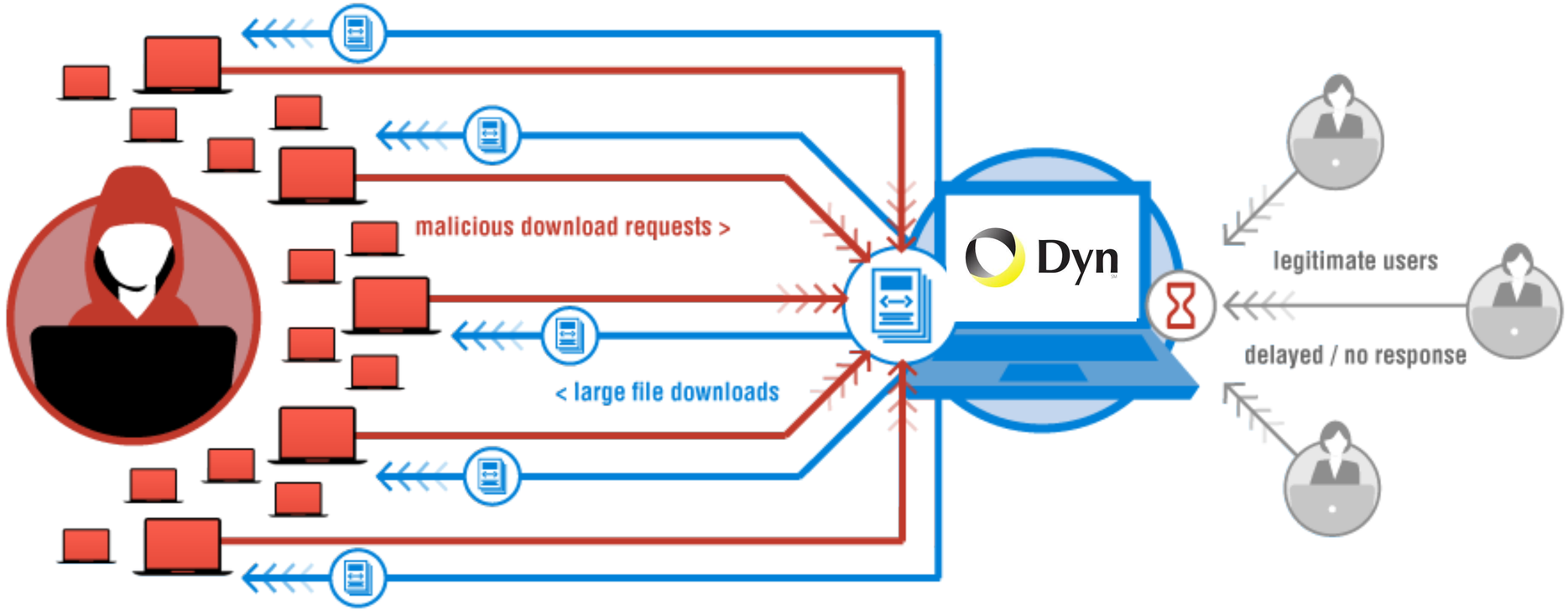
SM

What is the IP address for netflix.com?

52.204.167.205, 52.206.23.236, 52.206.122.138, …

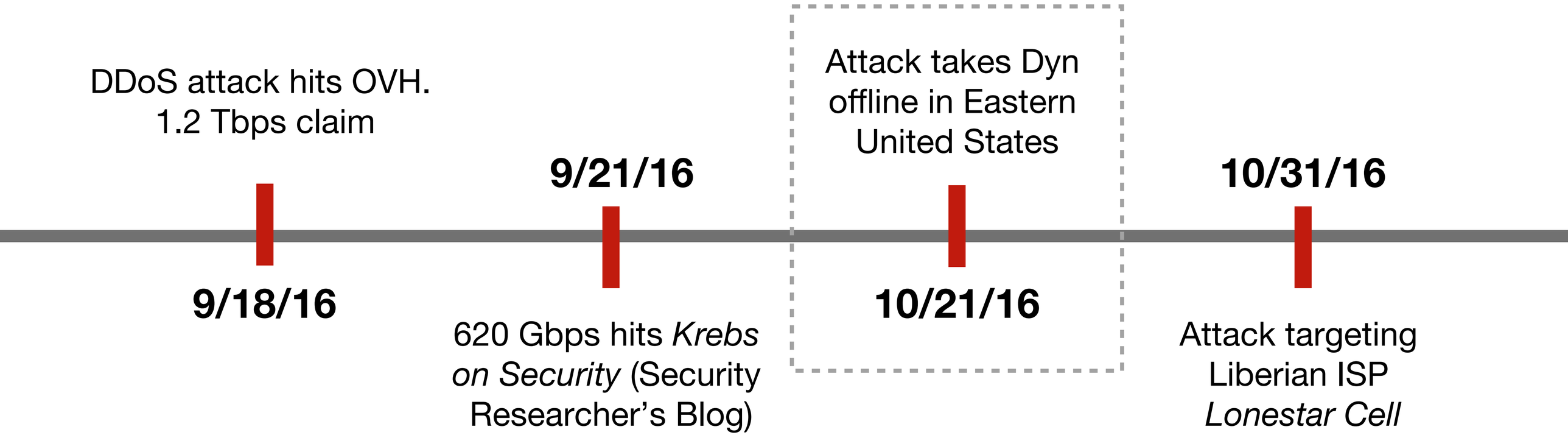
HTTPS Request

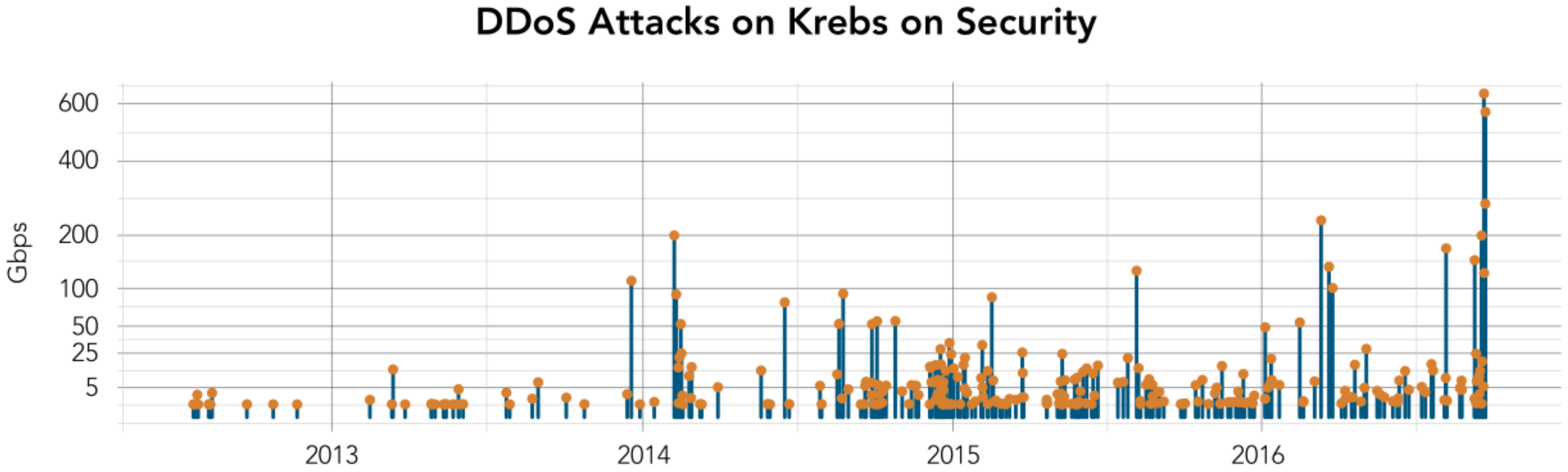
NETFLIX



> “We are still working on analyzing the data but the estimate at the time of this report is up to 100,000 malicious endpoints. […] There have been some reports of a magnitude in the 1.2 Tbps range; at this time we are unable to verify that claim.”

Image: Verisign

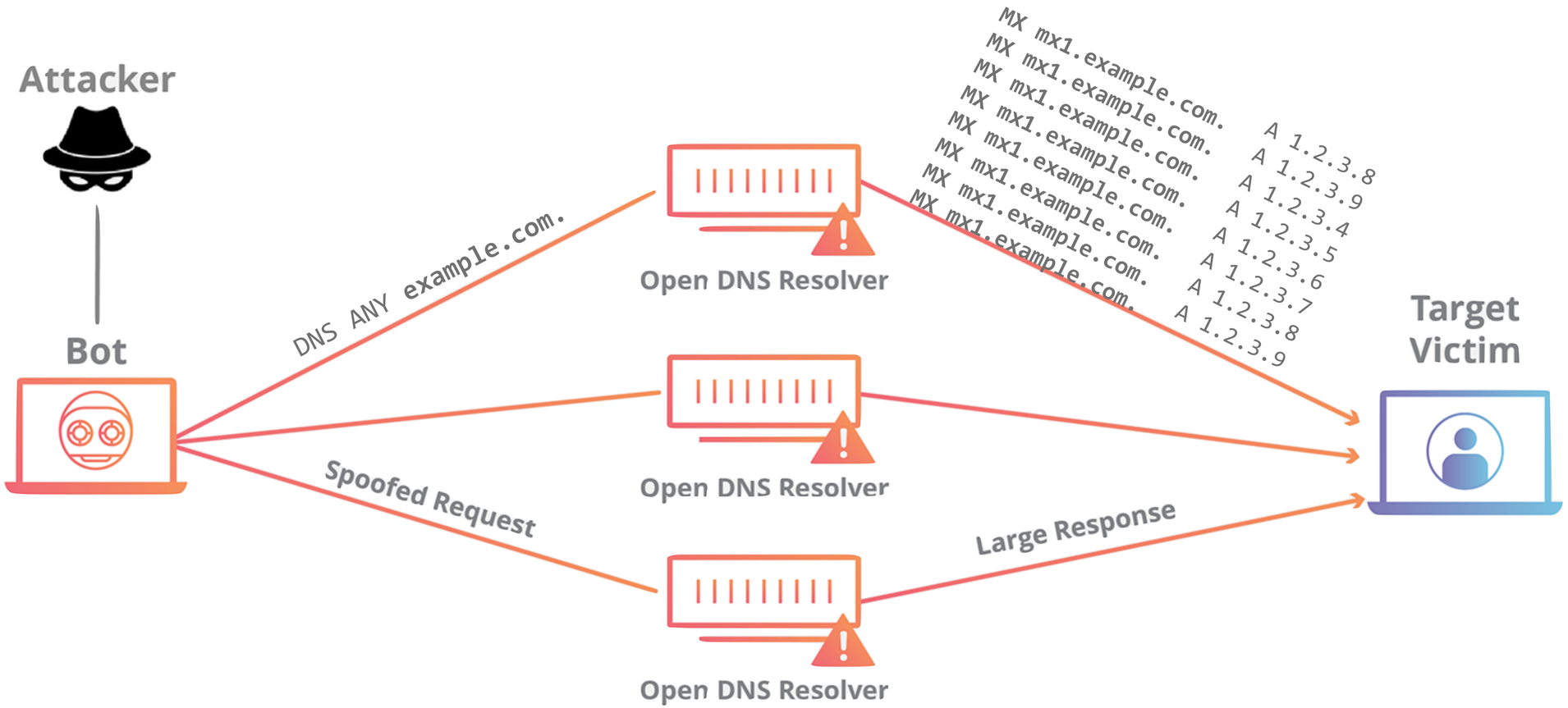

DDoS attack hits OVH.
1.2 Tbps claim
9/18/16
9/21/16
620 Gbps hits *Krebs on Security* (Security Researcher's Blog)
Attack takes Dyn offline in Eastern United States
10/21/16
10/31/16
Attack targeting Liberian ISP *Lonestar Cell*



> “The magnitude of the attacks seen during the final week were significantly larger than the majority of attacks Akamai sees on a regular basis. […] In fact, while the attack on September 20 was the largest attack ever mitigated by Akamai, the attack on September 22 would have qualified for the record at any other time, peaking at 555 Gbps.”

Source: 2017 Akamai State of the Internet

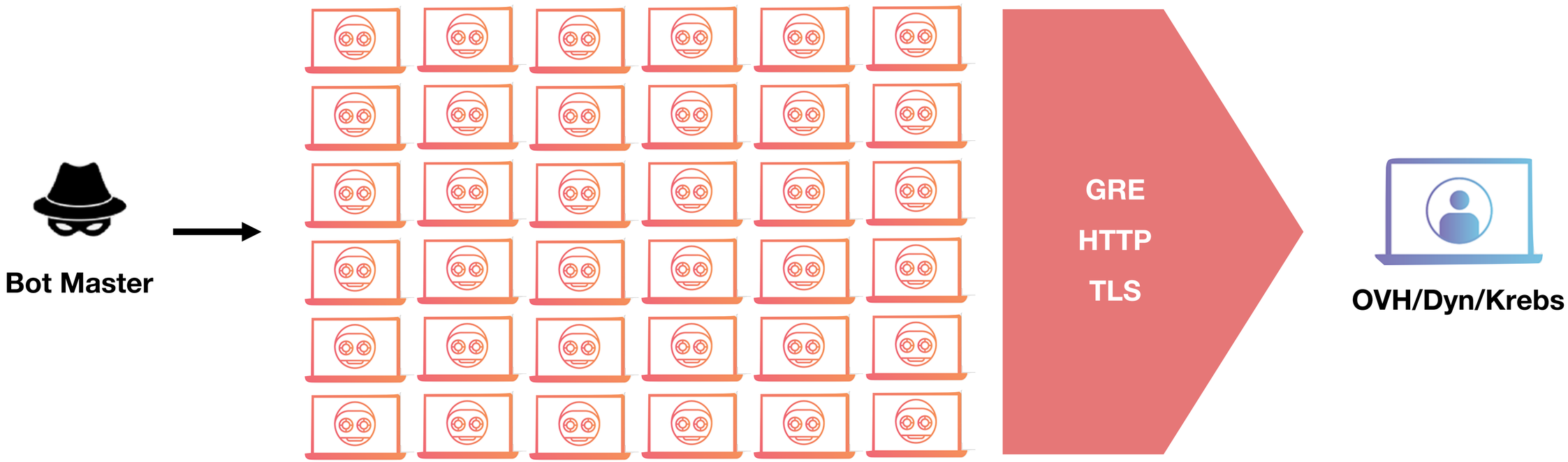
Typical Attack: DDoS Amplification



60-70x Increase in Size

Image: Cloudflare

New Attack Shape



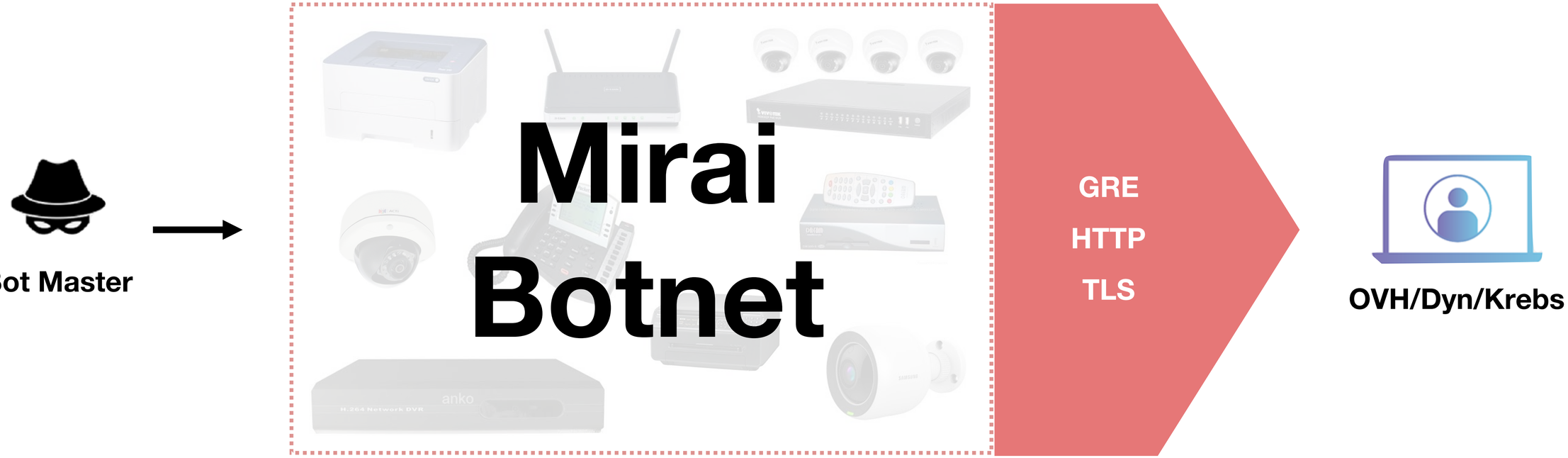
≈ 200K Hosts

A Botnet of IoT Devices

≈ ~~200K Hosts~~

200K IoT devices

The Mirai Botnet of IoT Devices

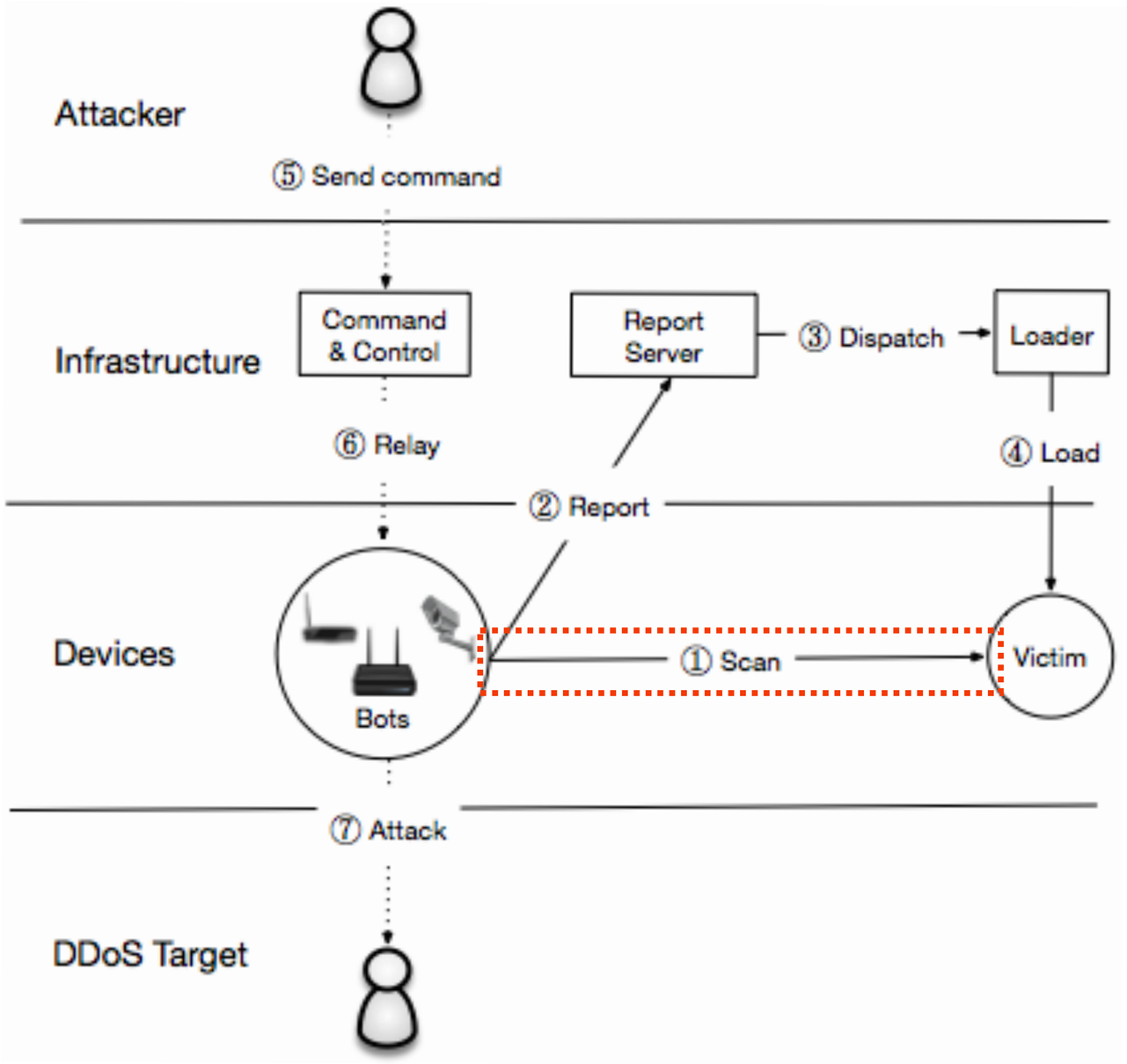


≈ ~~200K Hosts~~

200K IoT devices

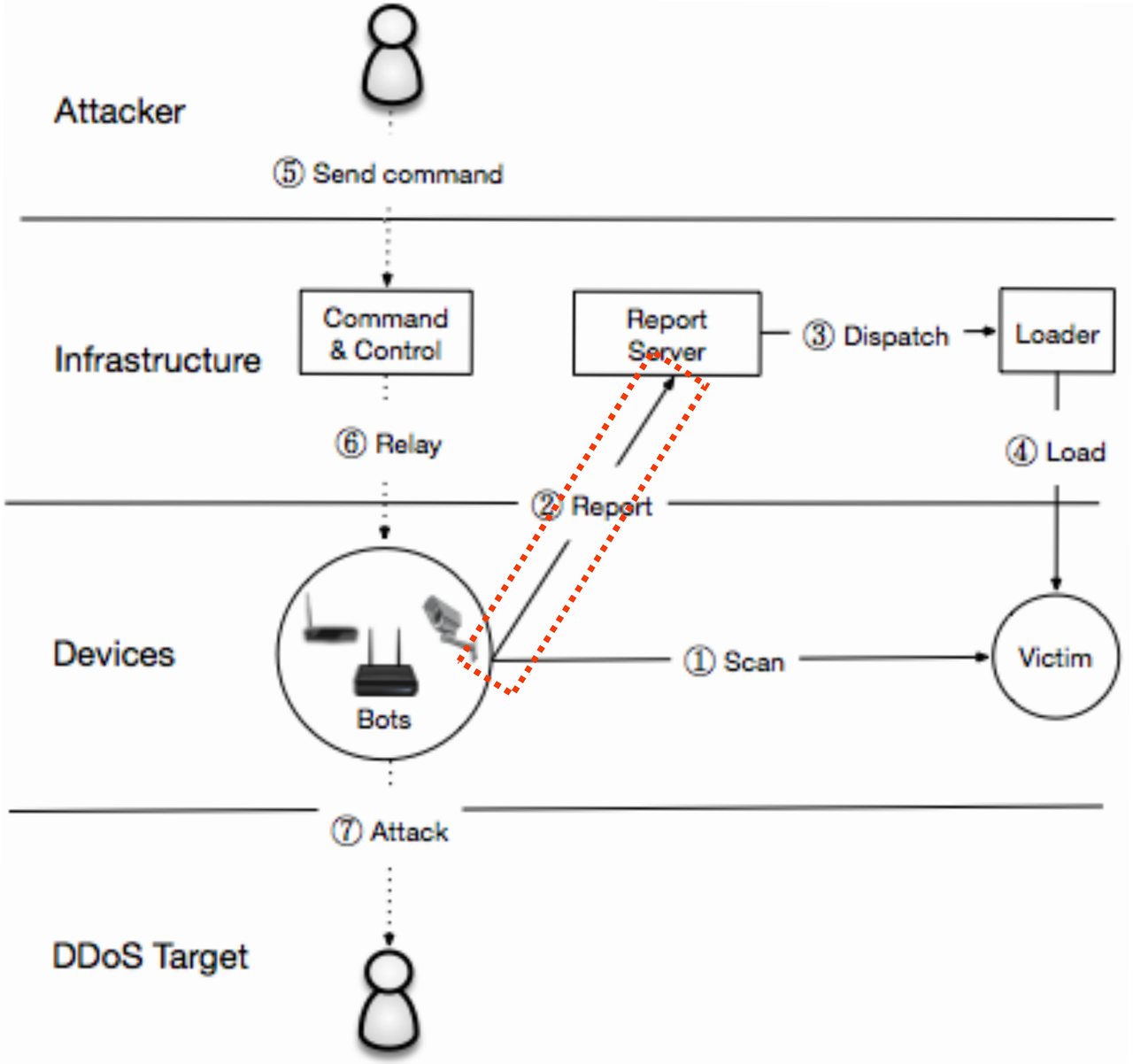
The Mirai Malware

1. Bots statelessly scan for victims on TCP/23 and TCP/2323. They attempt to login over telnet with a set of hardcoded credentials



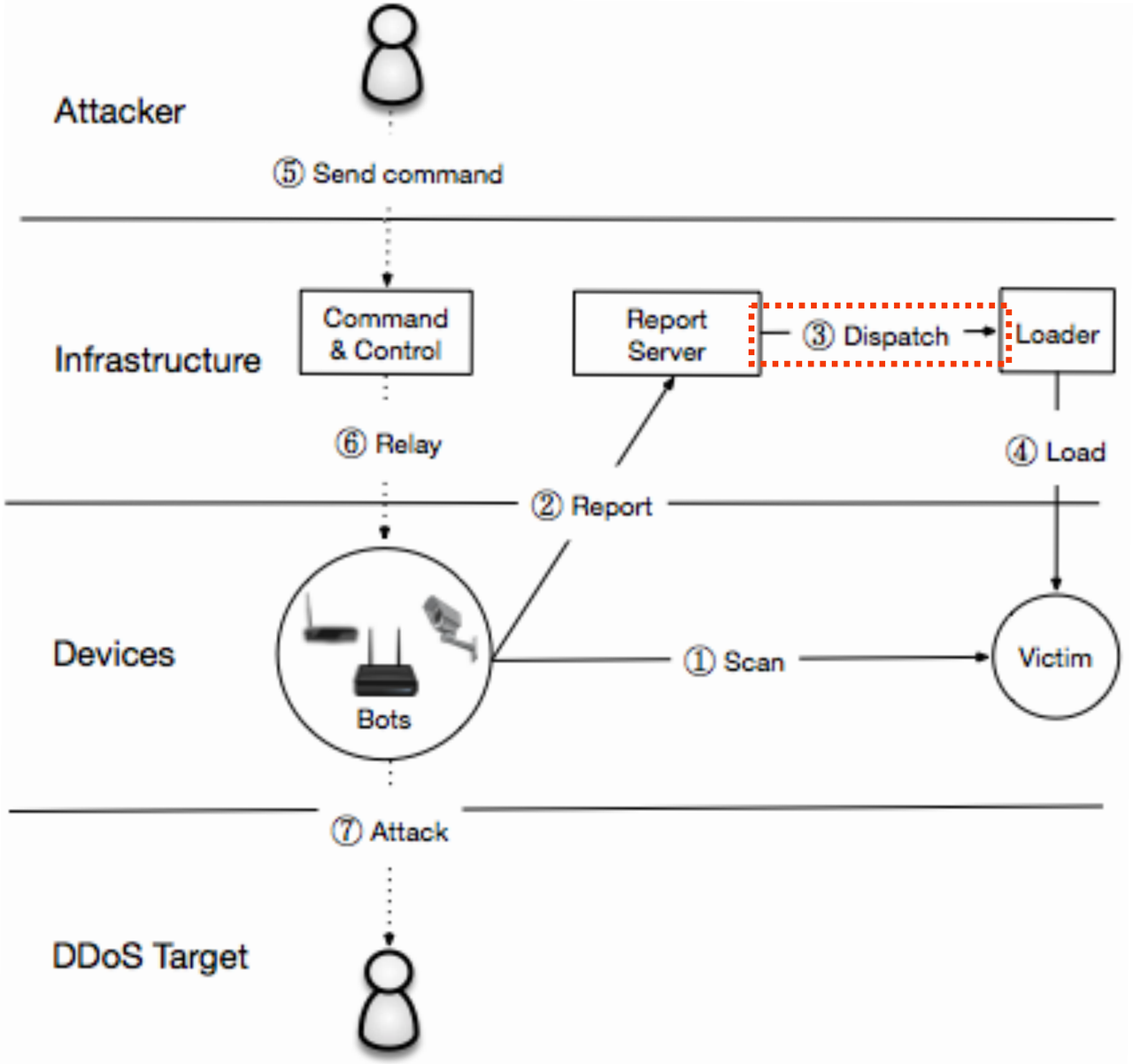
The Mirai Malware

1. Bots statelessly scan for victims on TCP/23 and TCP/2323. They attempt to login over telnet with a set of hardcoded credentials
2. **Scanner** reports details about vulnerable host to central **C2 server**



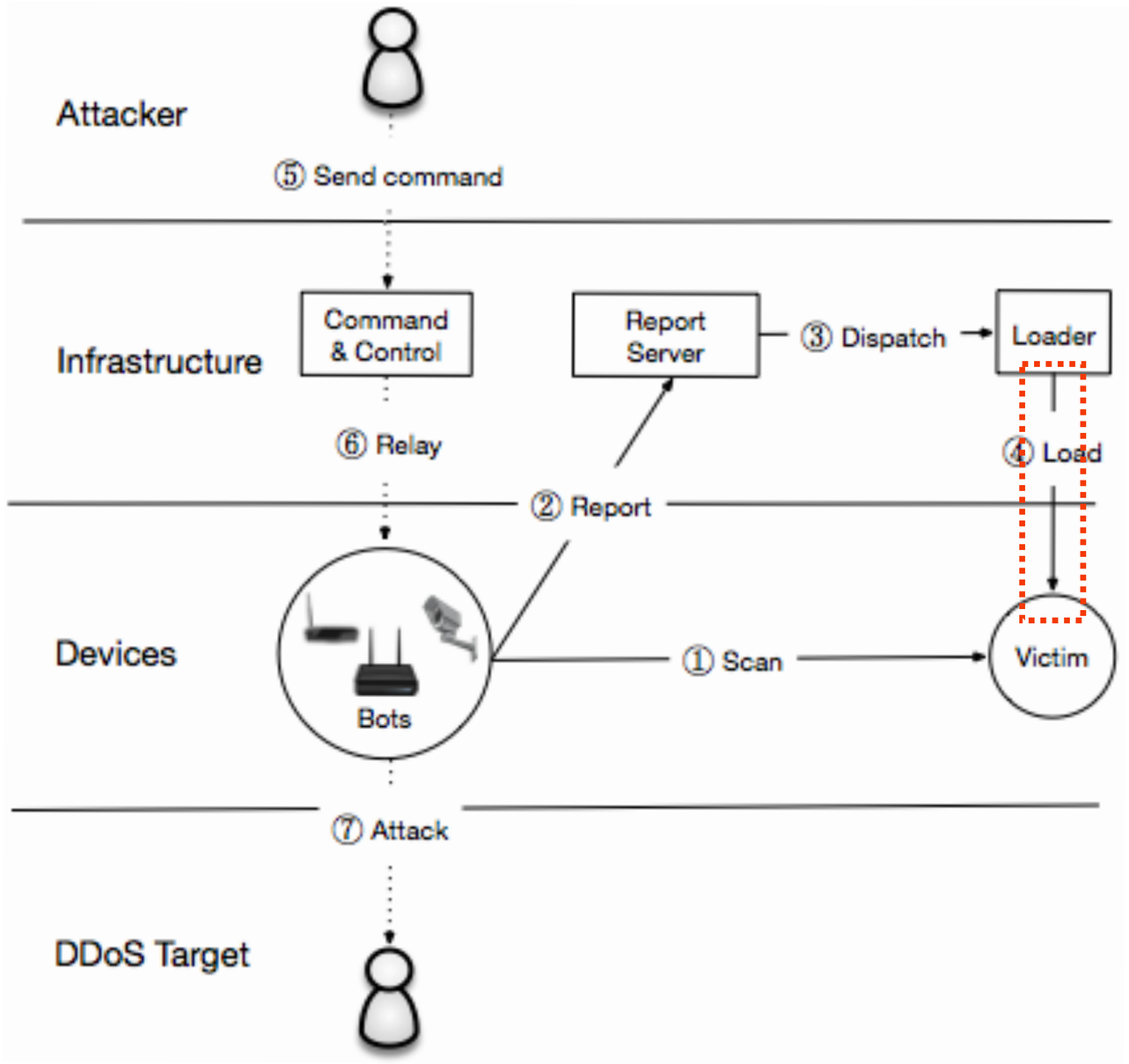
The Mirai Malware

1. Bots statelessly scan for victims on TCP/23 and TCP/2323. They attempt to login over telnet with a set of hardcoded credentials
2. **Scanner** reports details about vulnerable host to central **C2 server**
3. **C2 server** dispatches command to **loader** to load malware onto IoT device



The Mirai Malware

1. Bots statelessly scan for victims on TCP/23 and TCP/2323. They attempt to login over telnet with a set of hardcoded credentials
2. **Scanner** reports details about vulnerable host to central **C2 server**
3. **C2 server** dispatches command to **loader** to load malware onto IoT device
4. **Loader** logs into device, downloads and installs architecture-specific malware, kills telnet service, removes other malware, and waits for instructions

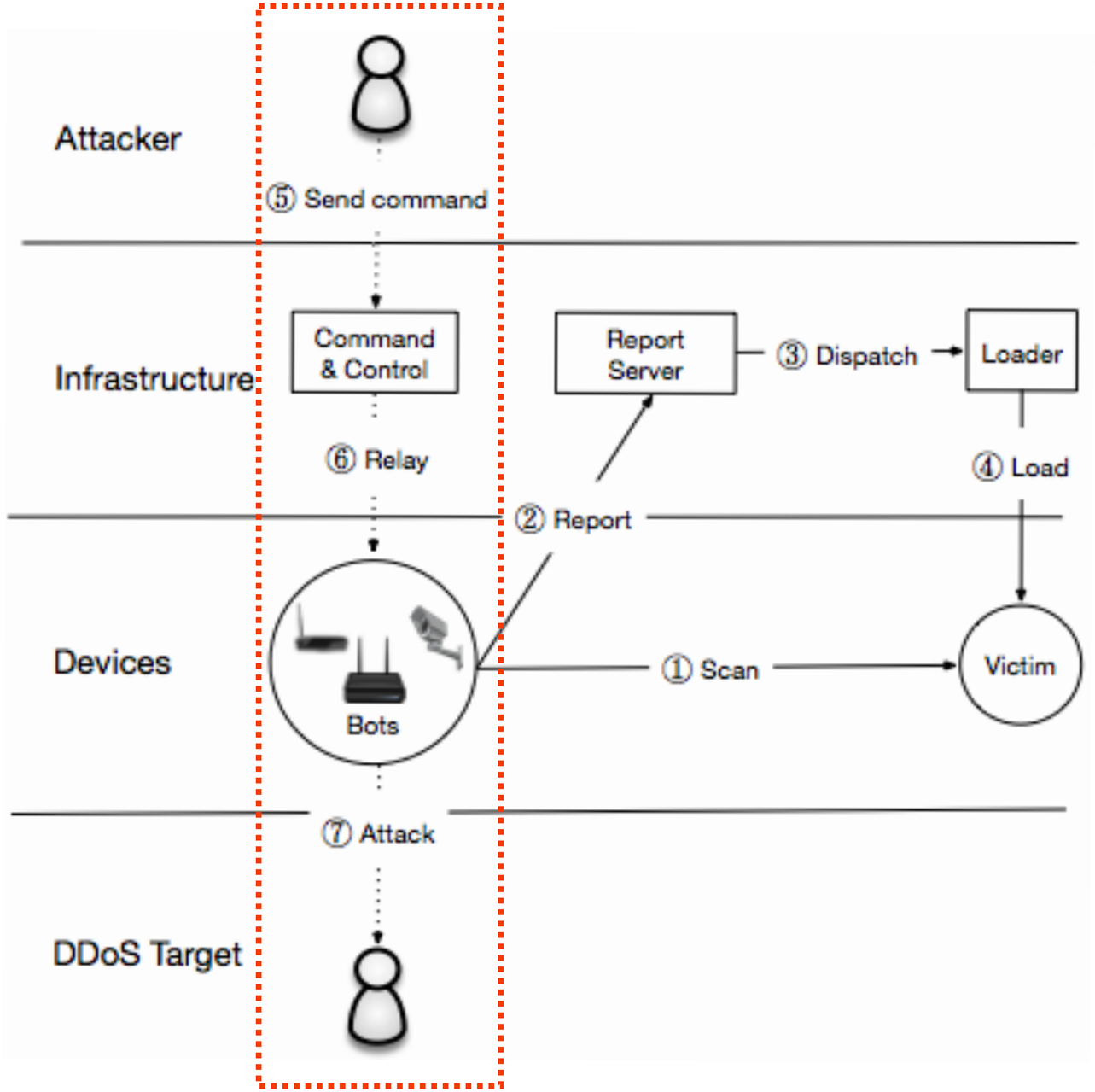


The Mirai Malware

5-7. Later, the **bot master** will issue commands to pause scanning and to start an attack

Attack Command:

- Action (e.g., START, STOP)
- Target IP(s)
- Attack Type (e.g., GRE, DNS, TCP)
- Attack Duration

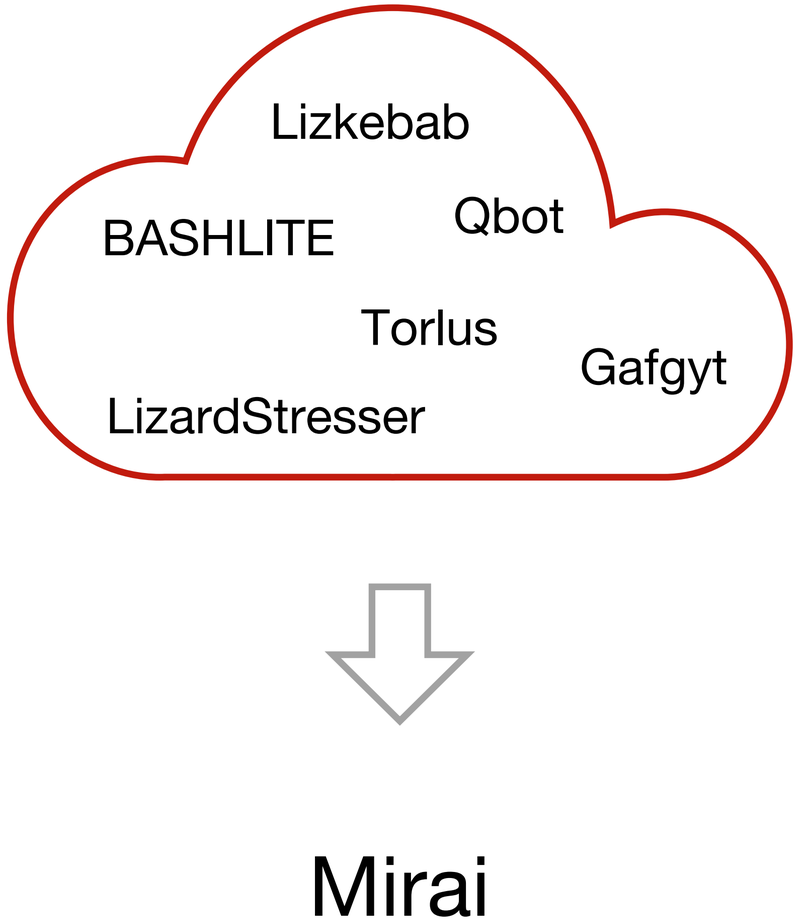


What made Mirai Successful?

The Mirai malware is (astoundingly) badly written. It uses no new or complex techniques.

Mirai was successful because:

1. IoT security is *terrible*
2. Attack simplicity enabled the malware to compromise heterogeneous hardware
3. Stateless scanning was an improvement over prior versions



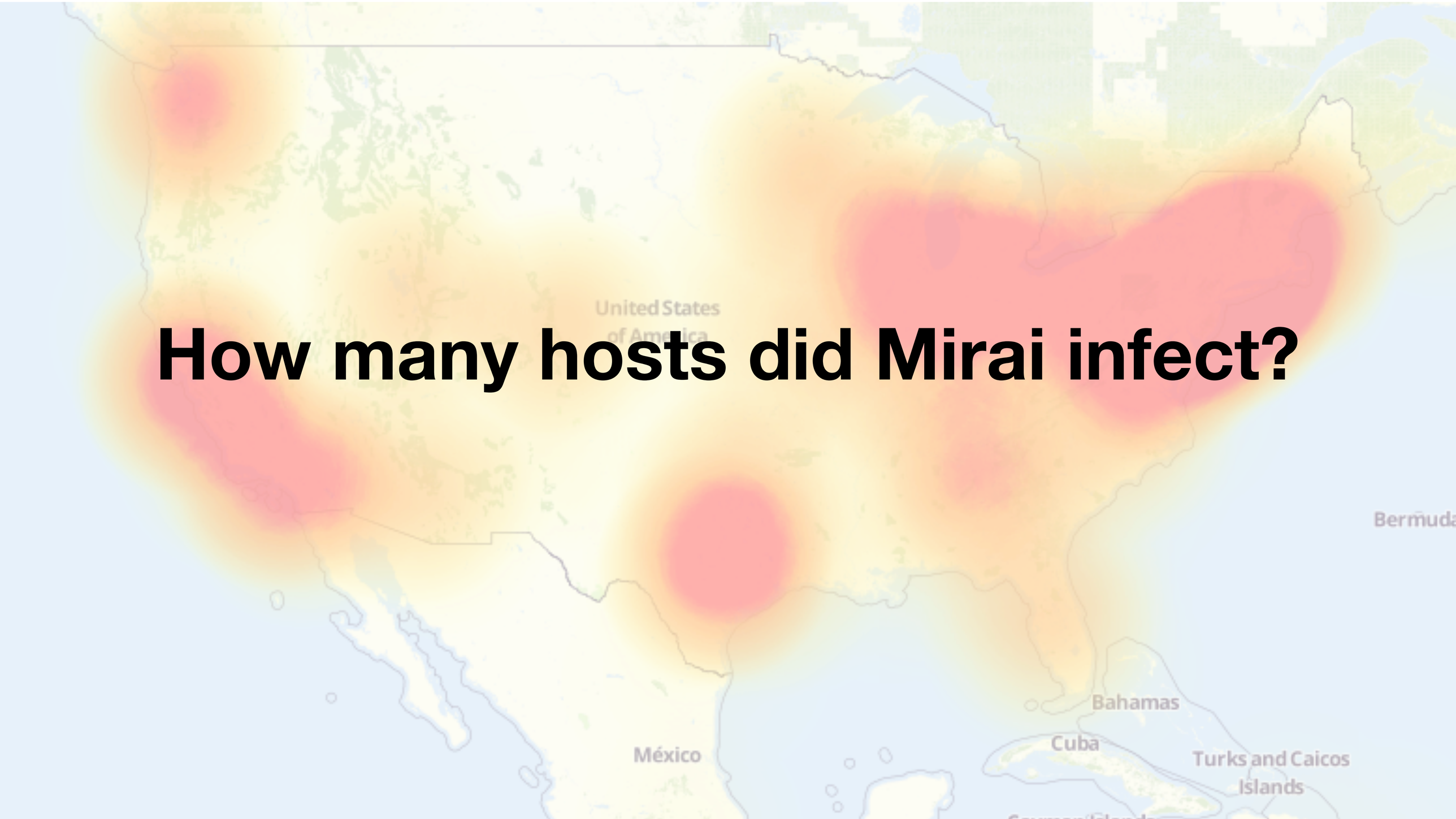
How many hosts did Mirai infect?

What types of devices were compromised?

Which manufacturers were responsible?

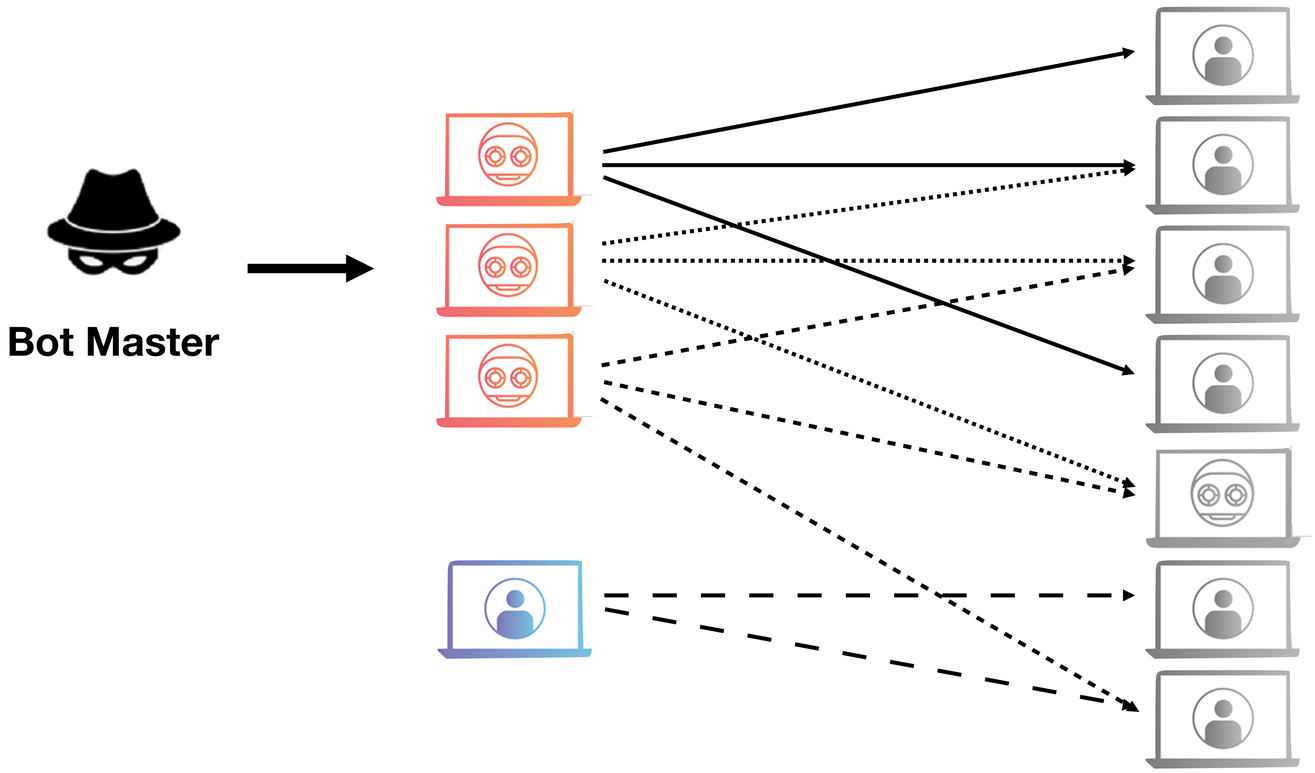
Why attack Dyn? Who else was attacked?

Who created Mirai? Why?



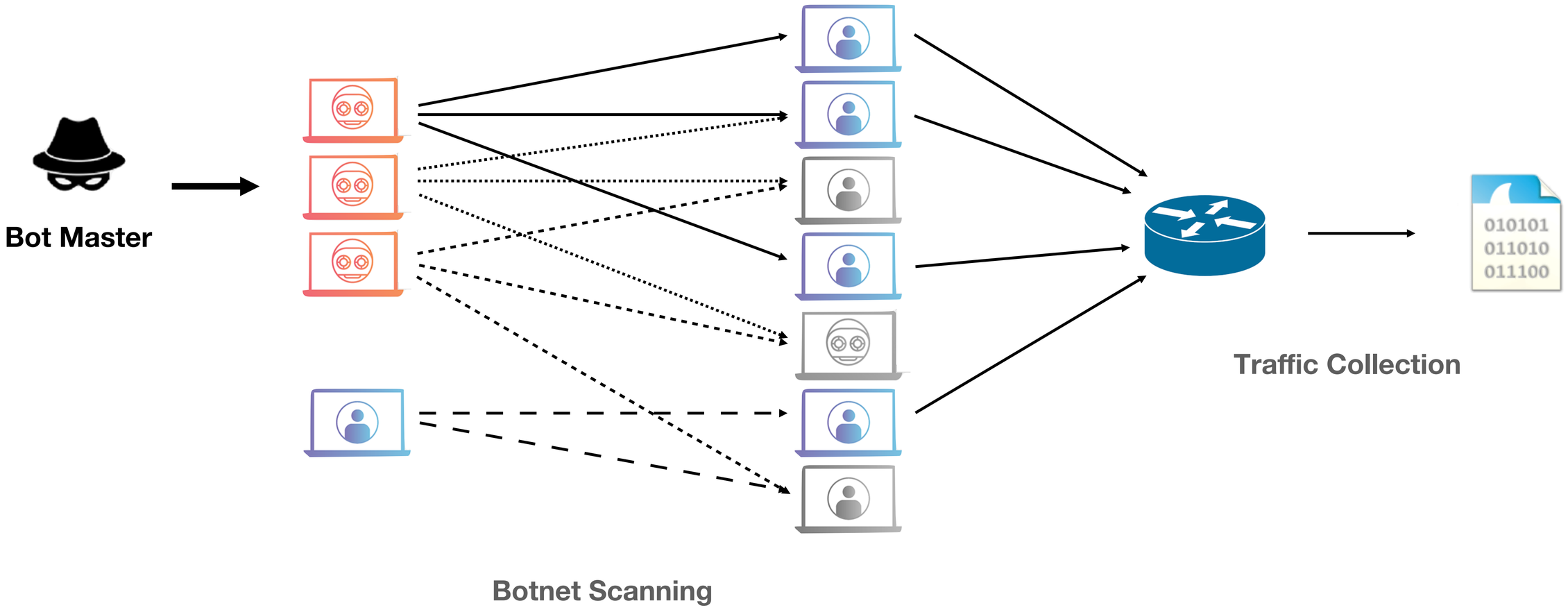
How many hosts did Mirai infect?

How do you measure botnet size?

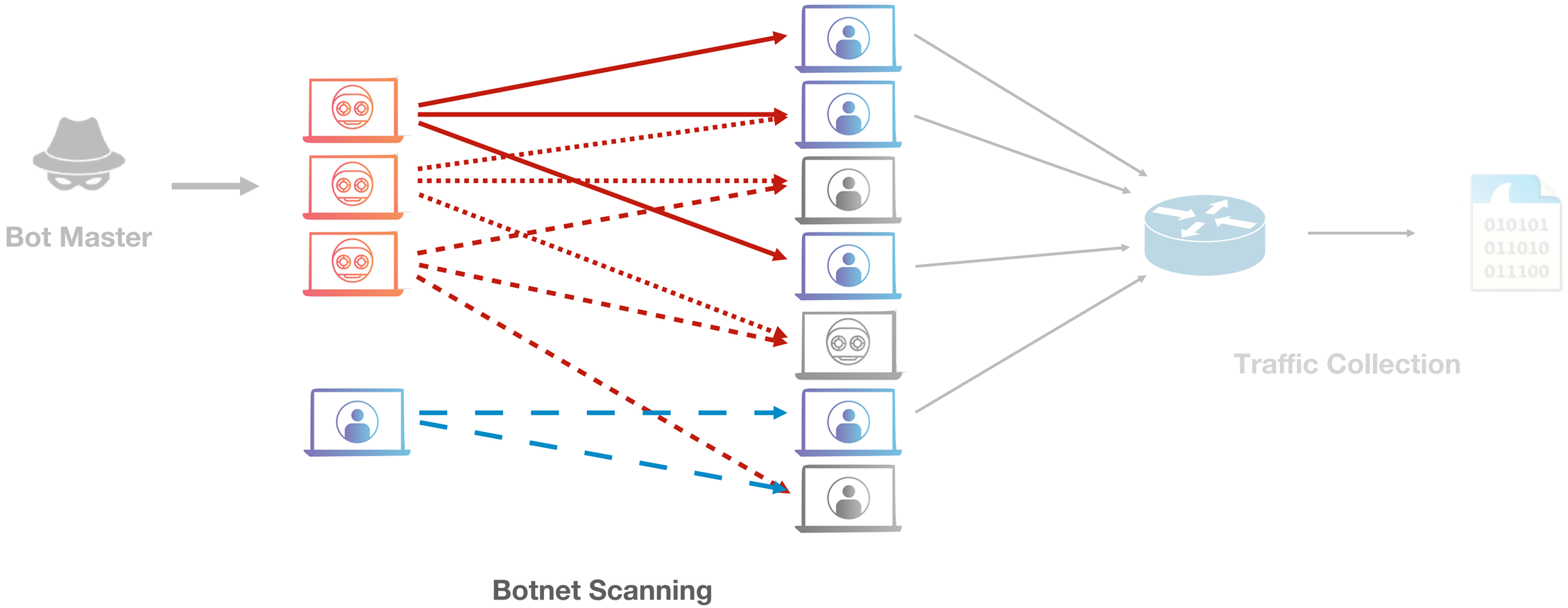


Botnet Scanning

How do you measure botnet size?

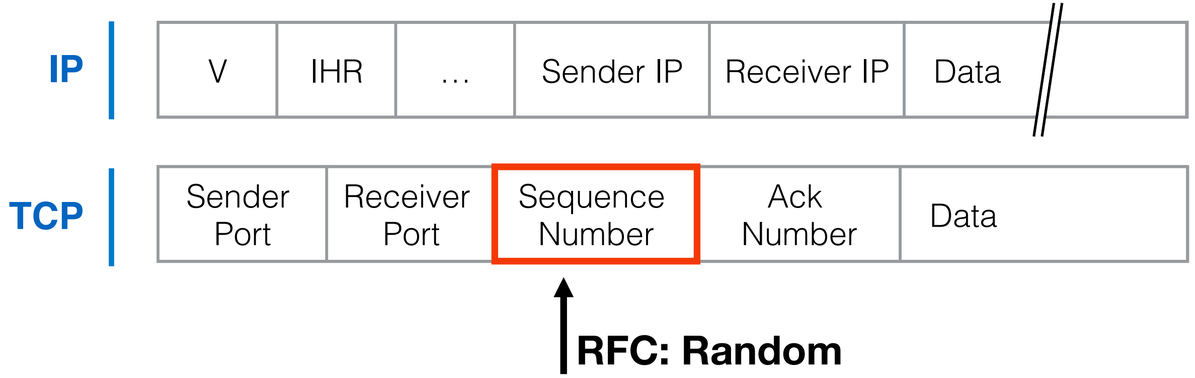


How do you measure botnet size?

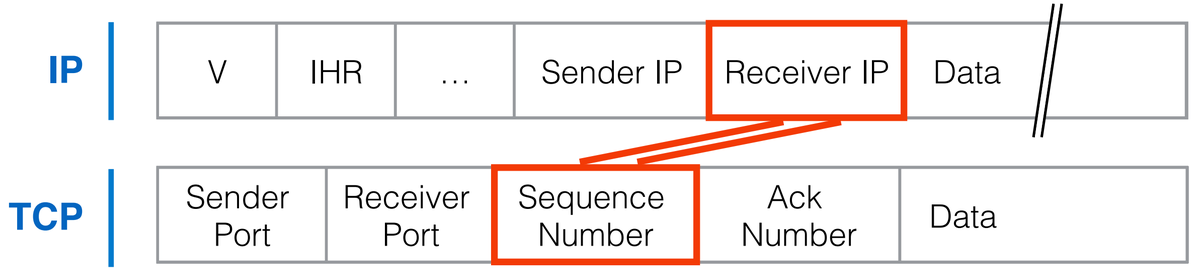


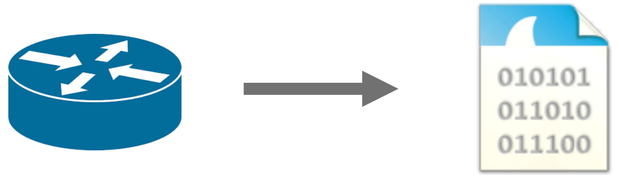
Fingerprinting Mirai Probes

Normal TCP/IP



Mirai Scanning





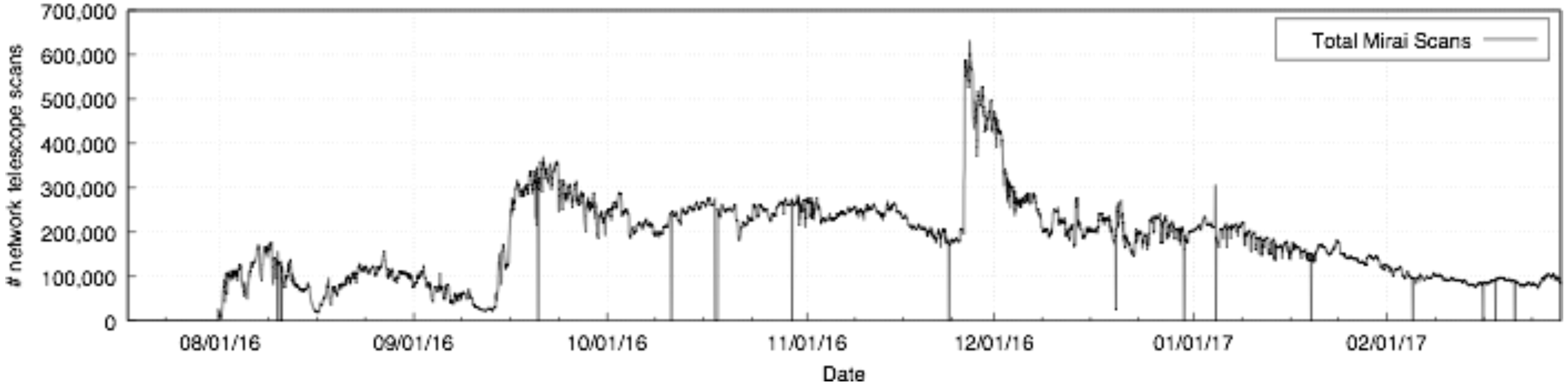
Merit Network Telescope

“/9” Block

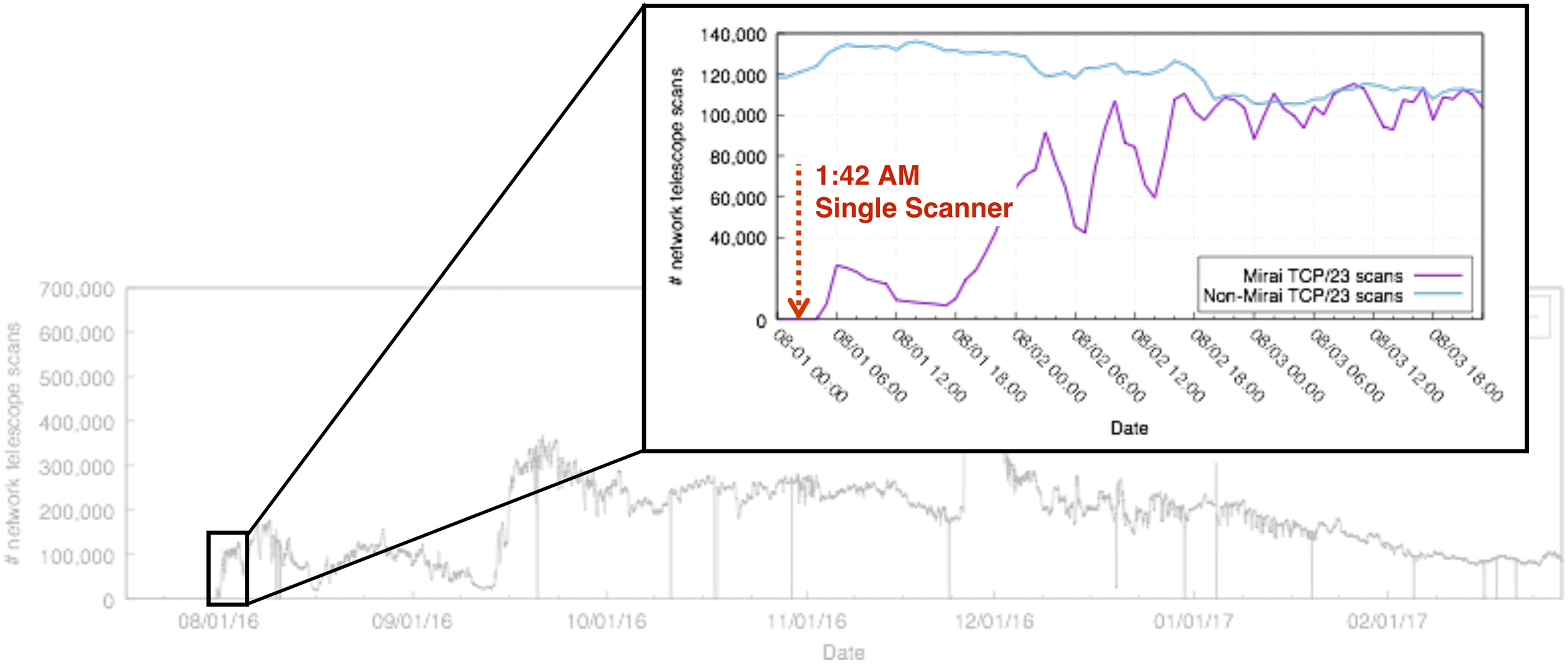
8M IPs

0.2% of IPv4

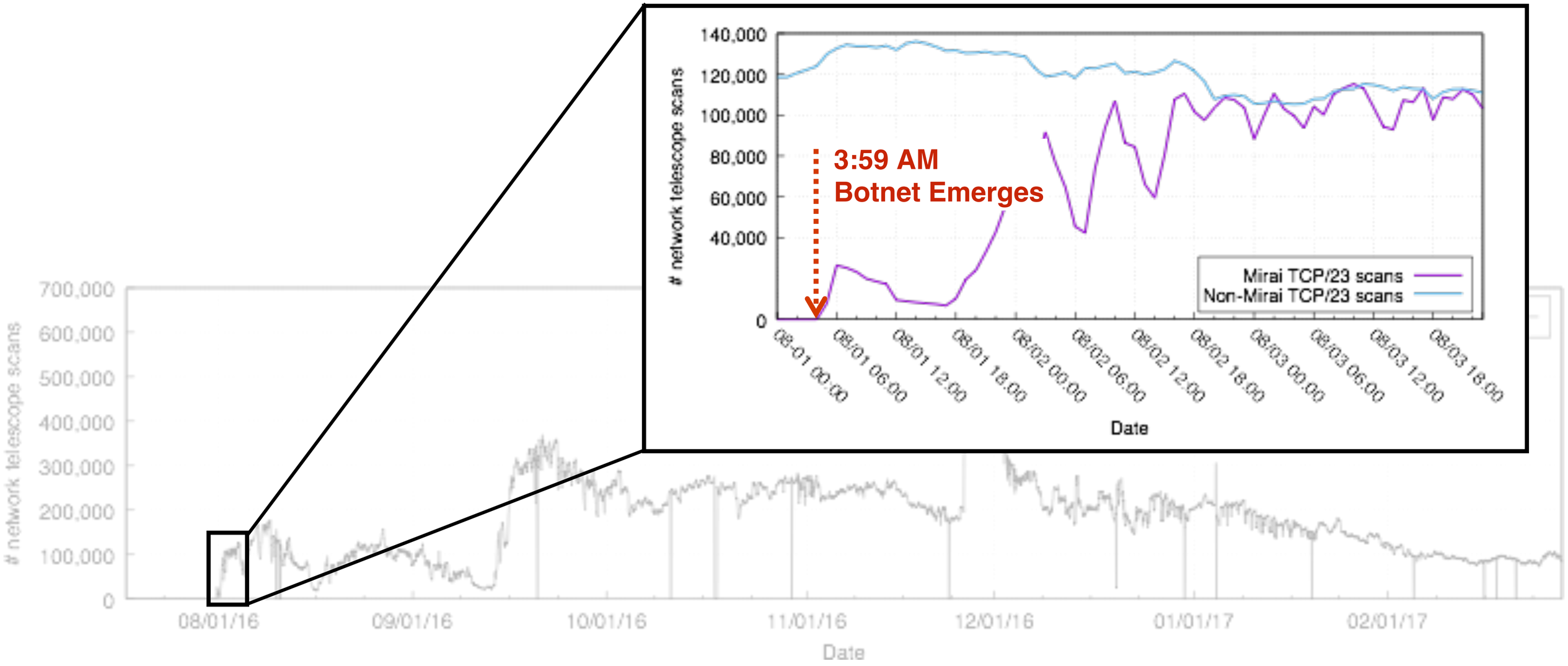
How large was Mirai?



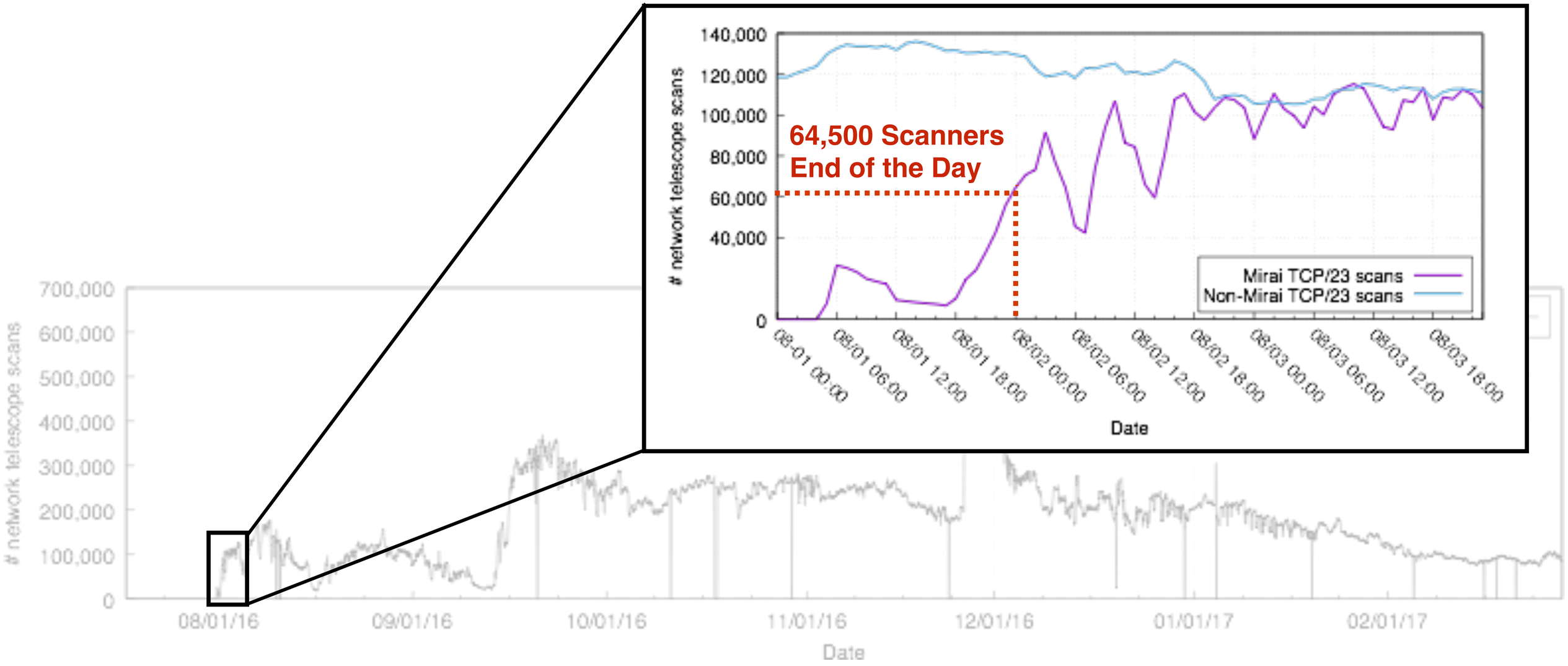
Initial Bootstrapping



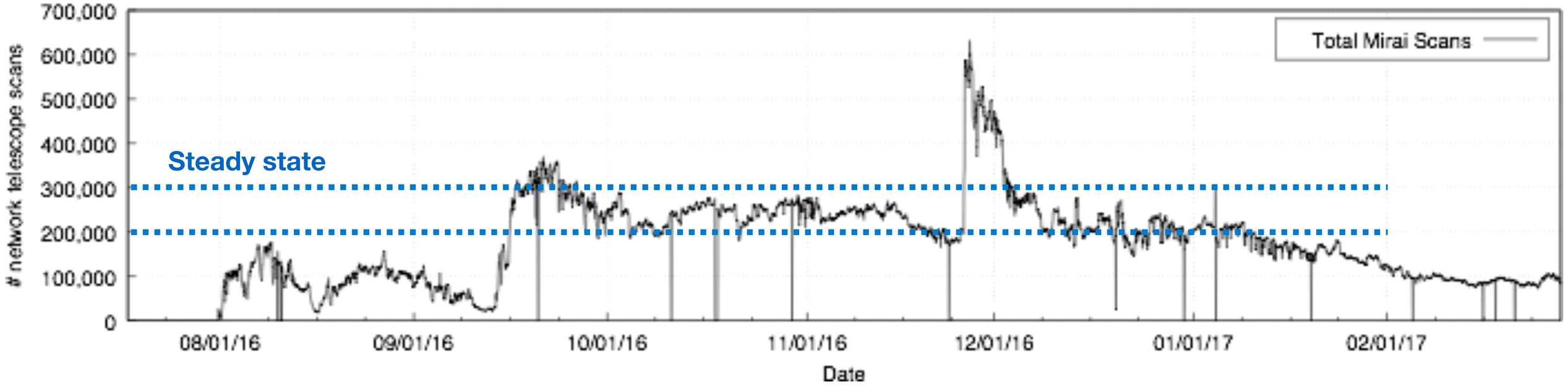
Initial Bootstrapping



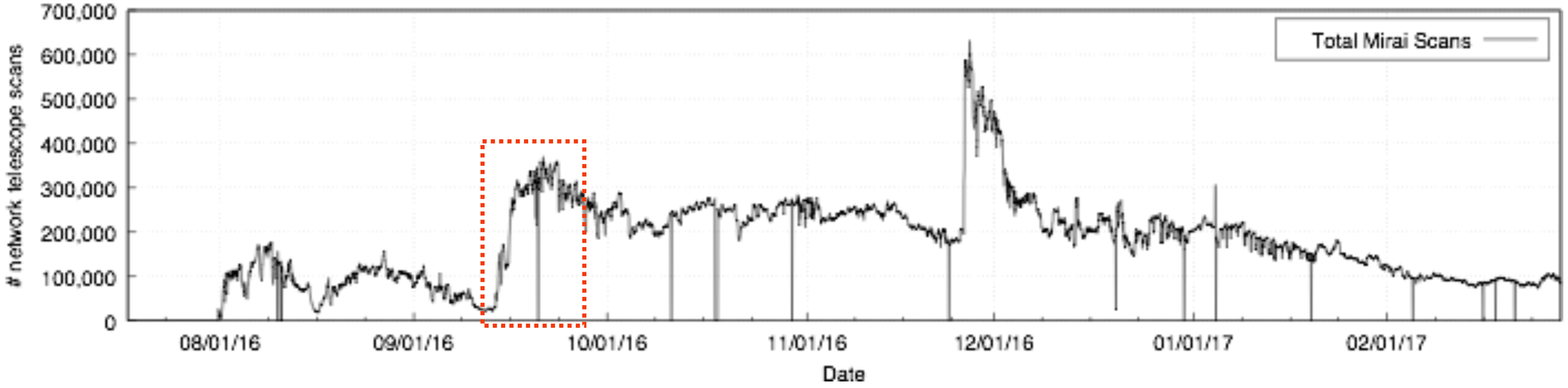
Initial Bootstrapping



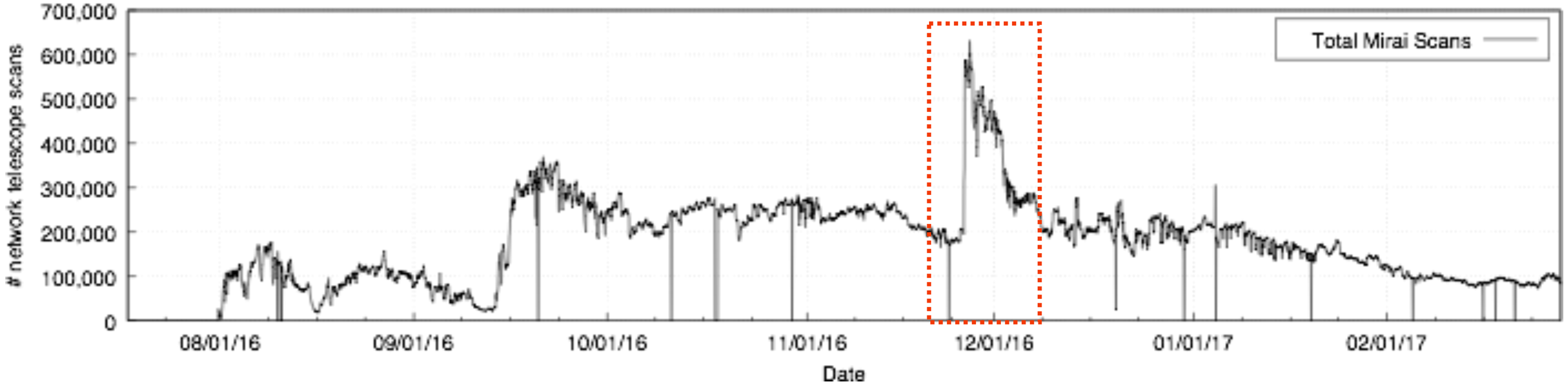
How large was Mirai?



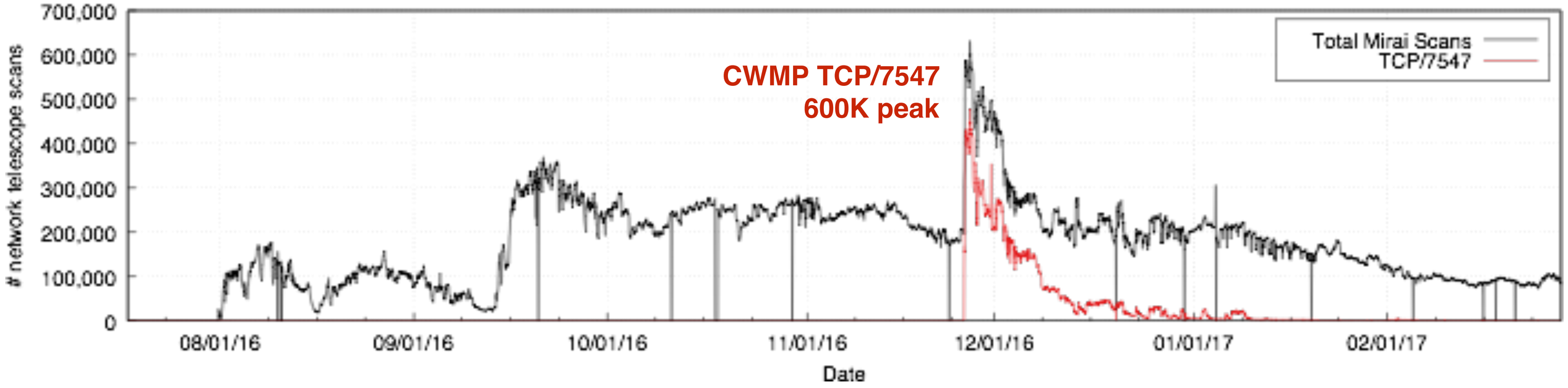
How large was Mirai?



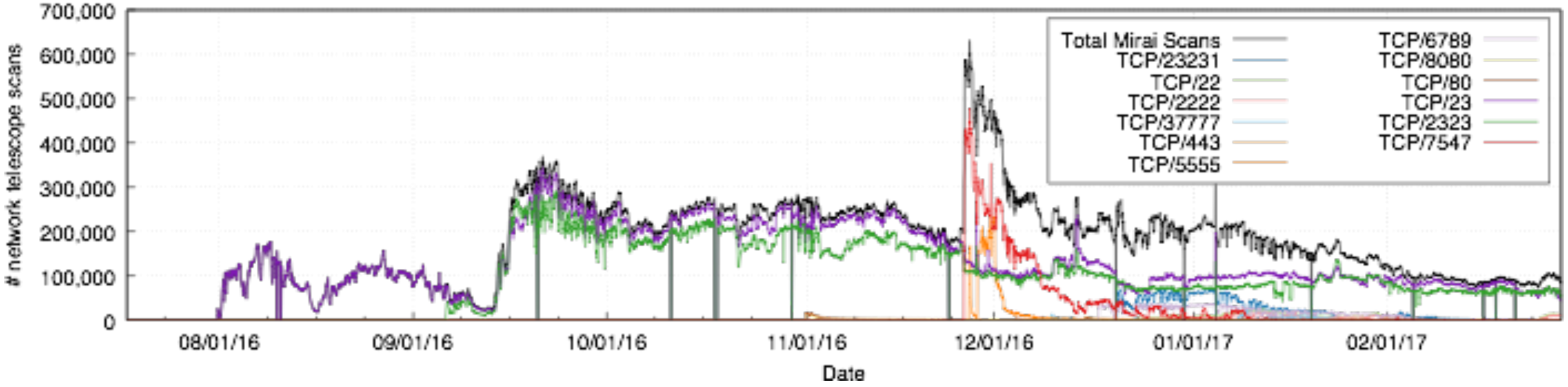
How large was Mirai?

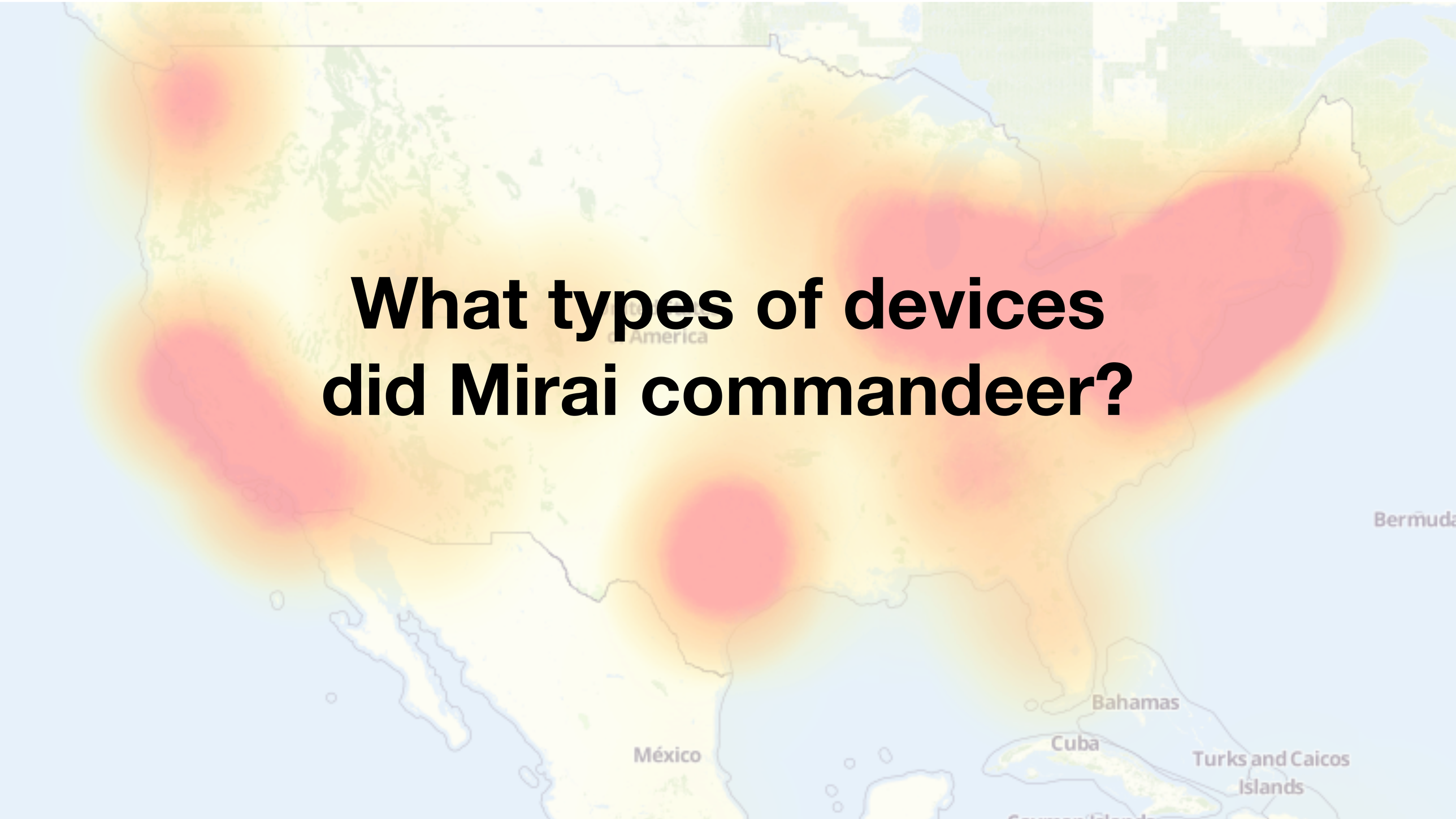


How large was Mirai?

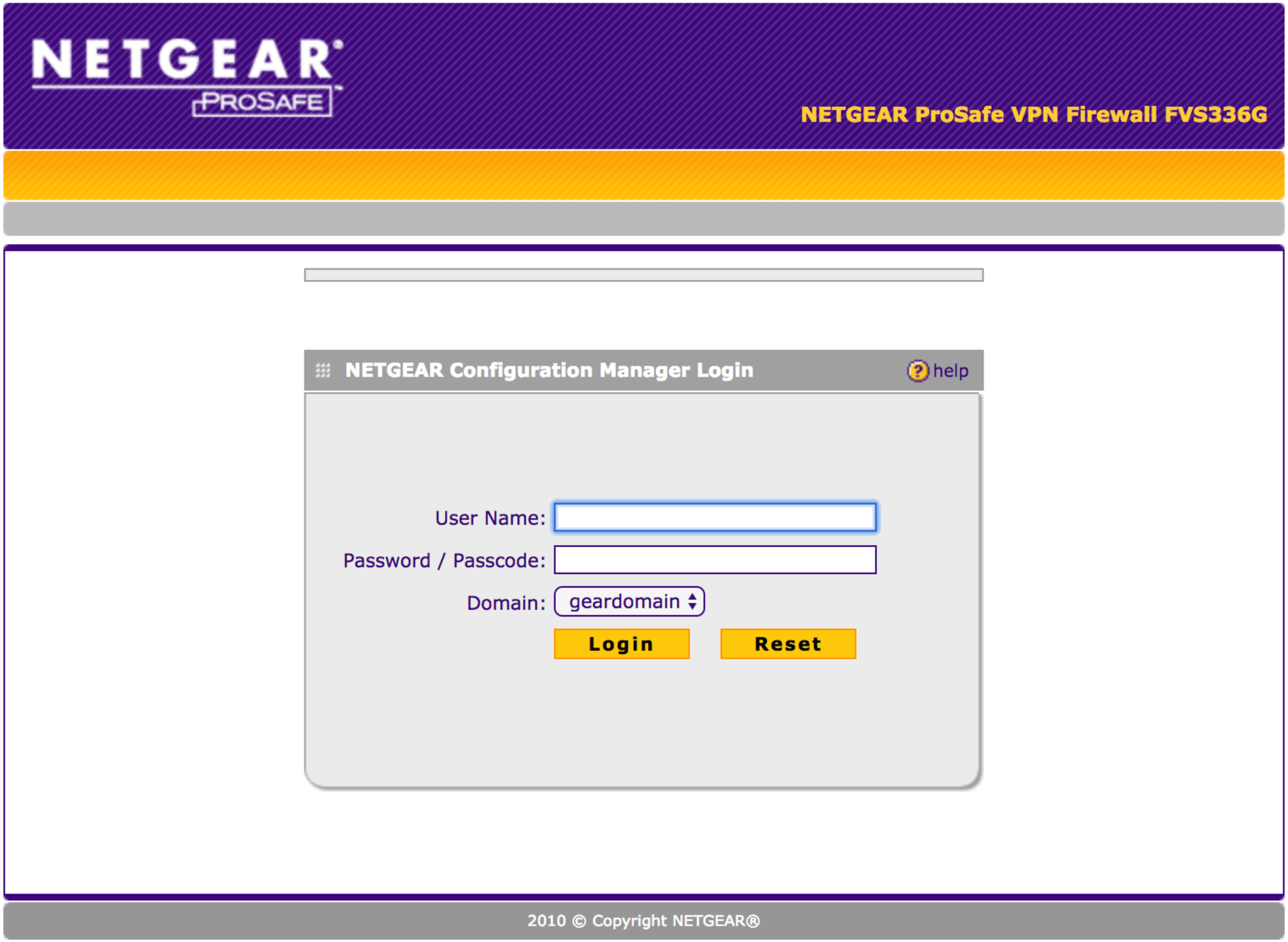


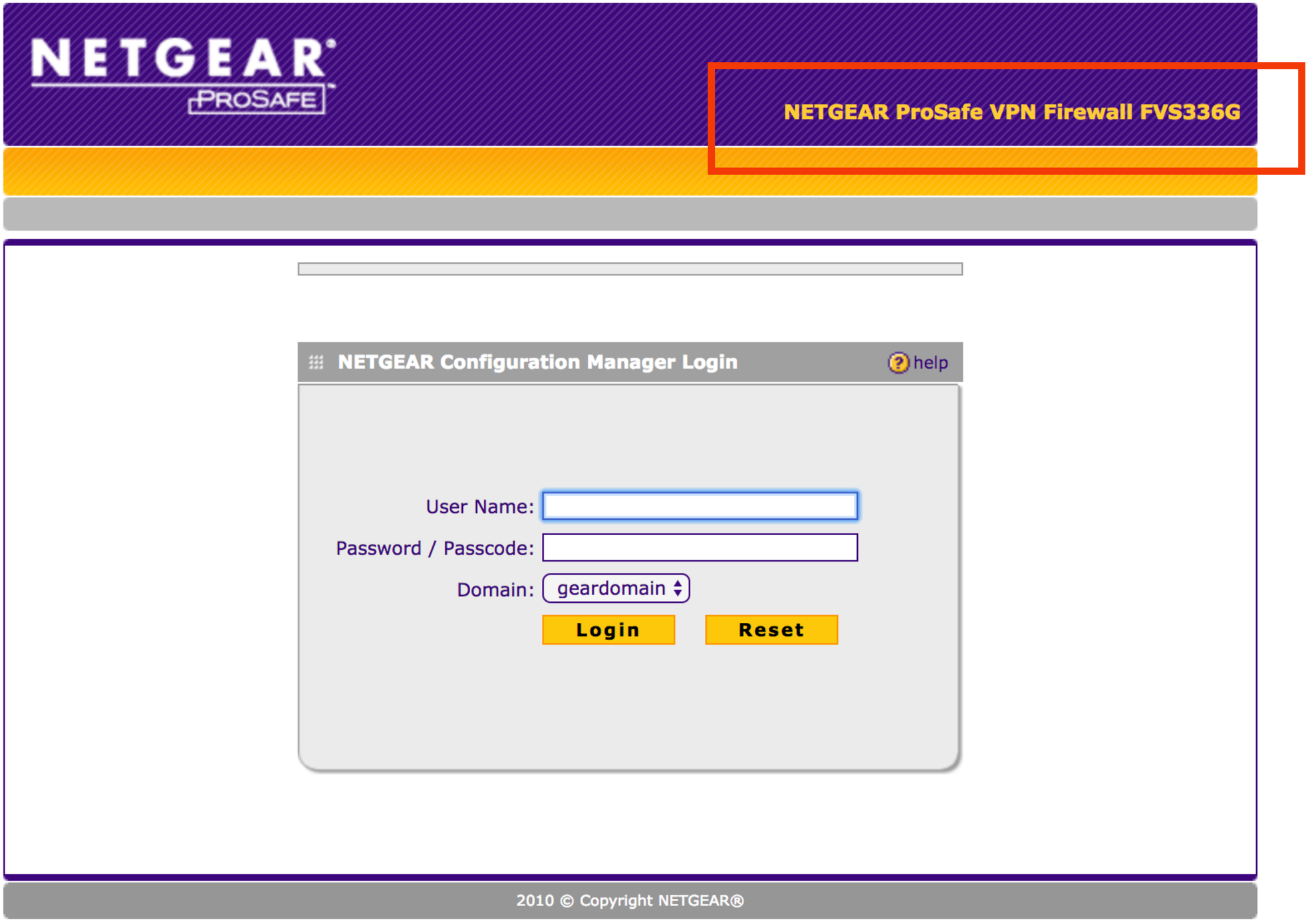
How large was Mirai?





What types of devices did Mirai commandeer?


NETGEAR
PROSAFE
NETGEAR ProSafe VPN Firewall FVS336G
NETGEAR Configuration Manager Login
help
User Name:
Password / Passcode:
Domain:
geardomain
Login
Reset
2010 © Copyright NETGEAR®


NETGEAR
PROSAFE
NETGEAR ProSafe VPN Firewall FVS336G
NETGEAR Configuration Manager Login
help
User Name:
Password / Passcode:
Domain:
geardomain
Login
Reset
2010 © Copyright NETGEAR®

censys

Search

ABOUT BLOG MY NETWORKS ADMIN MY ACCOUNT

IPv4 Hosts | Top Million Websites | Certificates | Tools | Help

Page: 1/430,309 **Results:** 10,757,703 **Time:** 403ms **Query Plan:** expanded

Filter by AS:

Uninet S.A. de C.V., MX: 2.39M

ATT-INTERNET4 - AT&T Services, Inc., US: 2.22M

VODAFONE_ES, ES: 429.41K

TRIPLETNET-AS-AP Triple T Internet/Triple T Broadband, TH: 316.77K

AS-NETIA Warszawa 02-822, PL: 247.44K

More

Filter by Protocol:

443/https: 8.91M

80/http: 2.72M

8080/http: 1.8M

22/ssh: 960.68K

21/ftp: 932.37K

5.40.167.148 (5.40.167.148.static.user.ono.com)

AS Cableuropa - ONO (6739) Spain

MikroTik Network MikroTik RouterOS 8080/http

EMBEDDED NETWORK

94.69.191.185 (ppp-94-69-191-185.home.otenet.gr)

GR Athens - Greece (6799) Greece

Hikvision Camera 8080/http

CAMERA

189.115.144.147 (189.115.144.147.static.host.gvt.net.br)

TELEFNICA BRASIL S.A (18881) Salvador, Bahia, Brazil

MikroTik Network MikroTik RouterOS 8080/http

EMBEDDED NETWORK

36.80.11.167

AS2-AP PT Telekomunikasi Indonesia... (17974) Bandung, West Java, Indonesia

MikroTik Network MikroTik RouterOS 8080/http

EMBEDDED NETWORK

94.179.251.243 (94.179.251.243.pool.3g.utel.ua)

UKRTELNET (6849) Ukraine

MikroTik Device 8080/http

EMBEDDED

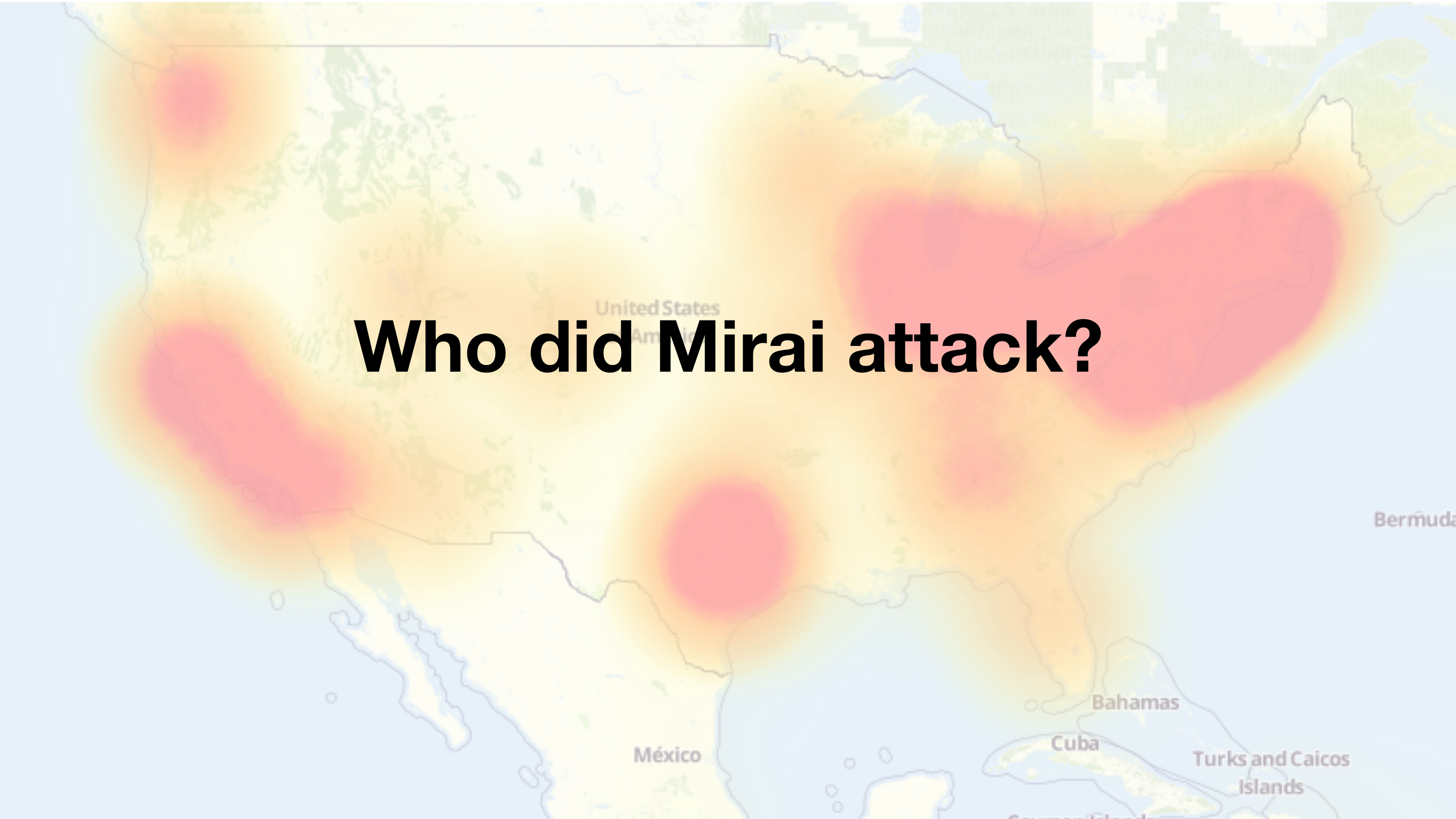
Types of Infected Devices

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%

Passwords in Malware

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				



Who did Mirai attack?

Collecting Binaries and Commands

Operated a telnet honeypot that looked like a vulnerable BusyBox (common IoT platform)

Collected passwords, binaries, C2 servers

Logged attack commands

Never sent attack traffic!

Top 10 Beyond Dyn, Krebs, and OVH…

Lonestar Cell	Liberian telecom
Sky Network	Brazilian Minecraft servers
104.85.165.1	Akamai router
feseli.com	Russian cooking blog
minomortaruolo.it	Italian political site
Voxility hosted C2	C2 server
Tuidang websites	Two Chinese political dissidence sites.
execrypt.com	Binary obfuscation service
auktionshilfe.info	Russian auction site
houtai.longqikeji.com	Game commerce site

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

September 1, 2016

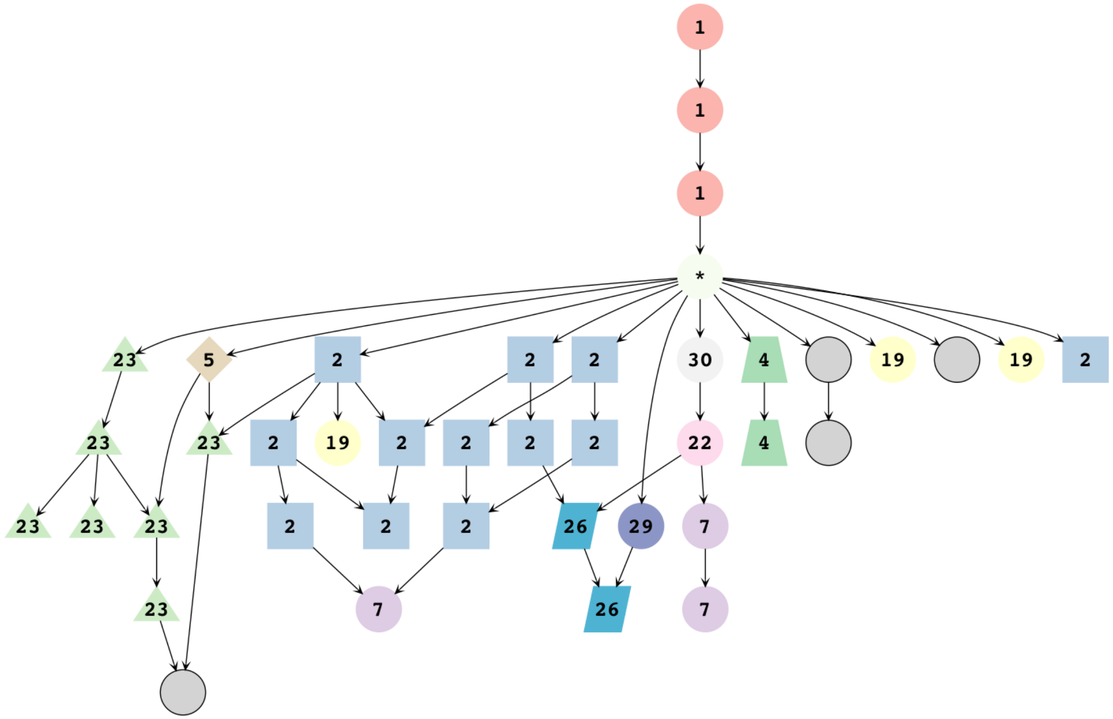
Evolution of Mirai

August: IP-based C2, no obfuscation

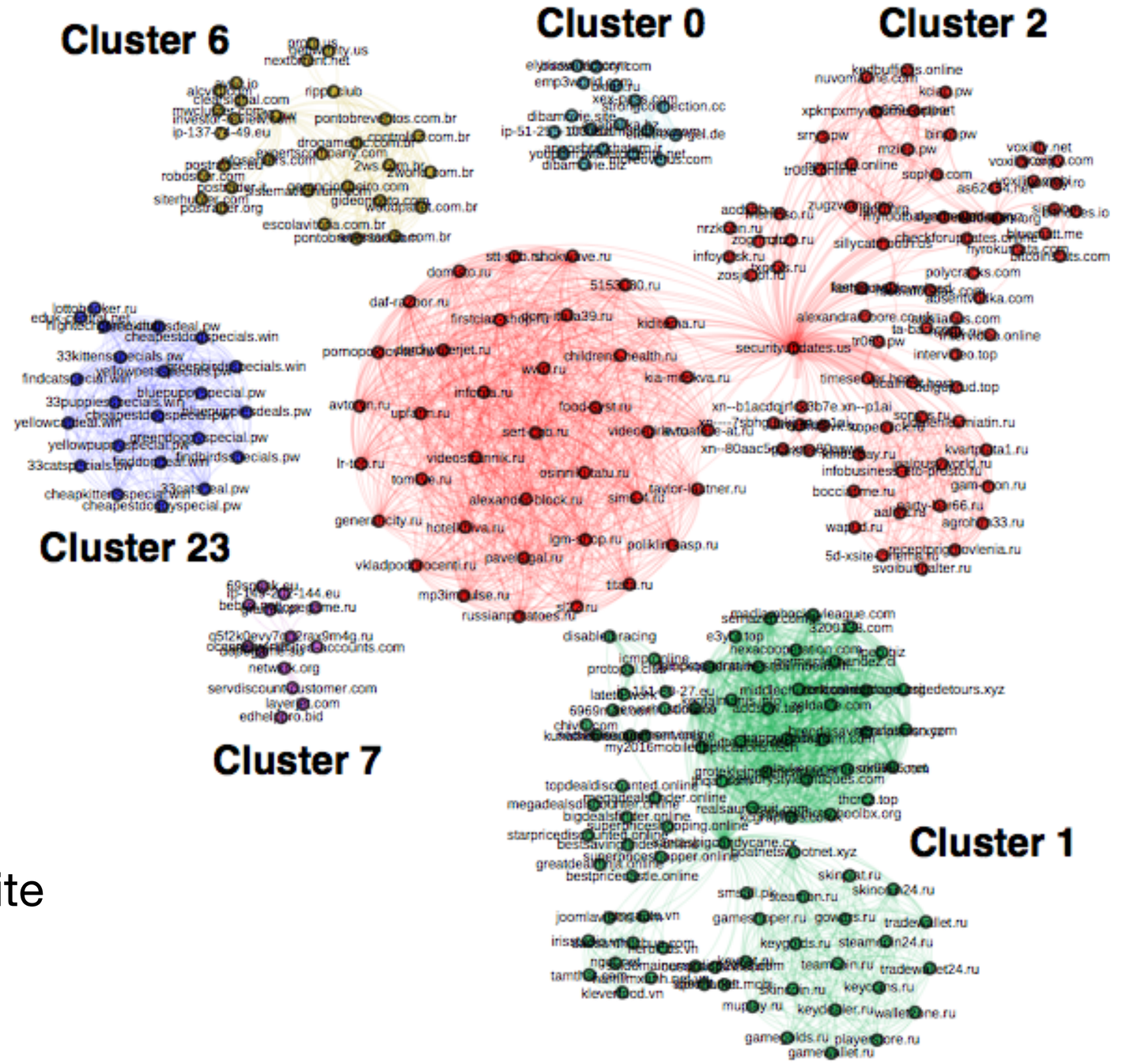
September: Domain C2, removes binary, obfuscated binary name

Post Public Release: 48 new sets of passwords, blacklist changes,

November: CWMP vulnerability scanning, DGAs, packed binaries



Major Variants



(1) Original Botnet: Krebs, OVH

(2) Liberian Provider, Russian Auction Site

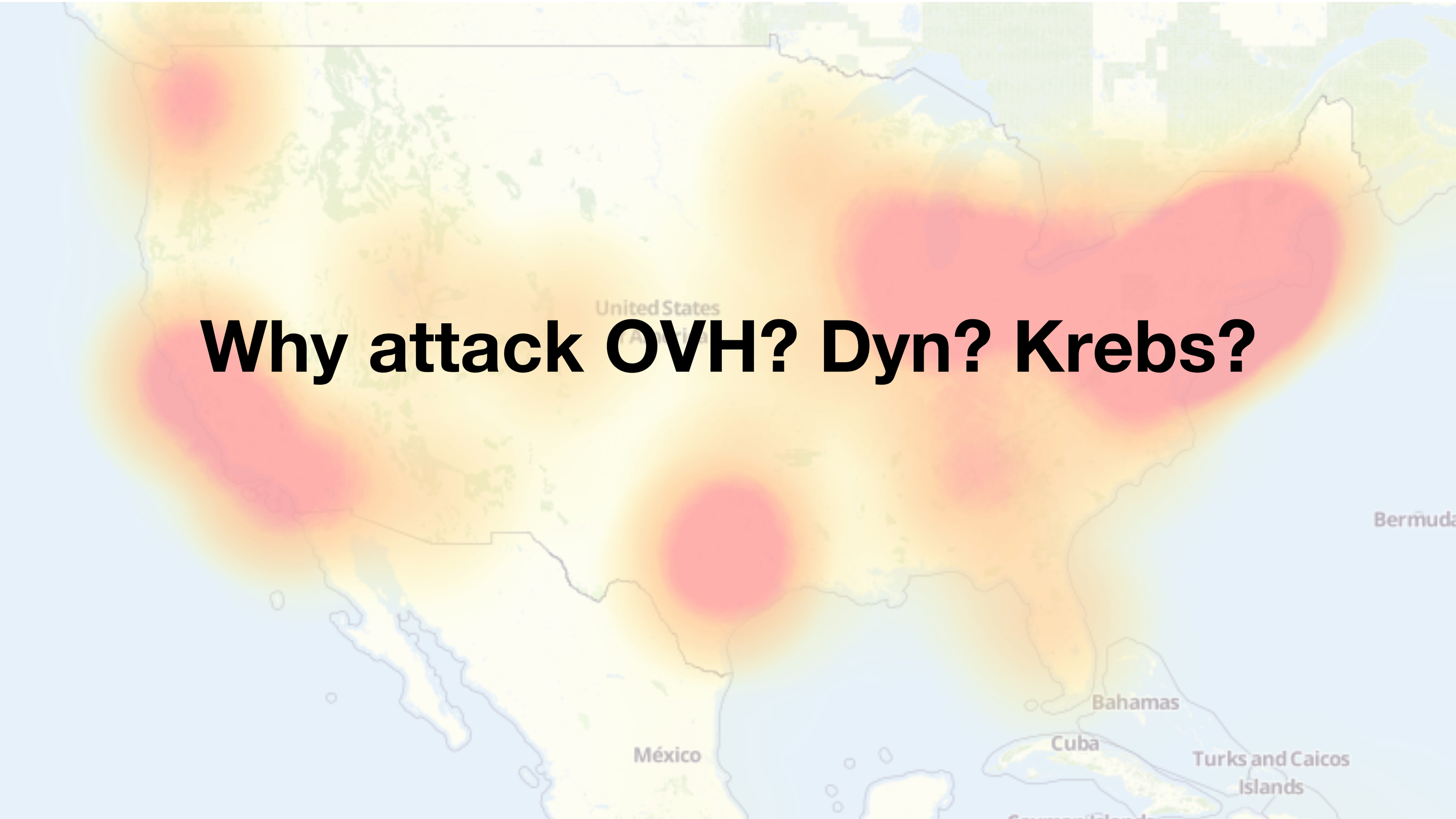
(6) Dyn Attack, Gaming Sites

(7) Russian Blog, Italian Politician, etc.

Example Booter

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	**22.00€** Lifetime	**50.00€** Lifetime	**60.00€** Lifetime	**90.00€** lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	**600** seconds boot time	**1200** seconds boot time	**1800** seconds boot time	**3600** seconds boot time
125Gbps total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity
Resolvers & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools
24/7 Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now



Why attack OVH? Dyn? Krebs?


MINECRAFT

Dyn Attack

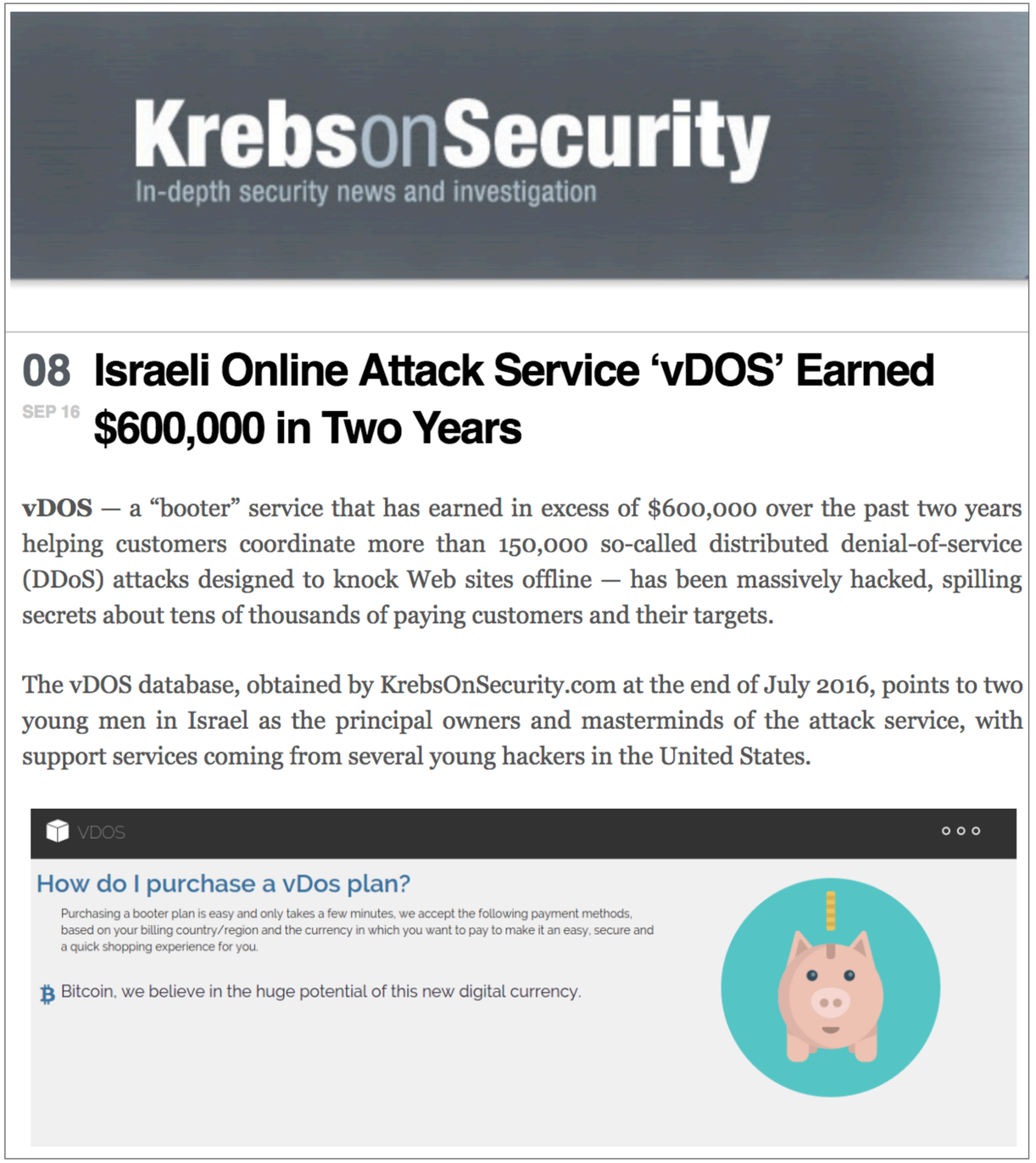
The New York Times

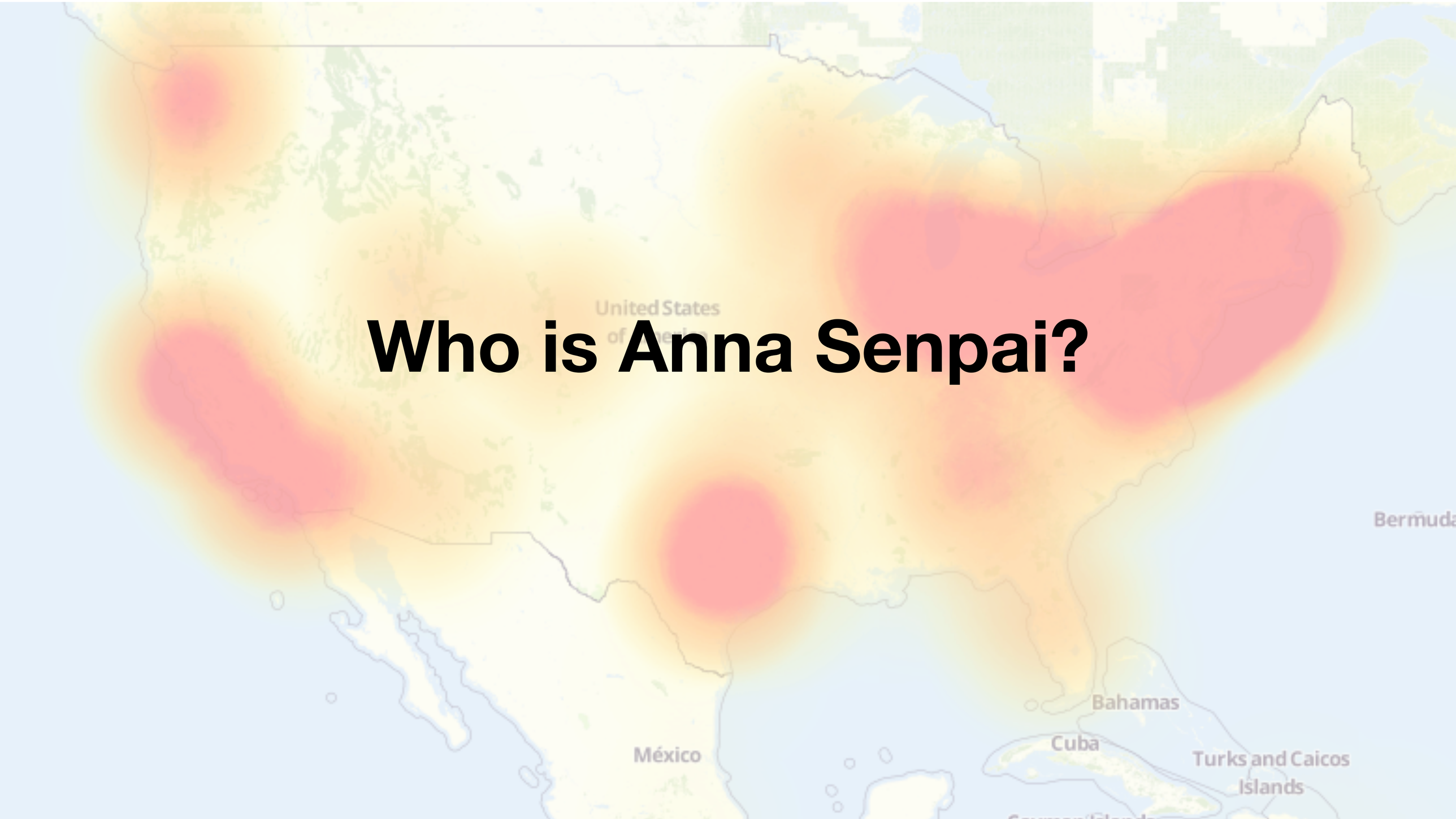
> “It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by “hacktivists.” Or a foreign power that wanted to remind the United States of its vulnerability.”

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**

Brian Krebs

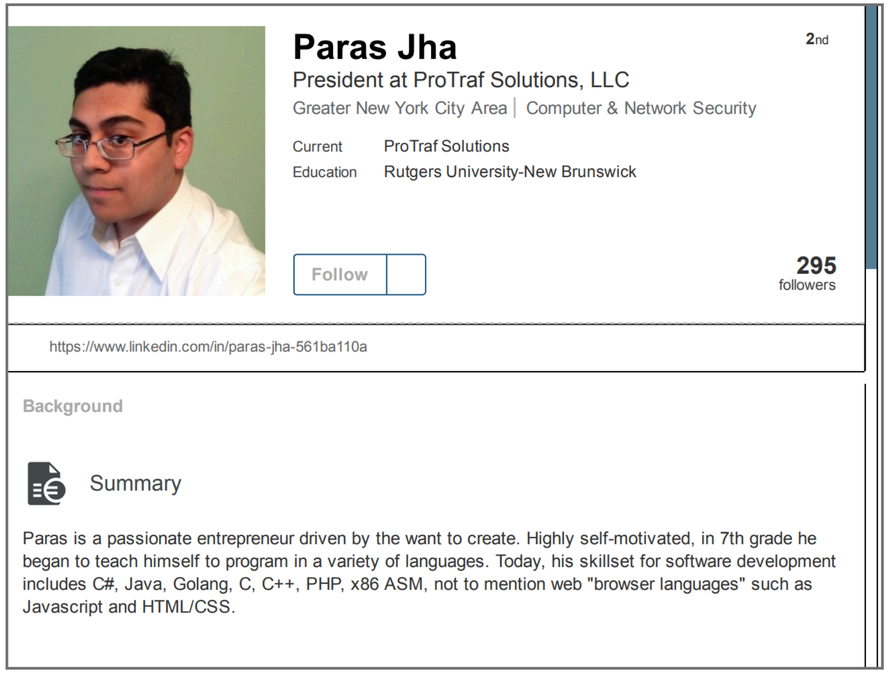
Retribution for article exposing the creators of vDOS—a popular booter





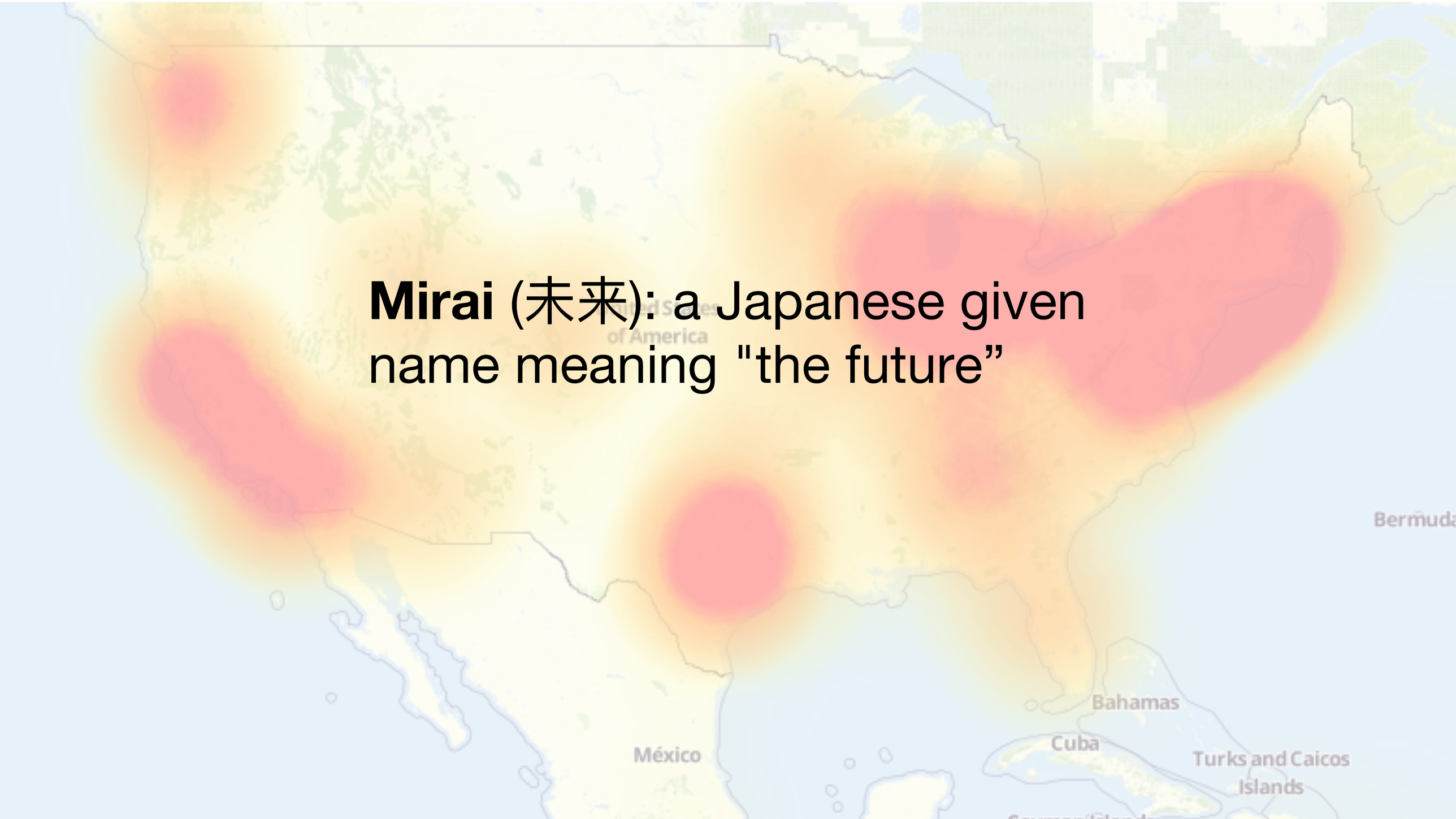
Who is Anna Senpai?

Arrest of Paras Jha, Josiah White, Dalton Norman



Jha and White were co-founders of Protraf Solutions LLC, a company that specialized in mitigating large-scale DDoS attacks

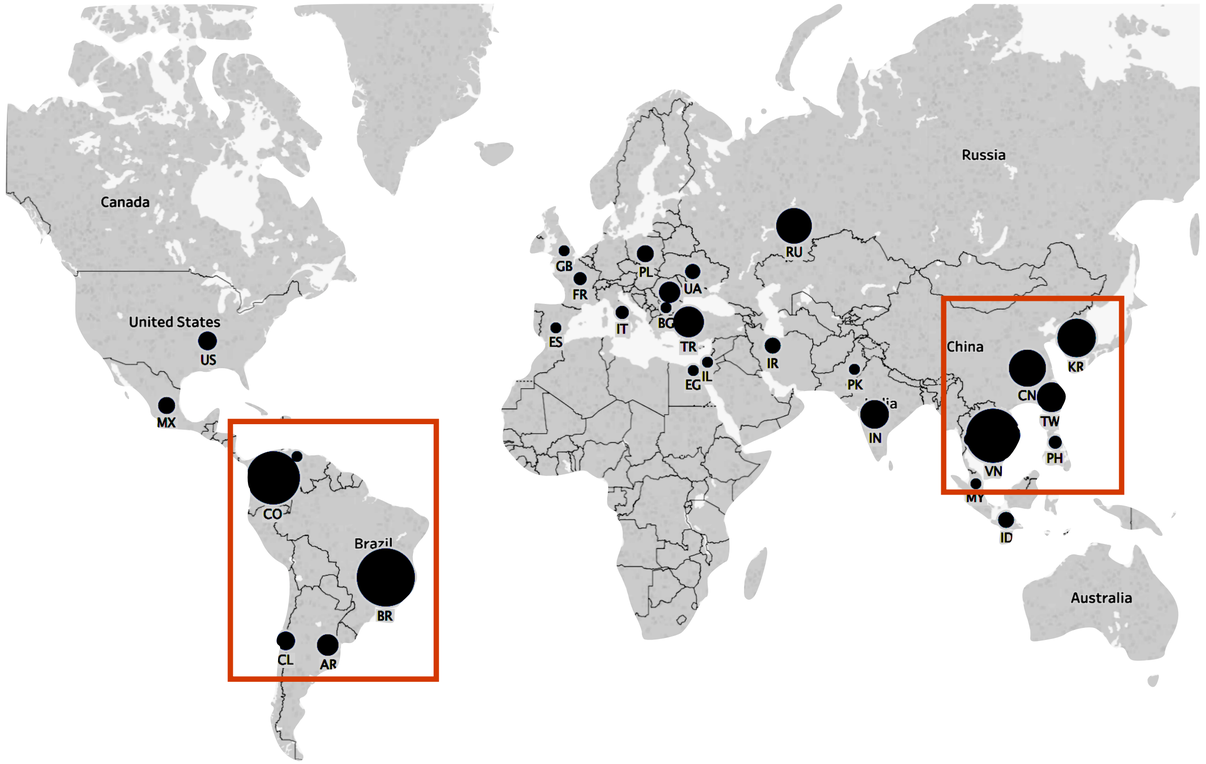
Primarily used botnet to extort Minecraft server operators



Mirai (未来): a Japanese given name meaning "the future”

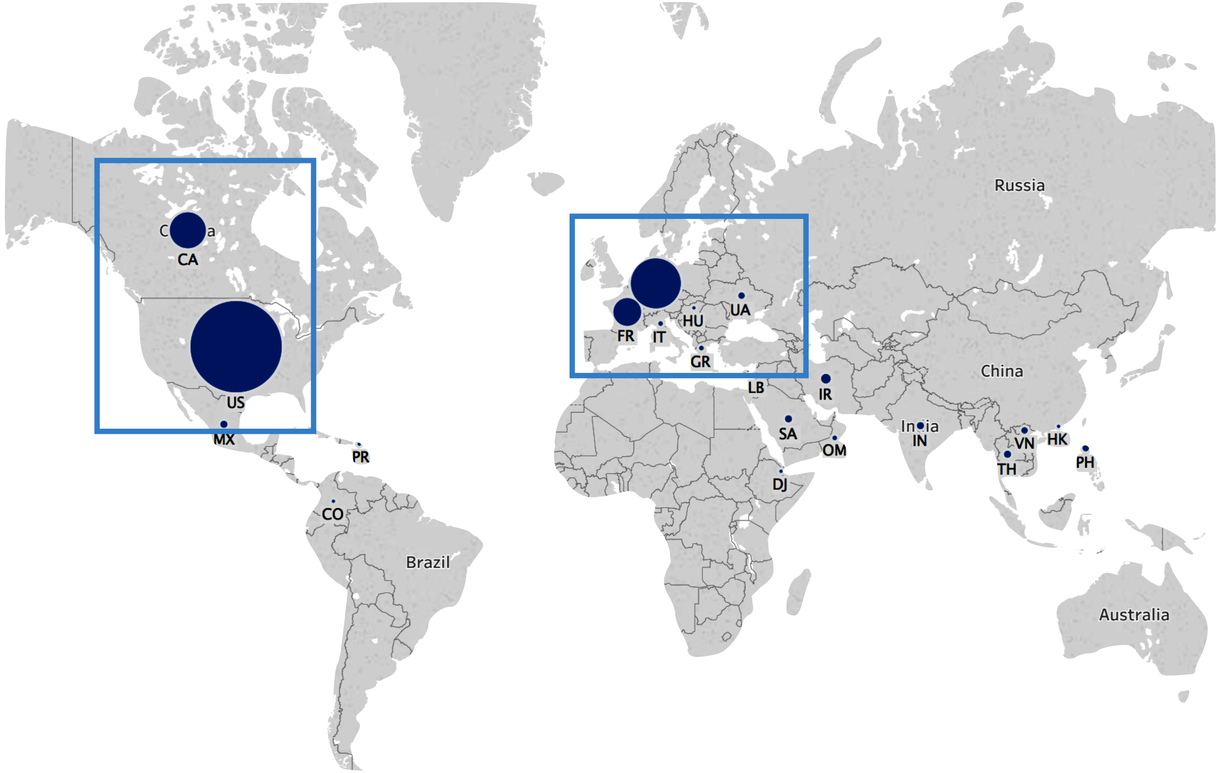
Geographic Bias

Mirai



South America + S.E. Asia
50% of Infections

TDSS/TDL4



N America + Europe
94% of Infections

Understanding the Mirai Botnet

Research Paper

Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, 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

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*

Abstract

The Mirai botnet, composed primarily of embedded and IoT devices, took the Internet by storm in late 2016 when it overwhelmed several high-profile targets with massive distributed denial-of-service (DDoS) attacks. In this paper, we provide a seven-month retrospective analysis of Mirai's growth to a peak of 600k infections and a history of its DDoS victims. By combining a variety of measurement perspectives, we analyze how the botnet emerged, what classes of devices were affected, and how Mirai variants evolved and competed for vulnerable hosts. Our measurements serve as a lens into the fragile ecosystem of IoT devices. We argue that Mirai may represent a sea change in the evolutionary development of botnets—the simplicity through which devices were infected and its precipitous growth, demonstrate that novice malicious techniques can compromise enough low-end devices to threaten even some of the best-defended targets. To address this risk, we recommend technical and non-technical interventions, as well as propose future research directions.

1 Introduction

Starting in September 2016, a spree of massive distributed denial-of-service (DDoS) attacks temporarily crippled Krebs on Security [46], OVH [43], and Dyn [36]. The initial attack on Krebs exceeded 600 Gbps in volume [46]—among the largest on record. Remarkably, this overwhelming traffic was sourced from hundreds of thousands of some of the Internet's least powerful hosts—Internet of Things (IoT) devices—under the control of a new botnet named Mirai.

While other IoT botnets such as BASHLITE [86] and Carna [38] preceded Mirai, the latter was the first to emerge as a high-profile DDoS threat. What explains Mirai's sudden rise and massive scale? A combination of factors—efficient spreading based on Internet-wide scanning, rampant use of insecure default passwords in IoT products, and the insight that keeping the botnet's behavior simple would allow it to infect many heterogeneous devices—all played a role. Indeed, Mirai has spawned many variants that follow the same infection strategy, leading to speculation that "IoT botnets are the new normal of DDoS attacks" [64].

In this paper, we investigate the precipitous rise of Mirai and the fragile IoT ecosystem it has subverted. We present longitudinal measurements of the botnet's growth, composition, evolution, and DDoS activities from August 1, 2016 to February 28, 2017. We draw from a diverse set of vantage points including network telescope probes, Internet-wide banner scans, IoT honeypots, C2 milkers, DNS traces, and logs provided by attack victims. These unique datasets enable us to conduct the first comprehensive analysis of Mirai and posit technical and non-technical defenses that may stymie future attacks.

We track the outbreak of Mirai and find the botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady state population of 200,000–300,000 infections. These bots fell into a narrow band of geographic regions and autonomous systems, with Brazil, Columbia, and Vietnam disproportionately accounting for 41.5% of infections. We confirm that Mirai targeted a variety of IoT and embedded devices ranging from DVRs, IP cameras, routers, and printers, but find Mirai's ultimate device composition was strongly influenced by the market shares and design decisions of a handful of consumer electronics manufacturers.

By statically analyzing over 1,000 malware samples, we document the evolution of Mirai into dozens of variants propagated by multiple, competing botnet operators. These variants attempted to improve Mirai's detection avoidance techniques, add new IoT device targets, and introduce additional DNS resilience. We find that Mirai harnessed its evolving capabilities to launch over 15,000 attacks against not only high-profile targets (e.g., Krebs

*Denotes primary, lead, or "first" author

Demystifying the Mirai Botnet

Zakir Durumeric
zakir@cs.stanford.edu

Stanford | ENGINEERING
Computer Science