CSCI-UA.9480
Introduction to Computer Security

Session 2.2
Denial of Service

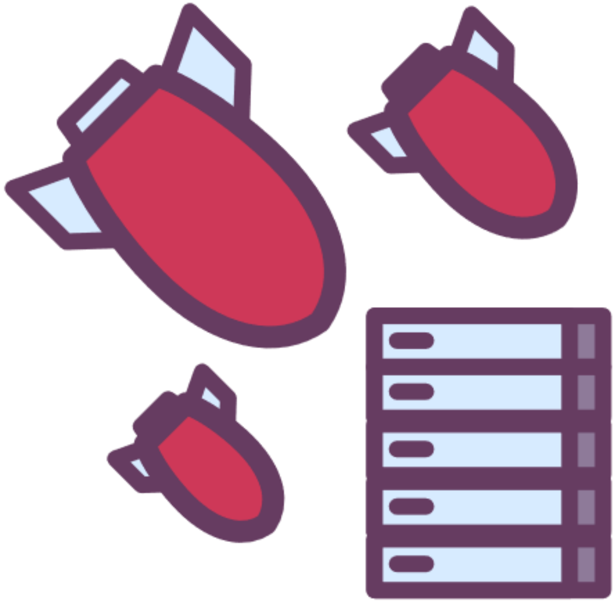
Prof. Nadim Kobeissi

Defining Denial of Service

2.2a

What is a Denial of Service attack?

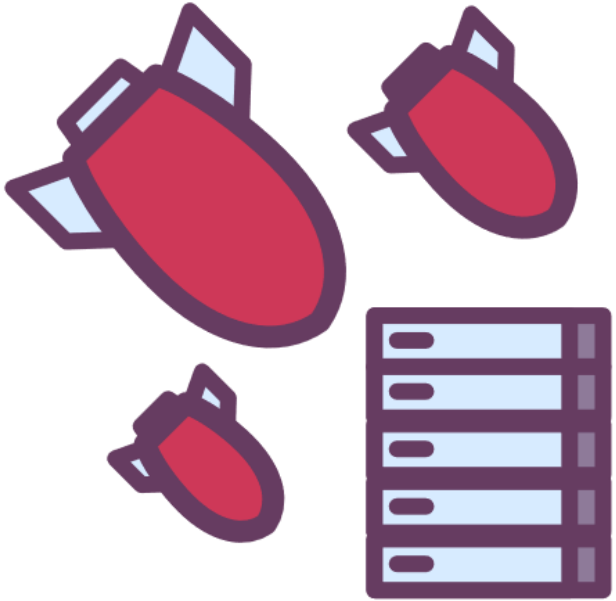
An attack *"where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet."*



What is a Denial of Service attack?

Some resource is being starved by an adversary:

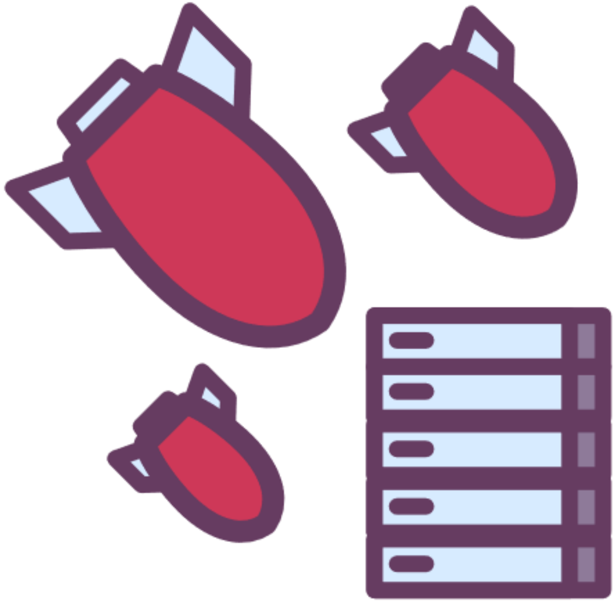
- Network overload?
- CPU overload?
- Memory overload?



What is a Denial of Service attack?

Some resource is being starved by an adversary:

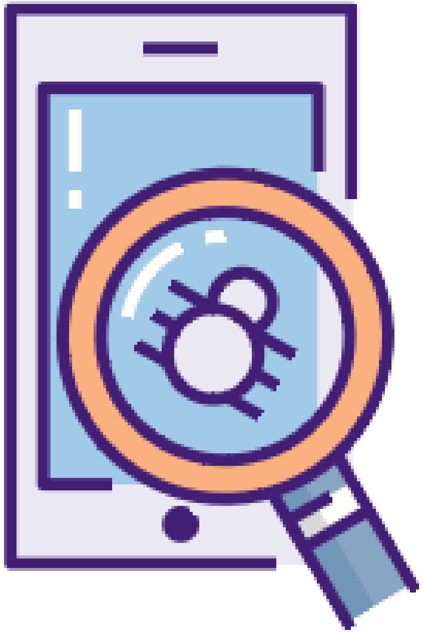
- Network overload: send too many packets.
- CPU/memory overload: force the server to carry out too many password stretching instances.
- Application overload: send too many database/API requests.



Examples of Denial of Service vectors.

UDP flood: unlike TCP, UDP has no flow control built in.

- *Fork bombs*: `:(){ :|: & };:`
- *SYN flood:* Initiate several TCP connections but never complete (ACK) them.
- *LAND attack:* Craft a TCP packet where the source and destination IP addresses are both equal to the victim’s IP.
- *Malformed packets:* exploit parsing errors.



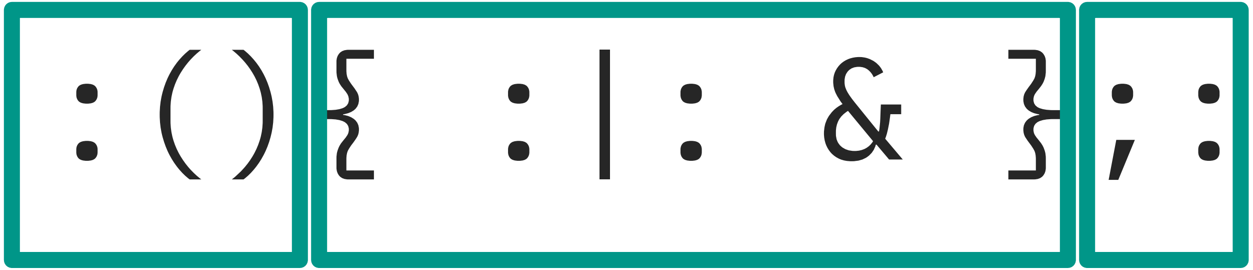
Test your knowledge!

Can you figure out why the following Bash command would be a “fork bomb”?

```
:(){ :|: & };:
```

Test your knowledge!

Can you figure out why the following Bash command would be a “fork bomb”?



```
:(){ :|: & };:
```

Define a function called “:”

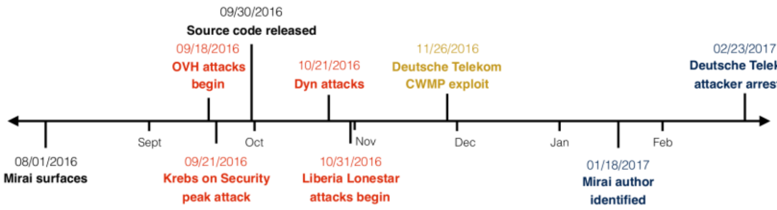
Run “:”, pipe output to “:” executed in the background.

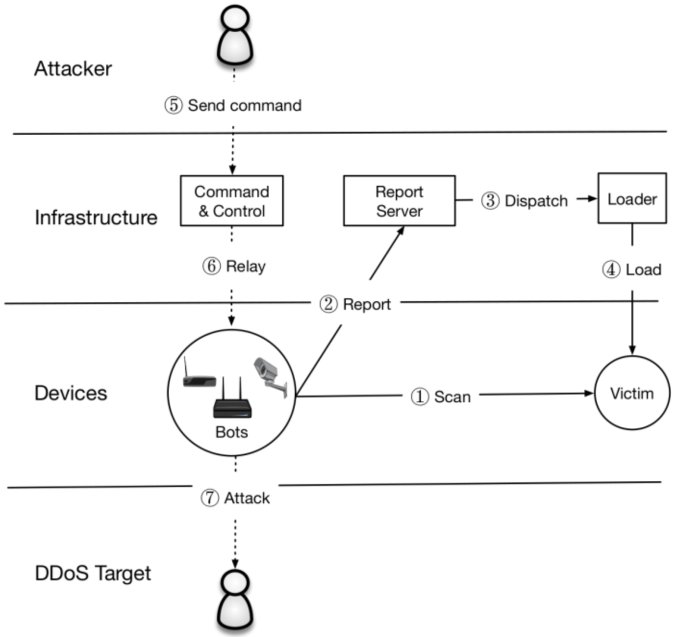
Run “;” for the first time.

DDoS: Distributed Denial of Service.

Example: Mirai botnet (600,000+ victims):

- Caused serious damage to many leading hosting providers (e.g. OVH, Dyn…)
- Among the highest ever recorded throughput for DoS attacks.

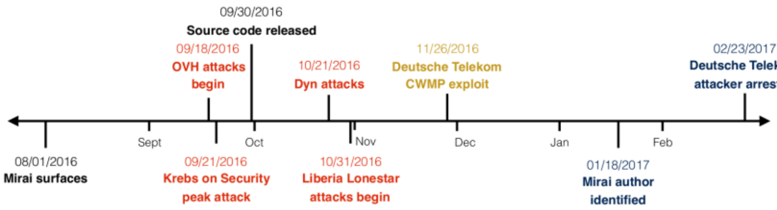


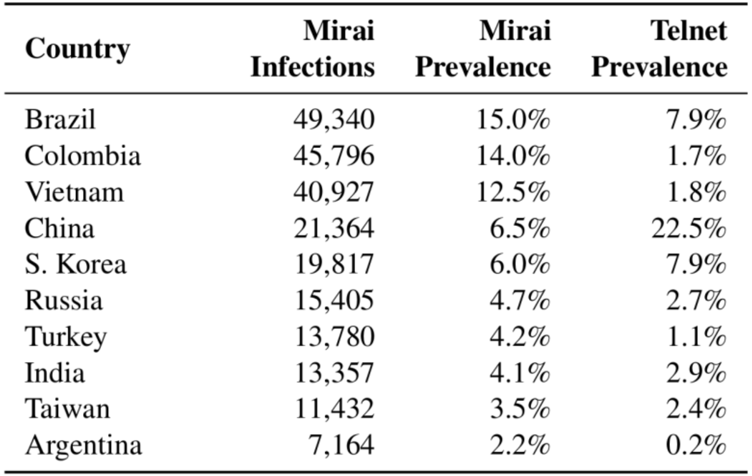


DDoS: Distributed Denial of Service.

Example: Mirai botnet (600,000+ victims):

- Caused serious damage to many leading hosting providers (e.g. OVH, Dyn…)
- Among the highest ever recorded throughput for DoS attacks.



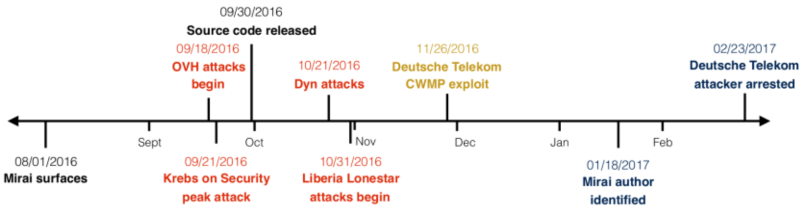


Country	Mirai Infections	Mirai Prevalence	Telnet Prevalence
Brazil	49,340	15.0%	7.9%
Colombia	45,796	14.0%	1.7%
Vietnam	40,927	12.5%	1.8%
China	21,364	6.5%	22.5%
S. Korea	19,817	6.0%	7.9%
Russia	15,405	4.7%	2.7%
Turkey	13,780	4.2%	1.1%
India	13,357	4.1%	2.9%
Taiwan	11,432	3.5%	2.4%
Argentina	7,164	2.2%	0.2%

DDoS: Distributed Denial of Service.

Example: Mirai botnet (600,000+ victims):

- Caused serious damage to many leading hosting providers (e.g. OVH, Dyn…)
- Among the highest ever recorded throughput for DoS attacks.



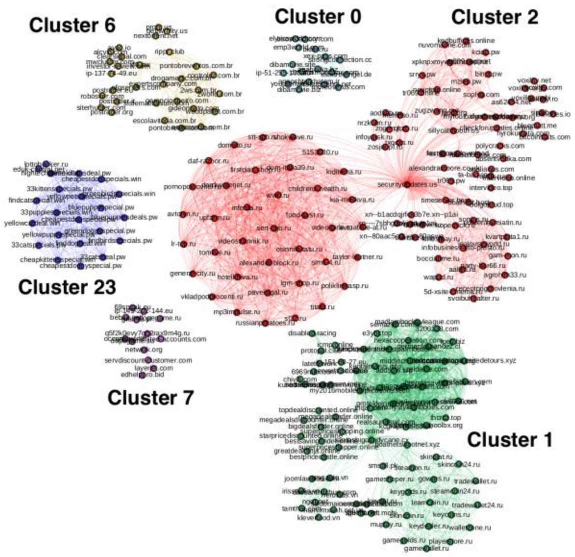
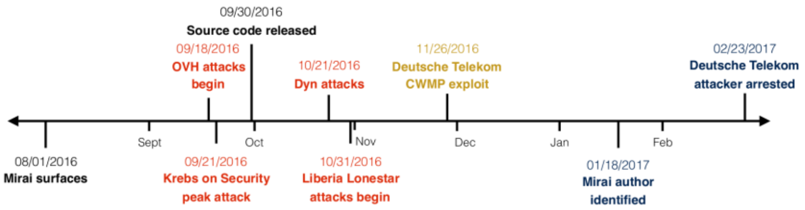


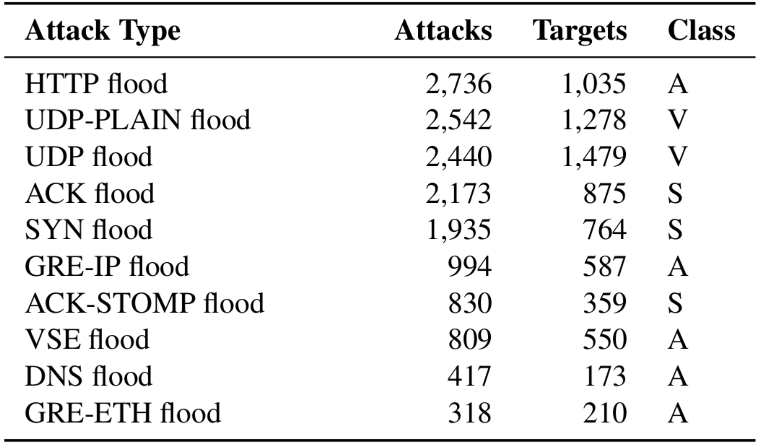
Figure 7: **C2 Domain Relationships**—We visualize related C2 infrastructure, depicting C2 domains as nodes and shared IPs as edges between two domains. The top six clusters by C2 domain count consisted of highly connected components, which represent agile, long-lived infrastructures in use by botmasters.

DDoS: Distributed Denial of Service.

Example: Mirai botnet (600,000+ victims):

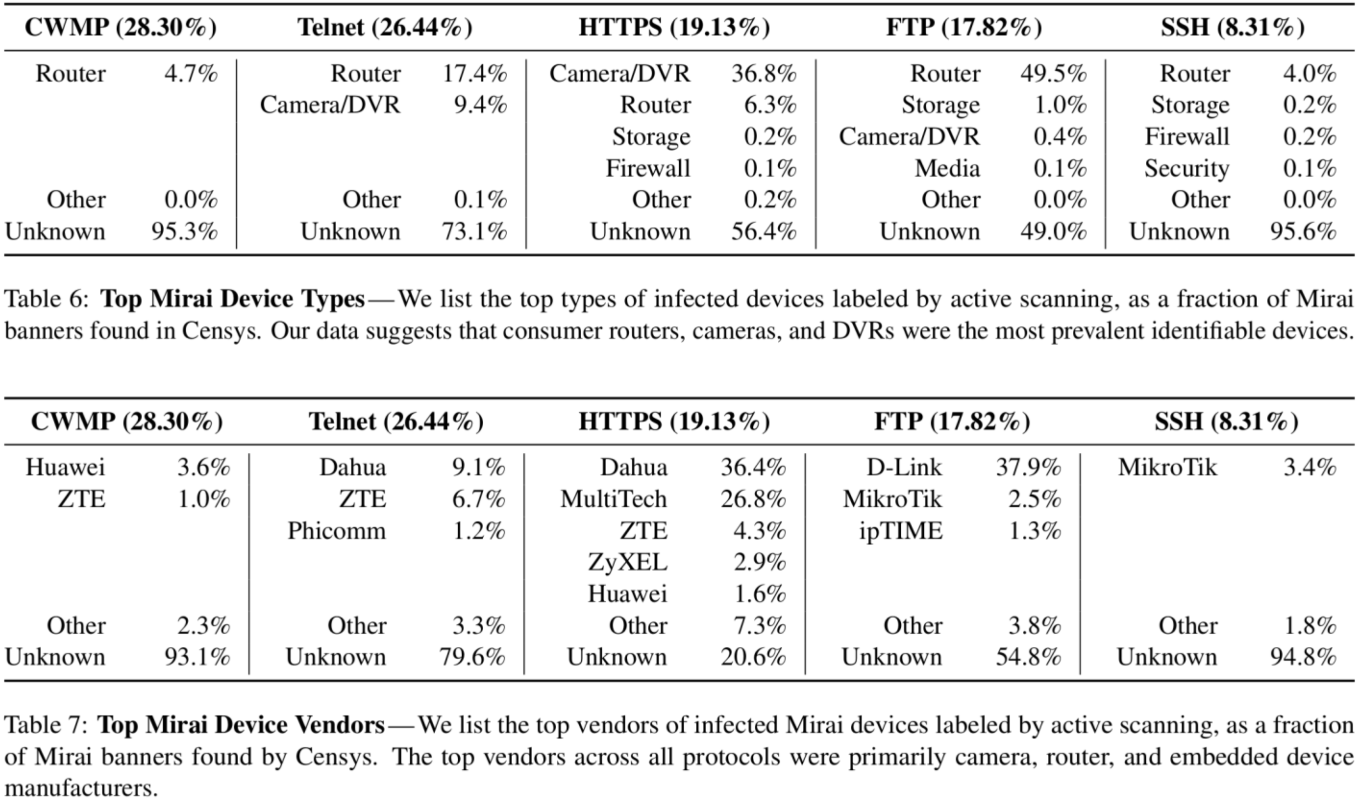
- Caused serious damage to many leading hosting providers (e.g. OVH, Dyn...)
- Among the highest ever recorded throughput for DoS attacks.





Attack Type	Attacks	Targets	Class
HTTP flood	2,736	1,035	A
UDP-PLAIN flood	2,542	1,278	V
UDP flood	2,440	1,479	V
ACK flood	2,173	875	S
SYN flood	1,935	764	S
GRE-IP flood	994	587	A
ACK-STOMP flood	830	359	S
VSE flood	809	550	A
DNS flood	417	173	A
GRE-ETH flood	318	210	A

DDoS: Mirai botnet device composition.



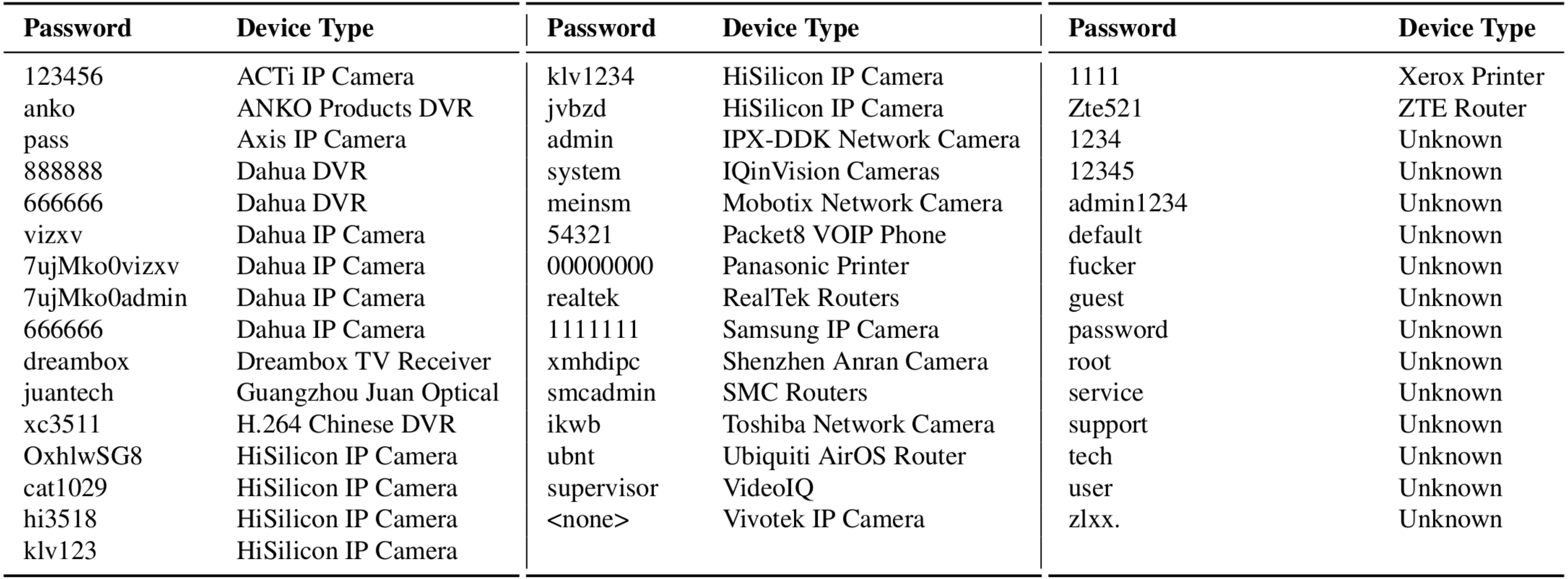
CWMP (28.30%)		Telnet (26.44%)		HTTPS (19.13%)		FTP (17.82%)		SSH (8.31%)	
Router	4.7%	Router	17.4%	Camera/DVR	36.8%	Router	49.5%	Router	4.0%
		Camera/DVR	9.4%	Router	6.3%	Storage	1.0%	Storage	0.2%
				Storage	0.2%	Camera/DVR	0.4%	Firewall	0.2%
				Firewall	0.1%	Media	0.1%	Security	0.1%
Other	0.0%	Other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

Table 6: **Top Mirai Device Types**—We list the top types of infected devices labeled by active scanning, as a fraction of Mirai banners found in Censys. Our data suggests that consumer routers, cameras, and DVRs were the most prevalent identifiable devices.

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%

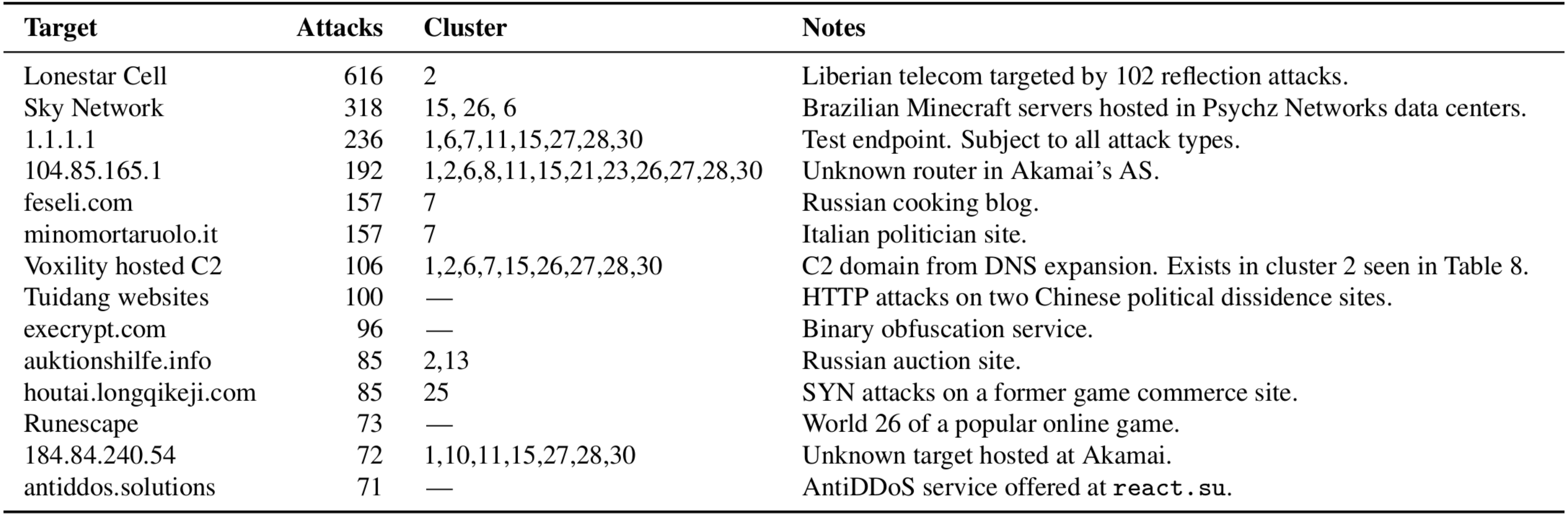
Table 7: **Top Mirai Device Vendors**—We list the top vendors of infected Mirai devices labeled by active scanning, as a fraction of Mirai banners found by Censys. The top vendors across all protocols were primarily camera, router, and embedded device manufacturers.

DDoS: Mirai botnet device composition.



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				

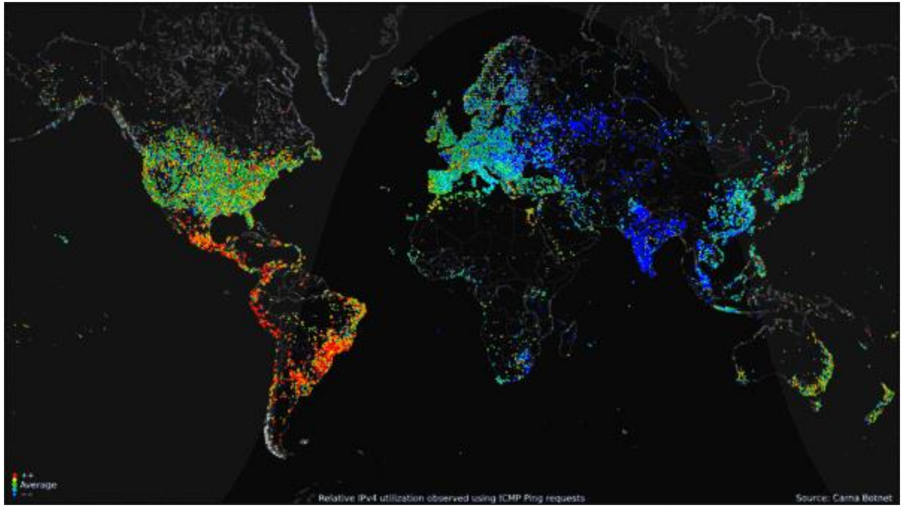
DDoS: Mirai botnet victims.



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`.

Examples of other botnets.

- *Srizbi botnet*: responsible for most of the spam in the world at some point.
- *Carna botnet*: used for estimating the size of the Internet.



Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

Another example: “Project Chanology”

Instead of a slide, at this point in the class we will watch this short documentary on Project Chanology:

https://www.youtube.com/watch?v=vRb6L7SCSro

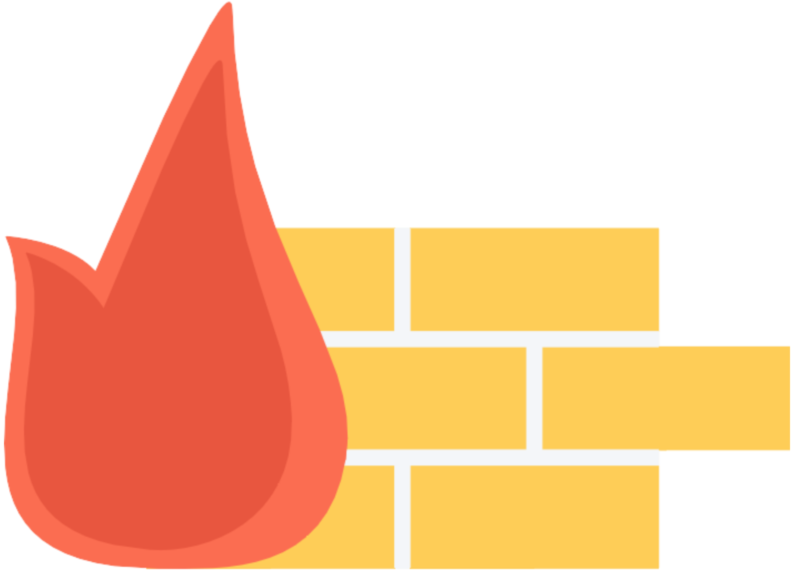
Mitigating Denial of Service Attacks

2.2b

Basic defenses against Denial of Service.

Firewalls, switches, and routers at ingress points of a network that use packet filtering.

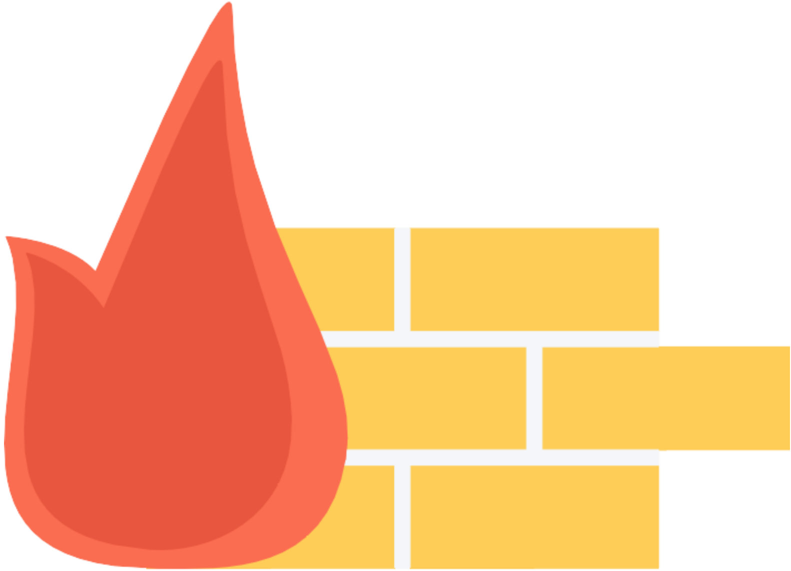
- Build models of normal and abnormal behavior and flag abnormal behavior.
- Intrusion detection systems that look for attack signatures or abnormally high rates of traffic or both.
- CAPTCHAs to ensure that a human and not a bot is carrying out the request.



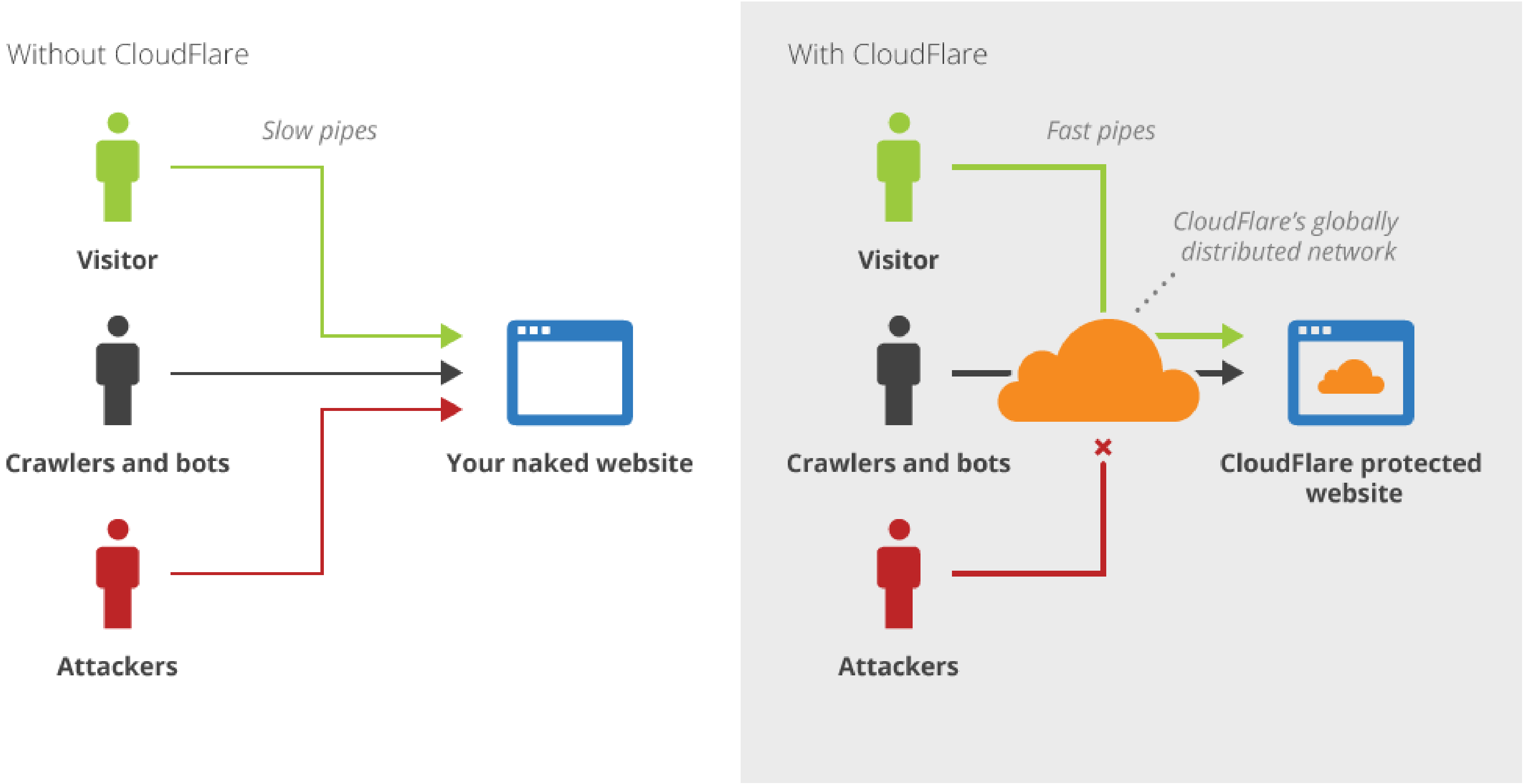
Basic defenses against Denial of Service.

CAPTCHAs to ensure that a human and not a bot is carrying out the request.

- Proof of work: request hashes, etc.



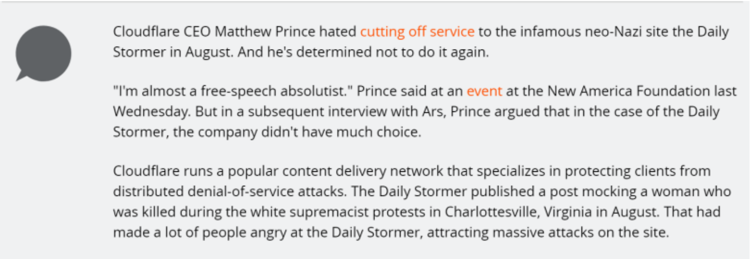
Content Delivery Networks: CloudFlare.



Content Delivery Networks (CDNs).

Akamai, CloudFlare, Amazon CloudFront, Microsoft Azure…

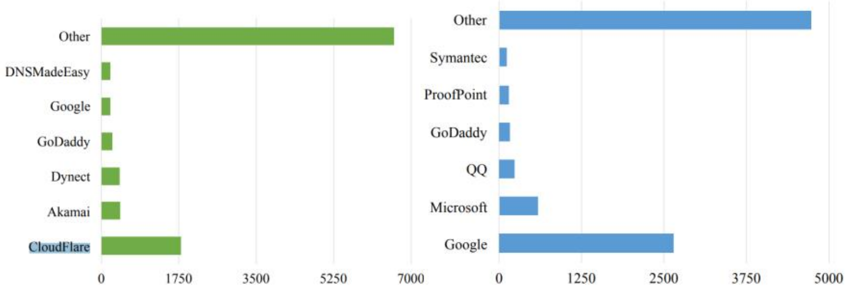
- Concerns regarding centralizing of Internet traffic (i.e. man-in-the-middle capabilities).
- Questions w.r.t. freedom of expression online:



Cloudflare CEO Matthew Prince hated cutting off service to the infamous neo-Nazi site the Daily Stormer in August. And he's determined not to do it again.

"I'm almost a free-speech absolutist." Prince said at an event at the New America Foundation last Wednesday. But in a subsequent interview with Ars, Prince argued that in the case of the Daily Stormer, the company didn't have much choice.

Cloudflare runs a popular content delivery network that specializes in protecting clients from distributed denial-of-service attacks. The Daily Stormer published a post mocking a woman who was killed during the white supremacist protests in Charlottesville, Virginia in August. That had made a lot of people angry at the Daily Stormer, attracting massive attacks on the site.



(a) Name Servers.

(b) Mail Servers.

Fig. 2: Provider repartition among the Alexa Top 10,000 global sites, as of October 2016. Notably, CloudFlare and Akamai also provide CDN services to domains under their name servers, allowing them stronger control over HTTP traffic.

Next time: Designing Secure Network Systems

2.3