2550 Intro to cybersecurity

L26: DDOS and Review

abhi shelat

Today's plan

1. P/F deadline.
2. Lecture summaries
3. Videos.
4. Course Evaluation
5. 1:1 signups.

Botnets, Distributed Denial of Service (DDoS)

Review of the Course.

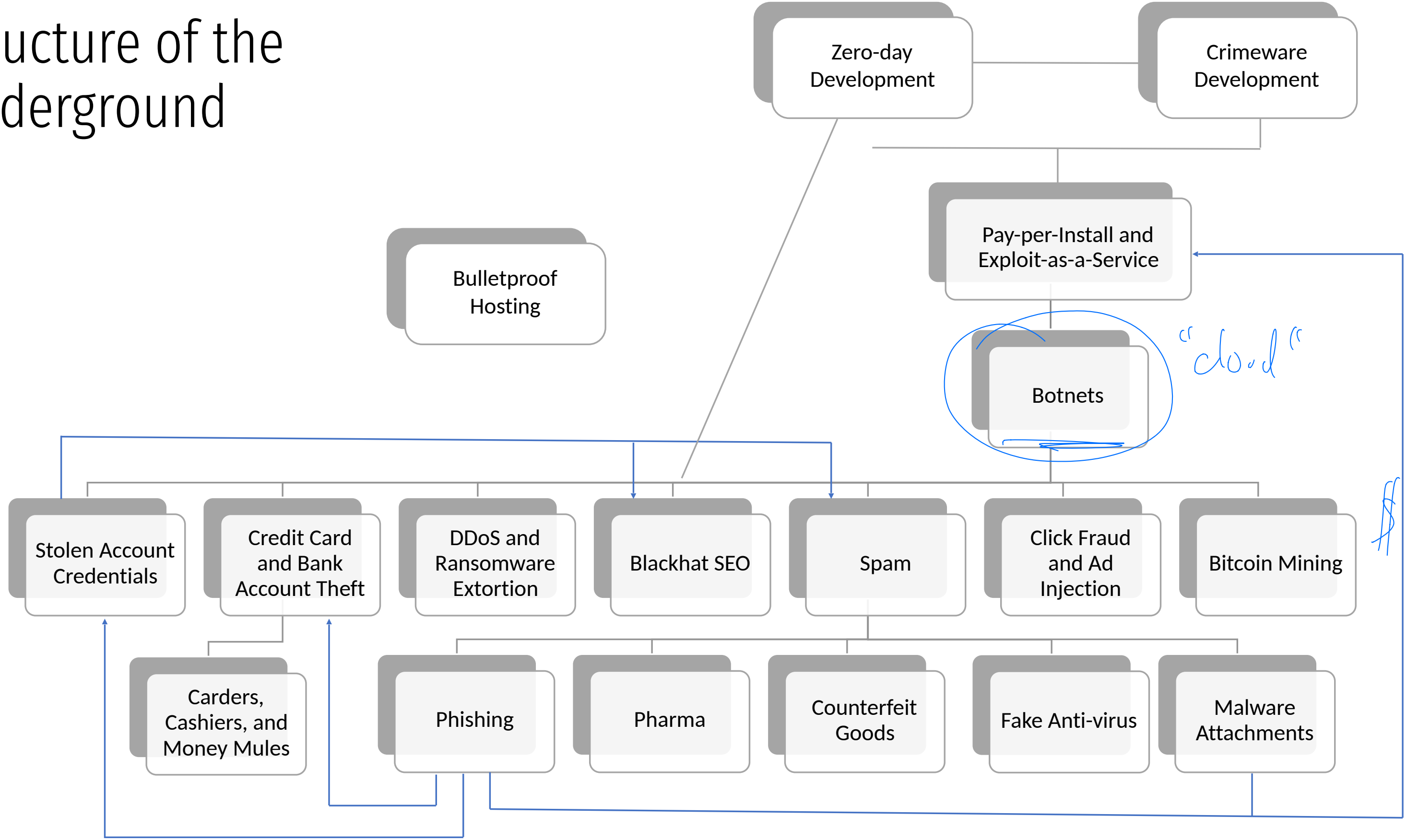
Crimeware

Malware, Spyware, Adware, Ransomware, Trojans, RATs, Bots…

Botnets

The backbone of the underground

Structure of the Underground



Zero-day Development

Crimeware Development

Pay-per-Install and Exploit-as-a-Service

Bulletproof Hosting

Botnets

"cloud"

Stolen Account Credentials

Credit Card and Bank Account Theft

DDoS and Ransomware Extortion

Blackhat SEO

Spam

Click Fraud and Ad Injection

Bitcoin Mining

$$

Carders, Cashiers, and Money Mules

Phishing

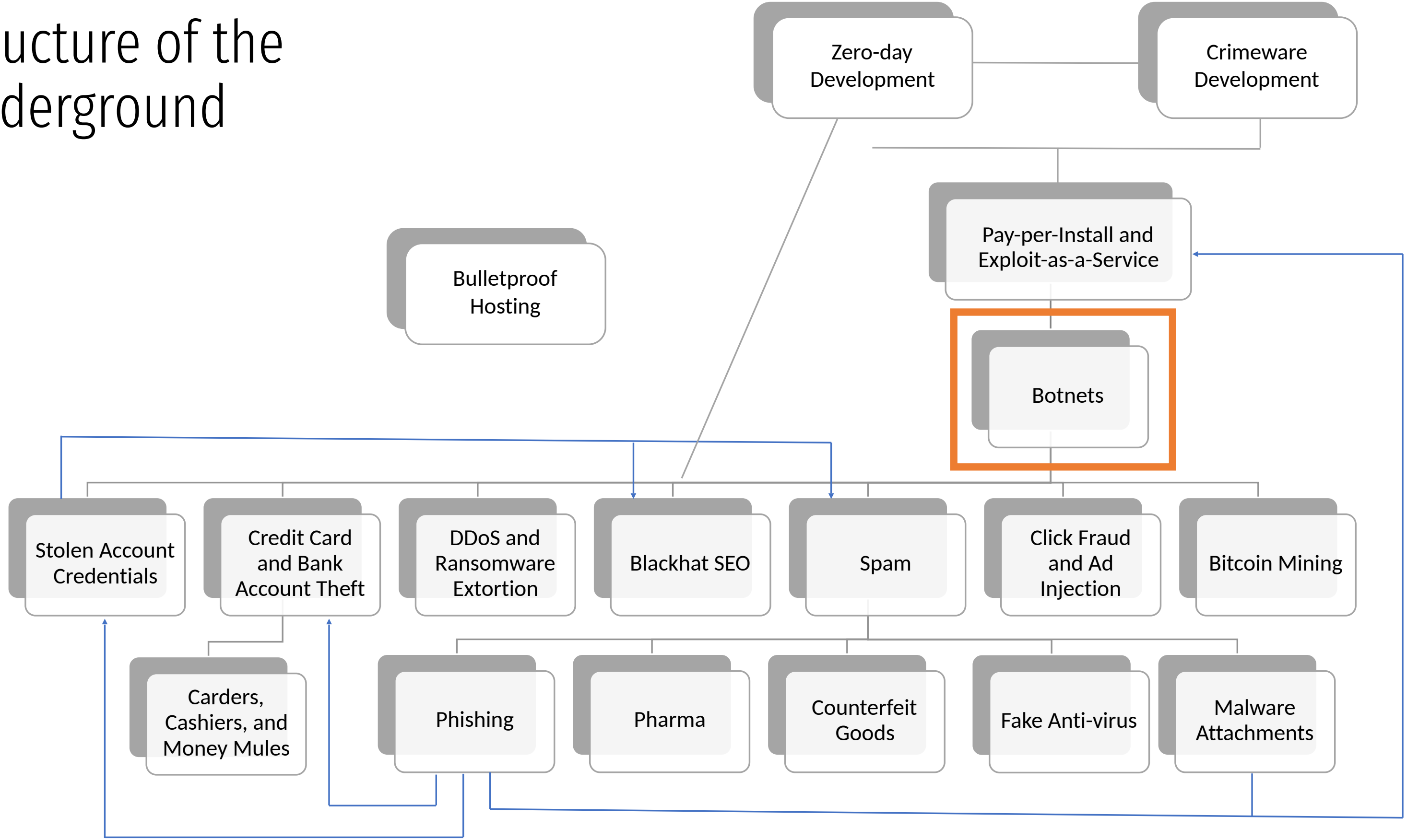
Pharma

Counterfeit Goods

Fake Anti-virus

Malware Attachments

Structure of the Underground


Zero-day Development
Crimeware Development
Bulletproof Hosting
Pay-per-Install and Exploit-as-a-Service
Botnets
Stolen Account Credentials
Credit Card and Bank Account Theft
DDoS and Ransomware Extortion
Blackhat SEO
Spam
Click Fraud and Ad Injection
Bitcoin Mining
Carders, Cashiers, and Money Mules
Phishing
Pharma
Counterfeit Goods
Fake Anti-virus
Malware Attachments

Common Methods of Compromise

1. Malware email attachments
   - Leverages social engineering
   - Attachment may be a malware program in disguise, or…
   - May leverage an exploit in another piece of software

Common Methods of Compromise

1. Malware email attachments
   - Leverages social engineering
   - Attachment may be a malware program in disguise, or…
   - May leverage an exploit in another piece of software
2. Scanning
   - Connect to servers and probe them for known vulnerabilities
   - Brute force remote access credentials, e.g. SSH

IP — 4 bytes

192.168.1.1

0-255

IP ~ 2^{32} ~ 4 billion IP addrs.

Common Methods of Compromise

1. Malware email attachments
   - Leverages social engineering
   - Attachment may be a malware program in disguise, or...
   - May leverage an exploit in another piece of software
2. Scanning
   - Connect to servers and probe them for known vulnerabilities
   - Brute force remote access credentials, e.g. SSH
3. Exploiting browser bugs
   - Known as drive-by exploits or drive-by downloads
   - Get the victim to visit a webpage containing exploits

Malware Attachments

Send spam containing malicious attachments

Use social engineering to trick users into downloading & opening the attachments

Malware Attachments

Send spam containing malicious attachments

Use social engineering to trick users into downloading & opening the attachments

Misleading Icons and File Extensions

funny.jpg.exe

contract.docx.exe

Malware Attachments

Send spam containing malicious attachments

Use social engineering to trick users into downloading & opening the attachments

Misleading Icons and File Extensions

funny.jpg

contract.docx

Malware Attachments

Send spam containing malicious attachments

Use social engineering to trick users into downloading & opening the attachments

Misleading Icons and File Extensions

funny.jpg.exe

contract.docx.exe

Scripting Languages

VisualBasic script macros

Flash and JavaScript

Malware Attachments

Send spam containing malicious attachments

Use social engineering to trick users into downloading & opening the attachments

Misleading Icons and File Extensions

funny.jpg.exe

contract.docx.exe

Scripting Languages

VisualBasic script macros

Flash and JavaScript

Exploitable Vulnerabilities

Any complex file format can potentially trigger exploitable bugs and contain shellcode

From Crimeware to Botnets

Infected machines are a fundamentally valuable resource

- Unique IP addresses for spamming
- Bandwidth for DDoS
- CPU cycles for bitcoin mining
- Credentials

many more. hosting e-commerce sites for drugs

From Crimeware to Botnets

Infected machines are a fundamentally valuable resource

- Unique IP addresses for spamming
- Bandwidth for DDoS
- CPU cycles for bitcoin mining
- Credentials

Early malware monetized these resources directly

- Infection and monetization were tightly coupled

From Crimeware to Botnets

Infected machines are a fundamentally valuable resource

- Unique IP addresses for spamming
- Bandwidth for DDoS
- CPU cycles for bitcoin mining
- Credentials

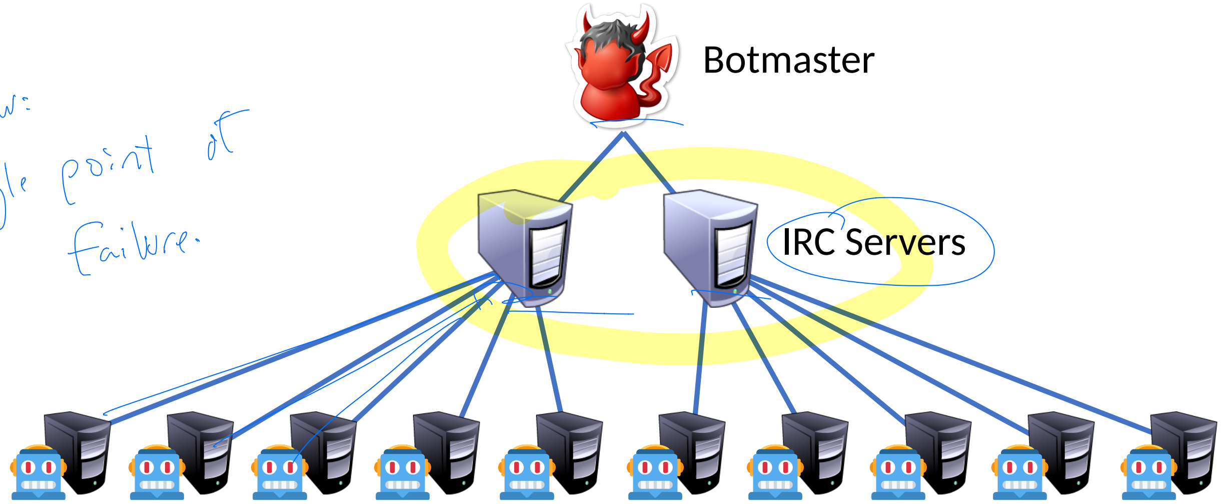
Early malware monetized these resources directly

- Infection and monetization were tightly coupled

Botnets allow criminals to rent access to infected hosts

- Infrastructure as a service, i.e. the cloud for criminals
- Command and Control (C&C) infrastructure for controlling bots
- Enables huge-scale criminal campaigns

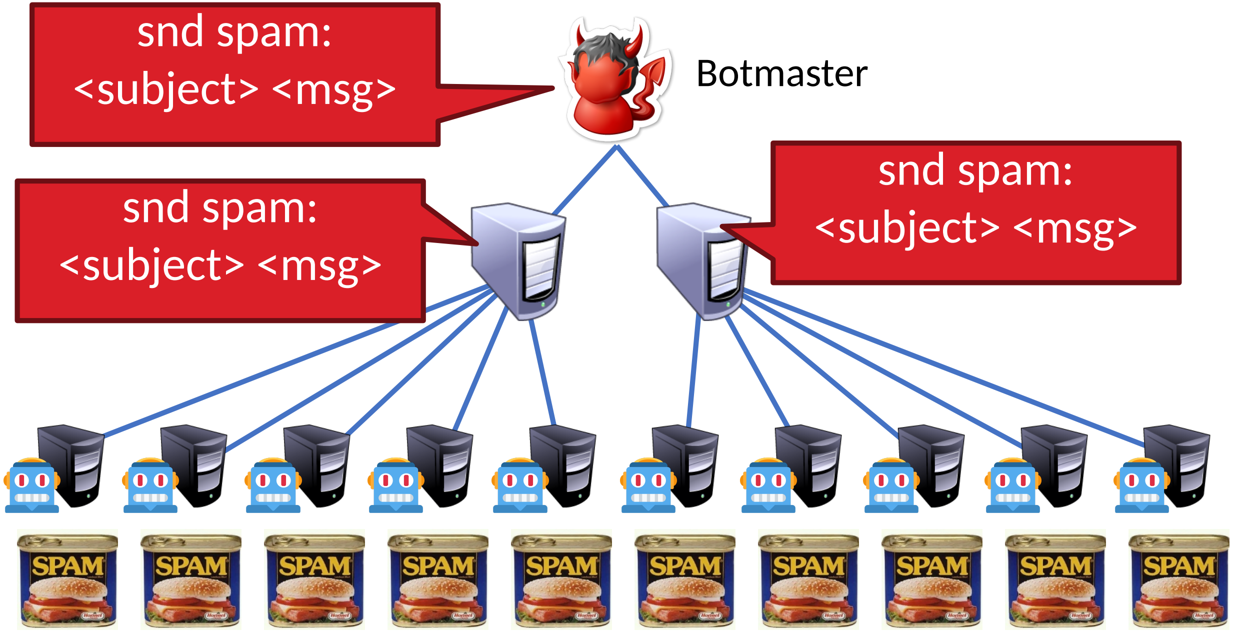
Old-School C&C: IRC Channels



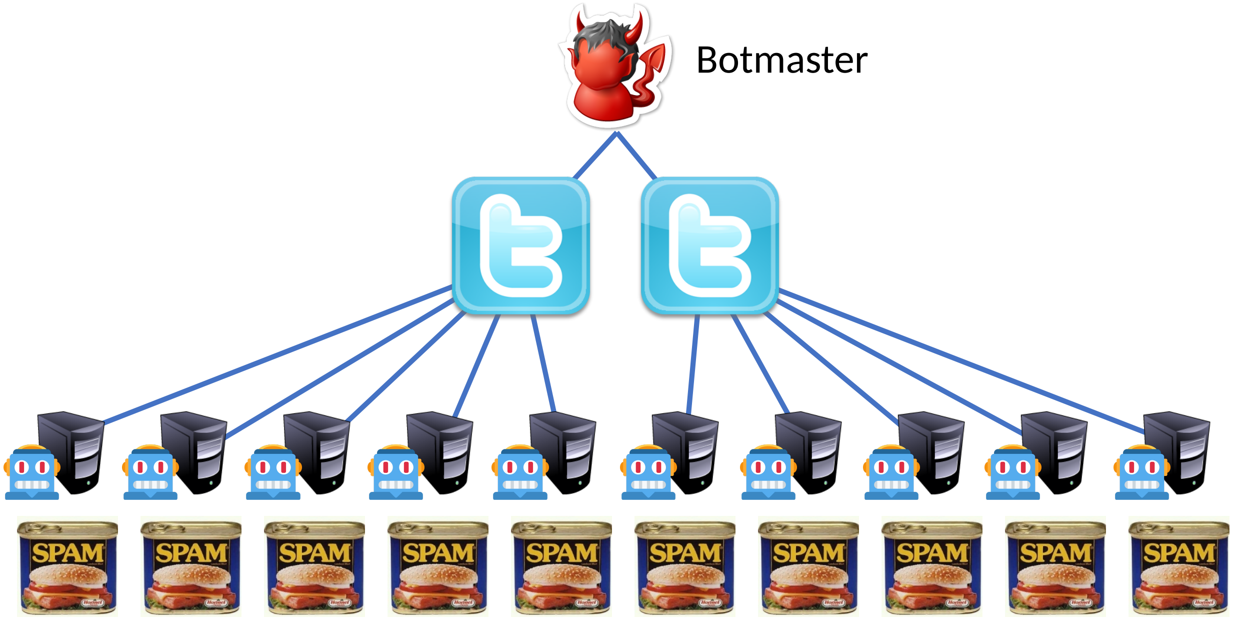
FLAW:
single point of
failure.

infected nodes

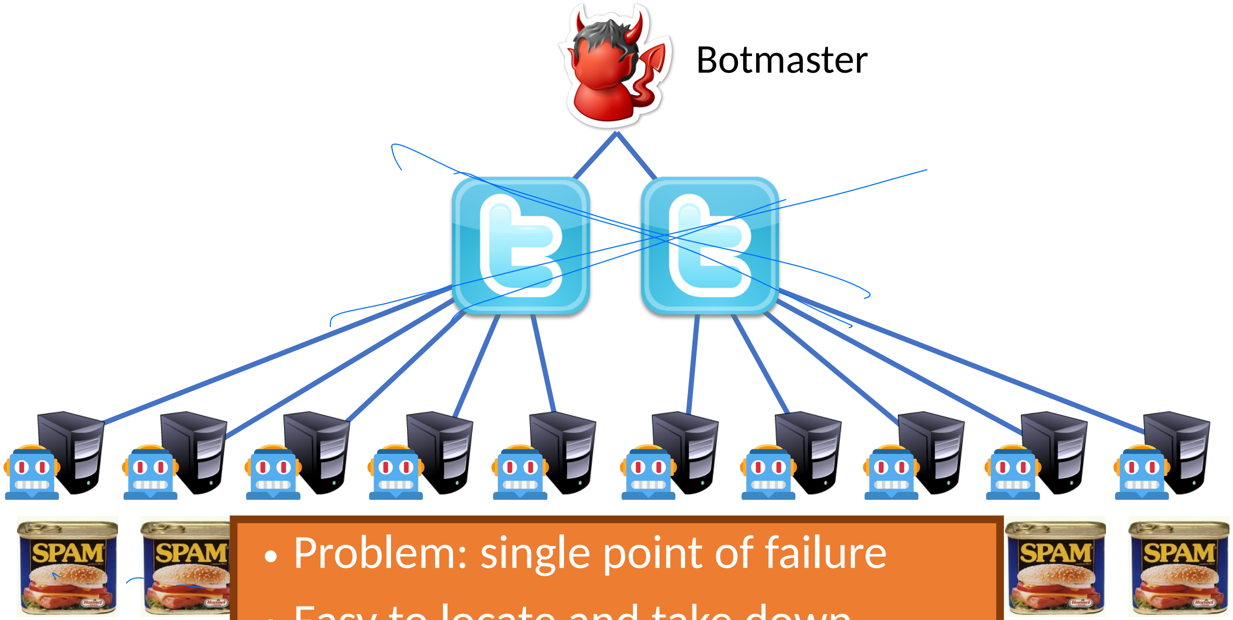
Old-School C&C: IRC Channels



Old-School C&C: IRC Channels

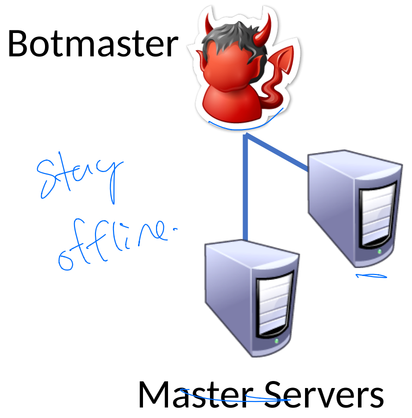


Old-School C&C: IRC Channels

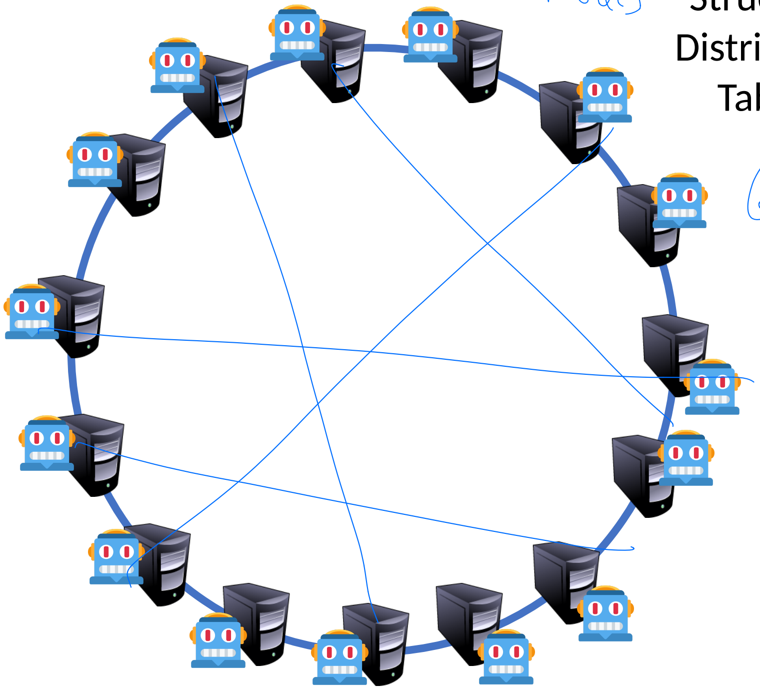


- Problem: single point of failure
- Easy to locate and take down

P2P Botnets



Stay offline.

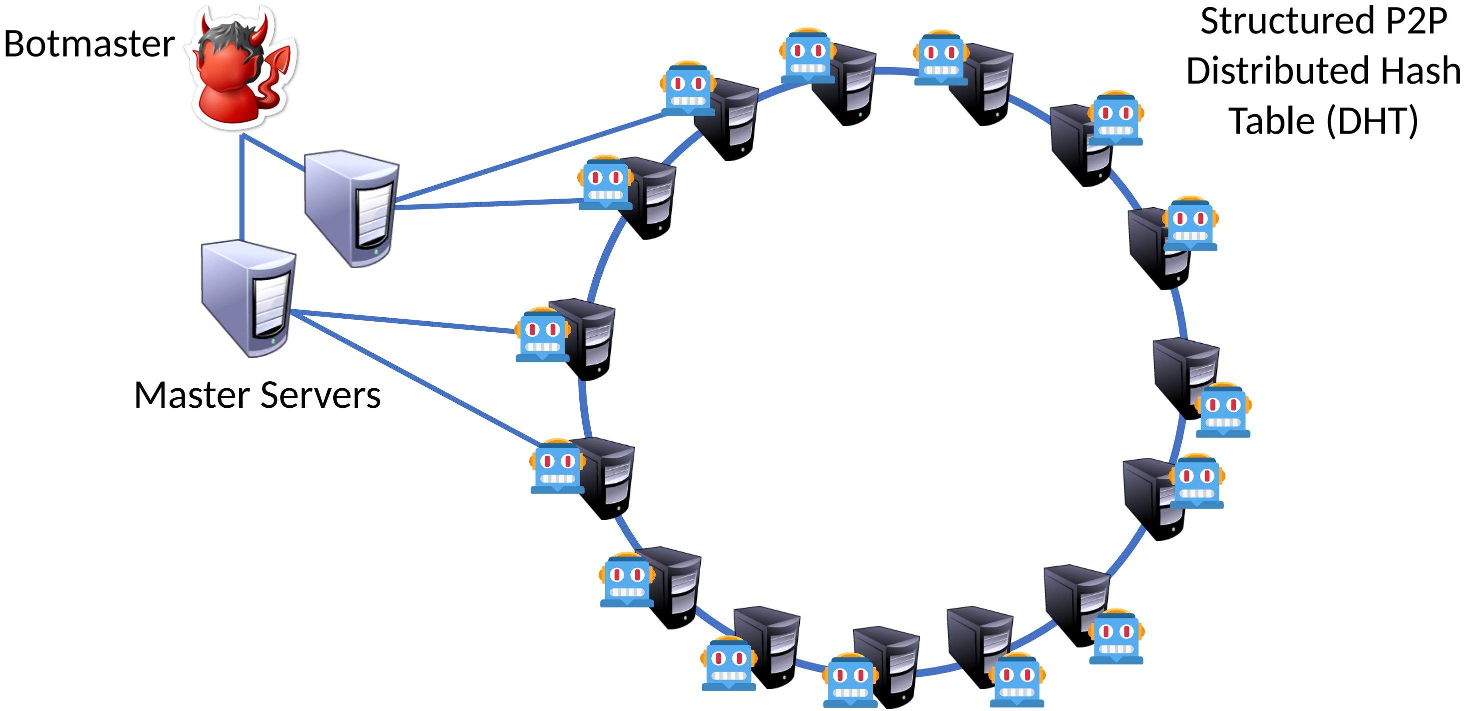


infected nodes

Structured P2P
Distributed Hash
Table (DHT)

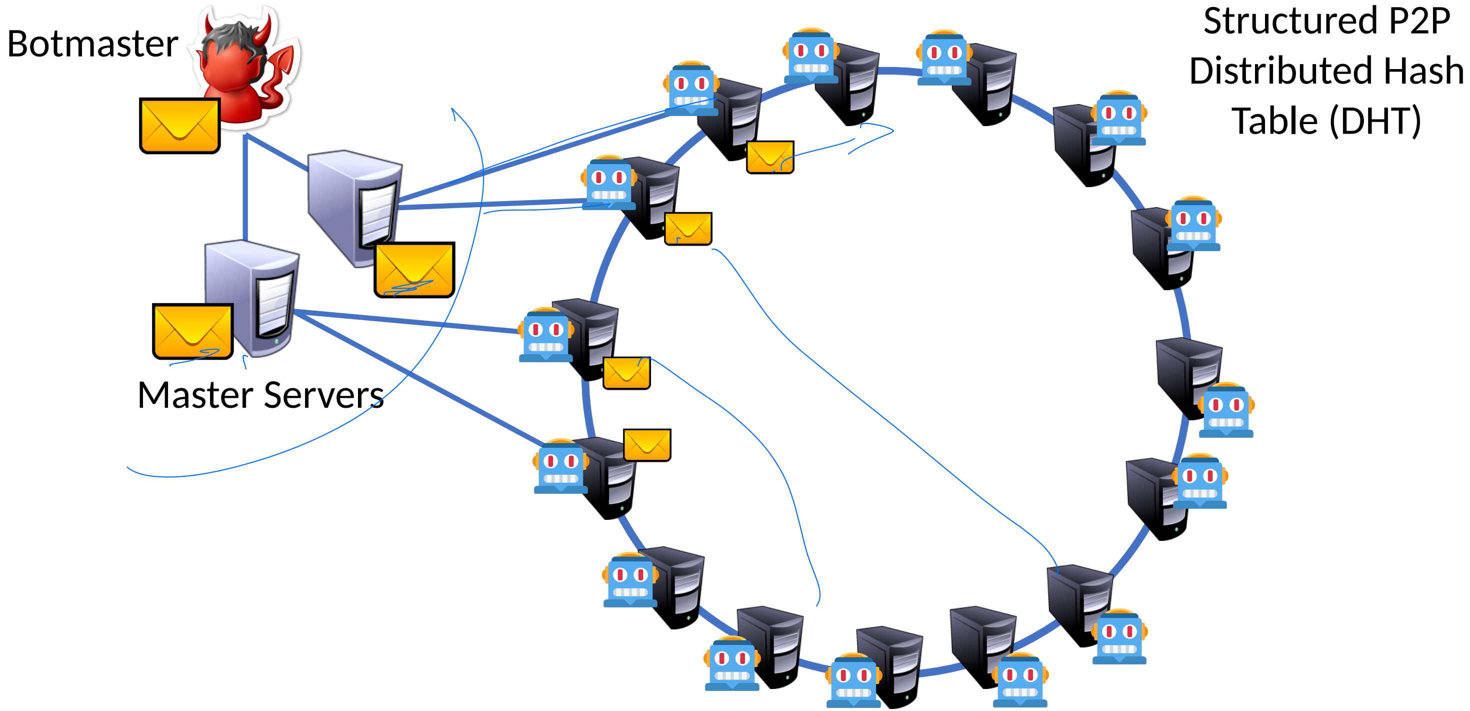
6-d of
Separation

P2P Botnets

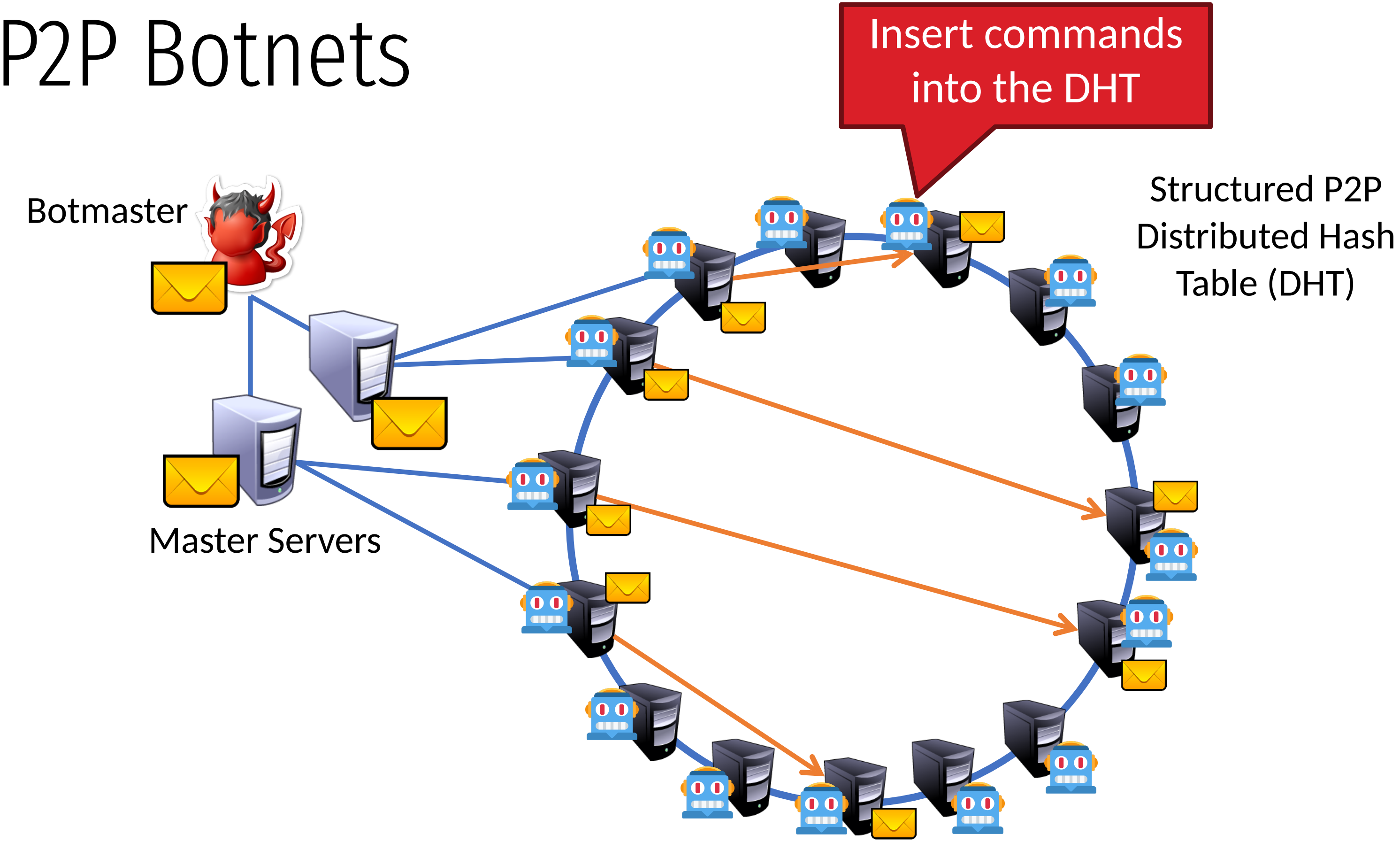

Botmaster
Master Servers
Structured P2P
Distributed Hash
Table (DHT)

P2P Botnets

instructions propogate thru the network



P2P Botnets



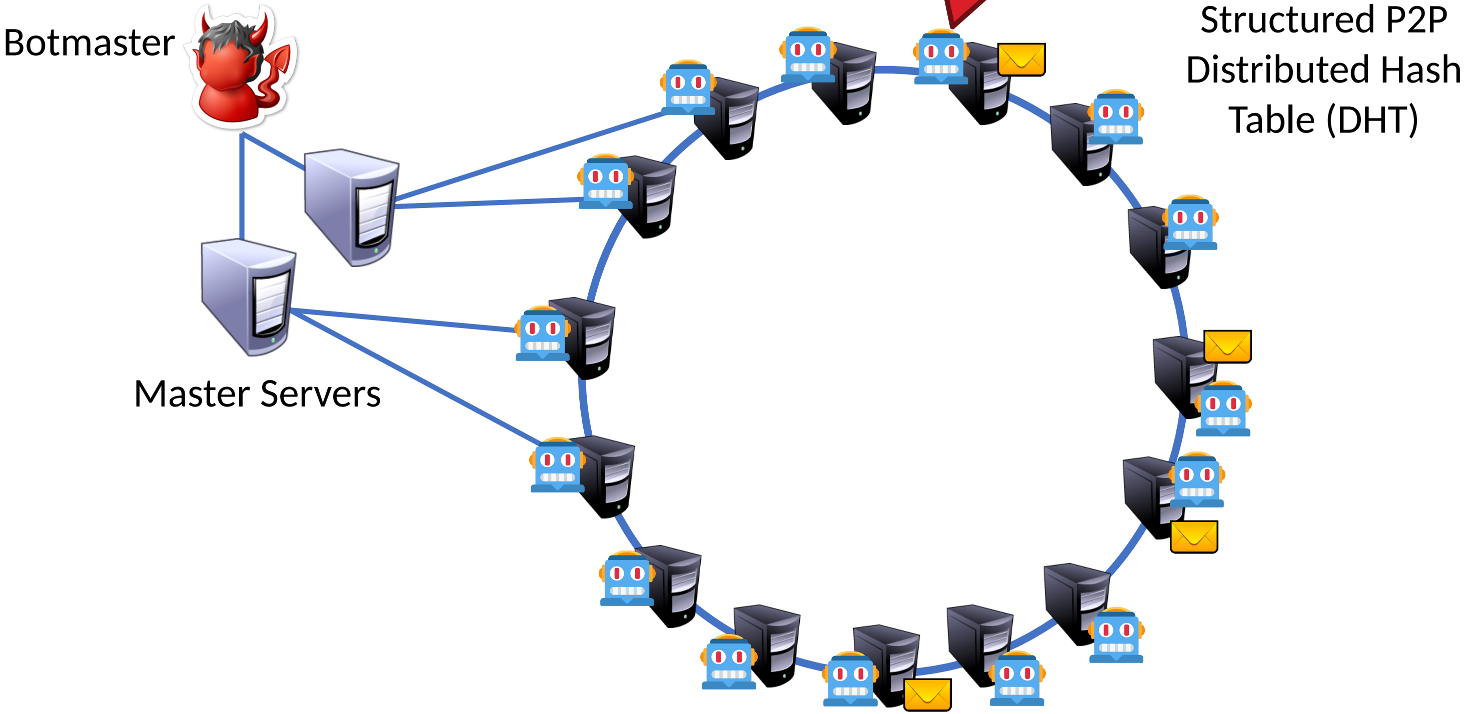
Insert commands into the DHT

Botmaster

Master Servers

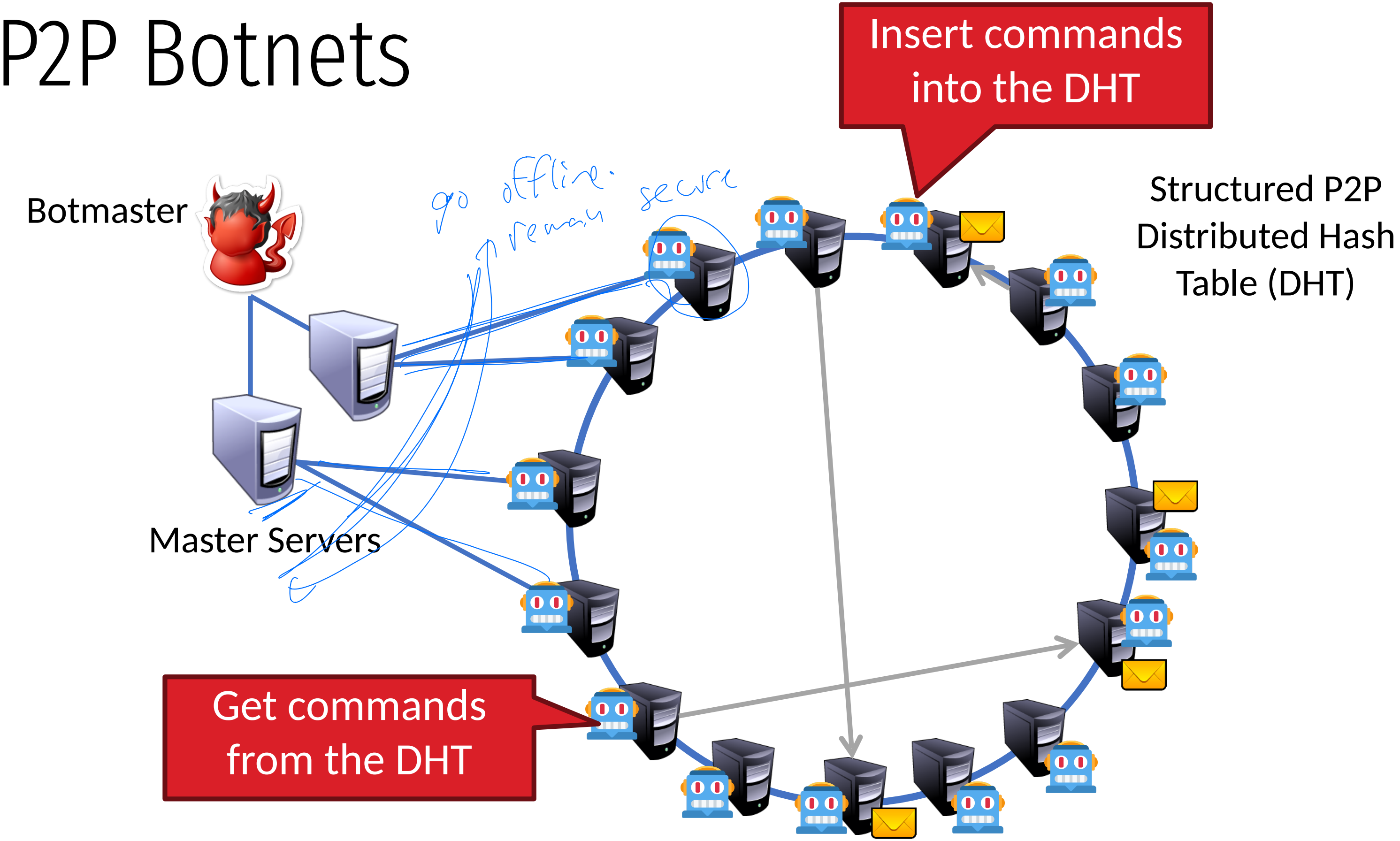
Structured P2P Distributed Hash Table (DHT)

P2P Botnets



Insert commands into the DHT

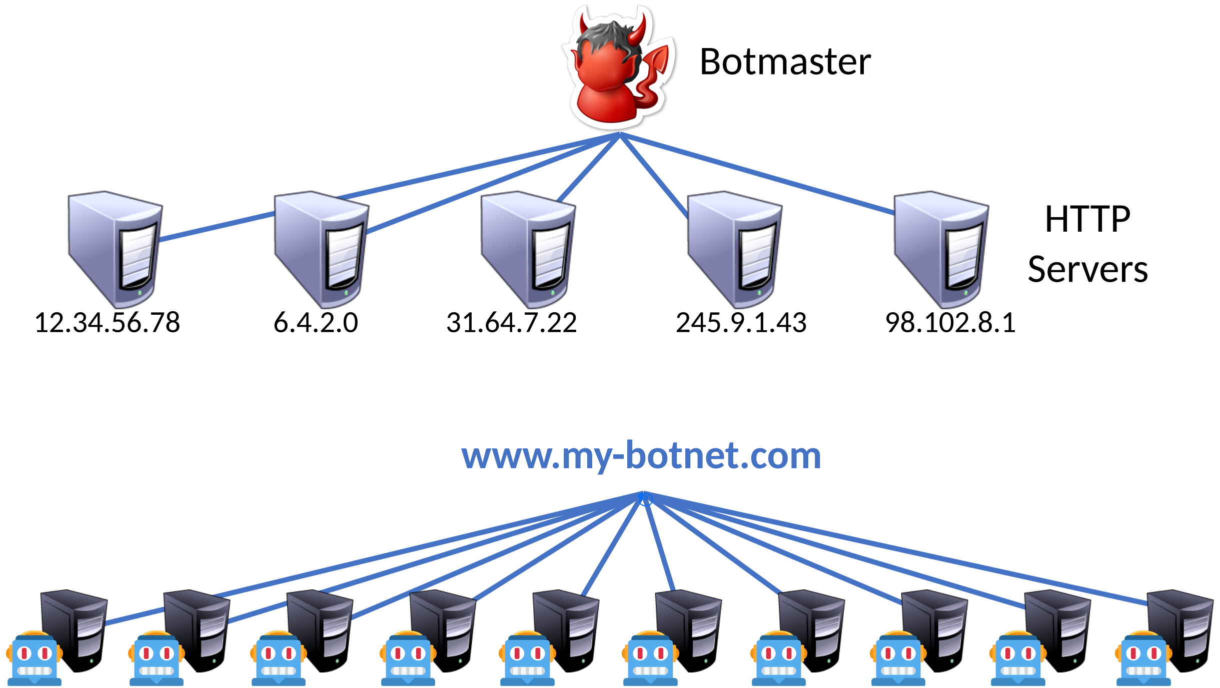
P2P Botnets



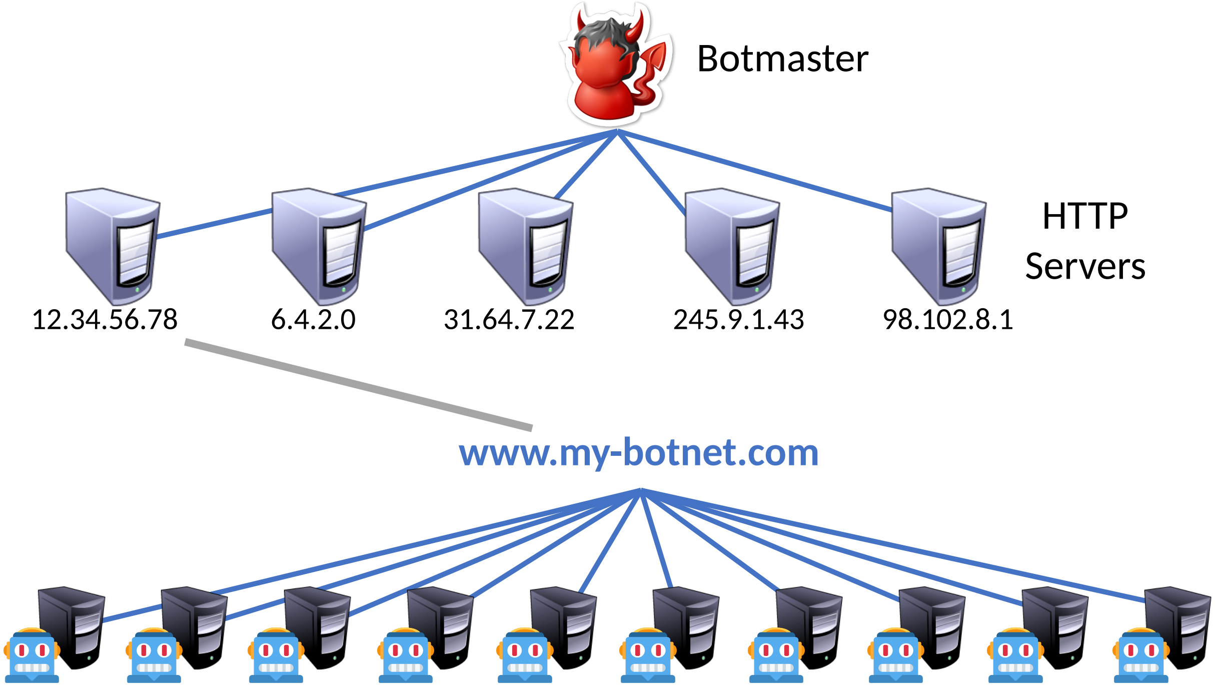
Insert commands into the DHT

Get commands from the DHT

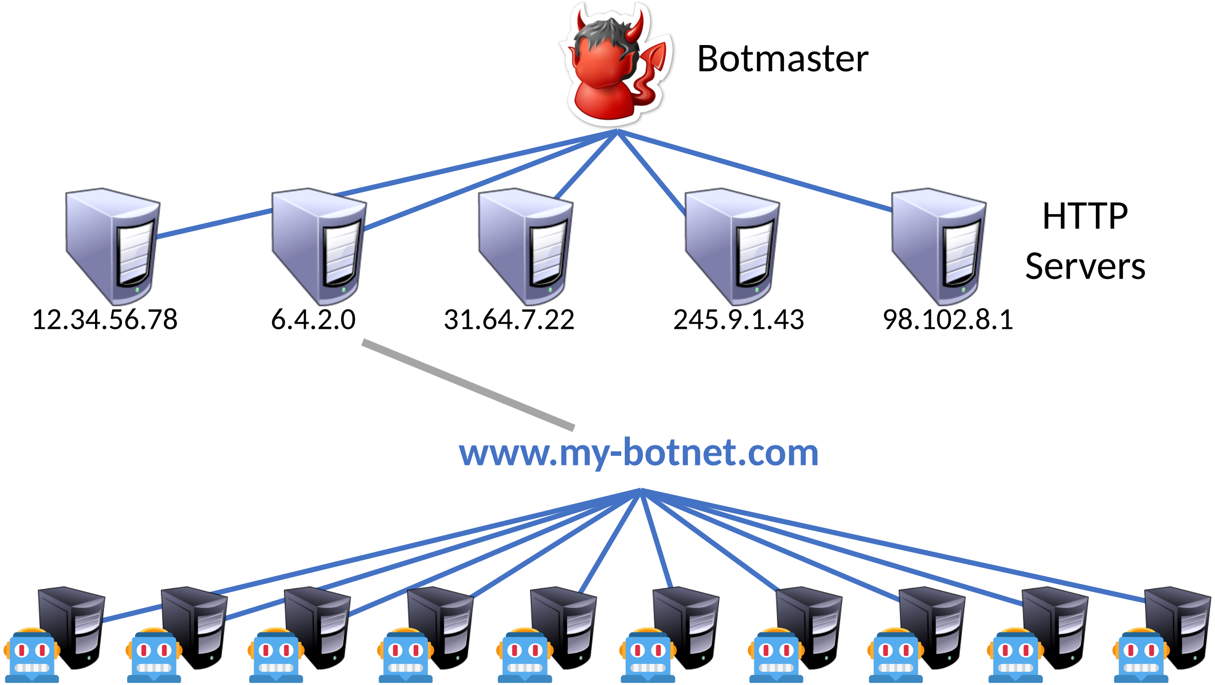
Fast Flux DNS



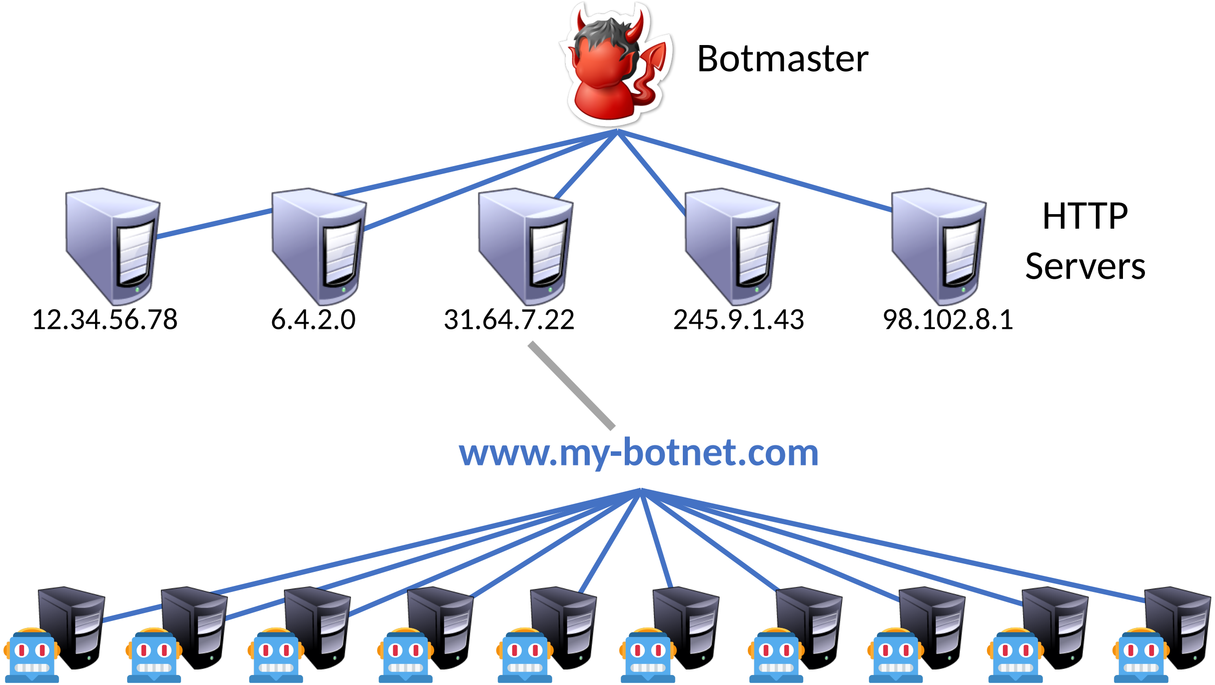
Fast Flux DNS



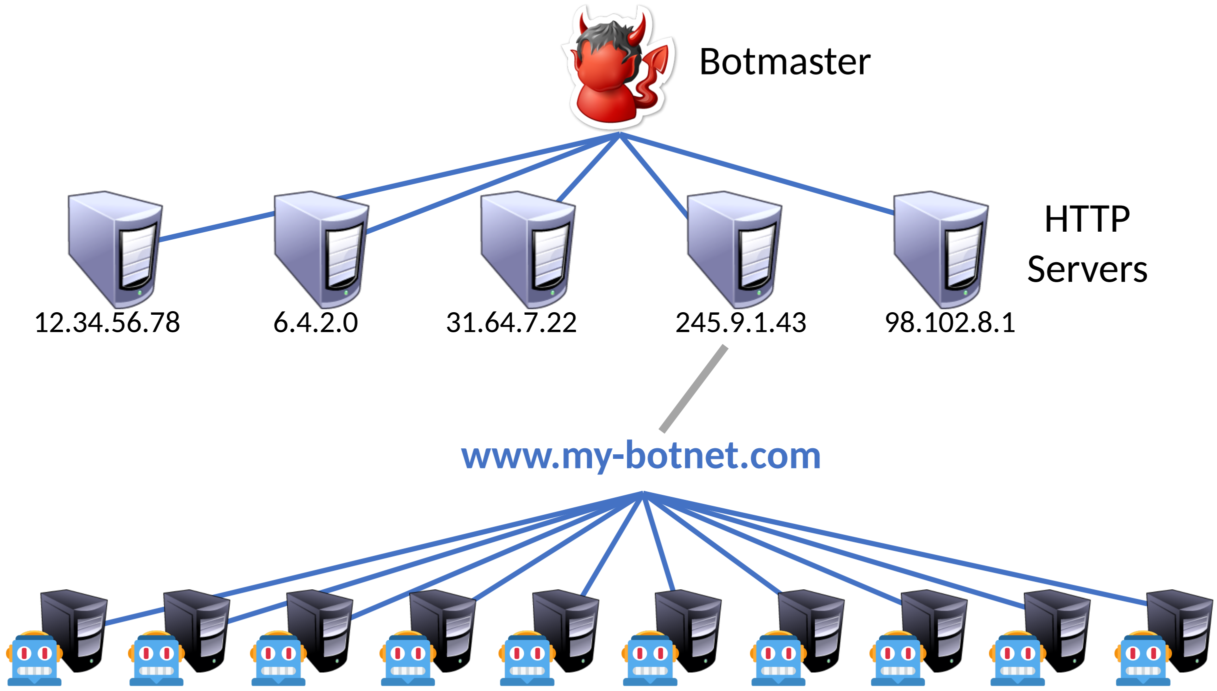
Fast Flux DNS



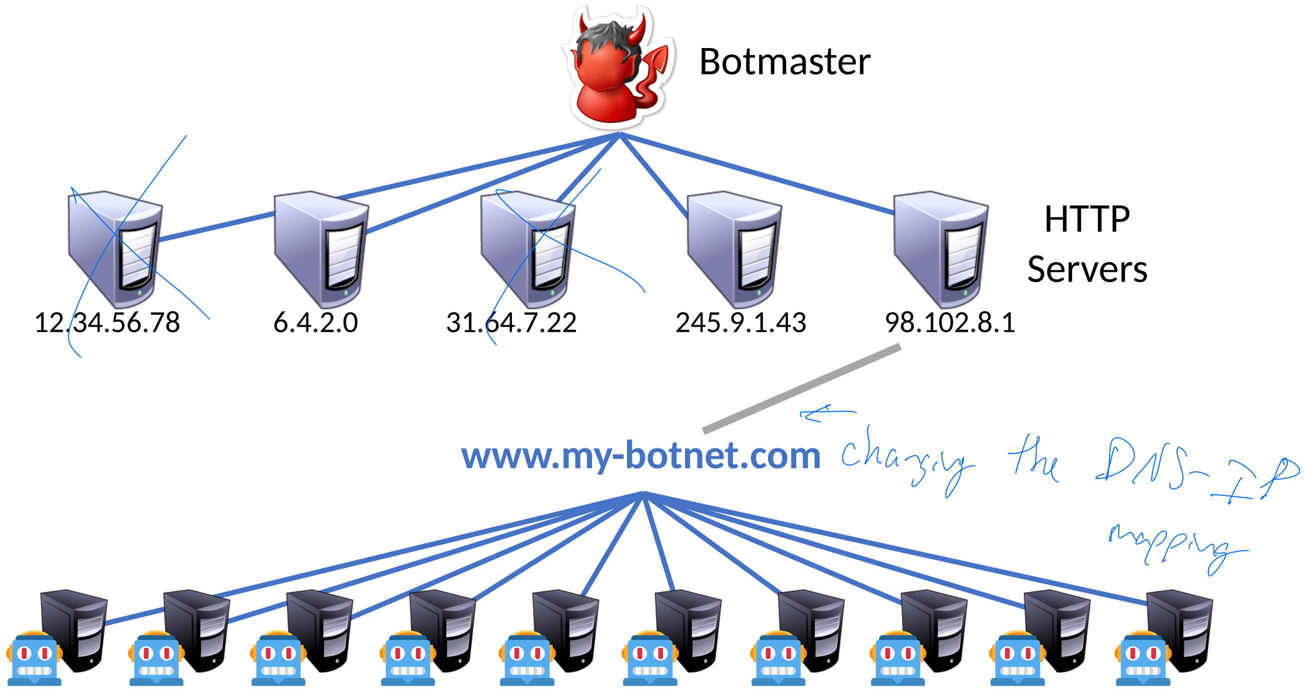
Fast Flux DNS



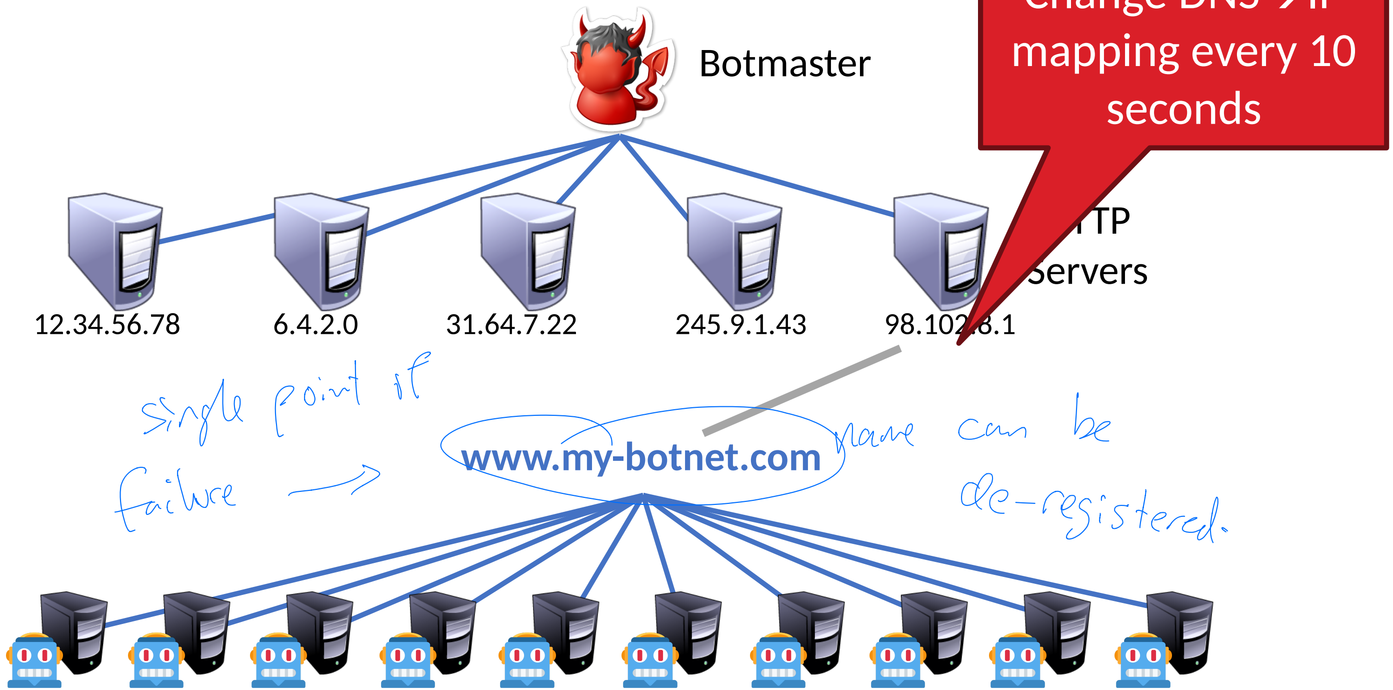
Fast Flux DNS



Fast Flux DNS



Fast Flux DNS

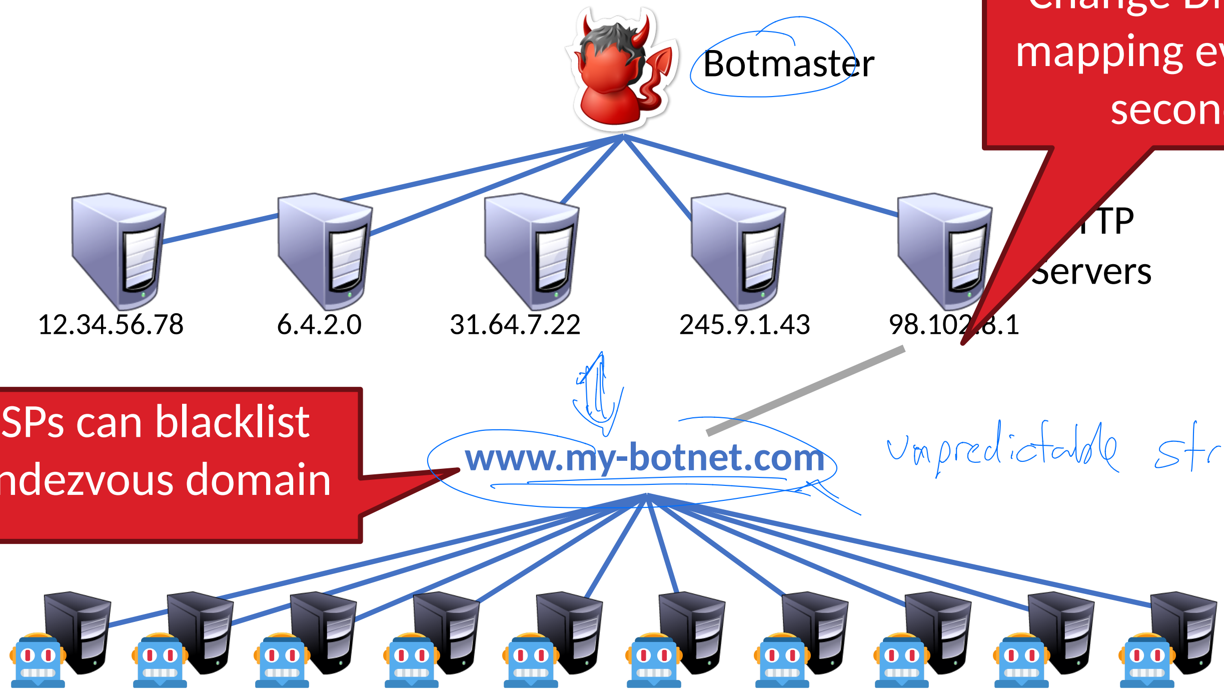


Change DNS→IP mapping every 10 seconds

single point of failure →

name can be de-registered.

Fast Flux DNS

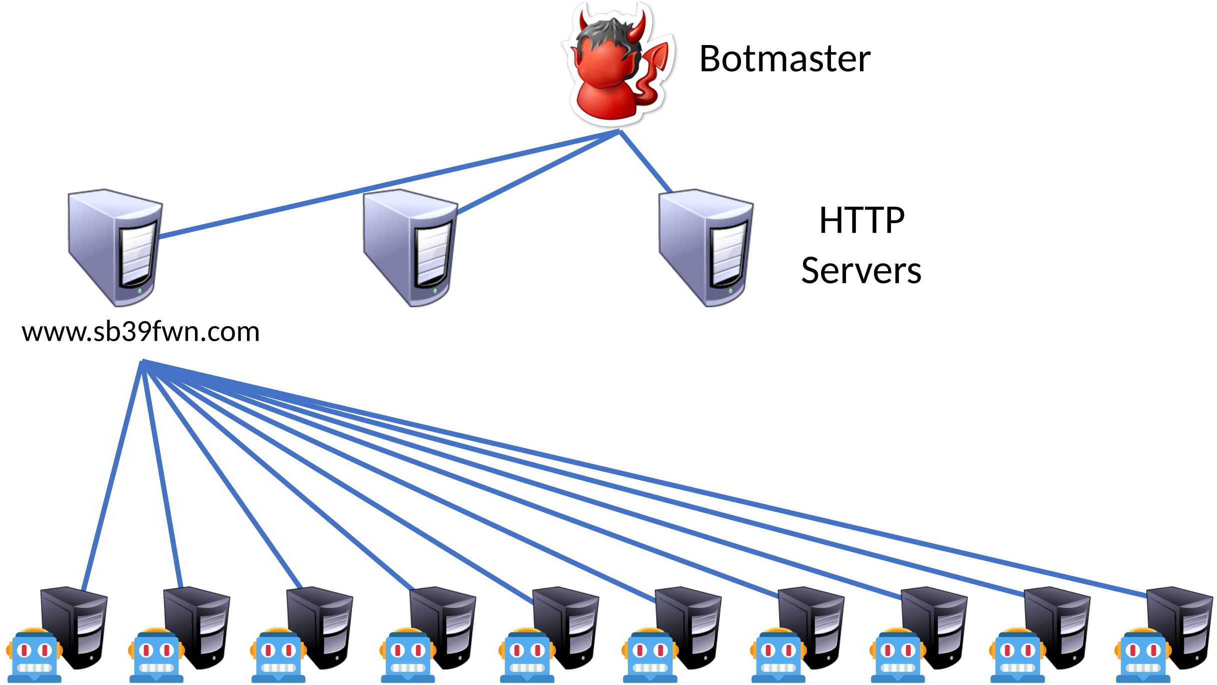


Change DNS→IP mapping every 10 seconds

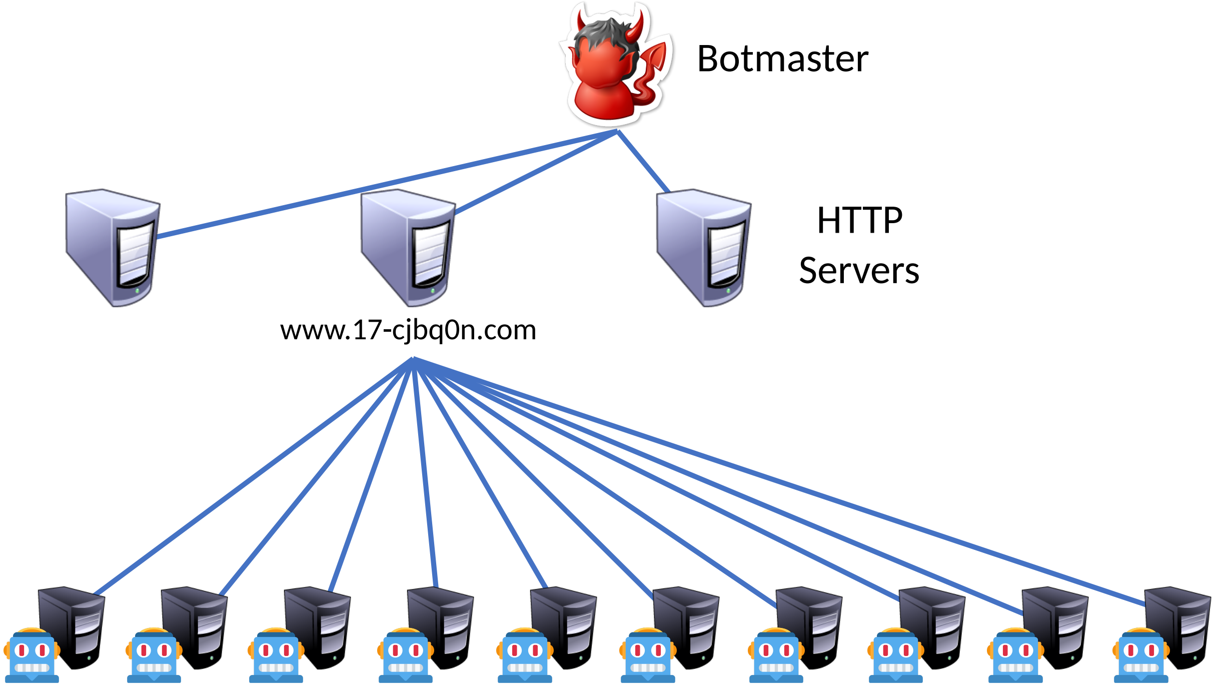
But: ISPs can blacklist the rendezvous domain

Unpredictable string

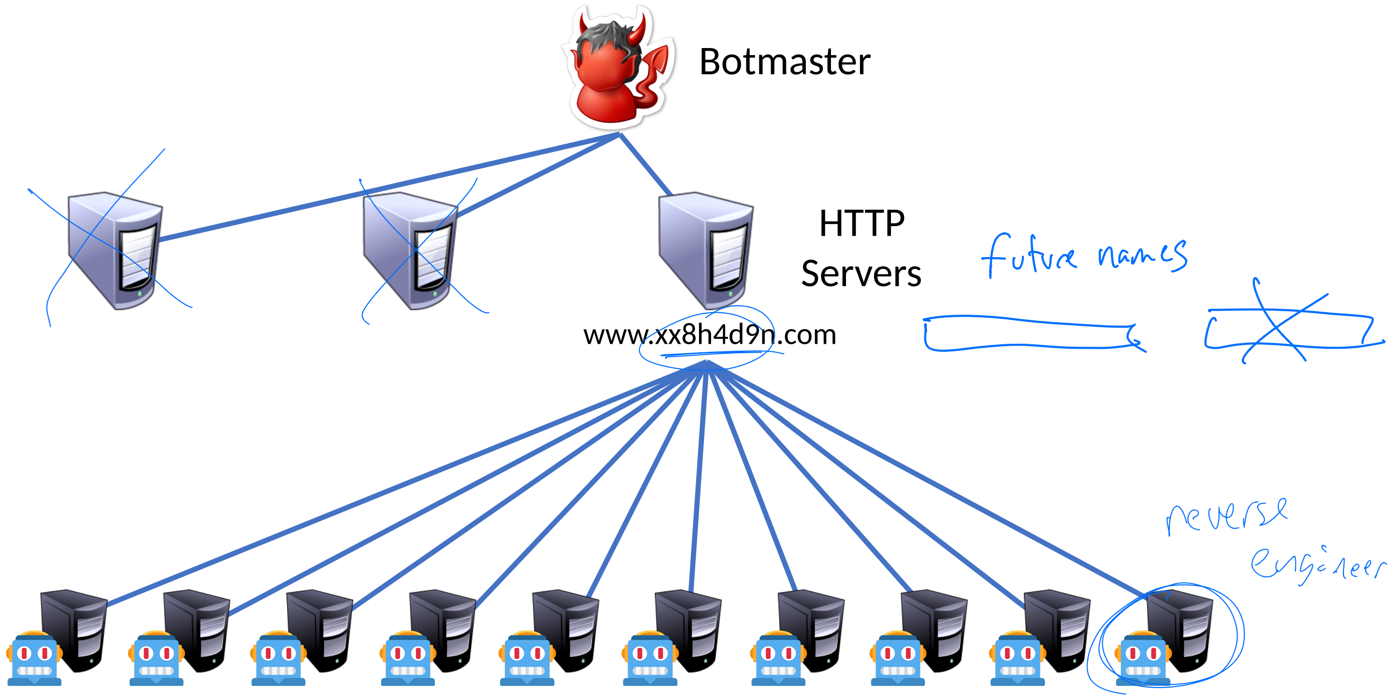
Domain Name Generation (DGA)



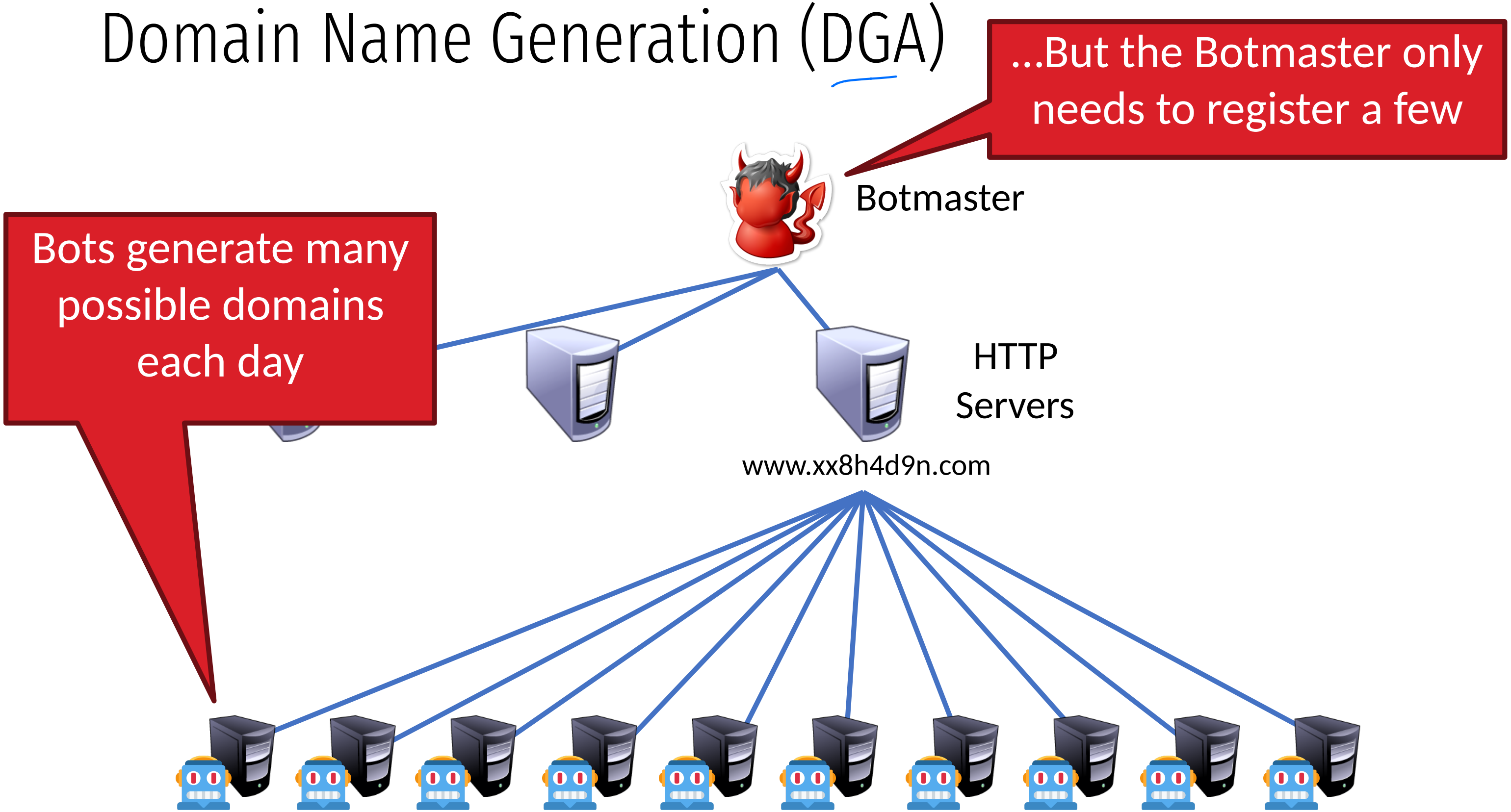
Domain Name Generation (DGA)



Domain Name Generation (DGA)



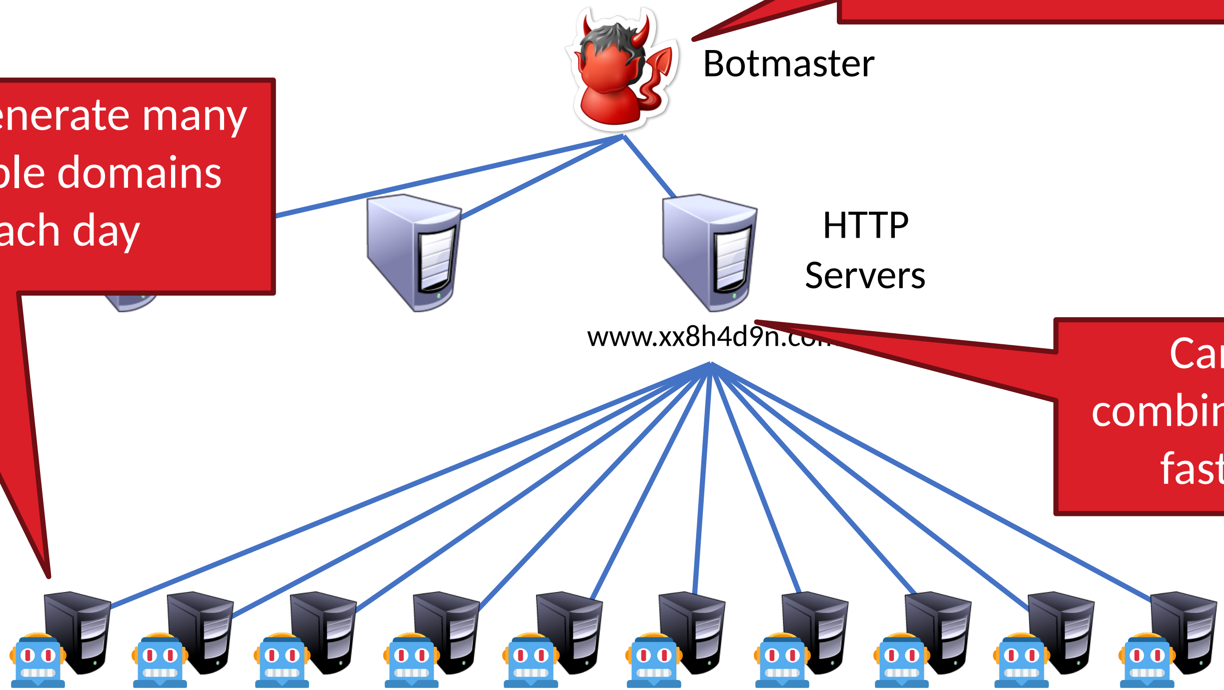
Domain Name Generation (DGA)



...But the Botmaster only needs to register a few

Bots generate many possible domains each day

Domain Name Generation (DGA)



...But the Botmaster only needs to register a few

Bots generate many possible domains each day

Can be combined with fast flux

“Your Botnet is My Botnet”

Takeover of the Torpig botnet

- Random domain generation + fast flux
- Team reverse engineered domain generation algorithm
- Registered 30 days of domains before the botmaster!
- Full control of the botnet for 10 days

“Your Botnet is My Botnet”

Takeover of the Torpig botnet

- Random domain generation + fast flux
- Team reverse engineered domain generation algorithm
- Registered 30 days of domains before the botmaster!
- Full control of the botnet for 10 days

Goal of the botnet: credential theft and phishing spam

- Steals credit card numbers, bank accounts, etc.
- Researchers gathered all this data

“Your Botnet is My Botnet”

Takeover of the Torpig botnet

- Random domain generation + fast flux
- Team reverse engineered domain generation algorithm
- Registered 30 days of domains before the botmaster!
- Full control of the botnet for 10 days

Goal of the botnet: credential theft and phishing spam

- Steals credit card numbers, bank accounts, etc.
- Researchers gathered all this data

Other novel point: accurate estimation of botnet size

Stopping Botnets

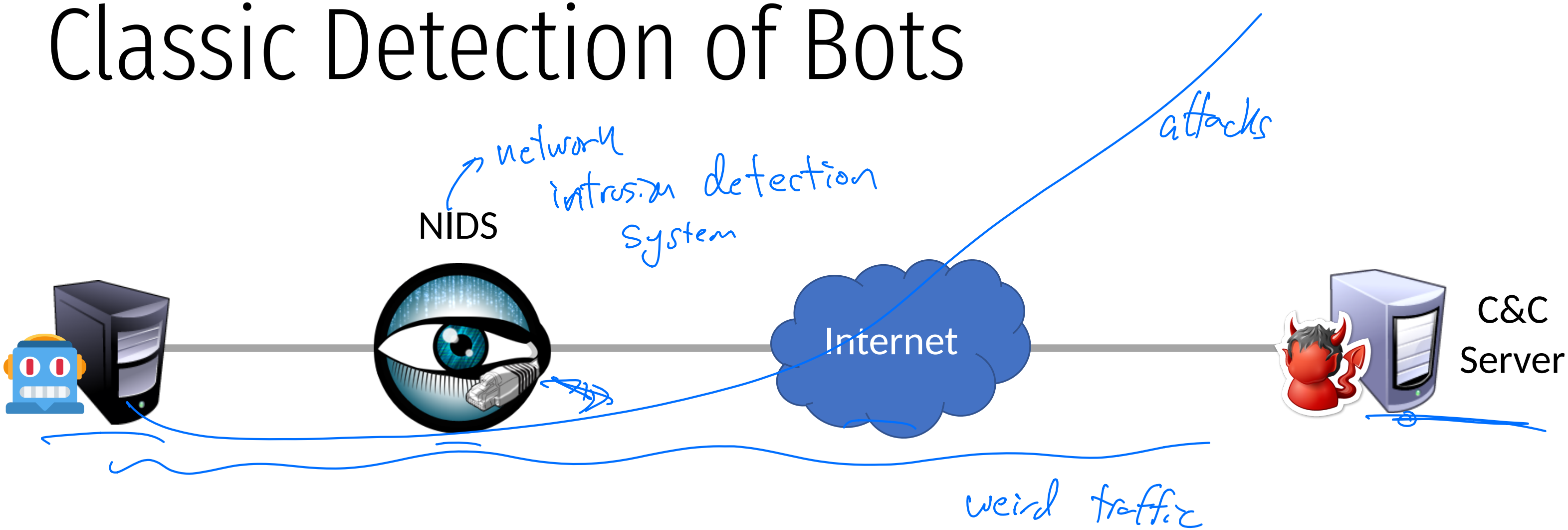
Individual perspective: ridding your network of bots

- Anti-virus and anti-malware
- Intrusion and anomaly detection to identify infections, block traffic

Global perspective: takedowns and arrests

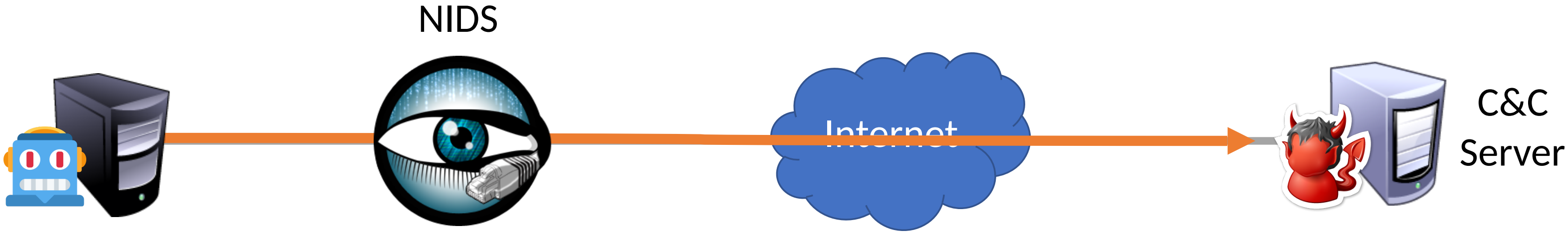
- Create a sinkhole (fake C&C server)
- Track down and arrest the perpetrators

Classic Detection of Bots

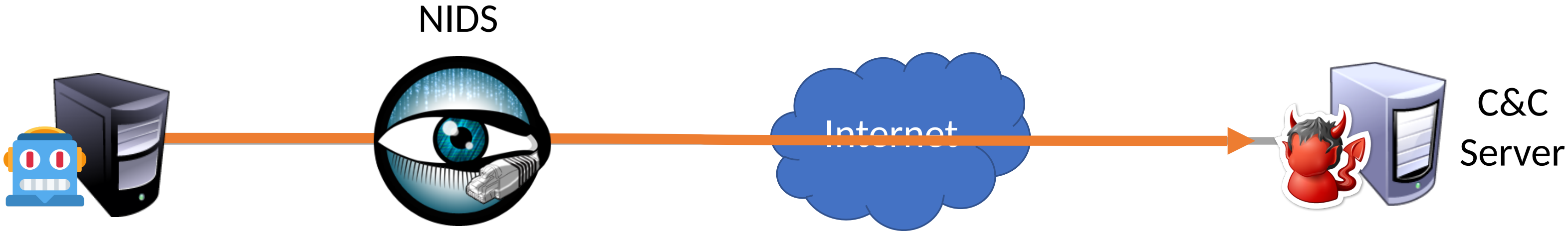


How can you tell if your machine is part of a botnet??

Classic Detection of Bots



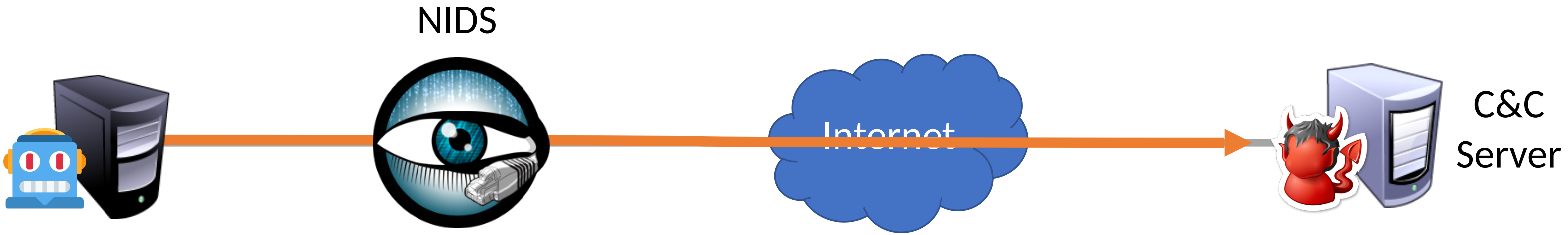
Classic Detection of Bots



- Unusual ports or protocols
  - IRC port 6667
- Message signatures
  - "cmd=spam; target=…"

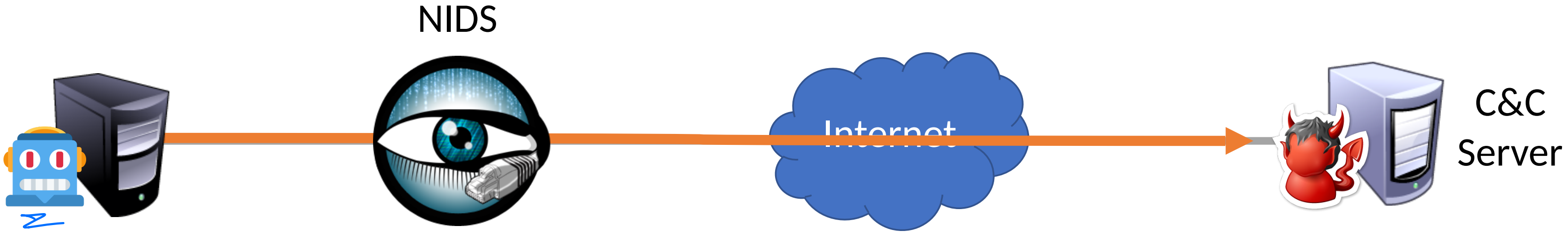
↑ can be encrypted

Classic Detection of Bots



- ✗ Unusual ports or protocols
  - IRC port 6667
- ✗ Message signatures
  - “cmd=spam; target=…”

Classic Detection of Bots



✗ Unusual ports or protocols

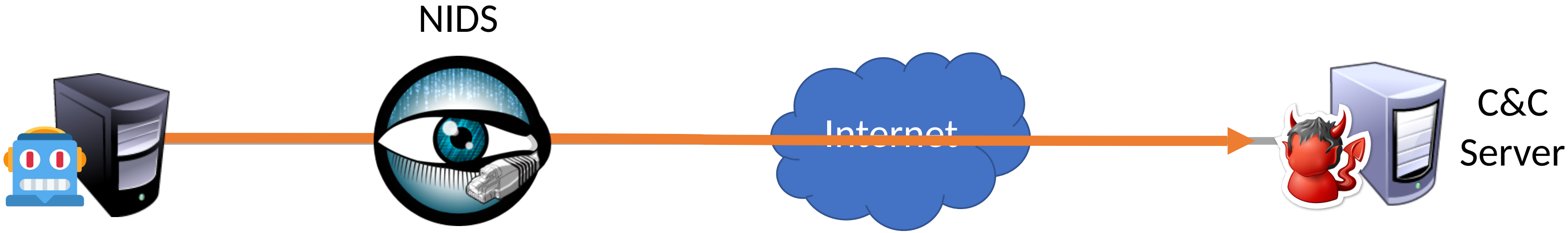
- IRC port 6667

✗ Message signatures

- “cmd=spam; target=…”

- Defeated by using standard ports
  - HTTP(S) ports 80/443 tls.

Classic Detection of Bots



❌ Unusual ports or protocols

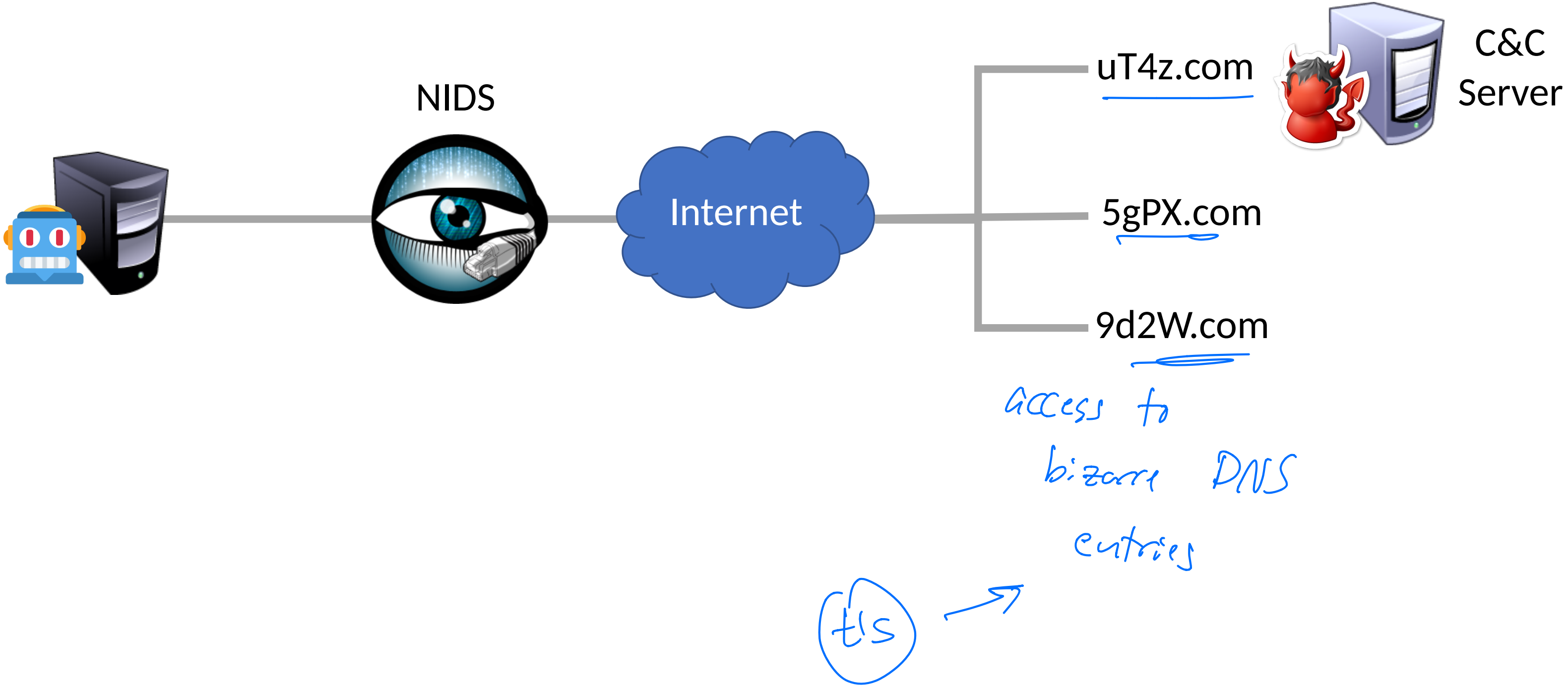
- IRC port 6667

❌ Message signatures

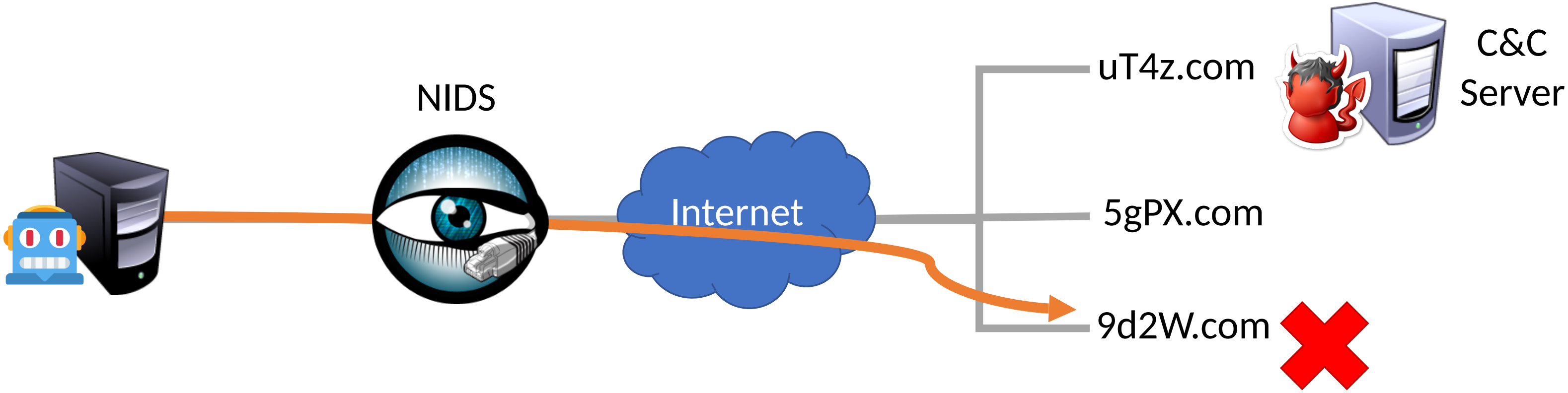
- “cmd=spam; target=…”

- Defeated by using standard ports
  - HTTP(S) ports 80/443
- Defeated by encryption

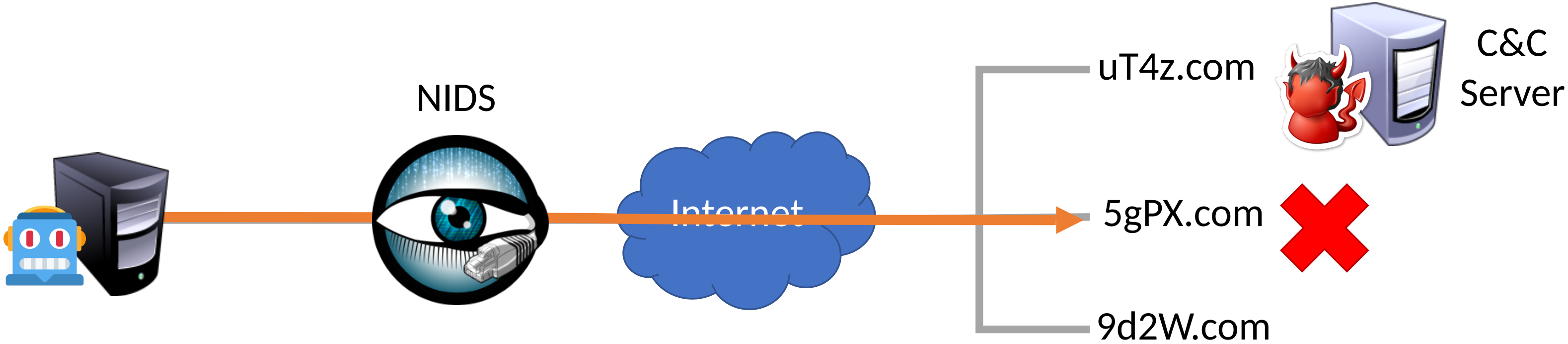
Detection of DGA and Fast Flux



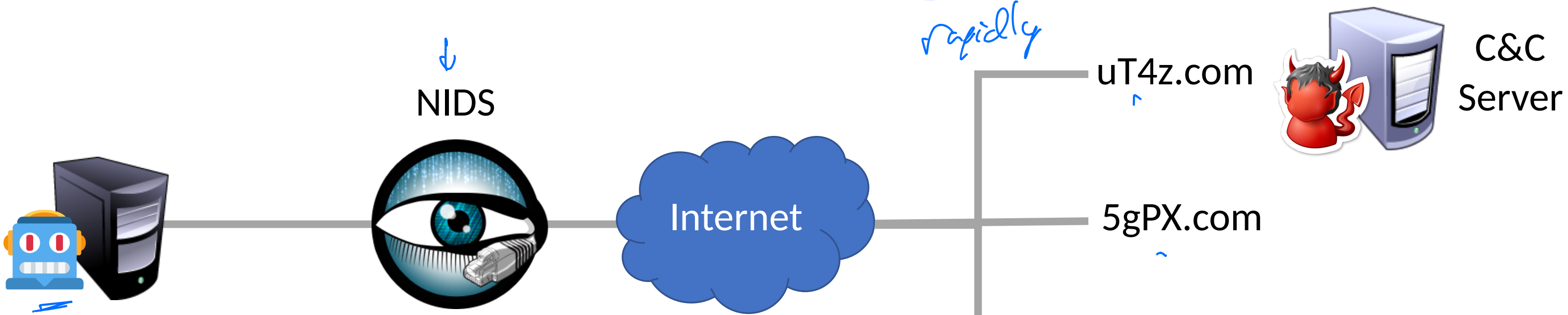
Detection of DGA and Fast Flux



Detection of DGA and Fast Flux



Detection of DGA and Fast Flux



NIDS

Internet

uT4z.com

5gPX.com

9d2W.com

C&C Server

rapidly

tests

basic signals of a compromise

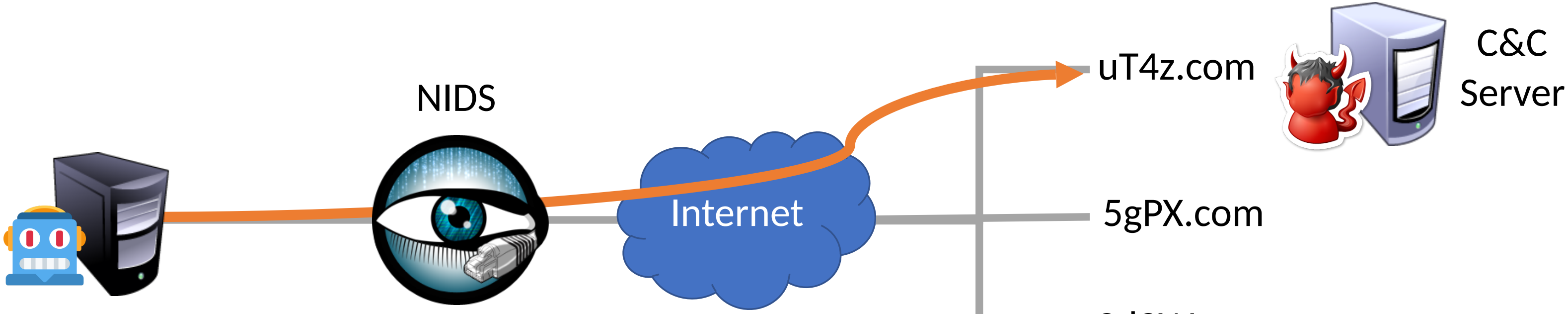
heuristics.

false positives

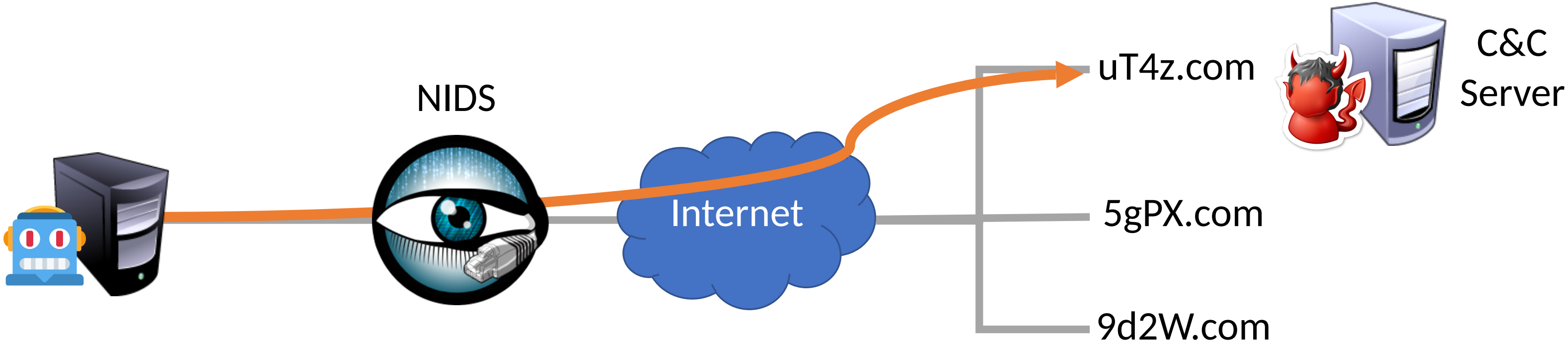
false negatives.

rules sets produced by the community

Detection of DGA and Fast Flux

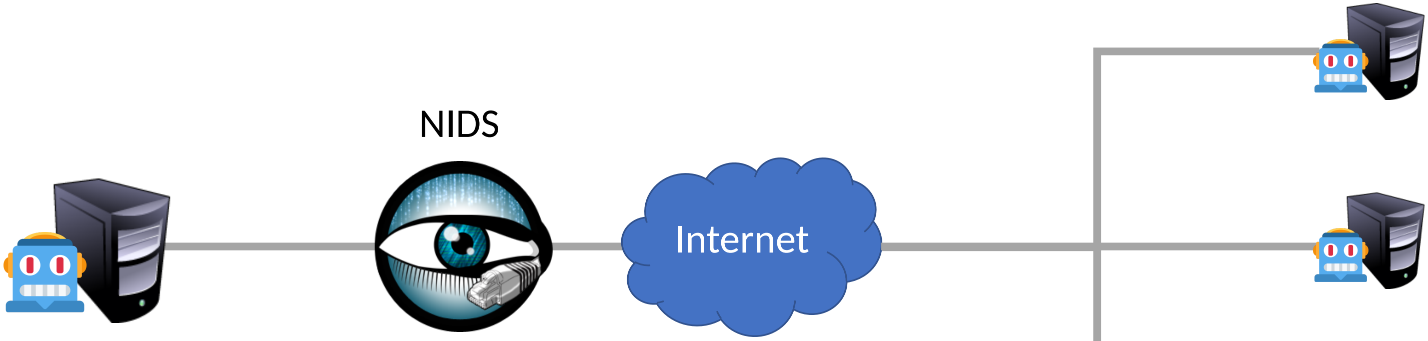


Detection of DGA and Fast Flux

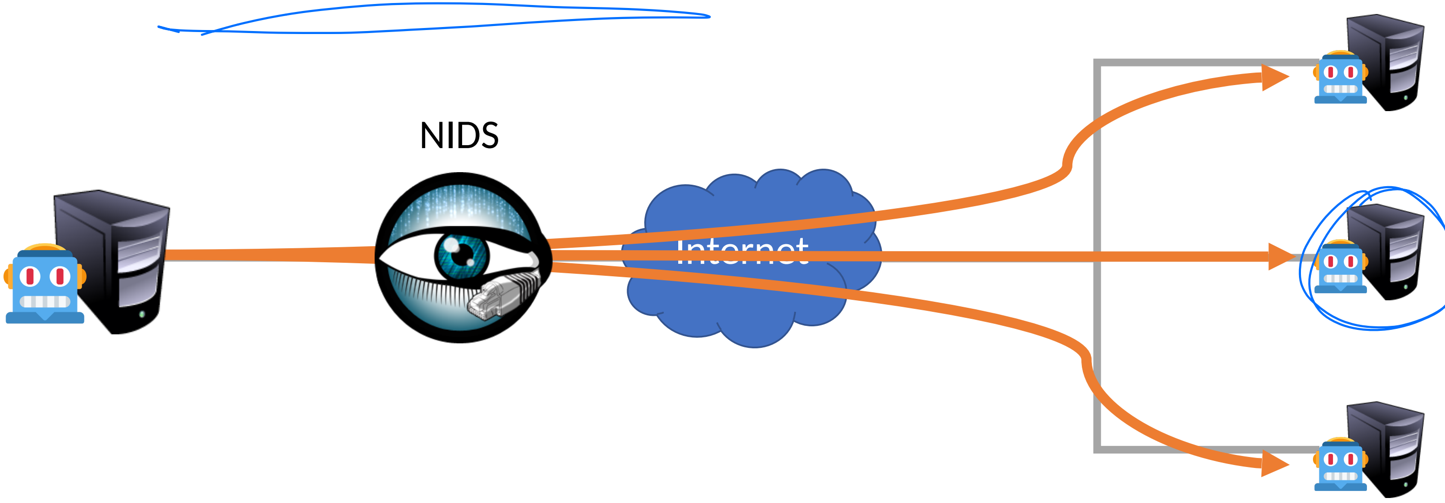


- For DGA: many failed DNS lookups
- For fast flux: multiple DNS lookups for one name, response has short TTL
  - 10 seconds – 10 minutes
  - Most DNS names have TTL of hours or days

Detection of P2P



Detection of P2P



reverse engineer to understand

- Many connections to seemingly random hosts
  - Bursty traffic patterns
  - Unexpected geographic patterns (connections to hosts in other countries)

Infamous Takedowns

Botnet Name	Timeframe	Estimated Size	Taken Down by…
DNS Changer	2006-2011	4M	FBI, Trend Micro
Rustock	2006-2011	150K-2.4M	FBI, Microsoft, Fireeye, Univ. of Washington
Grum	2008-2012	560K-840K	Fireeye, Spamhaus
Conficker	2008-2009	4M-13M	FBI, Microsoft, Symantec, ICANN
Citadel	2011-2013		FBI, Microsoft
Gameover Zeus/Cryptolocker	2012-2014		DoJ, FBI, Europol, Dell, Microsoft, Level3, McAfee, Symantec, Sophos, Trend Micro, Carnegie Mellon, Georgia Tech, etc.
SIMDA	2011-2015	770K	INTERPOL, Trend Micro, Microsoft, Kaspersky Lab
DRIDEX	2014-2015		FBI, Trend Micro
Avalanche	2009-2016	500K	FBI, Symantec, Fraunhofer

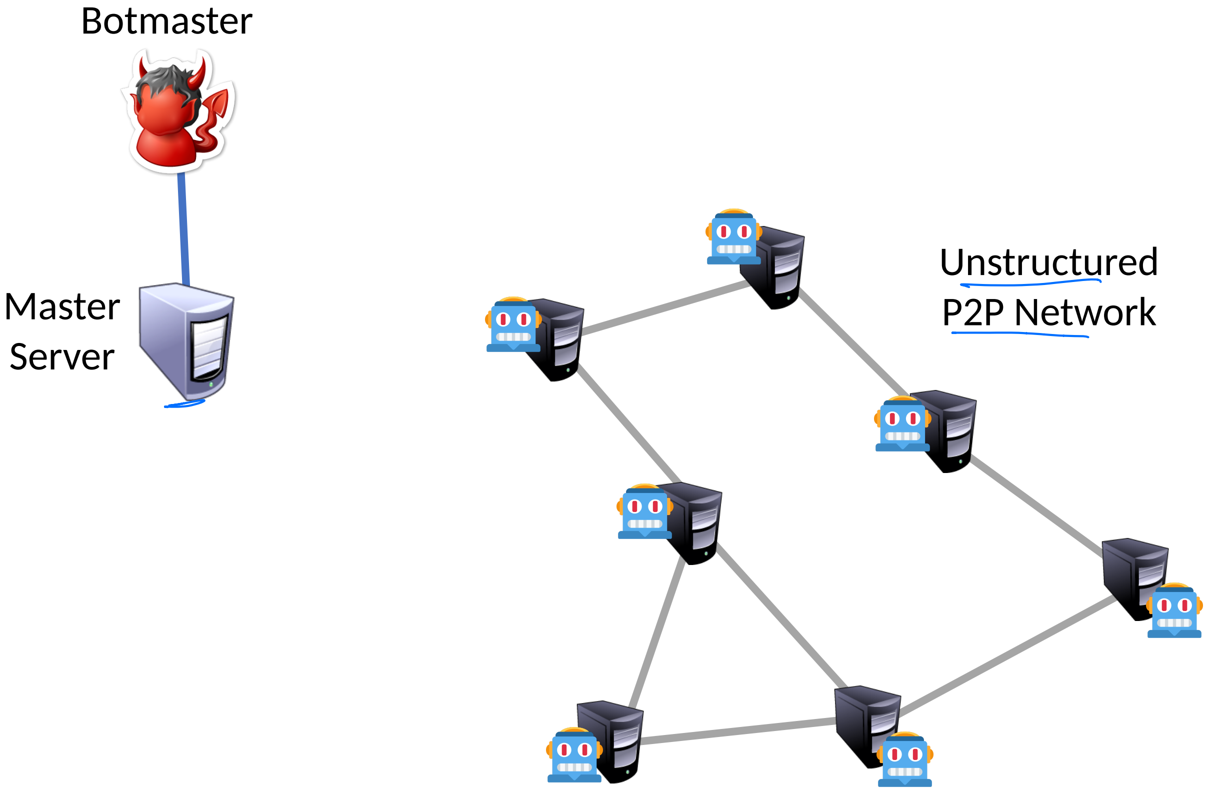
Kelihos

Resilient, P2P botnet

- Successor to Waledac, which was originally distributed via Conficker
- Five variants, spanning 2009-2017
- Roughly 100K-200K infections at any given time   400 K machines
- Spam, credential theft, Bitcoin mining and wallet theft

Taken down five times

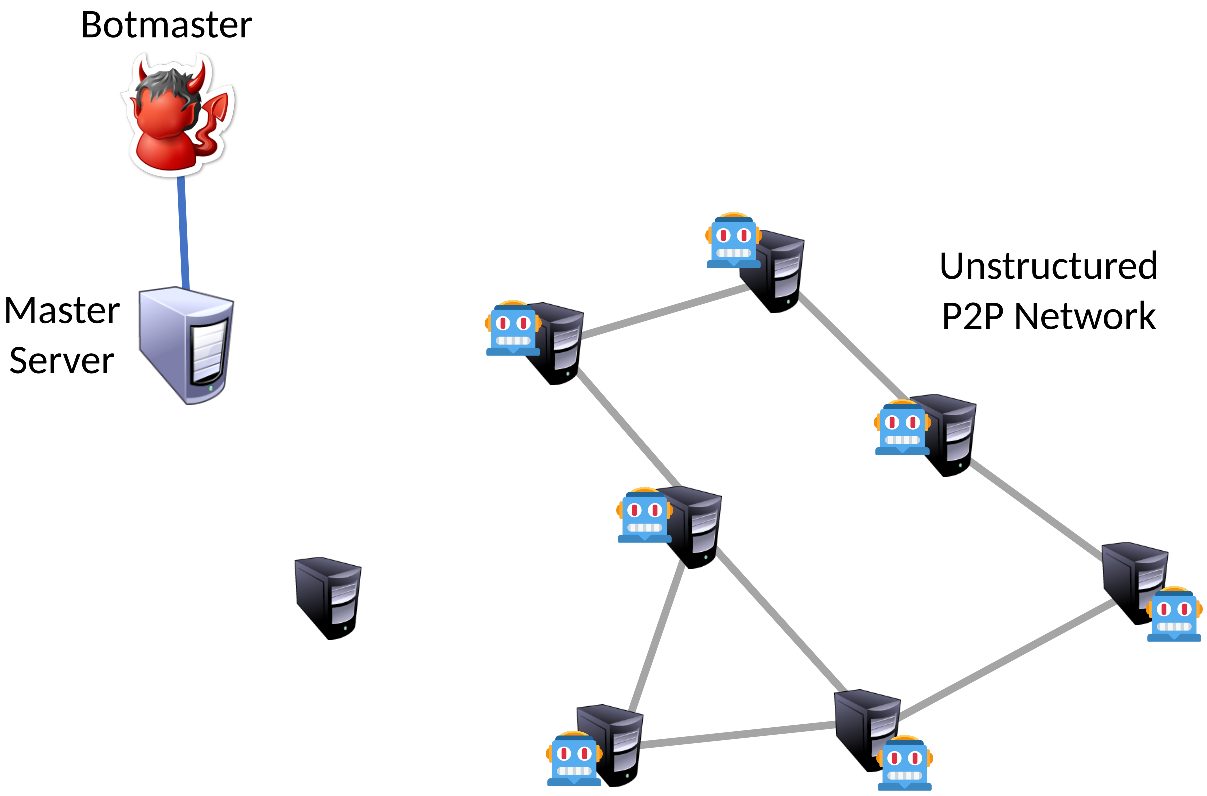
- Four times: authors produced a new version, built a new botnot
- Fifth time: author arrested (2018)



Botmaster

Master Server

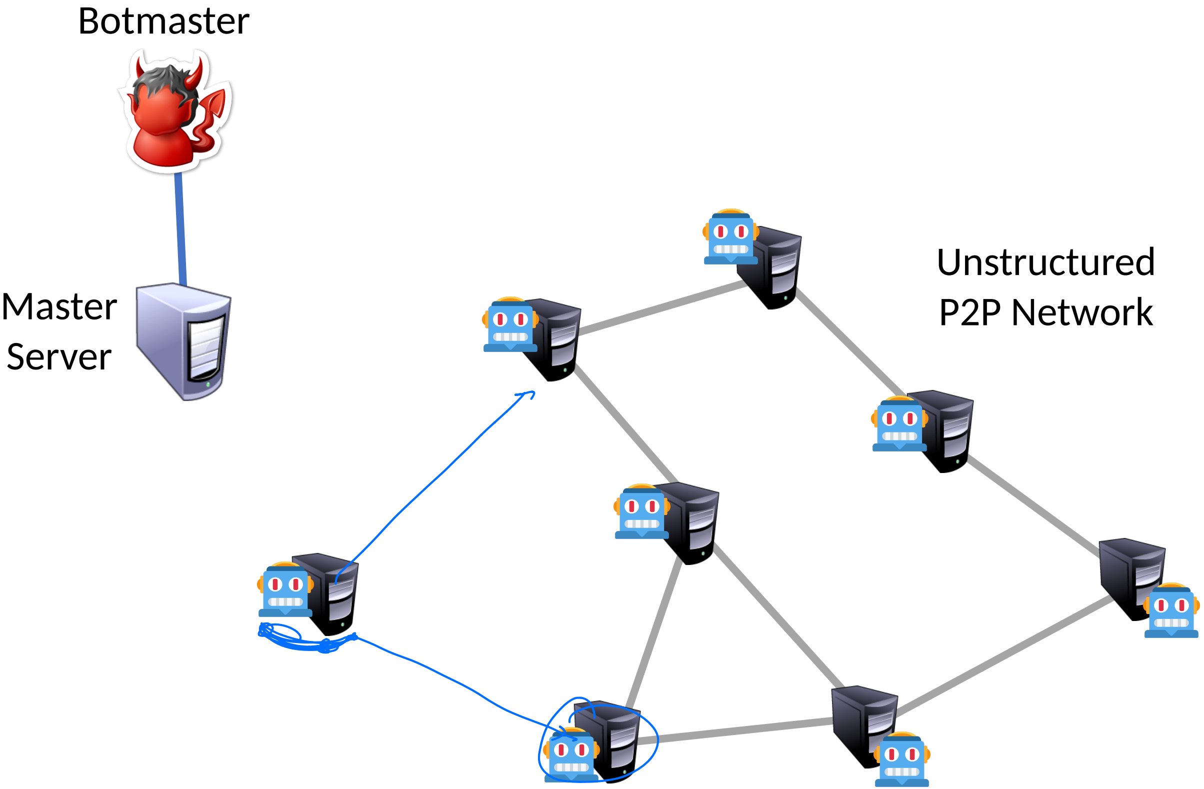
Unstructured P2P Network



Botmaster

Master Server

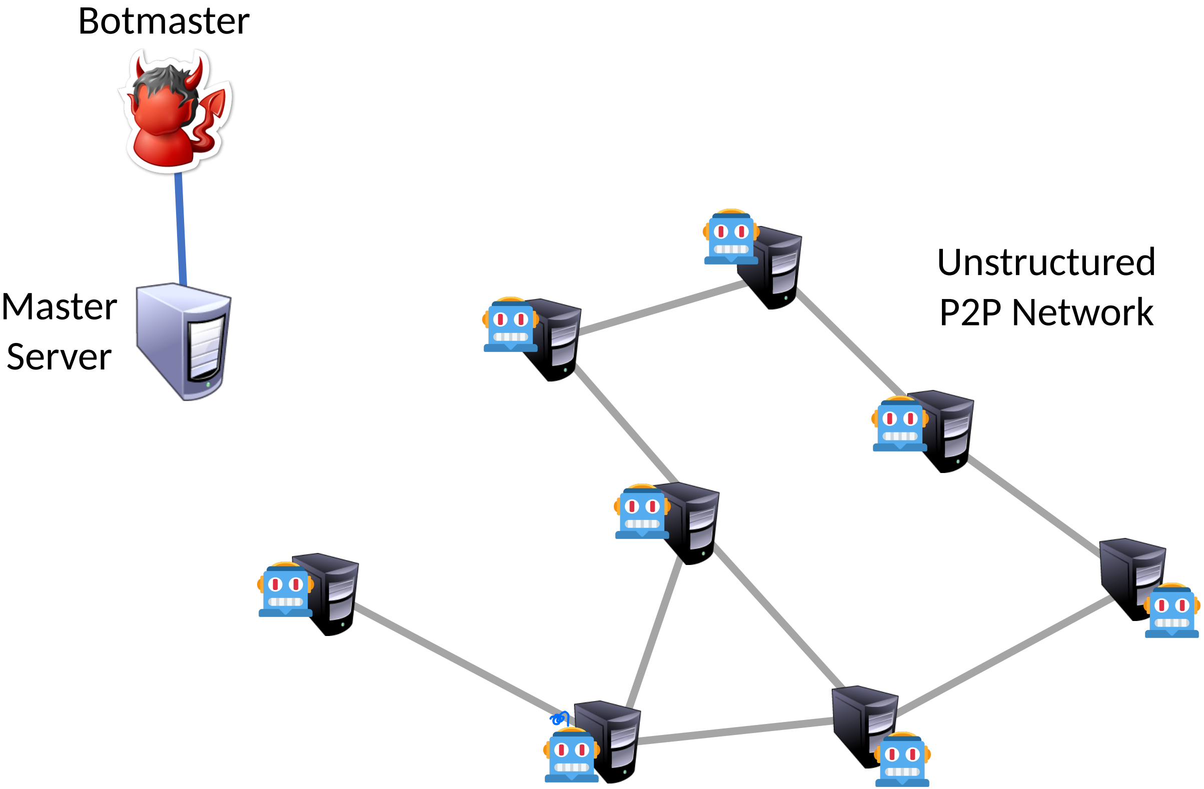
Unstructured P2P Network



Botmaster

Master Server

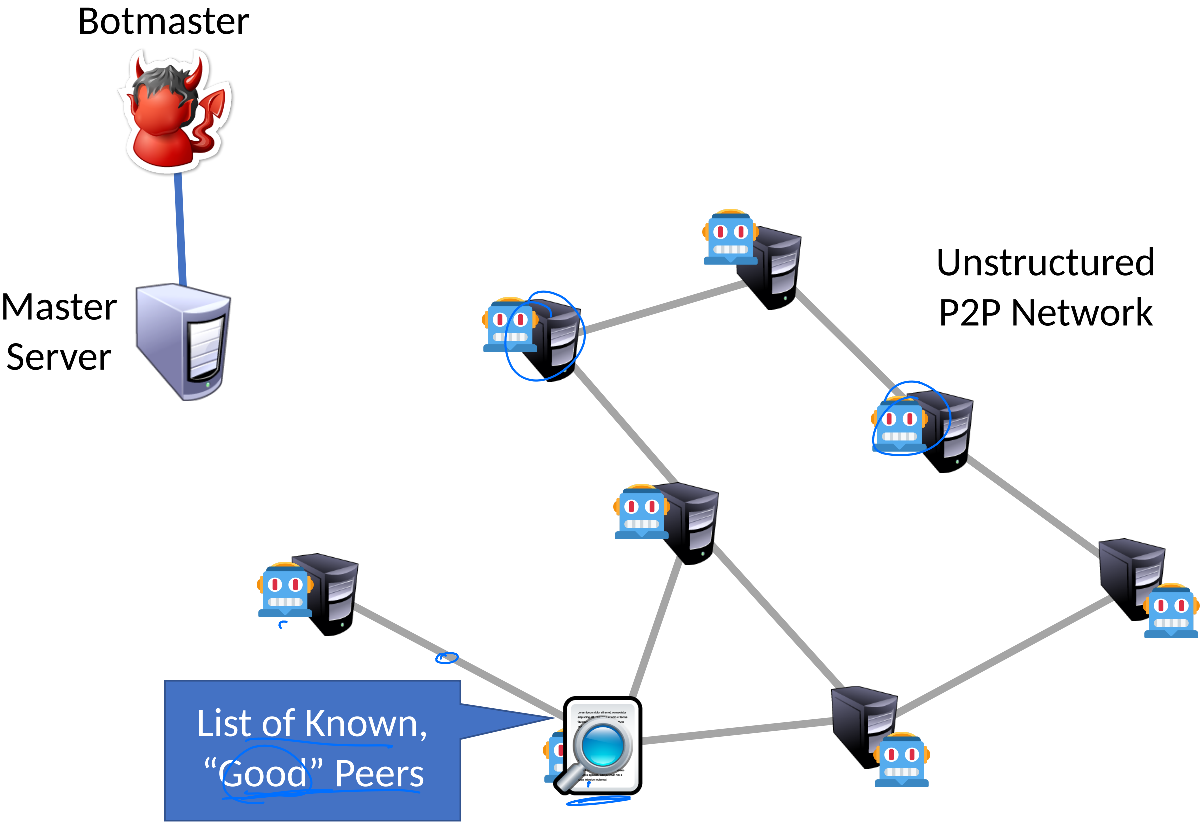
Unstructured P2P Network



Botmaster

Master Server

Unstructured P2P Network

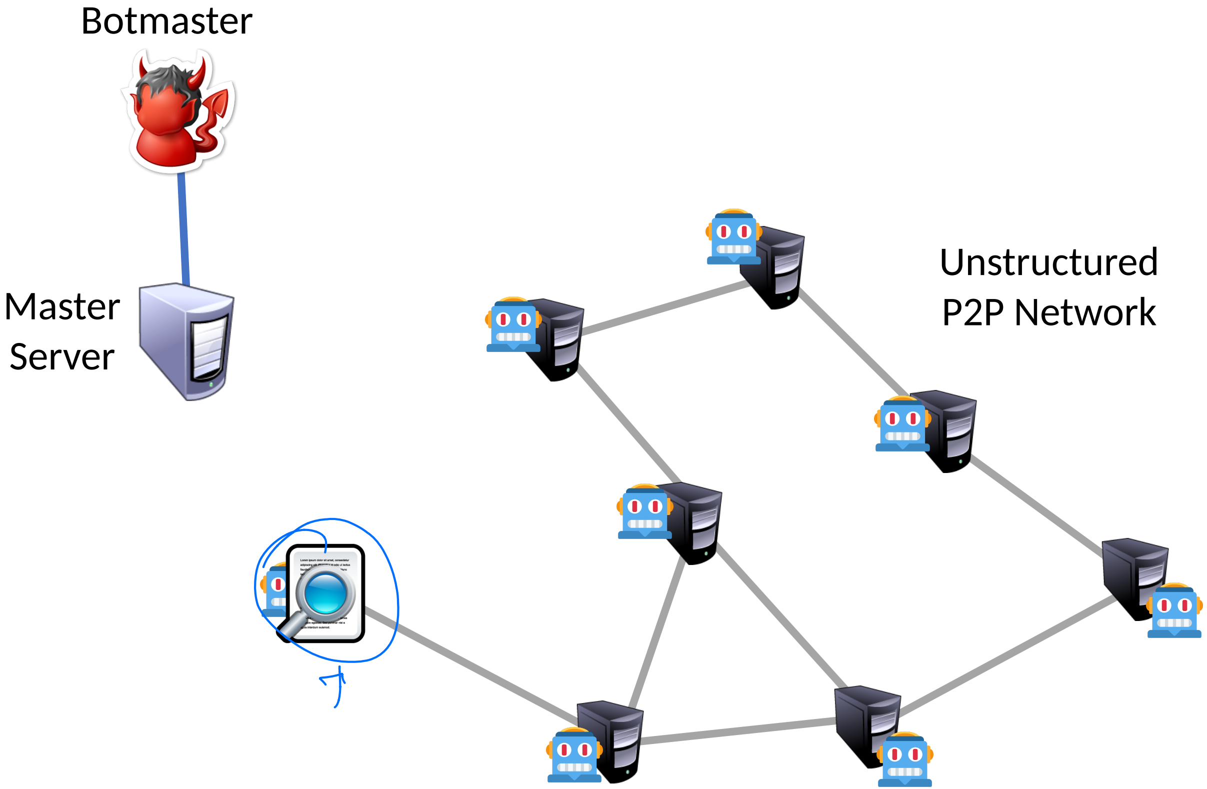


Botmaster

Master Server

Unstructured P2P Network

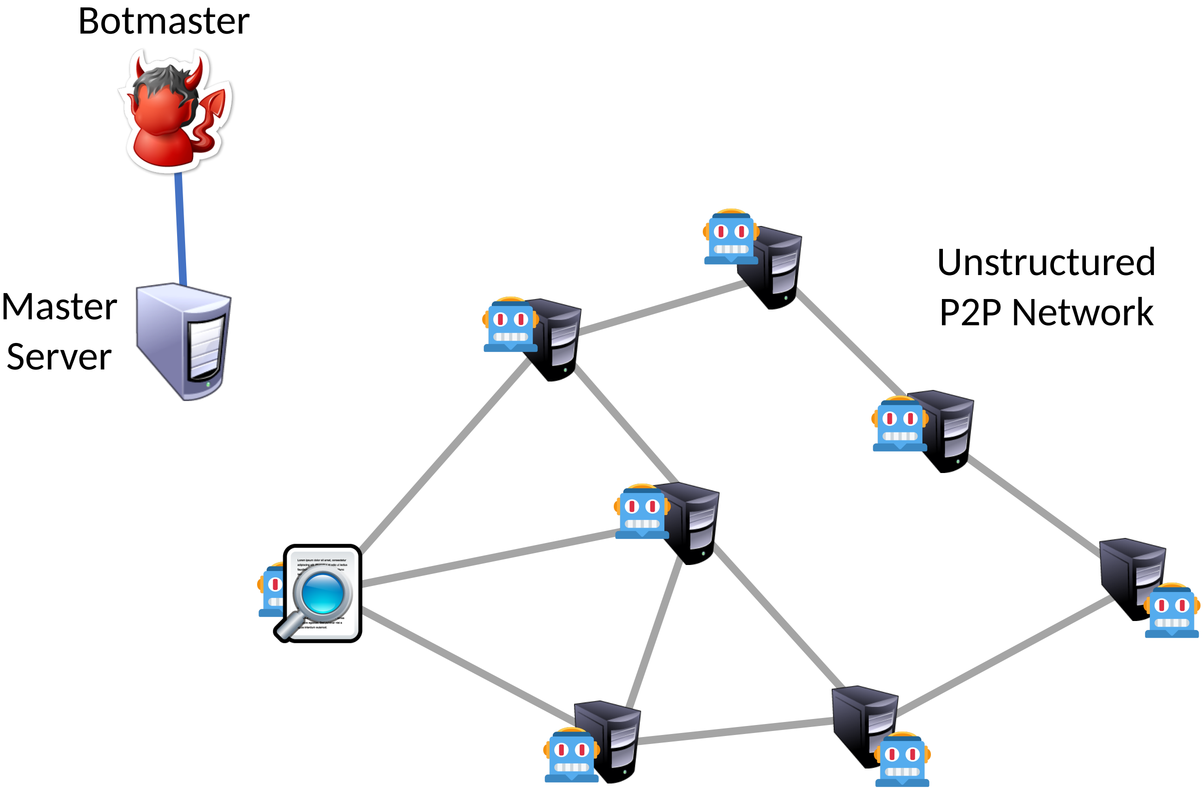
List of Known, “Good” Peers

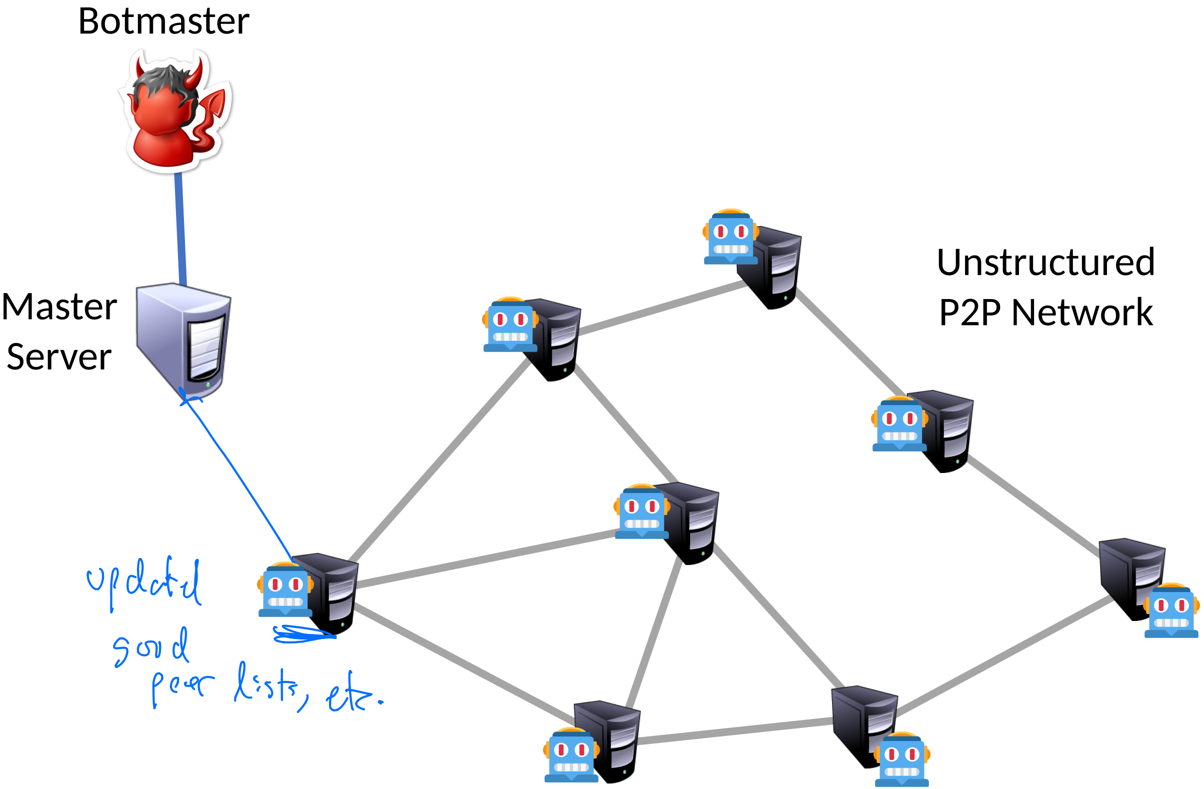


Botmaster

Master Server

Unstructured P2P Network


Botmaster
Master
Server
Unstructured
P2P Network



Botmaster

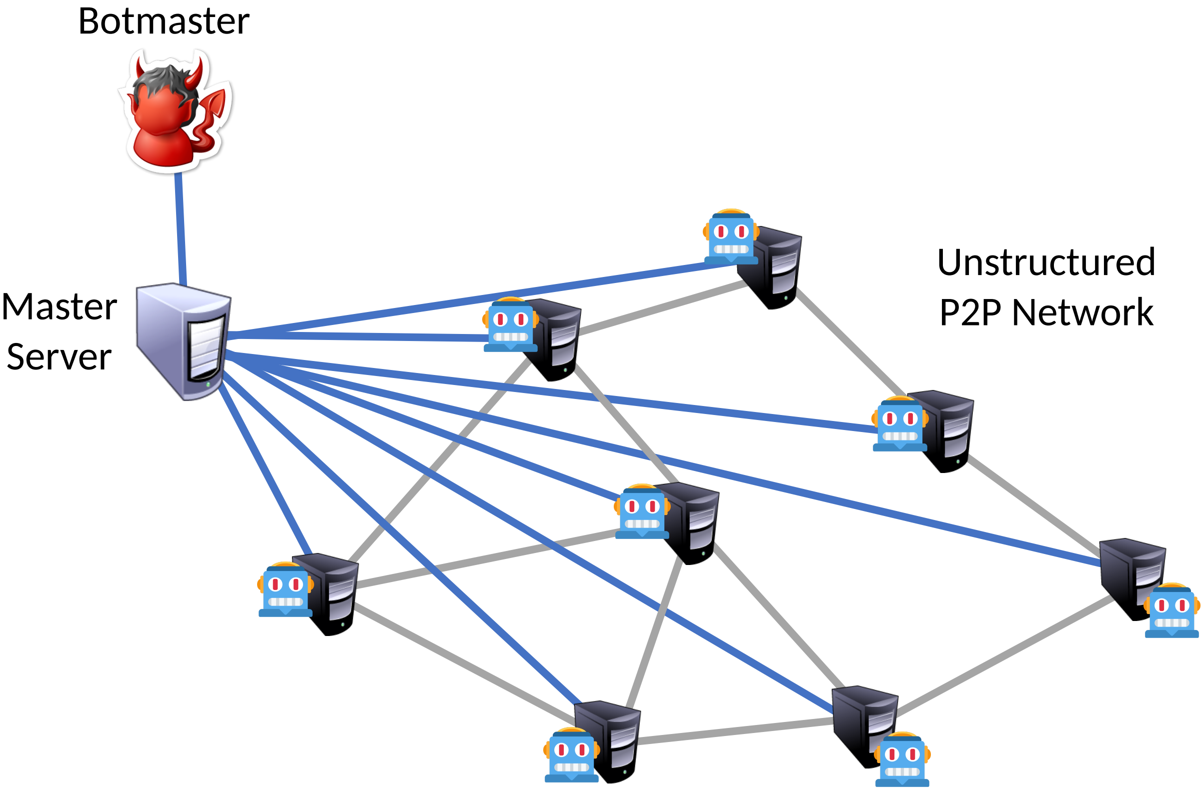
Master Server

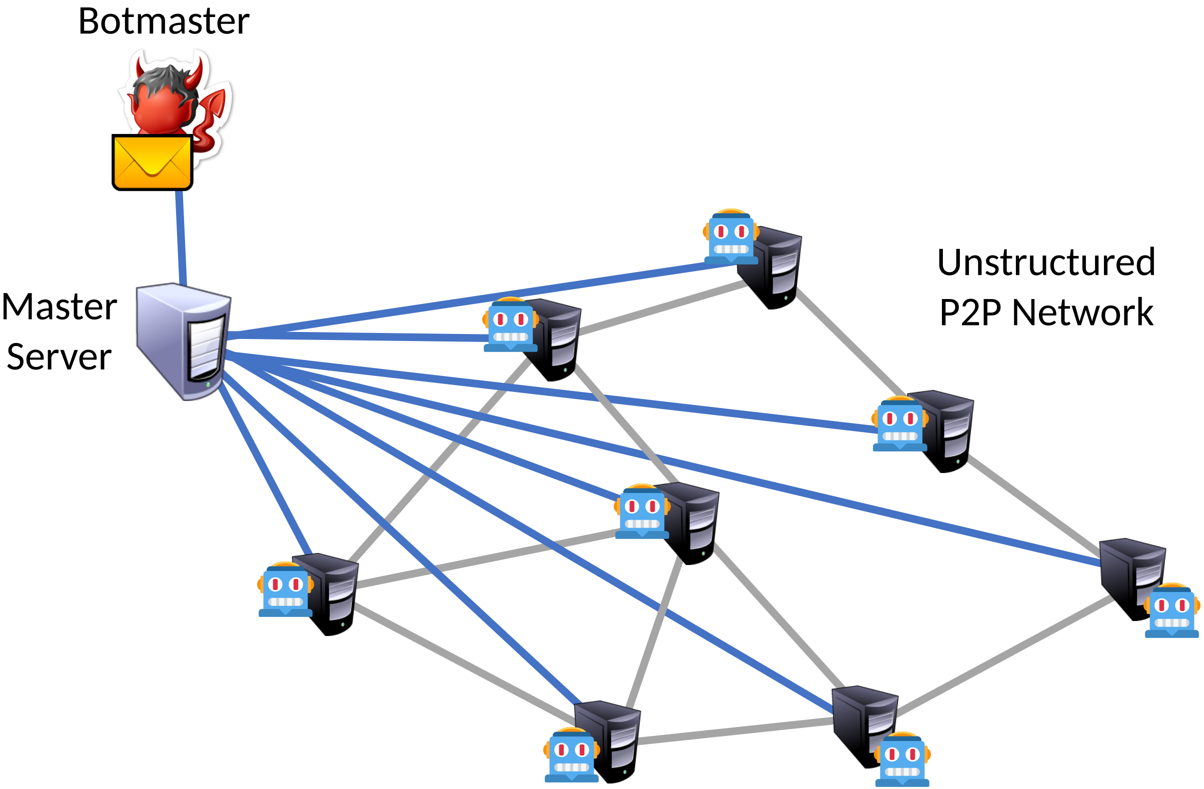
Unstructured P2P Network

updated

seed

peer lists, etc.

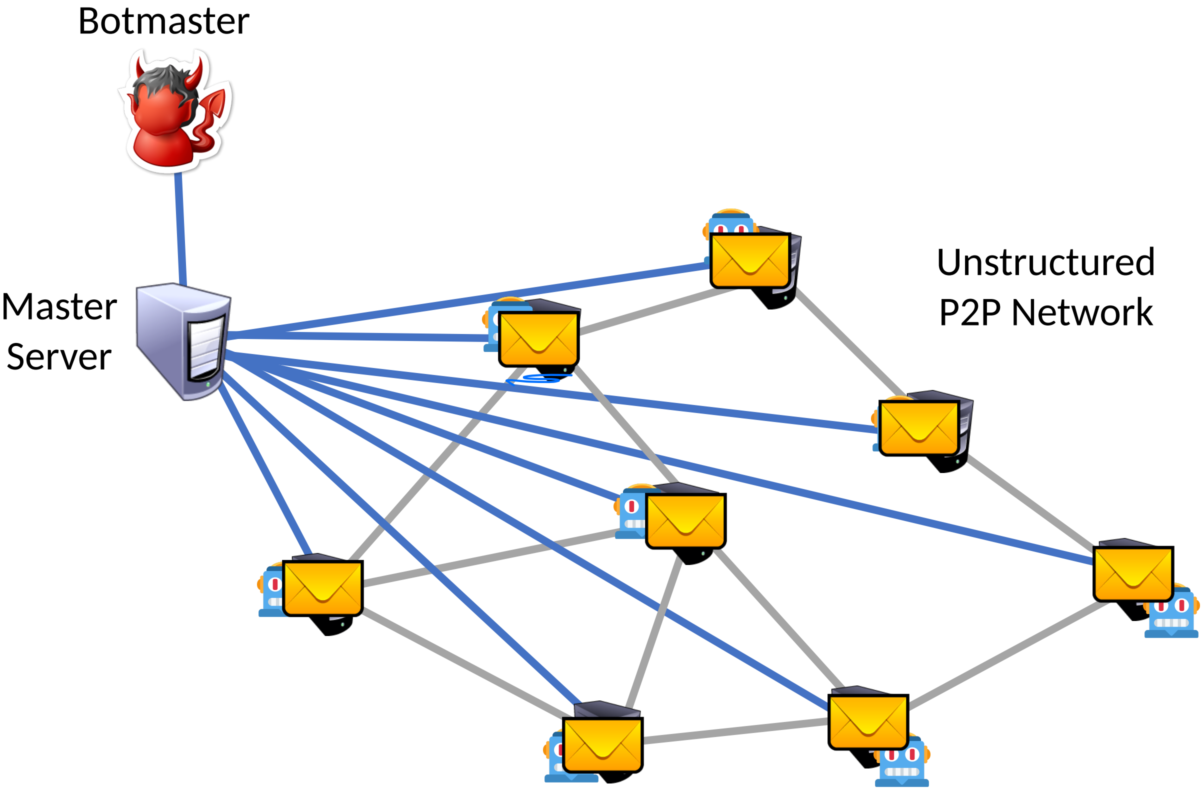

Botmaster
Master Server
Unstructured P2P Network

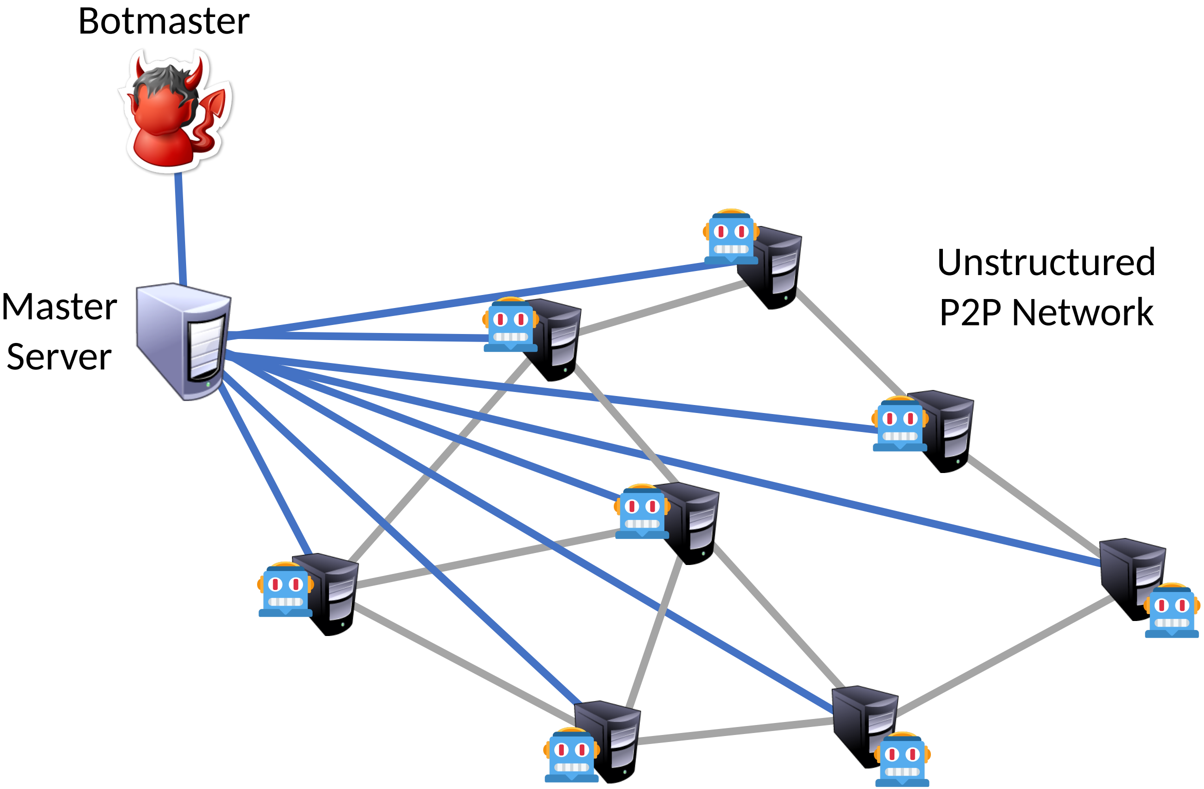


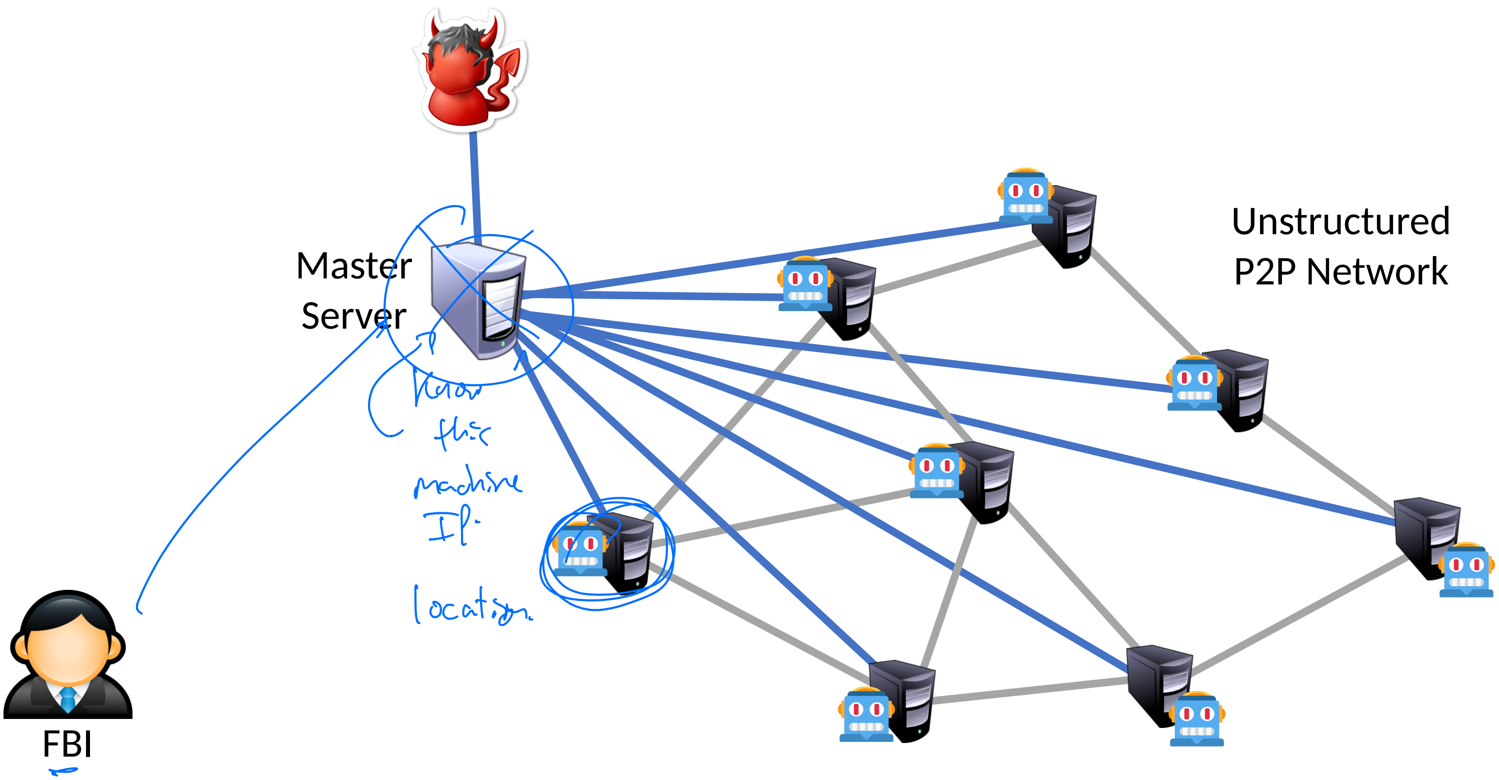
Botmaster

Master Server

Unstructured P2P Network


Botmaster
Master
Server
Unstructured
P2P Network


Botmaster
Master Server
Unstructured P2P Network



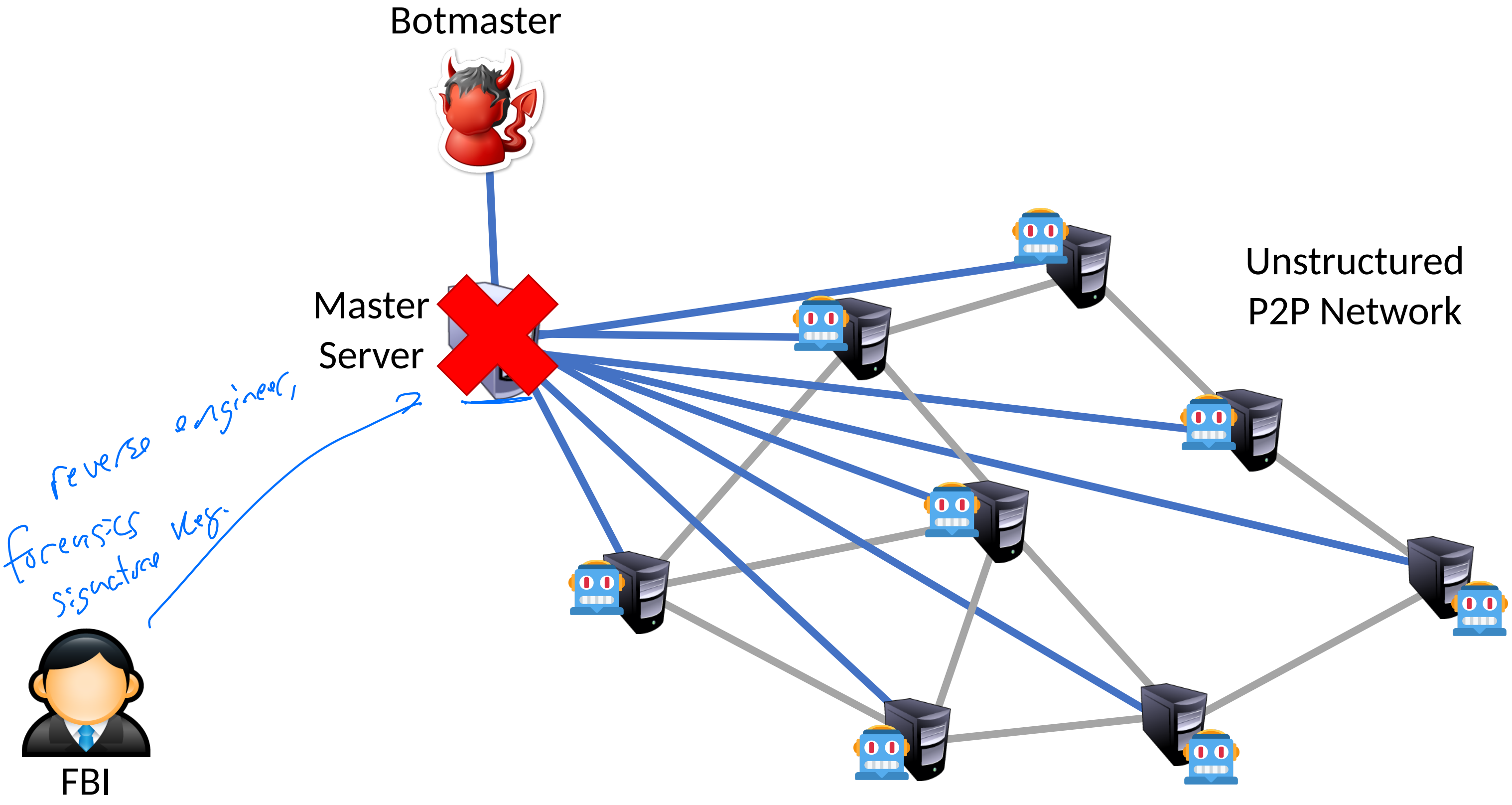
Botmaster

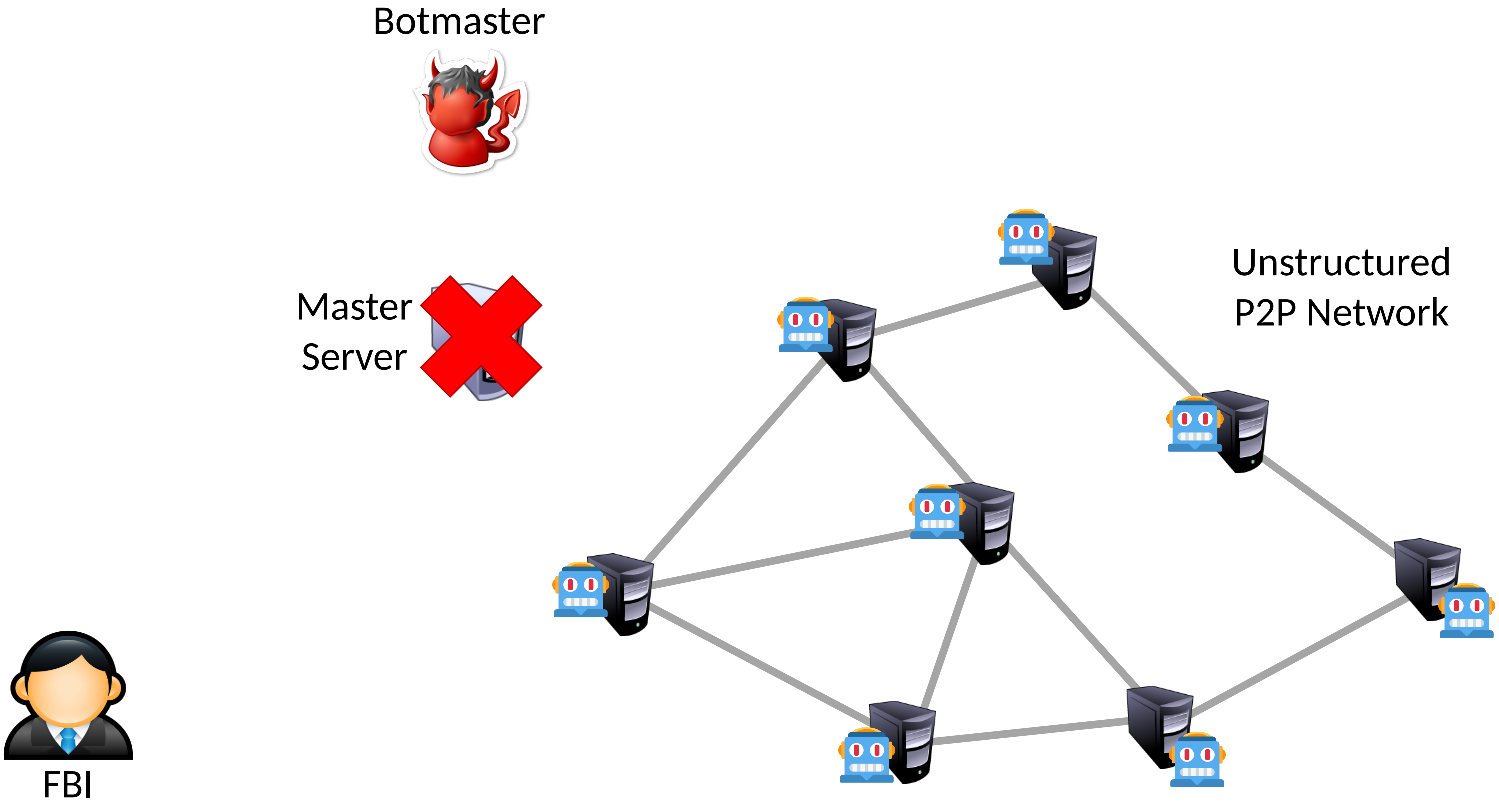
Master Server

Know this machine IP. location.

Unstructured P2P Network

FBI


Botmaster
Master Server
Unstructured P2P Network
reverse engineer,
forensics
signature reg.
FBI

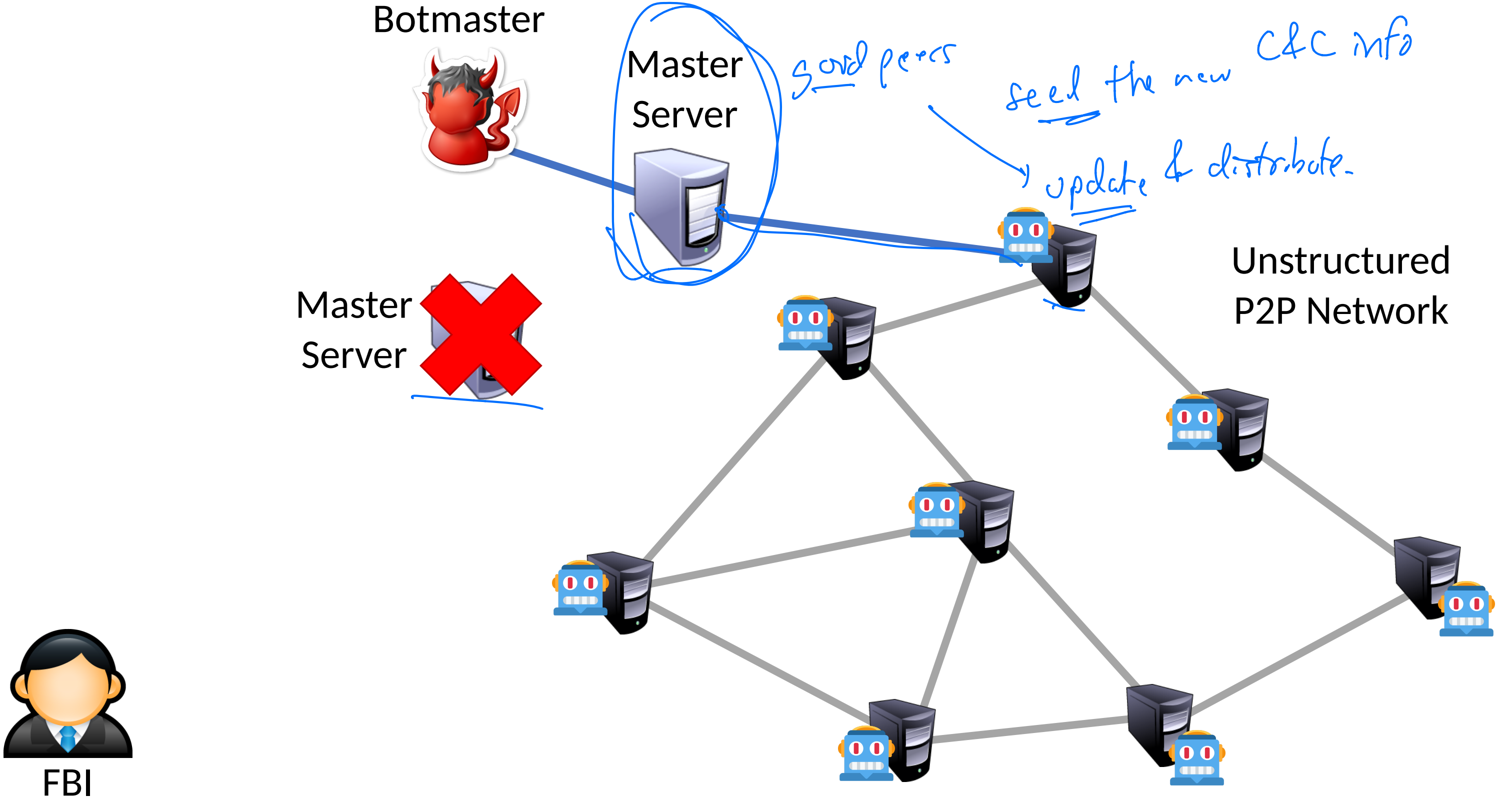


Botmaster

Master Server

Unstructured P2P Network

FBI



Botmaster

Master Server

send peers

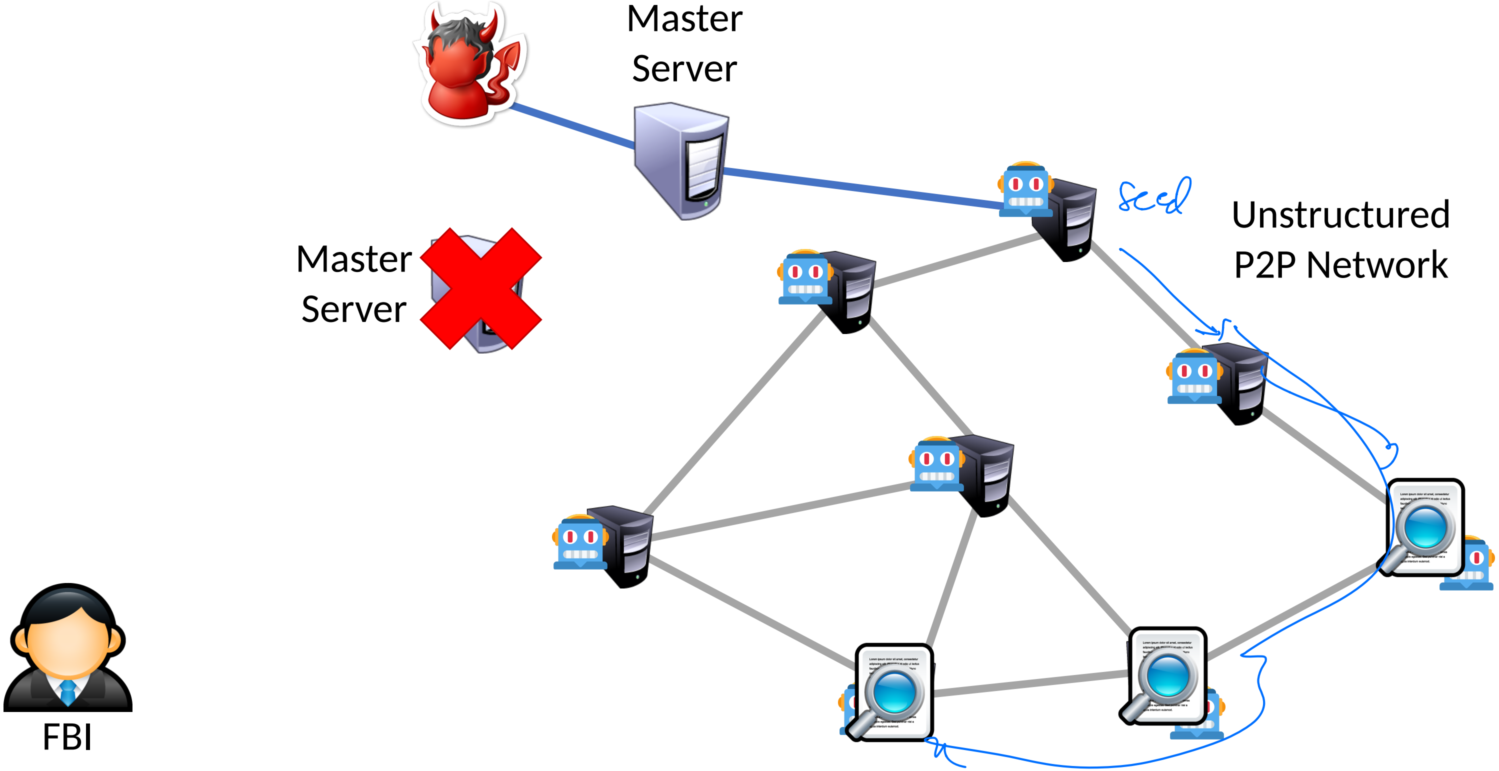
seed the new C&C info

update & distribute.

Master Server

Unstructured P2P Network

FBI



Botmaster

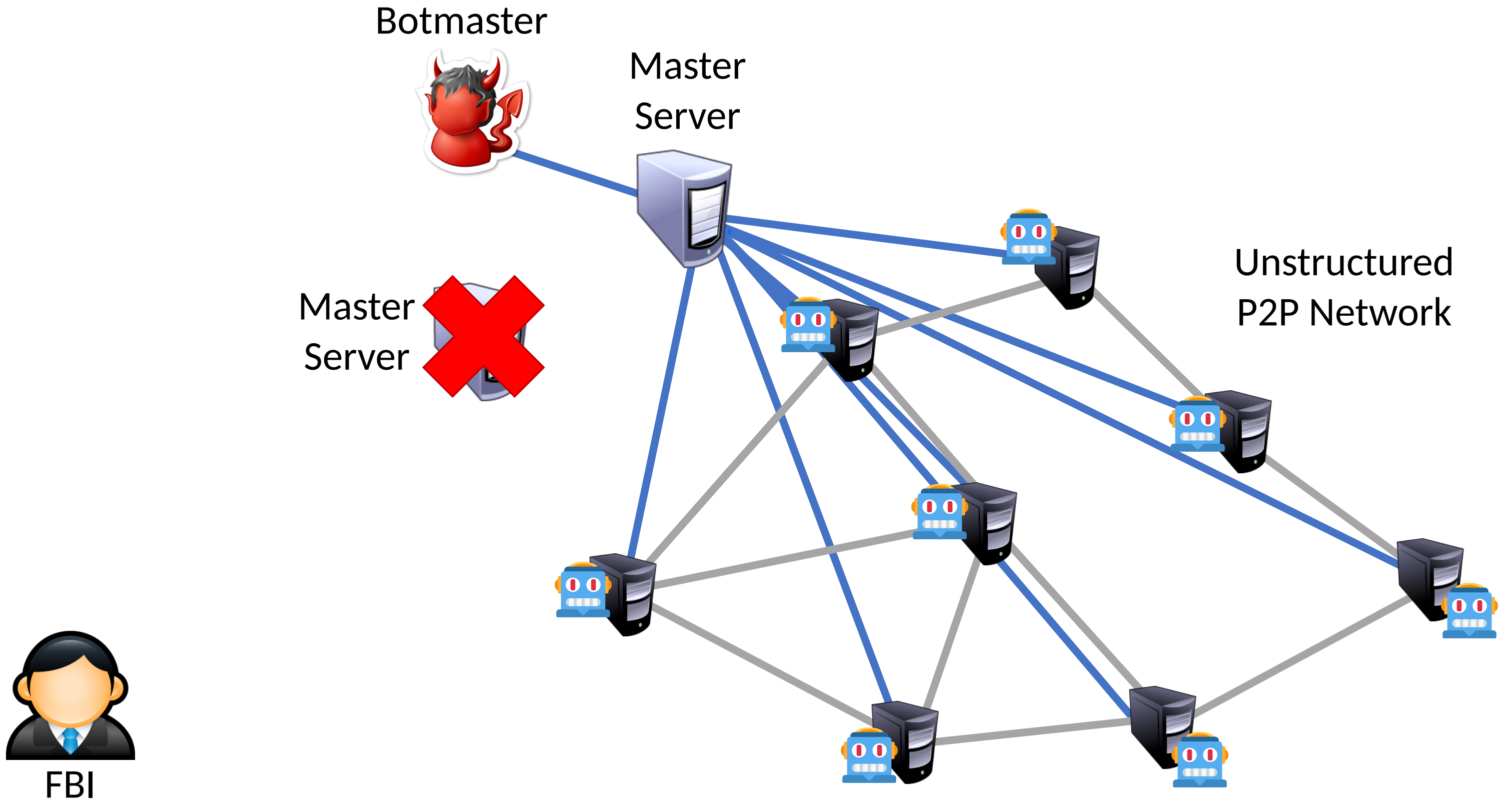
Master Server

Master Server

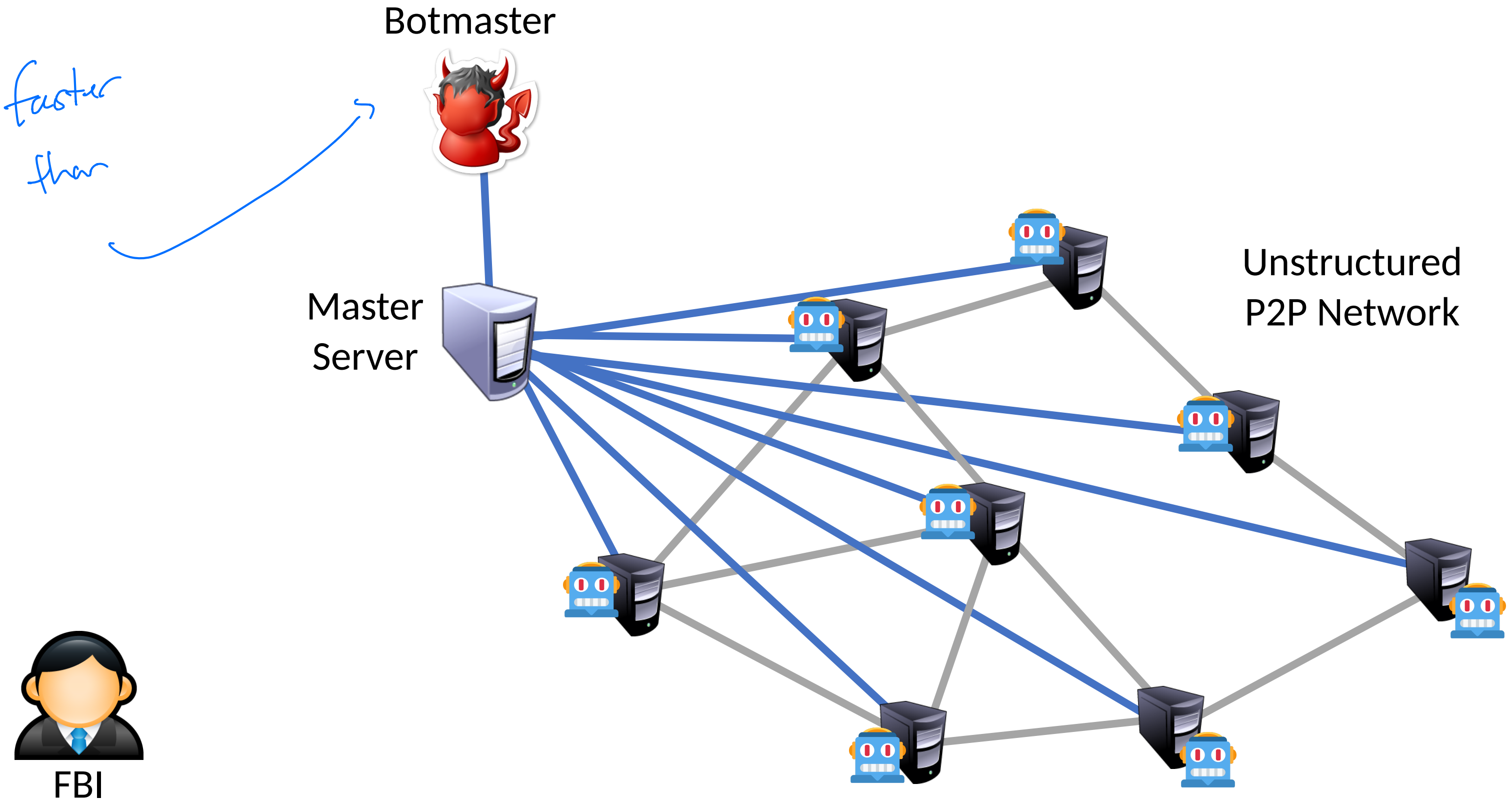
seed

Unstructured P2P Network

FBI


Botmaster
Master Server
Master Server
Unstructured P2P Network
FBI

faster than

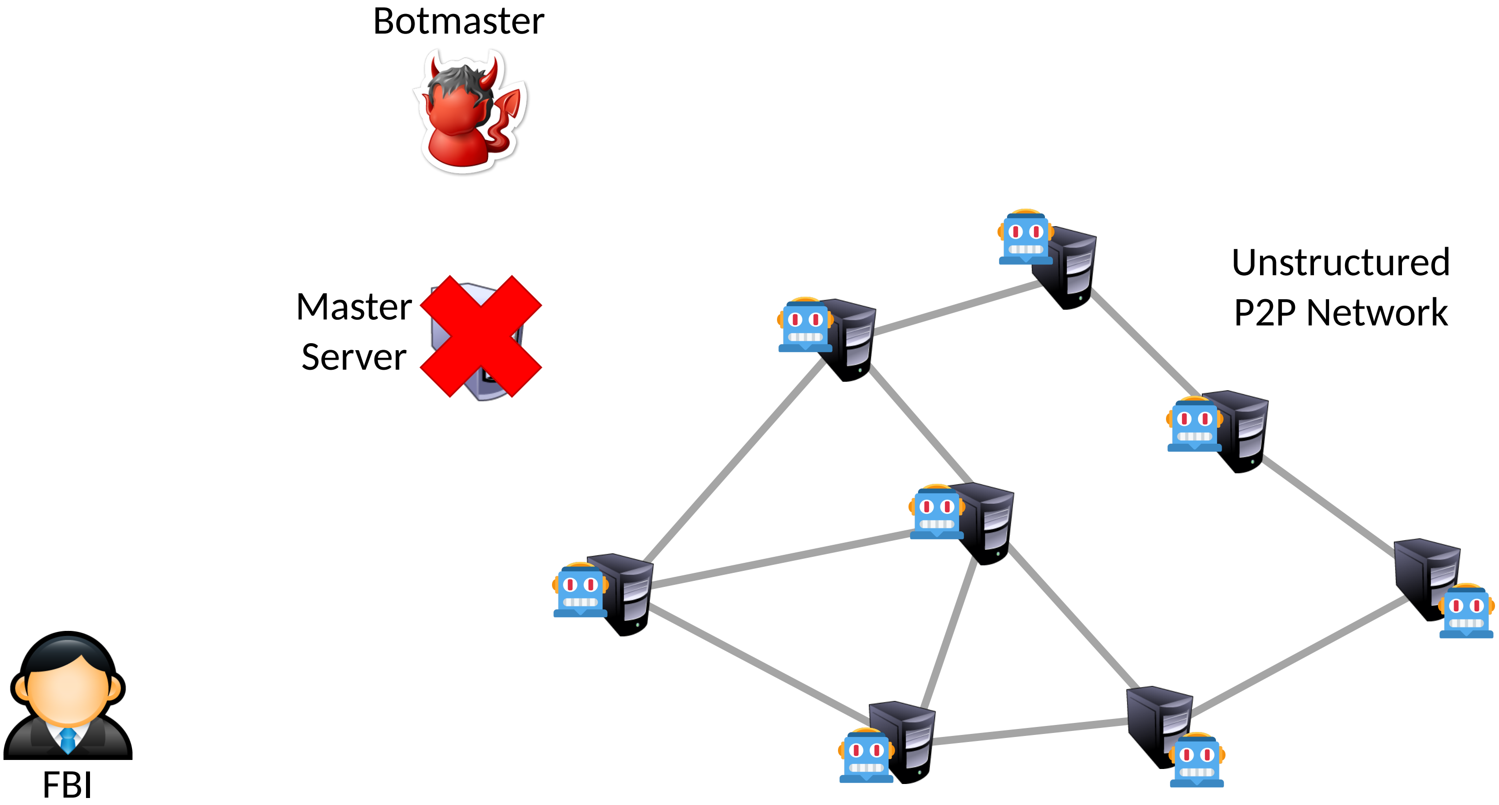


Botmaster

Master Server

Unstructured P2P Network

FBI

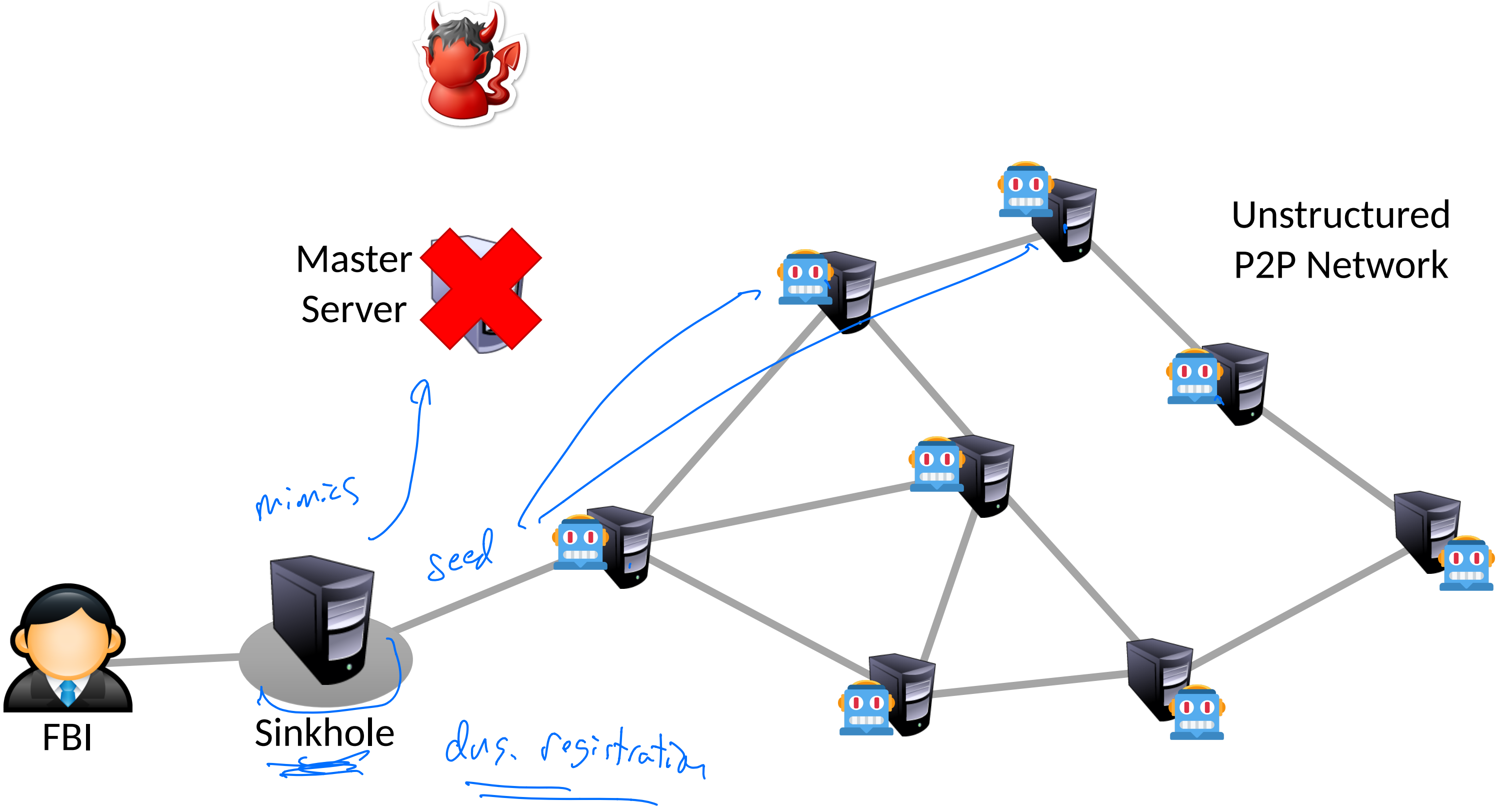


Botmaster

Master Server

Unstructured P2P Network

FBI



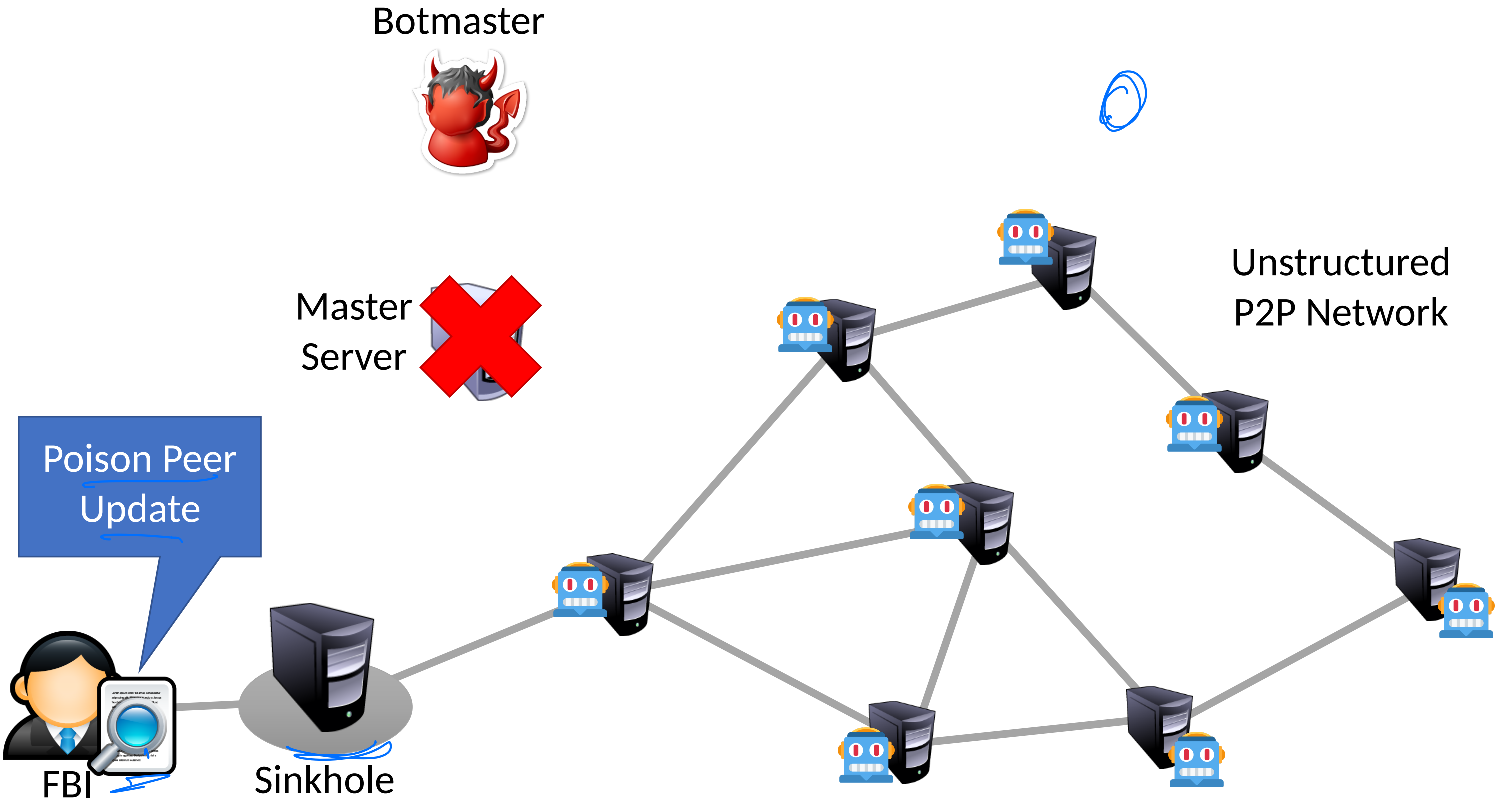
Botmaster

Master Server

Unstructured P2P Network

FBI

Sinkhole



Botmaster

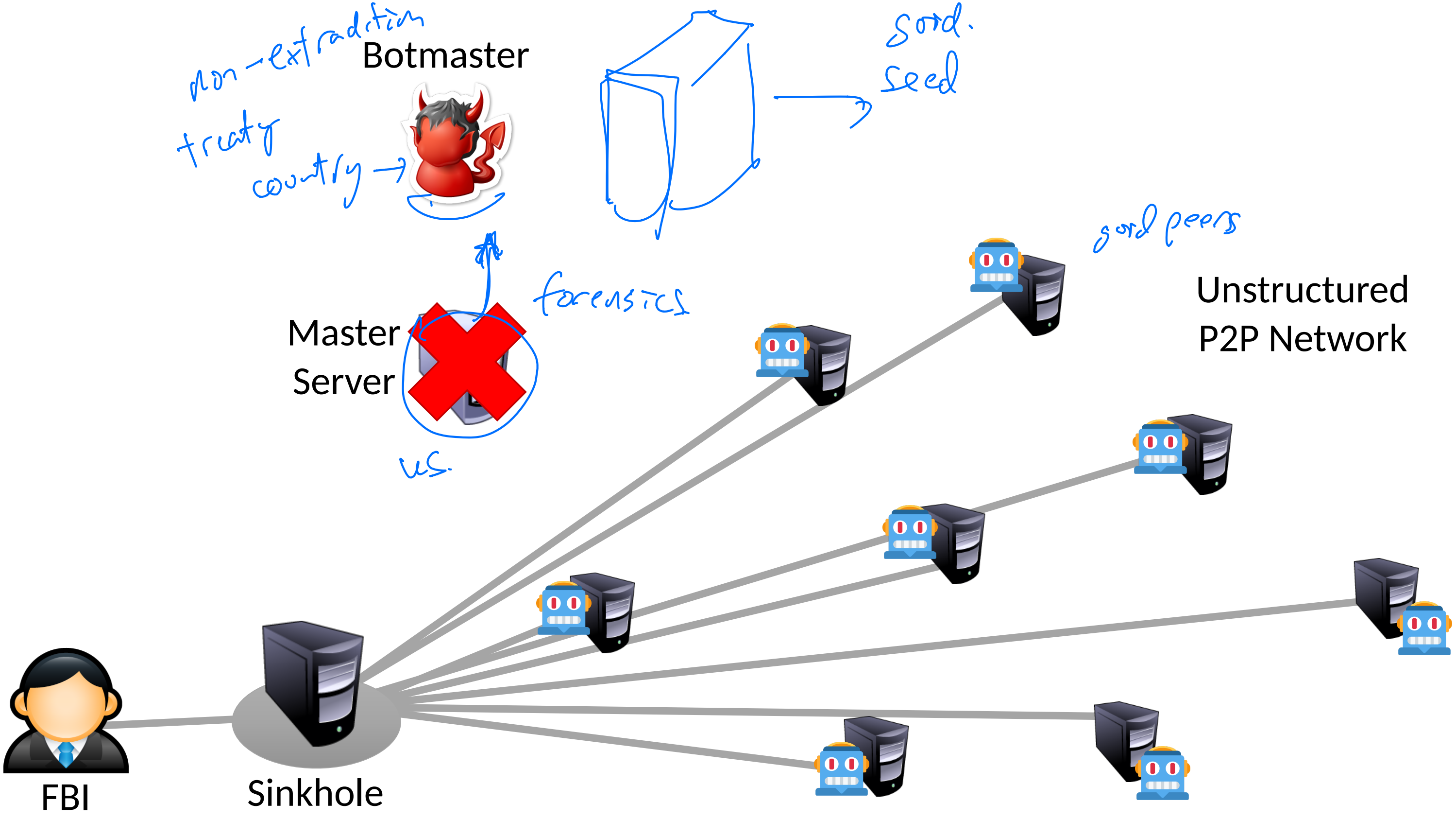
Master Server

Unstructured P2P Network

Poison Peer Update

FBI

Sinkhole



non-extradition treaty country

Botmaster

good. seed

forensics

Master Server

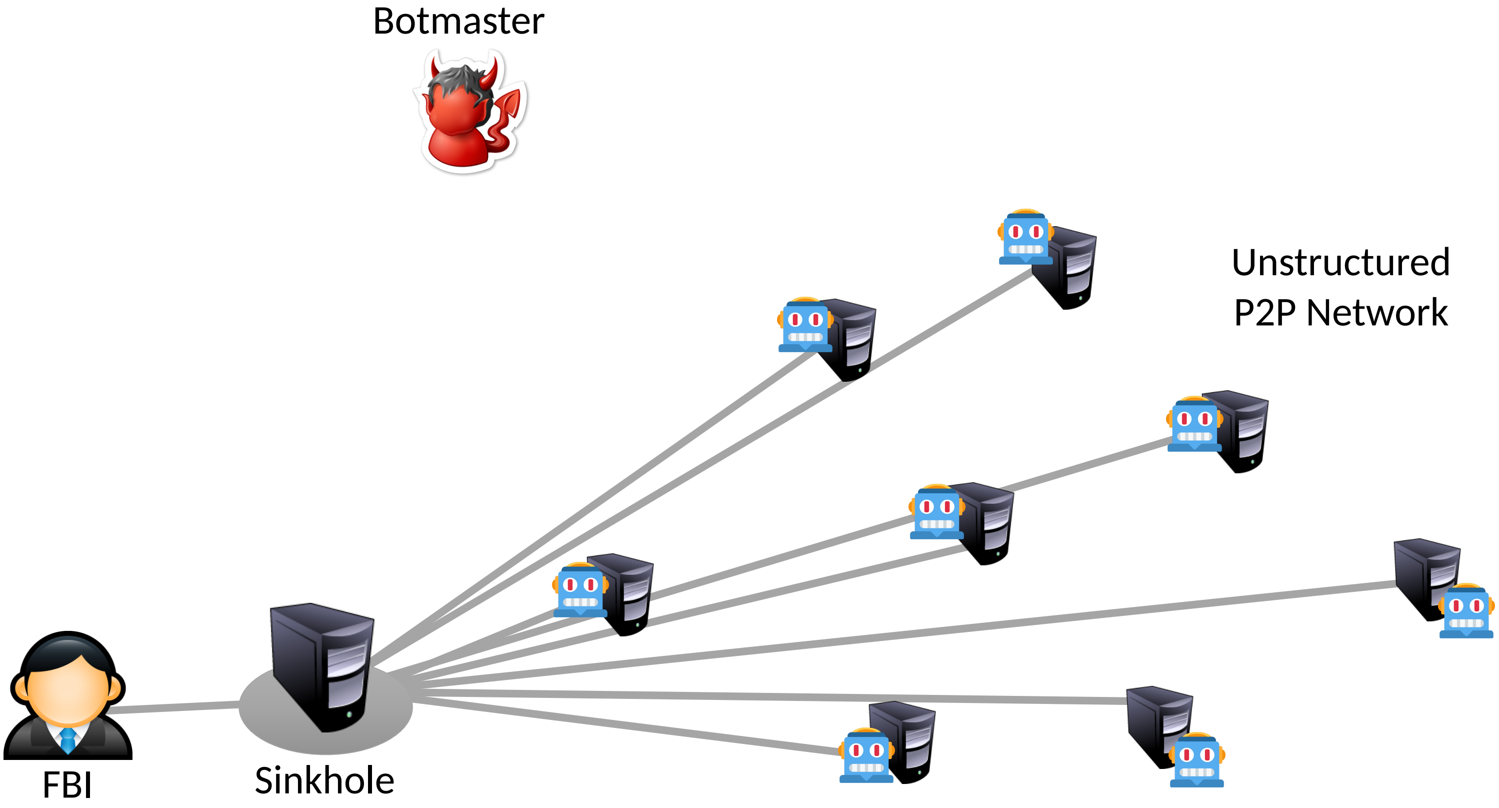
U.S.

good peers

Unstructured P2P Network

FBI

Sinkhole

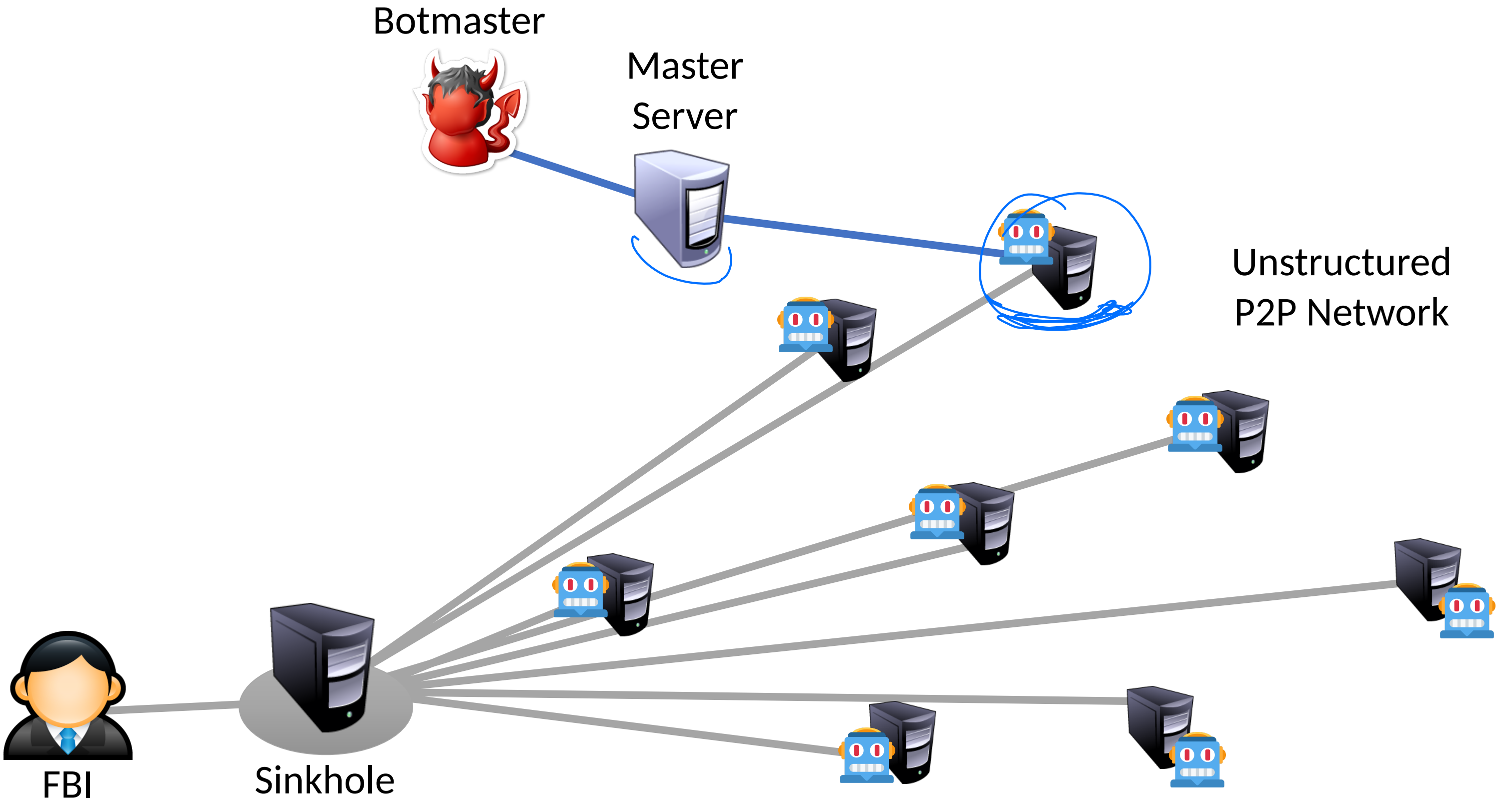


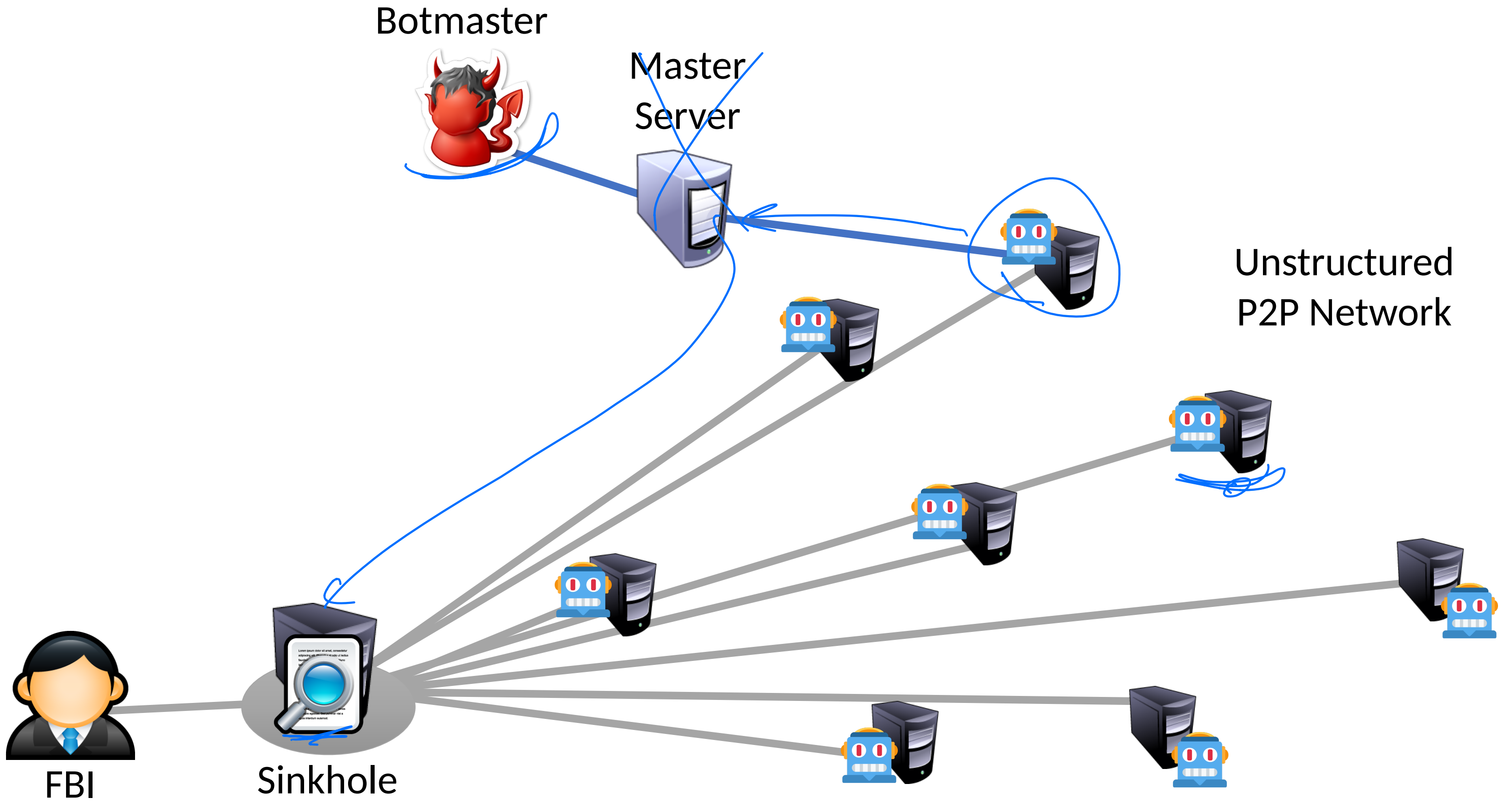
Botmaster

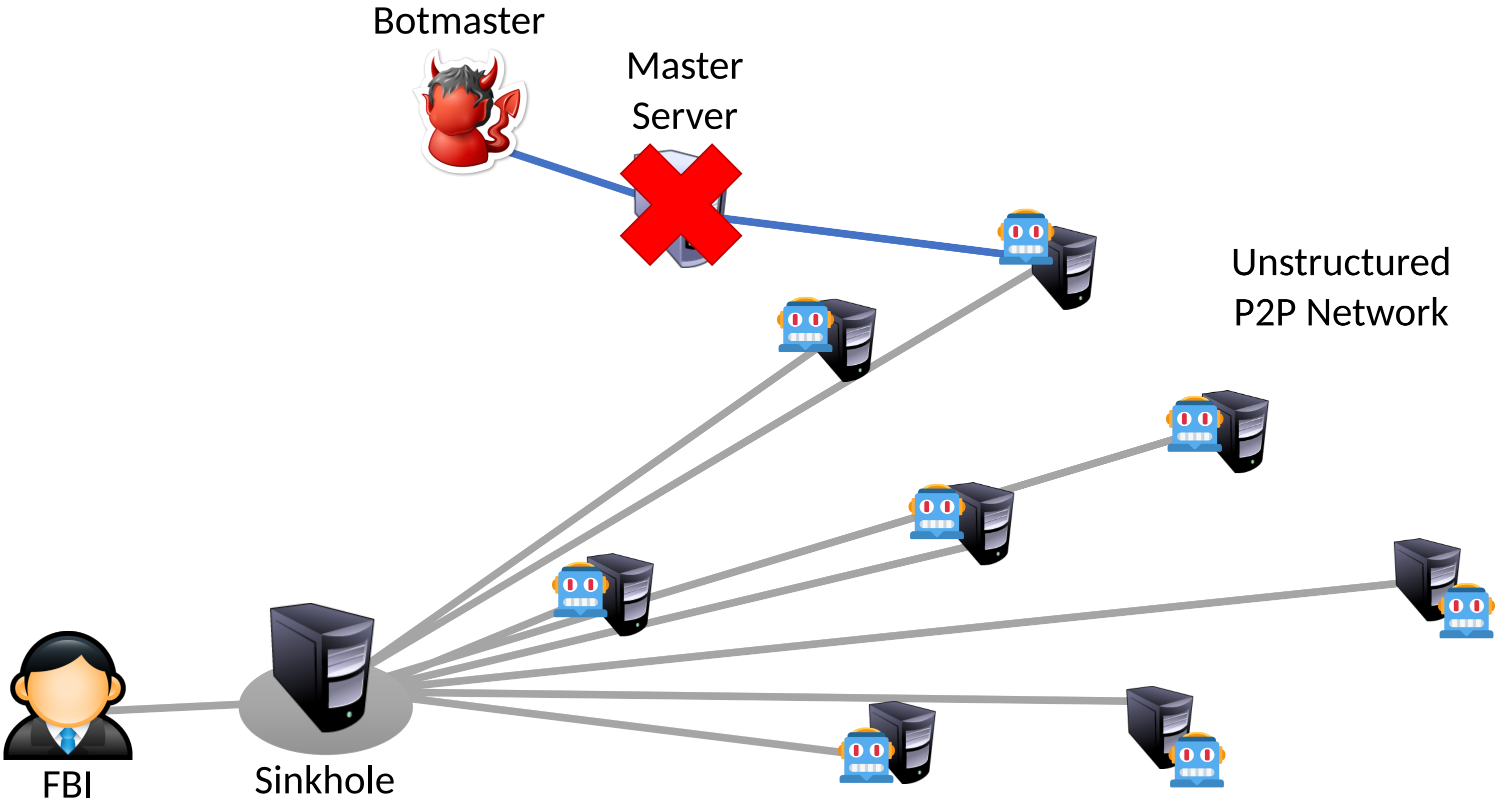
Unstructured P2P Network

FBI

Sinkhole


Botmaster
Master Server
Unstructured P2P Network
FBI
Sinkhole


Botmaster
~~Master Server~~
Unstructured
P2P Network
FBI
Sinkhole


Botmaster
Master Server
Unstructured P2P Network
FBI
Sinkhole

Botnet attack enable.

Denial of service

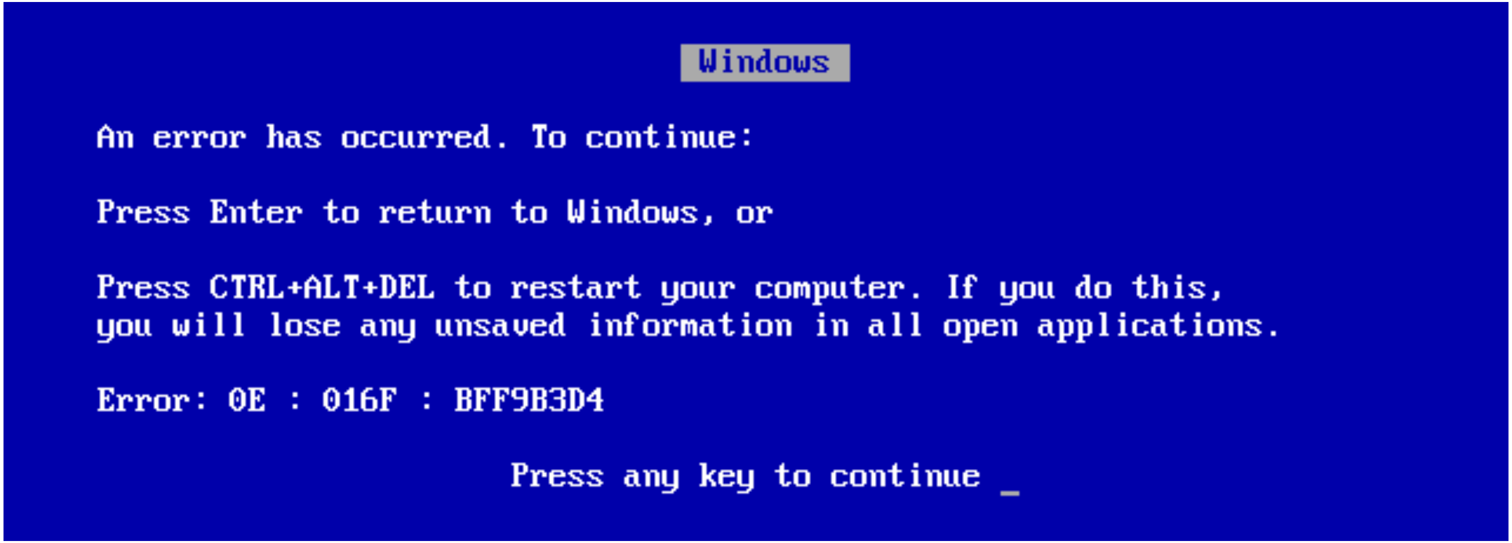
Ping of Death

```
$ ping –s 65535 66.66.0.255
```

size

Ping of Death

```
$ ping –s 65535 66.66.0.255
```



Windows

An error has occurred. To continue:

Press Enter to return to Windows, or

Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.

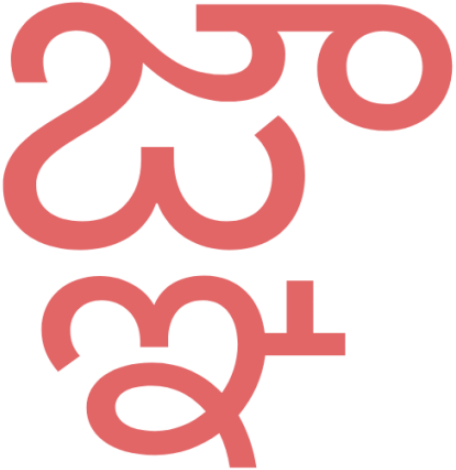
Error: 0E : 016F : BFF9B3D4

Press any key to continue _

iOS Teluga Unicode Bug

- February 2018: iPhones and iPads crash if they receive text or email containing a specific symbol in Indian “likely story??” parsing error in iOS code
- In some cases, reboot doesn’t solve the issue
  - Apps reload bugged messages automatically on startup and crash again
- Device wipe is sometimes the only fix

symbol



Denial of Service (DoS)

- Prevent users from being able to access a specific computer, service, or piece of data
- In essence, an attack on availability

Denial of Service (DoS)

- Prevent users from being able to access a specific computer, service, or piece of data
- In essence, an attack on availability
- Possible vectors:
  - Exploit bugs that lead to crashes
  - Exhaust the resources of a target

Network, Memory

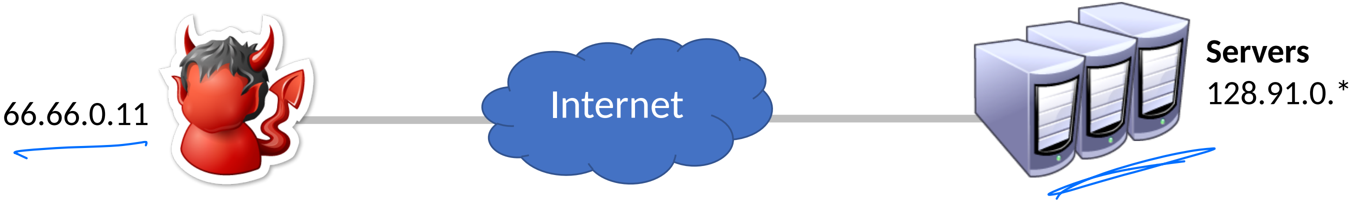
Denial of Service (DoS)

- Prevent users from being able to access a specific computer, service, or piece of data
- In essence, an attack on availability
- Possible vectors:
  - Exploit bugs that lead to crashes
  - Exhaust the resources of a target

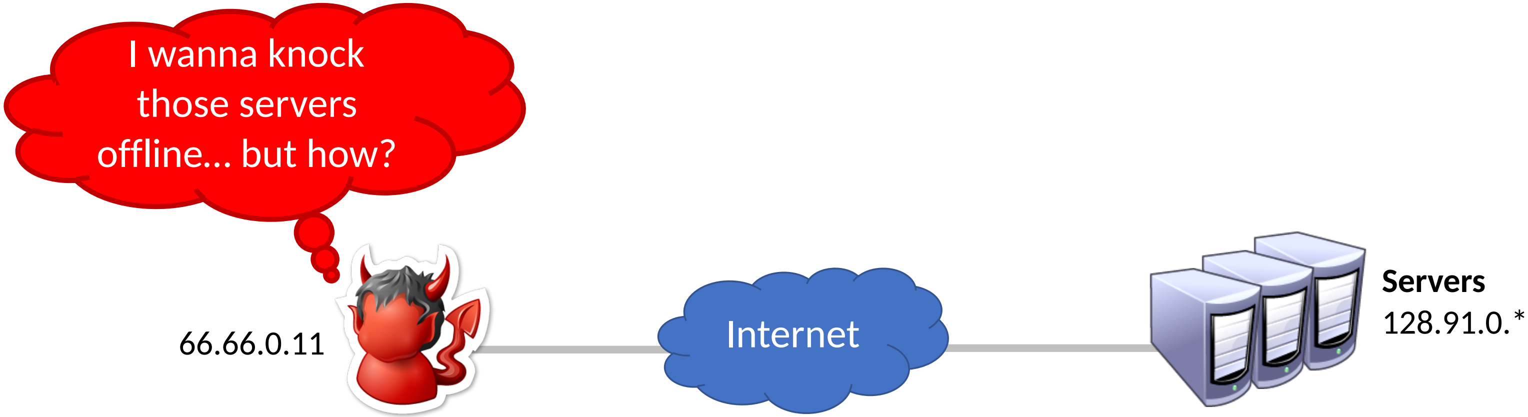
Denial of Service (DoS)

- Prevent users from being able to access a specific computer, service, or piece of data
- In essence, an attack on availability
- Possible vectors:
  - Exploit bugs that lead to crashes
  - Exhaust the resources of a target
- Often very easy to perform…
- … and fiendishly difficult to mitigate

Attacker Goals and Threat Model

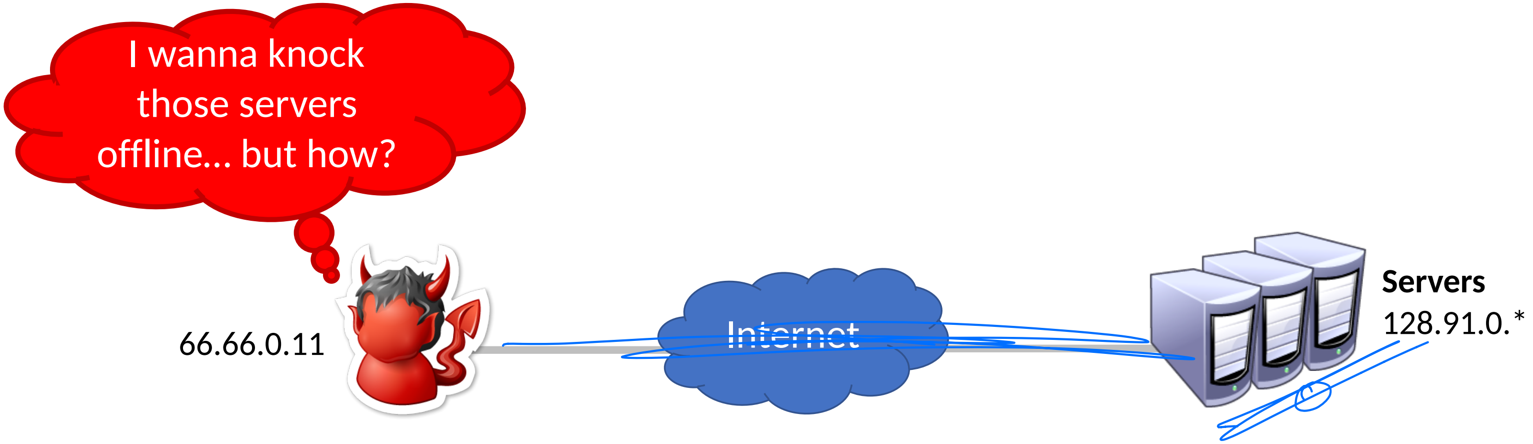


Attacker Goals and Threat Model



Attacker Goals and Threat Model

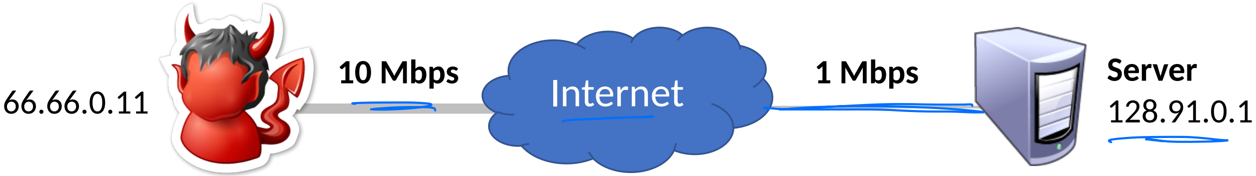
- Active attacker who may send arbitrary packets
- Goal is to reduce the availability of the victim



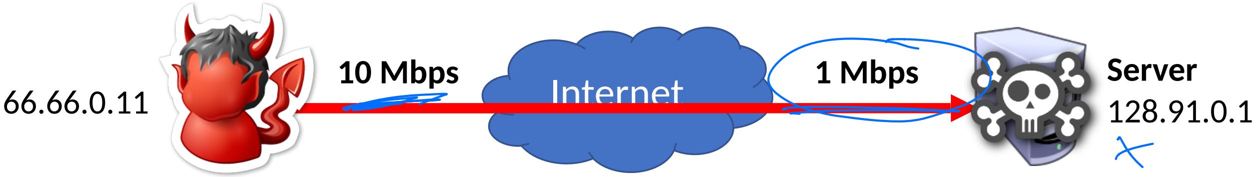
DoS Attack Parameters

1. How much bandwidth is available to the attacker?
   - Can be increased by controlling more resources…
   - Or tricking others into participating in the attack
2. What kind of packets do you send to victim?
   - Minimize effort and risk of detection for the attacker…
   - While also maximizing damage to the victim

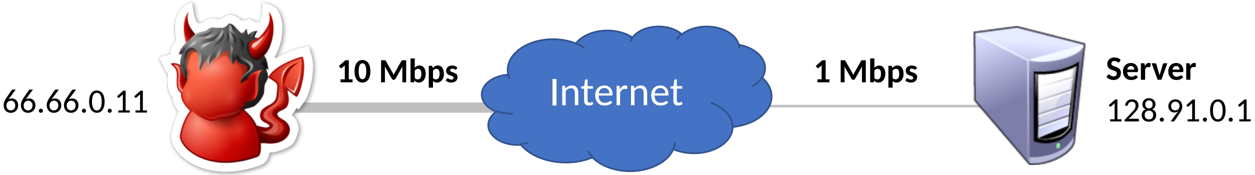
Exploiting Asymmetry



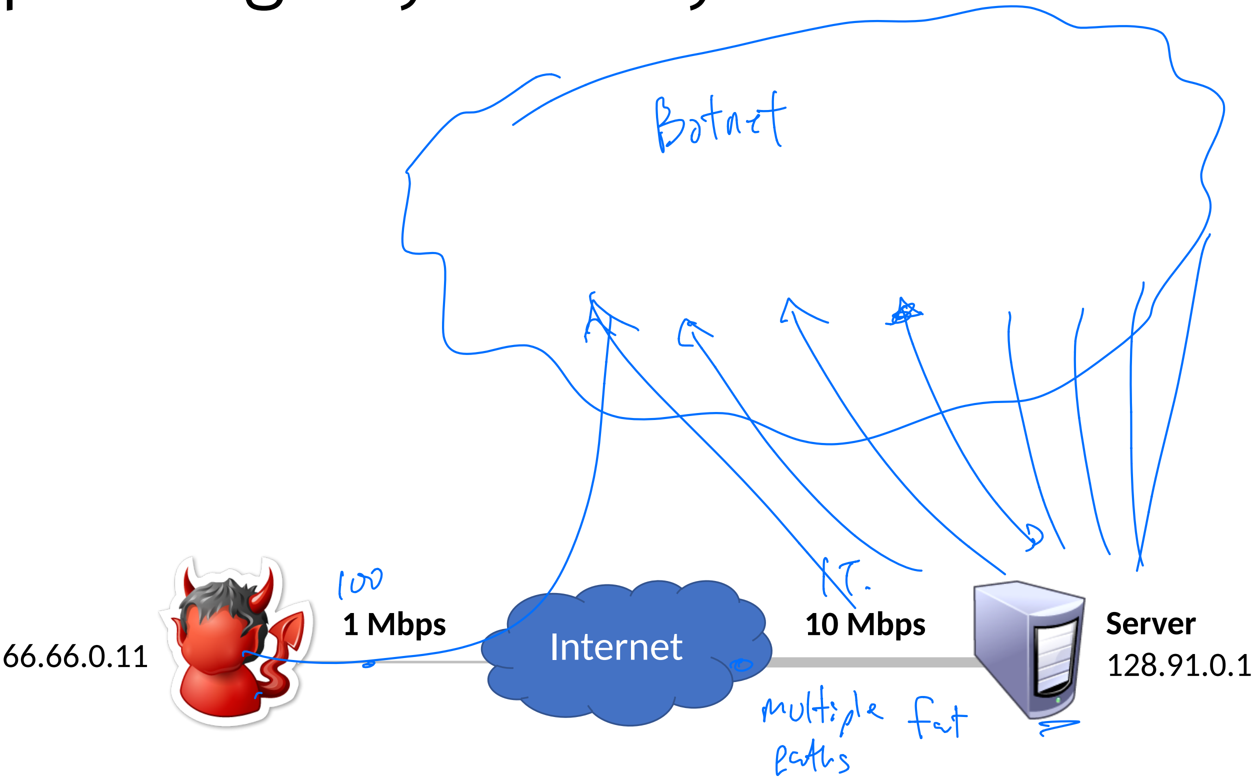
Exploiting Asymmetry



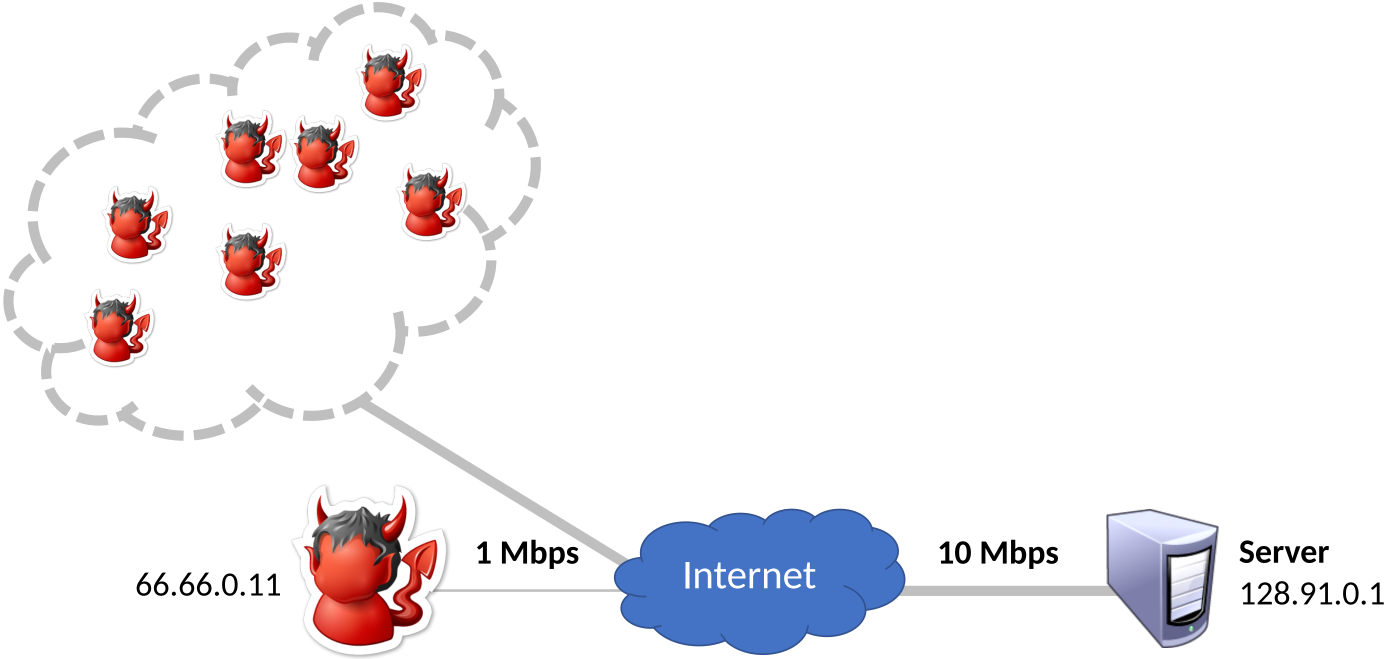
Exploiting Asymmetry



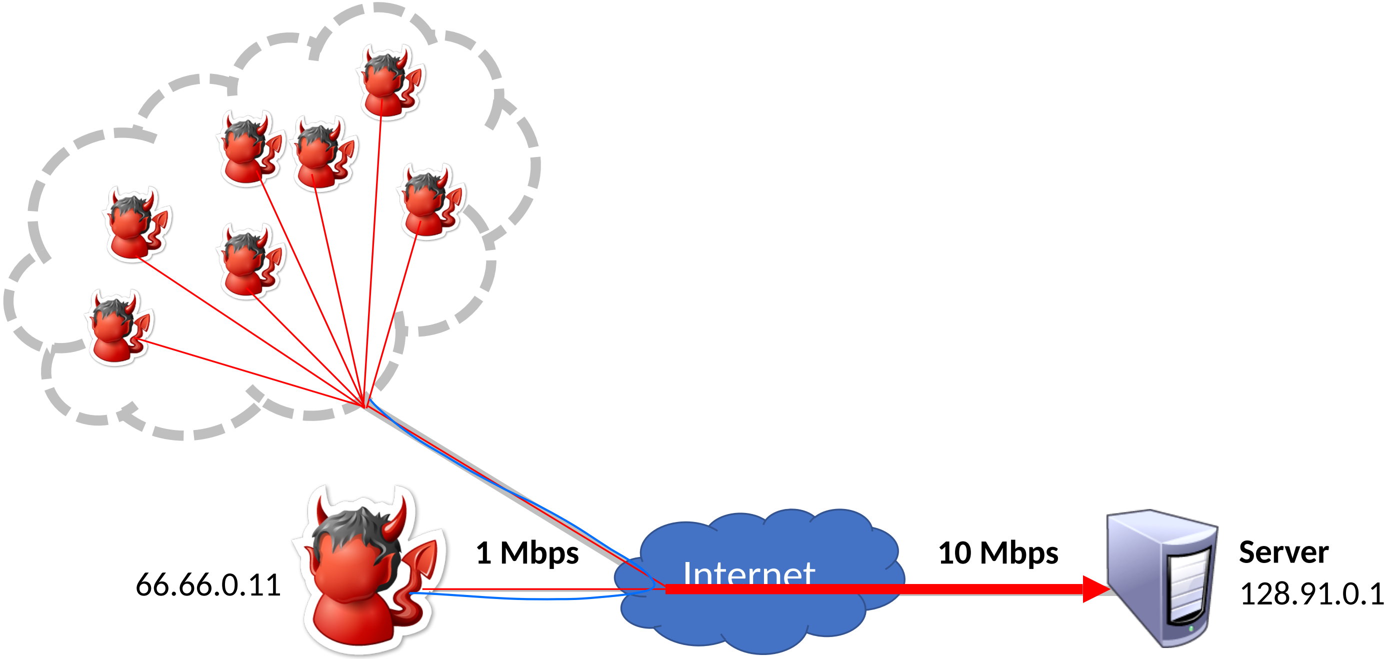
Exploiting Asymmetry



Exploiting Asymmetry



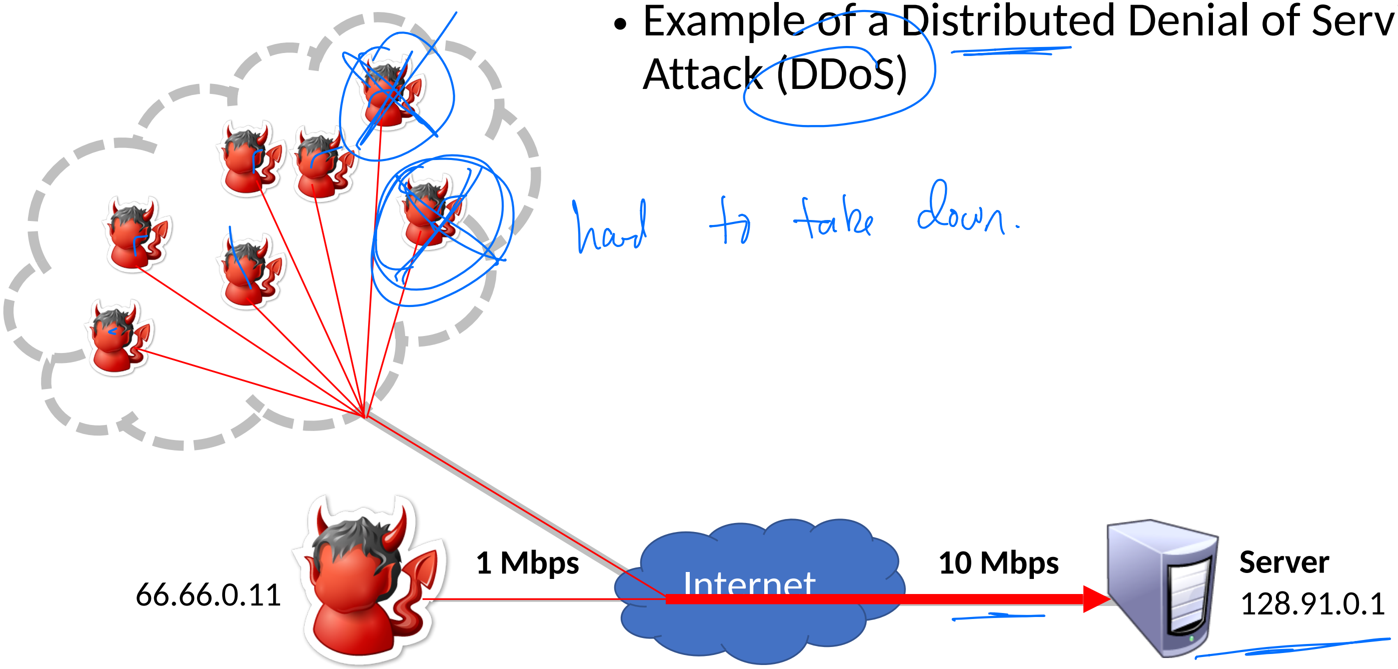
Exploiting Asymmetry



Exploiting Asymmetry

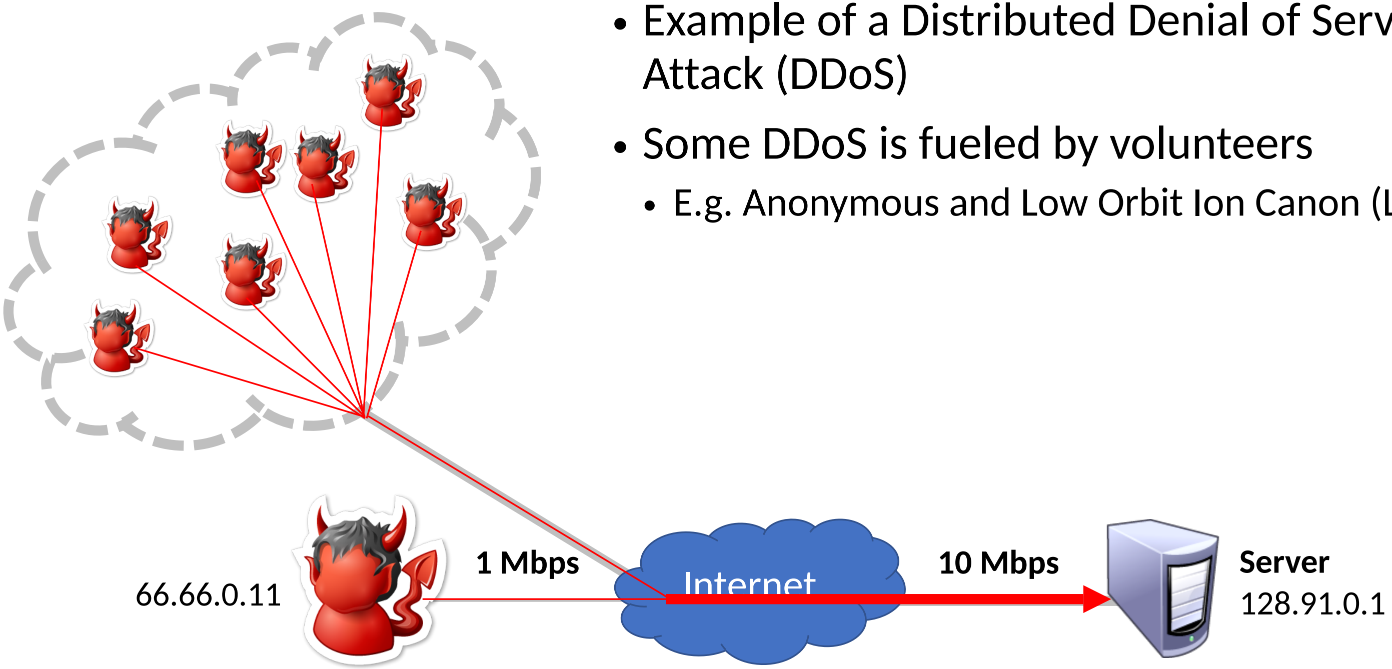
- Example of a Distributed Denial of Service Attack (DDoS)

hard to take down.



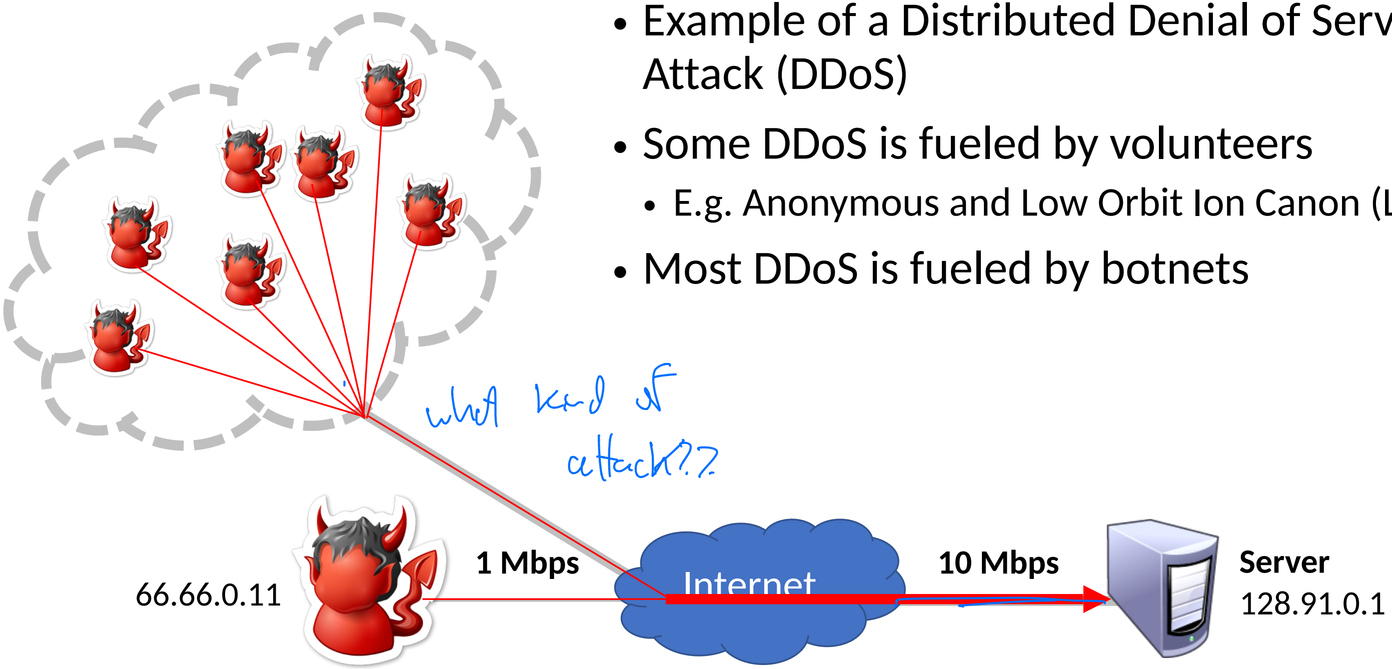
Exploiting Asymmetry

- Example of a Distributed Denial of Service Attack (DDoS)
- Some DDoS is fueled by volunteers
  - E.g. Anonymous and Low Orbit Ion Canon (LOIC)



Exploiting Asymmetry

- Example of a Distributed Denial of Service Attack (DDoS)
- Some DDoS is fueled by volunteers
  - E.g. Anonymous and Low Orbit Ion Canon (LOIC)
- Most DDoS is fueled by botnets

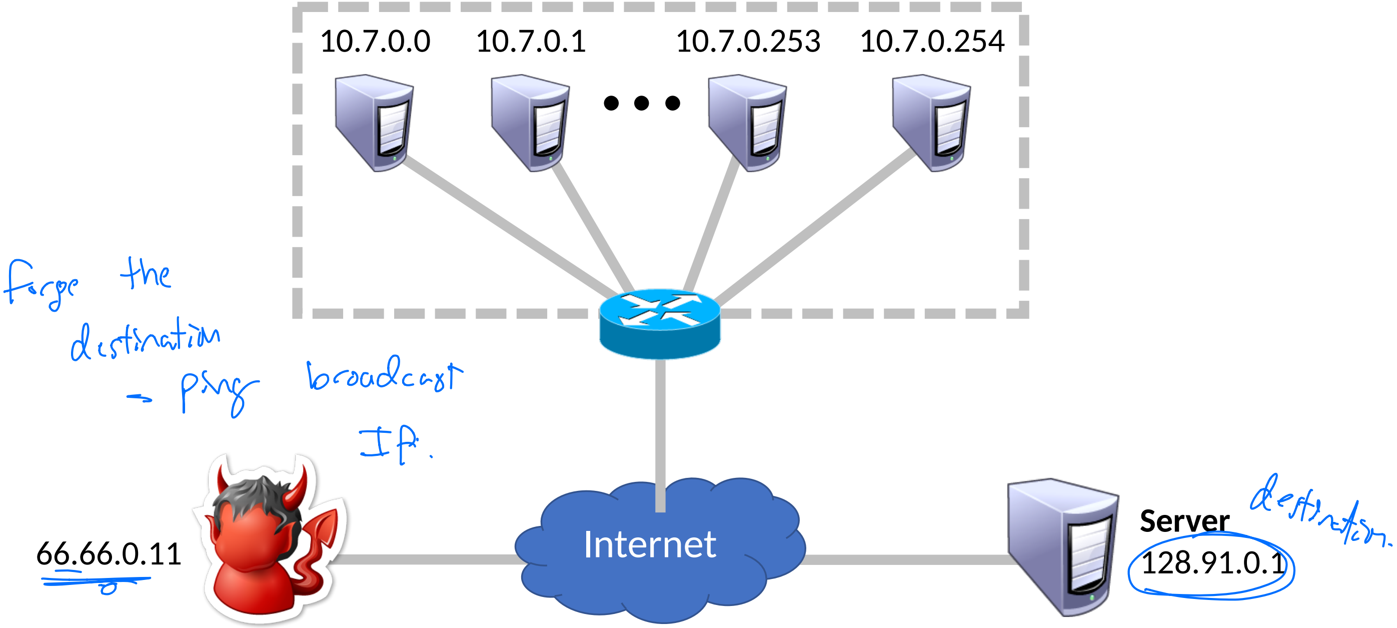


what kind of attack??

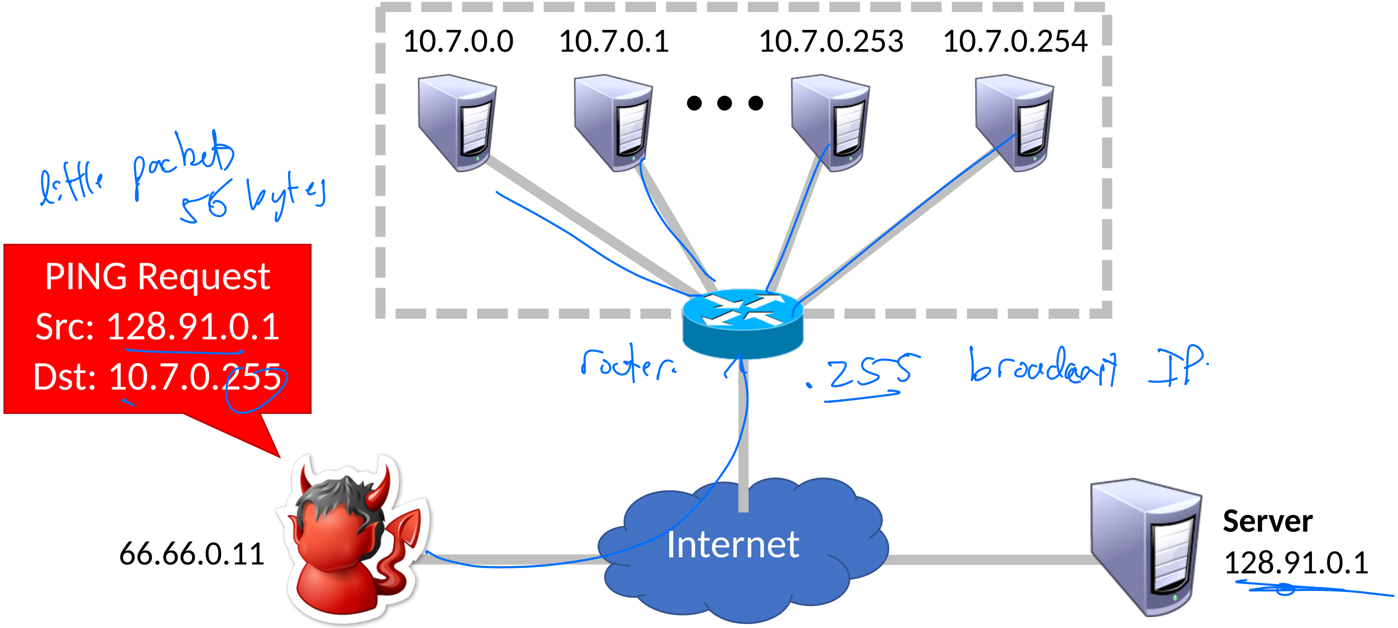
The Smurf Attack

- forge the destination

→ ping broadcast IP.



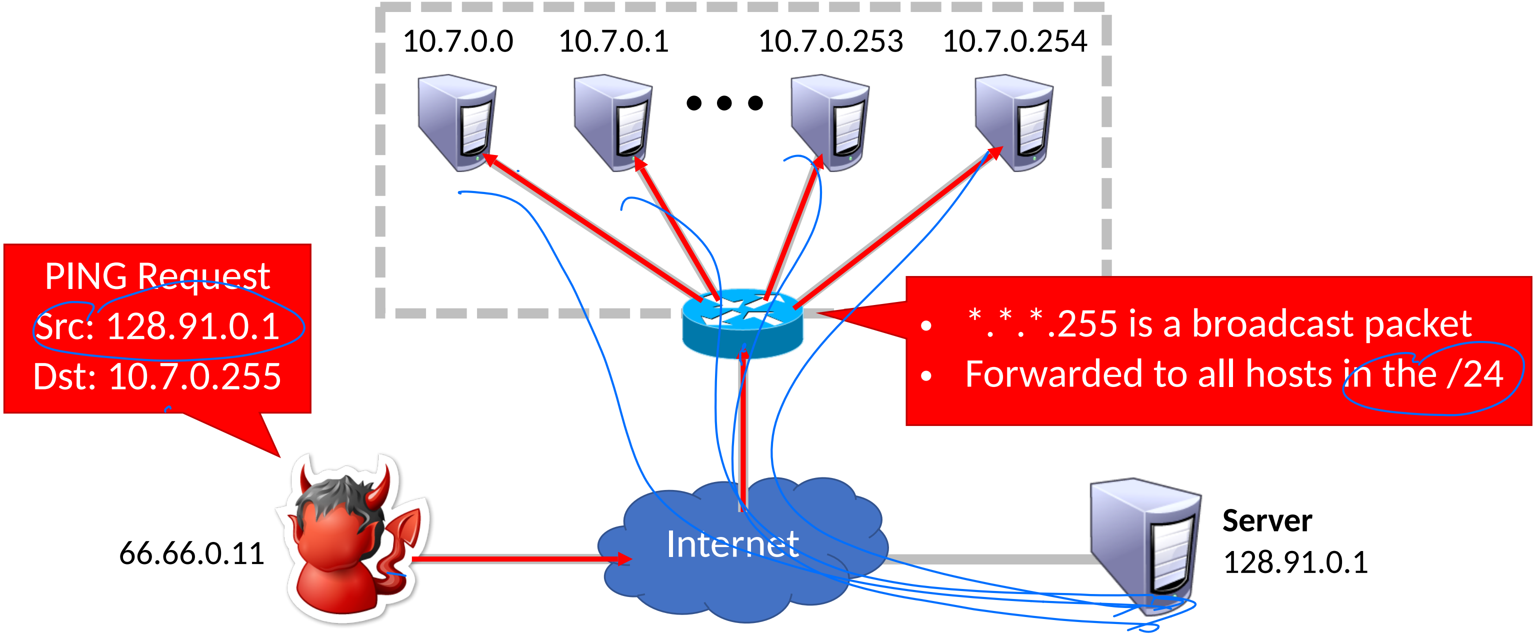
The Smurf Attack



little packets
56 bytes

PING Request
Src: 128.91.0.1
Dst: 10.7.0.255

The Smurf Attack



10.7.0.0

10.7.0.1

10.7.0.253

10.7.0.254

PING Request

Src: 128.91.0.1

Dst: 10.7.0.255

- *.*.*.255 is a broadcast packet
- Forwarded to all hosts in the /24

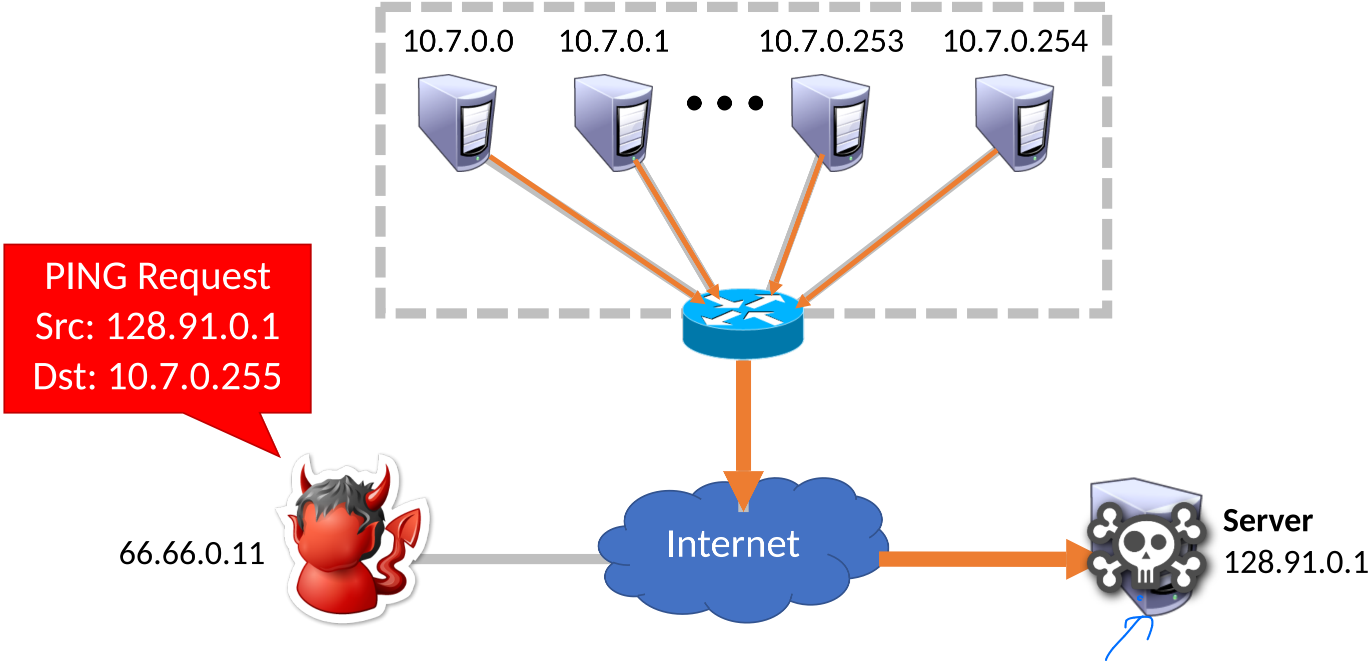
66.66.0.11

Internet

Server

128.91.0.1

The Smurf Attack



PING Request
Src: 128.91.0.1
Dst: 10.7.0.255

10.7.0.0

10.7.0.1

10.7.0.253

10.7.0.254

66.66.0.11

Internet

Server
128.91.0.1

Why Does Smurfing Work?

1. ICMP protocol does not include authentication
   - No connections
   - Receivers accept messages without verifying the source
   - Enables attackers to spoof the source of messages

No Authentication over IP networks.

Why Does Smurfing Work?

1. ICMP protocol does not include authentication
   - No connections
   - Receivers accept messages without verifying the source
   - Enables attackers to spoof the source of messages
2. Attacker benefits from an amplification factor

attacker
small packet → causes lots of traffic.

$$amp\ factor = \frac{total\ response\ size}{request\ size}$$

- Smurf amp factor – *[number of servers that respond to the broadcast]:1*

Modern defense

```
Router(config-if)# no ip directed-broadcast[5]
```

cisco rule for routers.

Reflection/Amplification Attacks

- Smurfing is an example of a reflection or amplification DDoS attack
- Fraggle attack also relies on broadcasts for amplification
  - Send spoofed UDP packets to IP broadcast addresses on port 7 (*echo*) and 13 (*chargen*)
    - *echo* – 1500 bytes/pkt requests, equal size responses
    - *chargen* -- 28 bytes/pkt request, 10K-100K bytes of ASCII in response
  - Amp factor
    - *echo – [number of hosts responding to the broadcast]:1*
    - *chargen – [number of hosts responding to the broadcast]*360:1*

DNS Reflection Attack

- Spoof DNS requests to many **open** DNS resolvers
    - DNS is a UDP-based protocol, no authentication of requests
    - Open resolvers accept requests from any client
        - E.g. 8.8.8.8, 8.8.4.4, 1.1.1.1, 1.0.0.1
    - February 2014 – 25 million open DNS resolvers on the internet

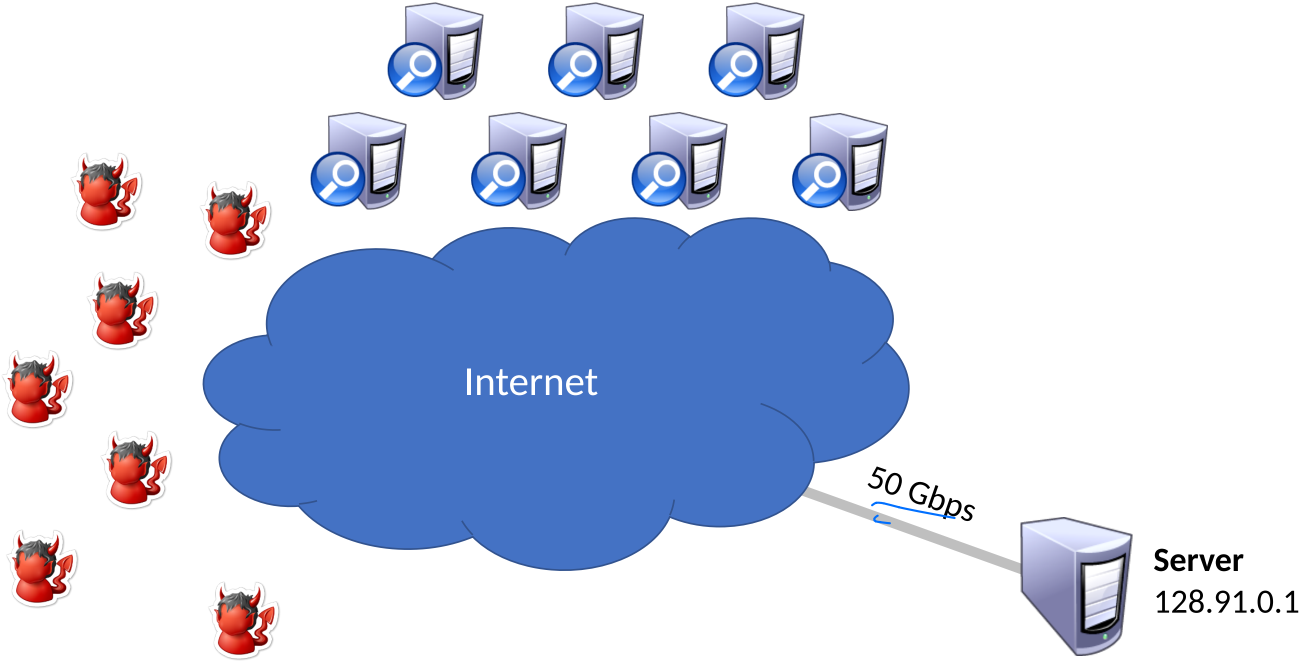
DNS Reflection Attack

- Spoof DNS requests to many **open** DNS resolvers
  - DNS is a UDP-based protocol, no authentication of requests
  - Open resolvers accept requests from any client
    - E.g. 8.8.8.8, 8.8.4.4, 1.1.1.1, 1.0.0.1
  - February 2014 – 25 million open DNS resolvers on the internet
- 64 byte DNS queries generate large responses
  - Old-school "A" record query → maximum 512 byte response
  - EDNS0 extension "ANY" record query → 1000-6000 byte response
    - E.g. $ dig ANY isc.org
  - Amp factor – *180:1*

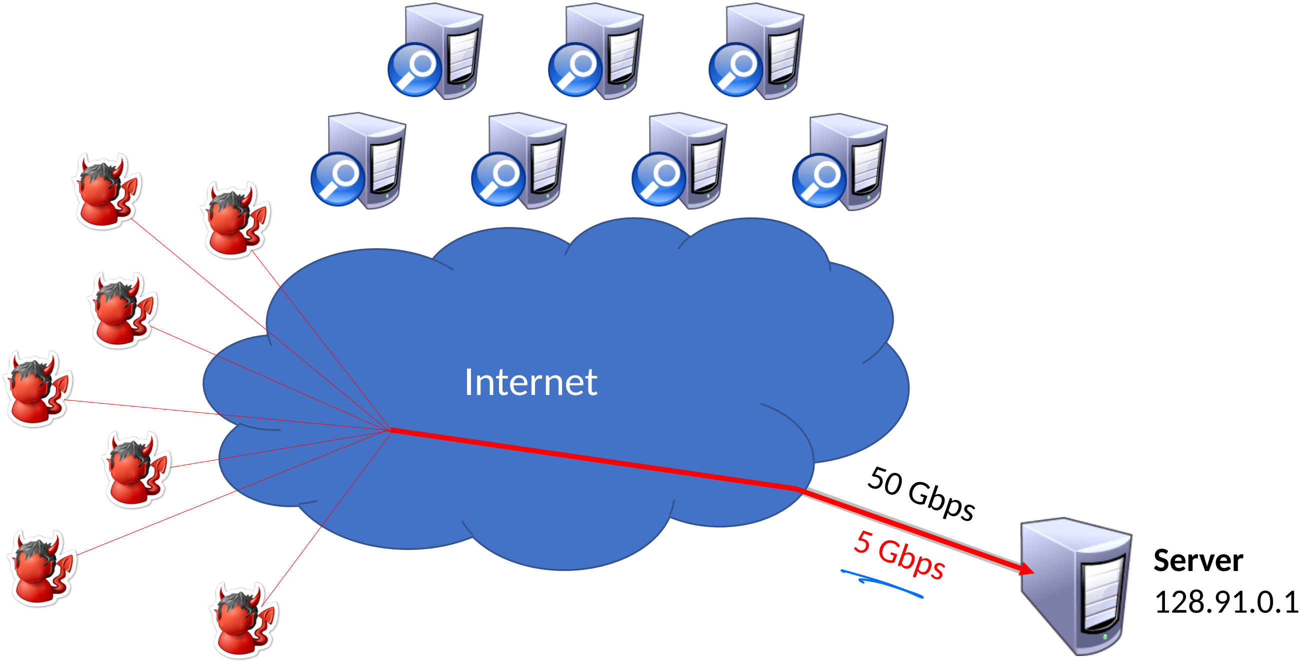
DNS Reflection Attack

- Spoof DNS requests to many **open** DNS resolvers
  - DNS is a UDP-based protocol, no authentication of requests
  - Open resolvers accept requests from any client
    - E.g. 8.8.8.8, 8.8.4.4, 1.1.1.1, 1.0.0.1
  - February 2014 – 25 million open DNS resolvers on the internet
- 64 byte DNS queries generate large responses
  - Old-school “A” record query → maximum 512 byte response
  - EDNS0 extension “ANY” record query → 1000-6000 byte response
    - E.g. $ dig ANY isc.org
  - Amp factor – *180:1*
- Attackers have been known to register their own domains and install very large records just to enable reflection attacks!

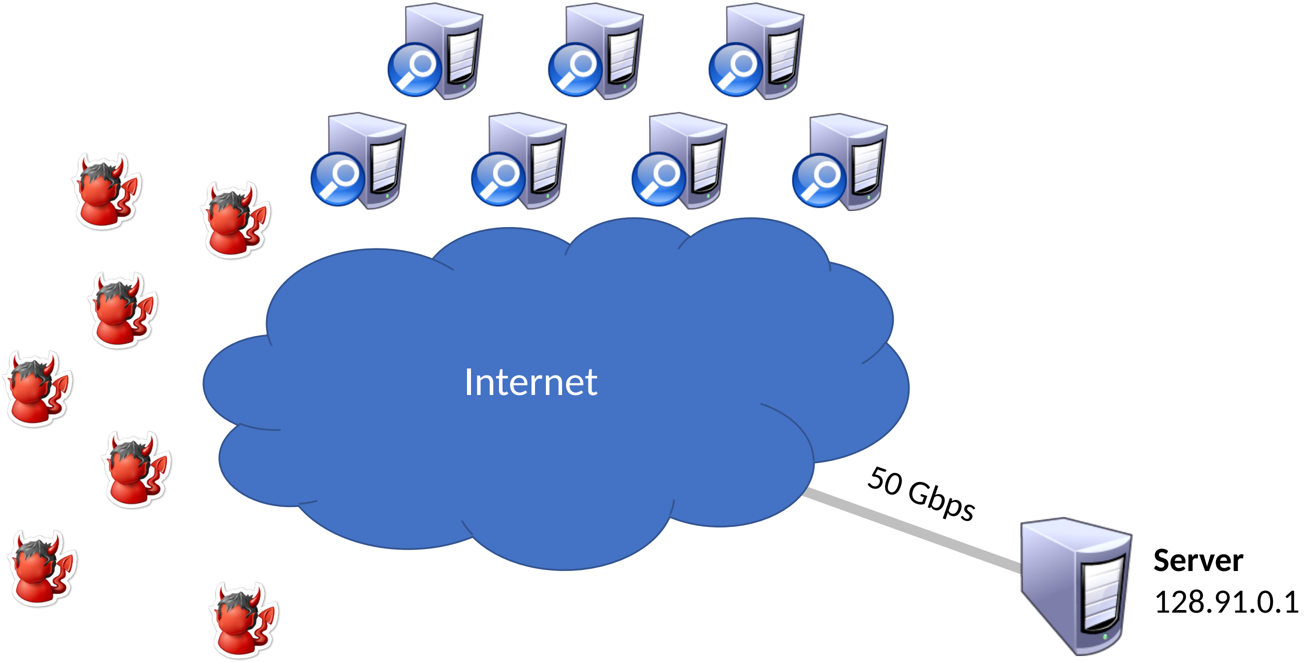
Reflection Example



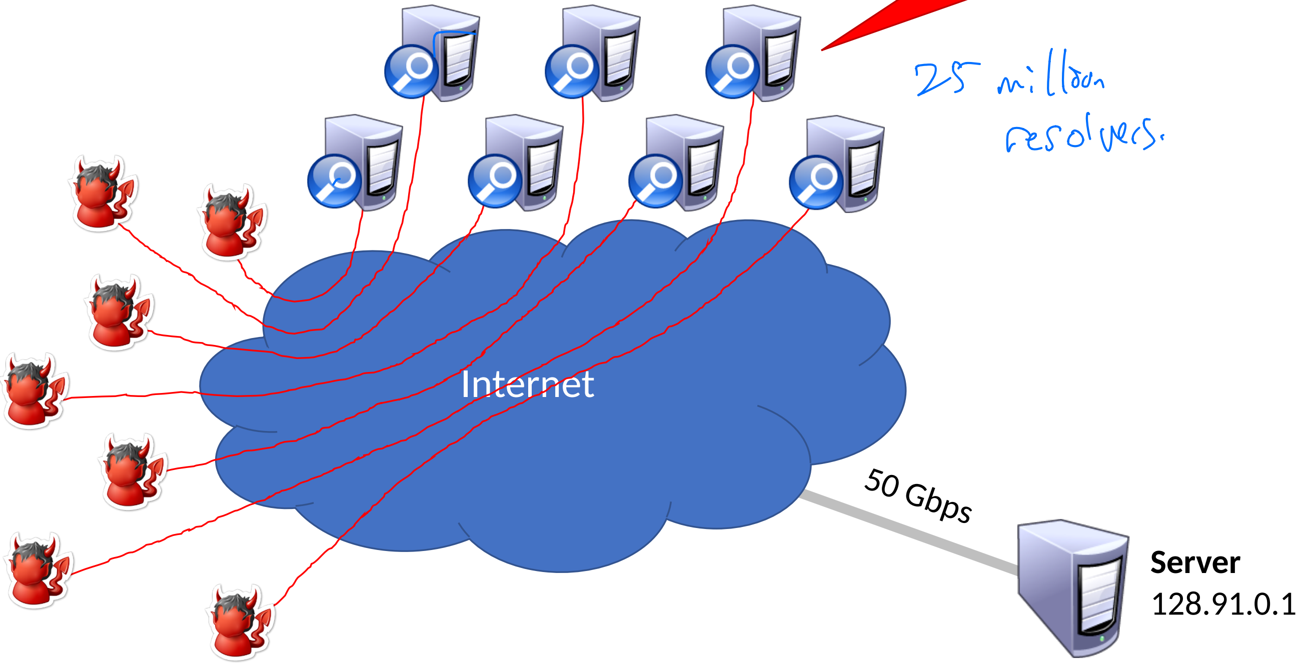
Reflection Example



Reflection Example

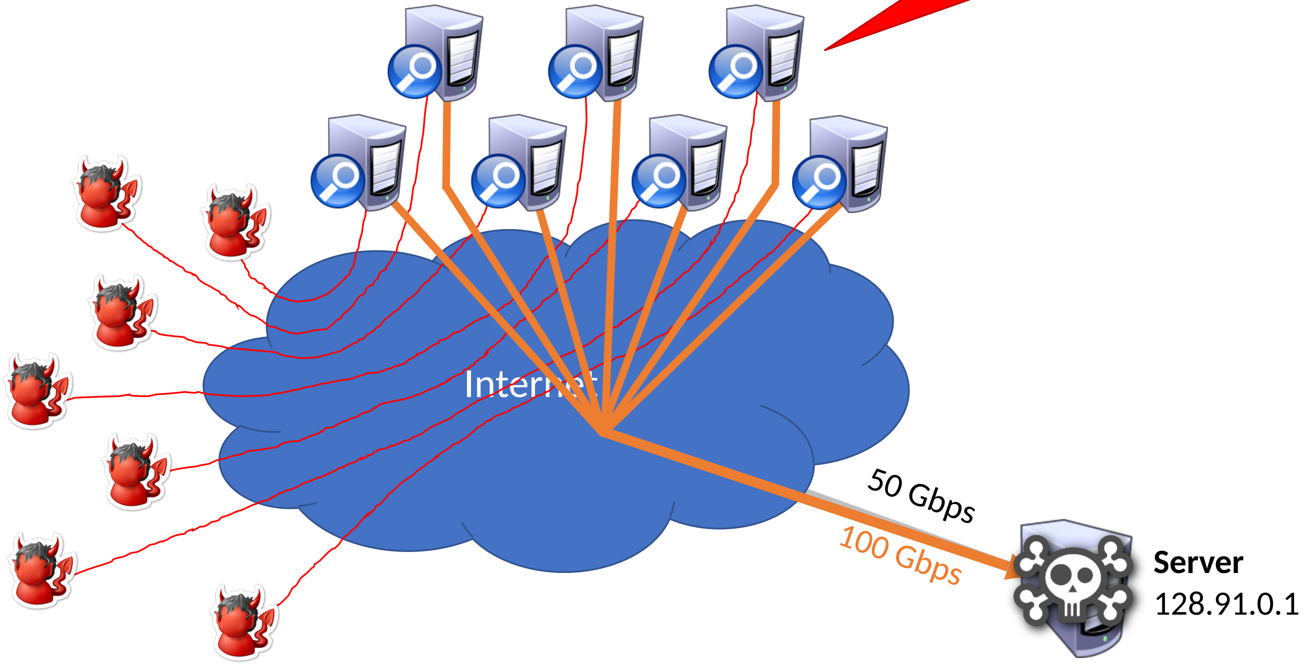


Reflection Example



Reflection Example

DNS Request
Src: 128.91.0.1
Dst: whatever

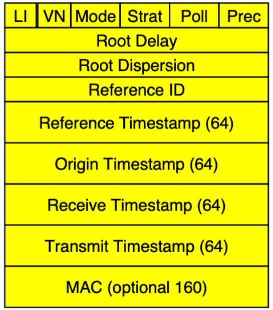


NTP Reflection Attack

time.apple.com

network time protocol

- Spoof requests to open Network Time Protocol (NTP) servers
  - NTP is a UDP-based protocol, no authentication of requests
  - May 2014 – 2.2 million open NTP servers on the internet
- 234 byte queries generate large responses
  - *monlist* query: server returns a list of all recent connections
  - Other queries are possible, i.e. *version* and *showpeers*
  - Amp factor – from *10:1* to *560:1*



LI	VN	Mode	Strat	Poll	Prec
Root Delay					
Root Dispersion					
Reference ID					
Reference Timestamp (64)					
Origin Timestamp (64)					
Receive Timestamp (64)					
Transmit Timestamp (64)					
MAC (optional 160)					

memcached Reflection Attack

- Spoof requests to open memcached servers
  - Popular <key:value> server used to cache web objects
  - memcached uses a UDP-based protocol, no authentication of requests
  - February 2018 – 50k open memcached servers on the internet
- 1460 byte queries generate large responses
  - A single query can request multiple 1MB <key:value> pairs from the database
  - Amp factor – up to *50000:1*

Reflection Amplification

Protocol	Amplification Factor
memcached	50000
NTP	557
chargen	359
DNS	179
QOTD	140
BitTorrent	54
SSDP	31
SNMPv2	6
Steam	6
NetBIOS	4

Infamous DDoS Attacks

When	Against Who	Size	How
March 2013	Spamhaus	120 Gbps	Botnet + DNS reflection
February 2014	Cloudflare	400 Gbps	Botnet + NTP reflection
September 2016	Krebs	620 Gbps	Mirai IoT
October 2016	Dyn (major DNS provider)	1.2 Tbps	Mirai
March 2018	Github	1.35 Tbps	Botnet + memcached refection

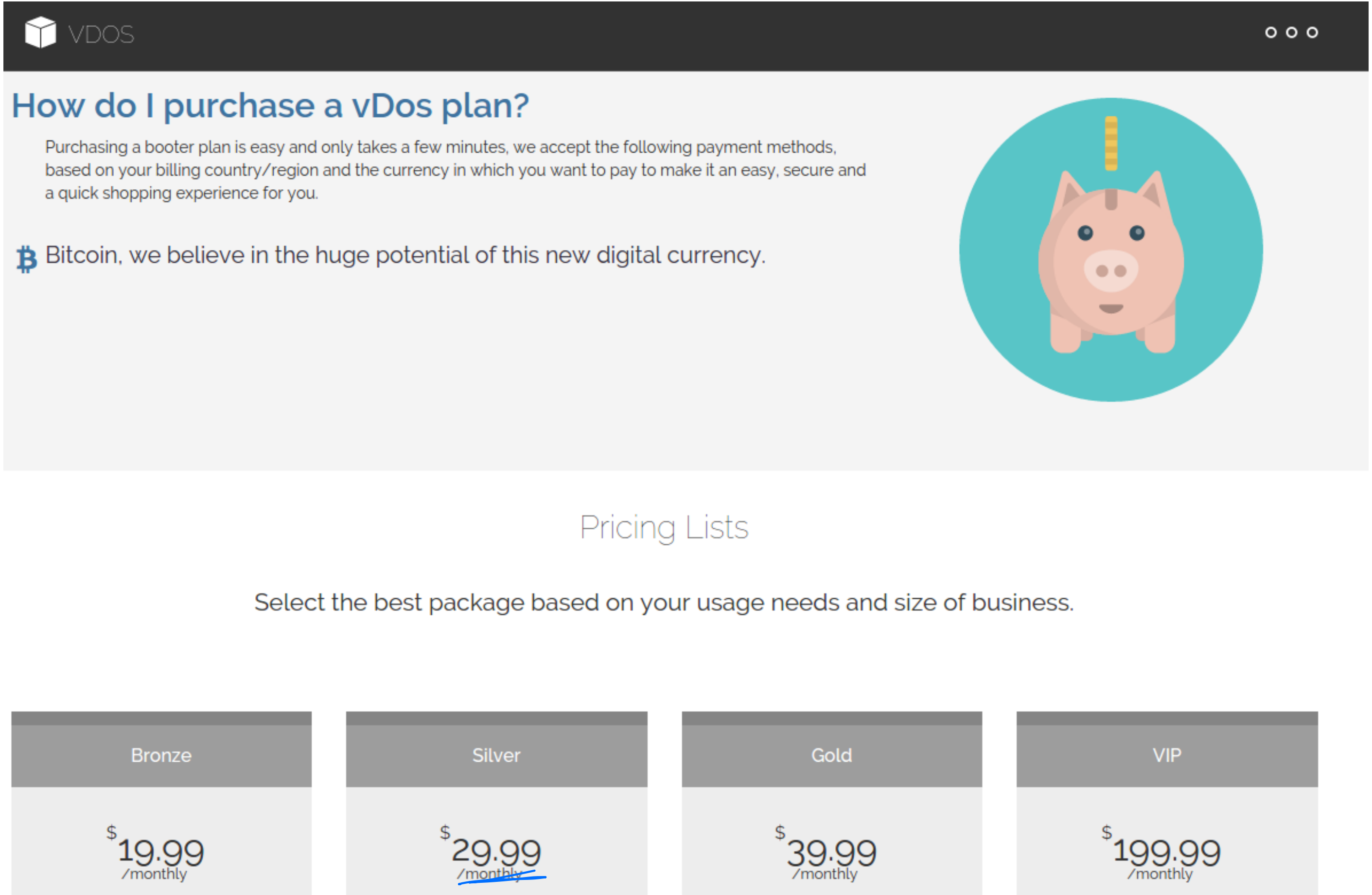
Denial of Service as a Service

- Booters and Stressors
- Websites that claim to "test" a website for resilience against DDoS
  - Send huge amounts of traffic to a target for a fee
  - $10-$100 depending on the amount of traffic and duration of the "test"

10¢ per gb of incoming traffic

Denial of Service as a Service

- Booters and Stressors
- Websites that claim to “test” a website for resilience against DDoS
    - Send huge amounts of traffic to a target for a fee
    - $10-$100 depending on the amount of traffic and duration of the “test”
- Obvious front for criminal DDoS attacks
    - Users can “test”, i.e. attack, any website they want for a fee
    - Attack bandwidth drawn from botnets and bulletproof hosts
- Many, many stressor services operating out in the open



VDOS

How do I purchase a vDos plan?

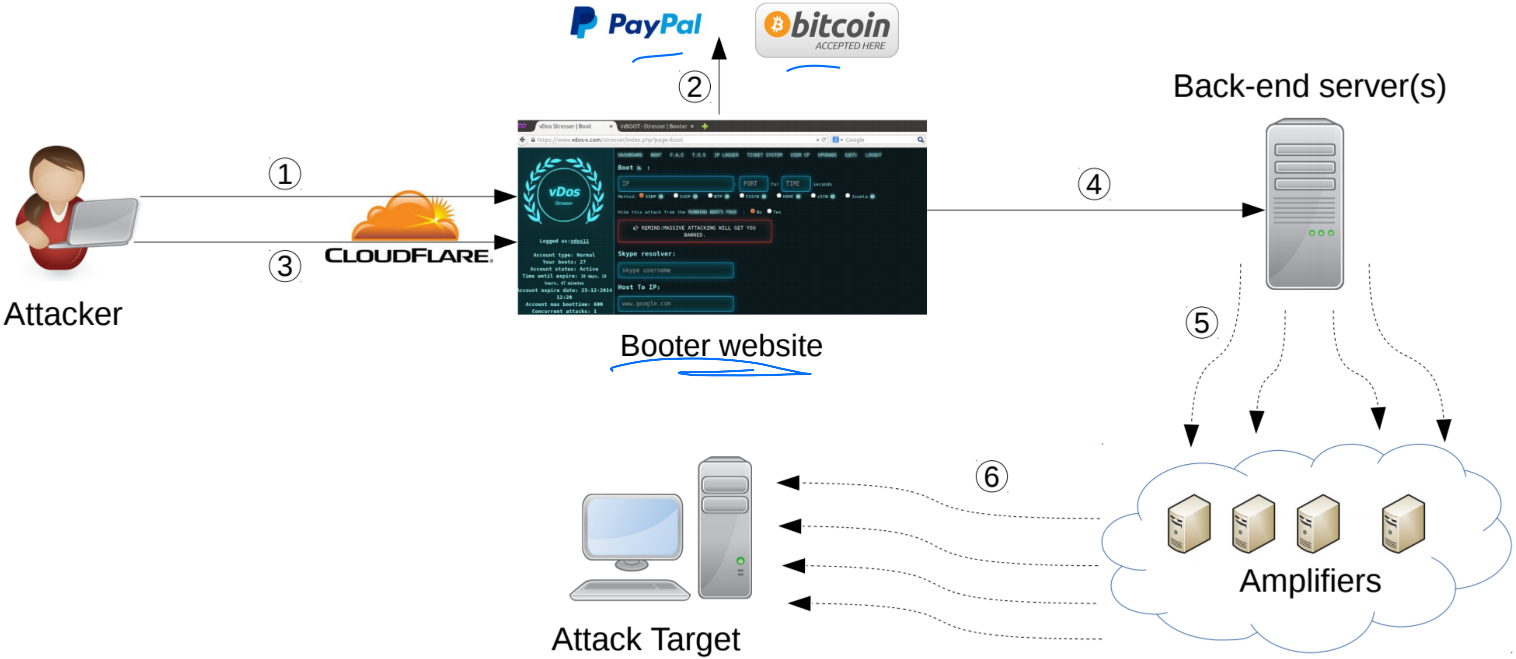
Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

Ƀ Bitcoin, we believe in the huge potential of this new digital currency.

Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
$19.99 /monthly	$29.99 /monthly	$39.99 /monthly	$199.99 /monthly



vDos Stresser | Boot
inBOOT - Stresser | Booter
https://www.vdos-s.com/stresser/index.php?page=boot

DASHBOARD BOOT F.A.E T.O.S IP LOGGER TICKET SYSTEM USER CP UPGRADE ✉(0) LOGOUT

Boot :

IP : PORT for TIME seconds

Method: ● SSDP ○ SUDP ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ Joomla

Hide this attack from the RUNNING BOOTS PAGE : ● No ○ Yes

REMIND:MASSIVE ATTACKING WILL GET YOU BANNED.

Skype resolver:

skype username

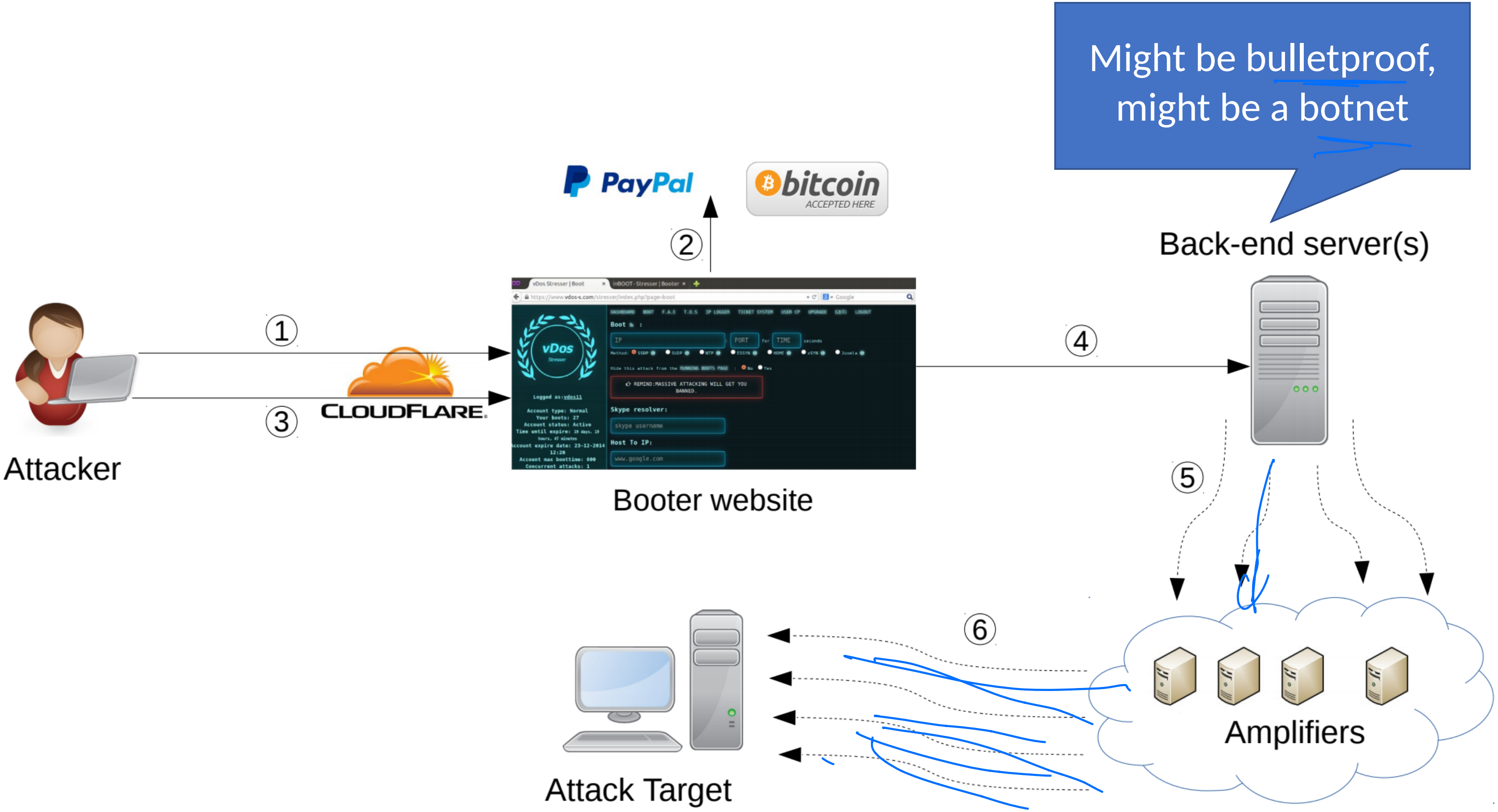
Host To IP:

www.google.com

vDos Stresser

Logged as:vdos11

Account type: Normal
Your boots: 27
Account status: Active
Time until expire: 19 days, 19 hours, 47 minutes
Account expire date: 23-12-2014 12:20
Account max boottime: 600
Concurrent attacks: 1



Might be bulletproof, might be a botnet

vDos Stresser | Boot
inBOOT - Stresser | Booter
https://www.vdos-s.com/stresser/index.php?page=boot

DASHBOARD BOOT F.A.E T.O.S IP LOGGER TICKET SYSTEM USER CP UPGRADE ✉(0) LOGOUT

vDos Stresser

Logged as:vdos11

Account type: Normal
Your boots: 27
Account status: Active
Time until expire: 19 days, 19 hours, 47 minutes
Account expire date: 23-12-2014 12:20
Account max boottime: 600
Concurrent attacks: 1

Boot :

IP : PORT for TIME seconds

Method: ● SSDP ○ SUDP ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ Joomla

Hide this attack from the RUNNING BOOTS PAGE : ● No ○ Yes

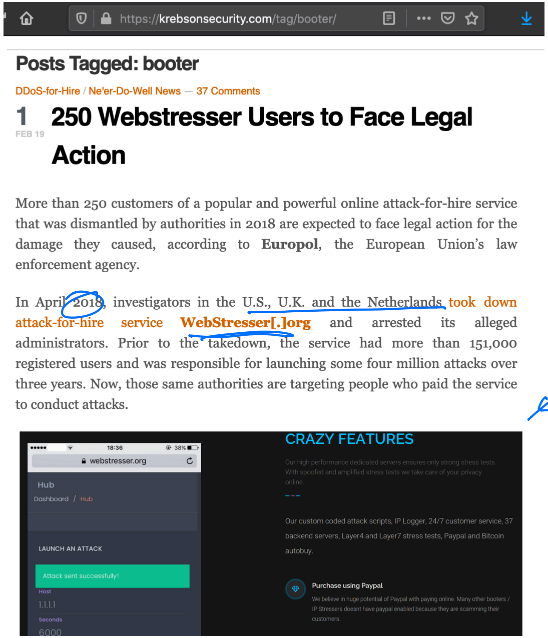
REMIND:MASSIVE ATTACKING WILL GET YOU BANNED.

Skype resolver:

skype username

Host To IP:

www.google.com



Posts Tagged: booter

DDoS-for-Hire / Ne'er-Do-Well News — 37 Comments

1 FEB 19

250 Webstresser Users to Face Legal Action

More than 250 customers of a popular and powerful online attack-for-hire service that was dismantled by authorities in 2018 are expected to face legal action for the damage they caused, according to **Europol**, the European Union's law enforcement agency.

In April 2018, investigators in the U.S., U.K. and the Netherlands took down attack-for-hire service **WebStresser[.]org** and arrested its alleged administrators. Prior to the takedown, the service had more than 151,000 registered users and was responsible for launching some four million attacks over three years. Now, those same authorities are targeting people who paid the service to conduct attacks.

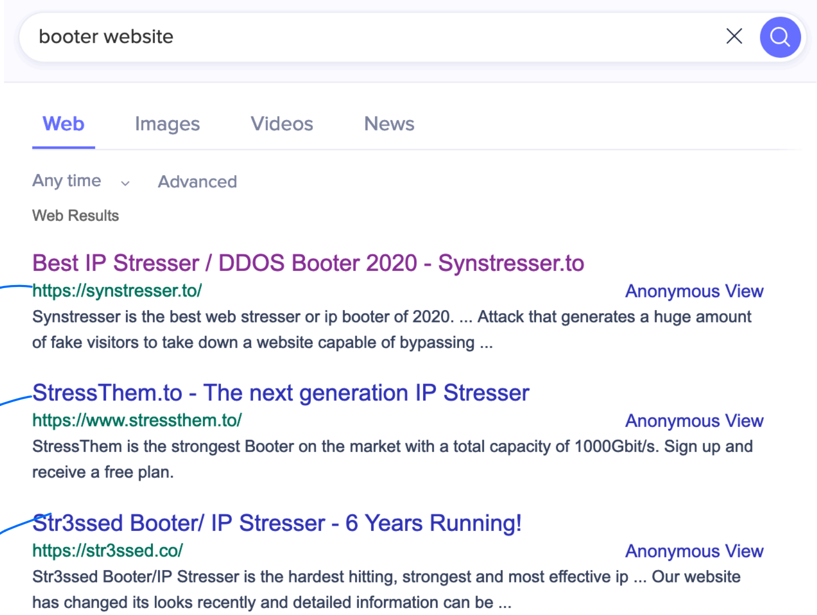
CRAZY FEATURES

Our high performance dedicated servers ensures only strong stress tests. With spoofed and amplified stress tests we take care of your privacy online.

Our custom coded attack scripts, IP Logger, 24/7 customer service, 37 backend servers, Layer4 and Layer7 stress tests, Paypal and Bitcoin autobuy.

Purchase using Paypal

We believe in huge potential of Paypal with paying online. Many other booters / IP Stressers doesnt have paypal enabled because they are scamming their customers.



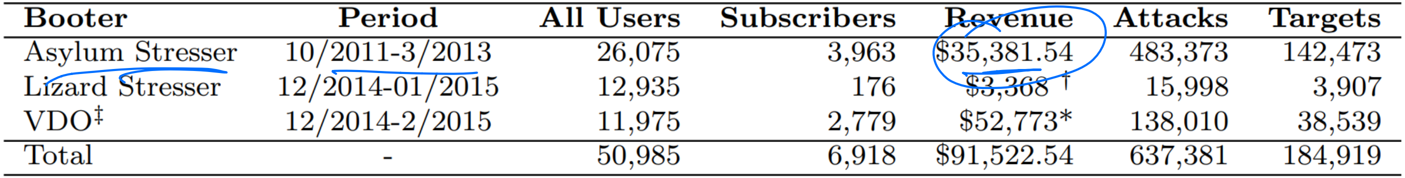
Web Results

Best IP Stresser / DDOS Booter 2020 - Synstresser.to
https://synstresser.to/ — Anonymous View
Synstresser is the best web stresser or ip booter of 2020. ... Attack that generates a huge amount of fake visitors to take down a website capable of bypassing ...

StressThem.to - The next generation IP Stresser
https://www.stressthem.to/ — Anonymous View
StressThem is the strongest Booter on the market with a total capacity of 1000Gbit/s. Sign up and receive a free plan.

Str3ssed Booter/ IP Stresser - 6 Years Running!
https://str3ssed.co/ — Anonymous View
Str3ssed Booter/IP Stresser is the hardest hitting, strongest and most effective ip ... Our website has changed its looks recently and detailed information can be ...

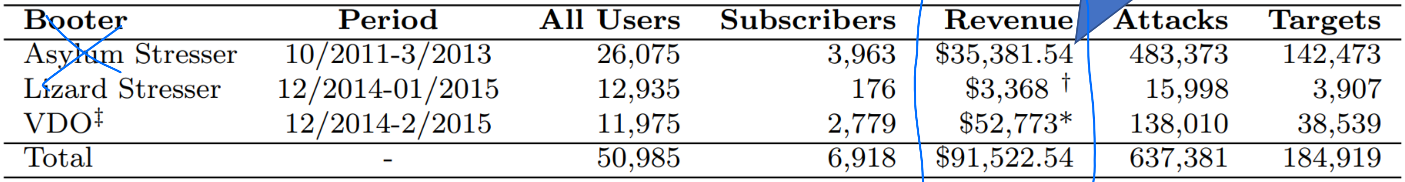
Hacked & Dumped Booter Services



Booter	Period	All Users	Subscribers	Revenue	Attacks	Targets
Asylum Stresser	10/2011-3/2013	26,075	3,963	$35,381.54	483,373	142,473
Lizard Stresser	12/2014-01/2015	12,935	176	$3,368 †	15,998	3,907
VDO‡	12/2014-2/2015	11,975	2,779	$52,773*	138,010	38,539
Total	-	50,985	6,918	$91,522.54	637,381	184,919

Hacked & Dumped Booter Services

99.4% via Paypal

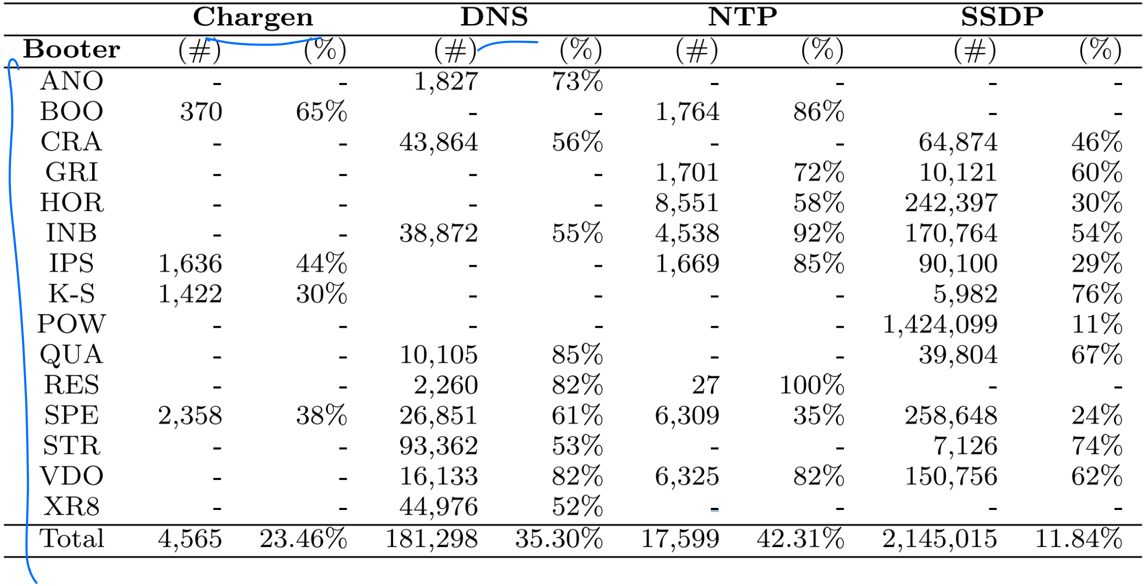


Booter	Period	All Users	Subscribers	Revenue	Attacks	Targets
Asylum Stresser	10/2011-3/2013	26,075	3,963	$35,381.54	483,373	142,473
Lizard Stresser	12/2014-01/2015	12,935	176	$3,368 †	15,998	3,907
VDO‡	12/2014-2/2015	11,975	2,779	$52,773*	138,010	38,539
Total	-	50,985	6,918	$91,522.54	637,381	184,919

clear mitigation: paypal can stop accepting payments for such services

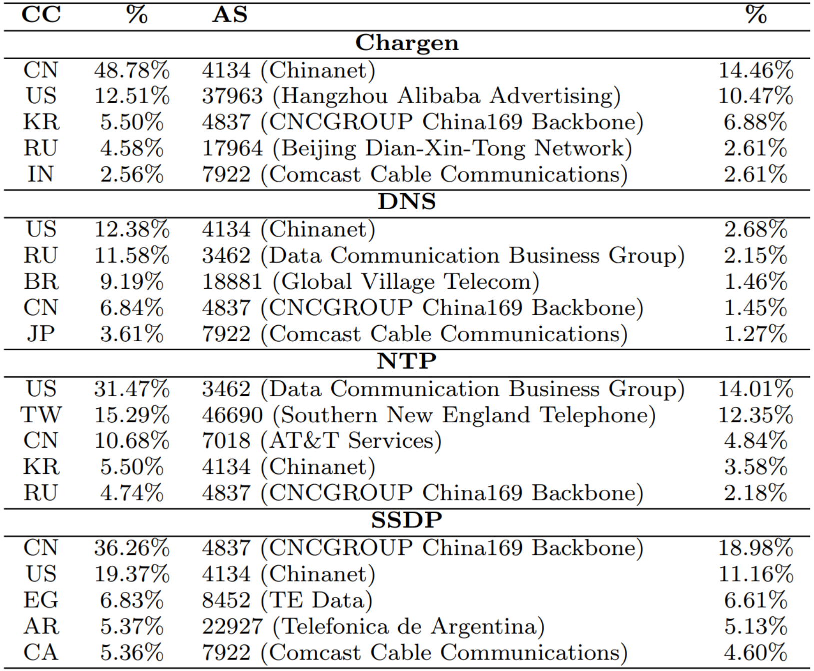
(bottleneck: bank/payment for crimeware)

Booter Attack Characteristics



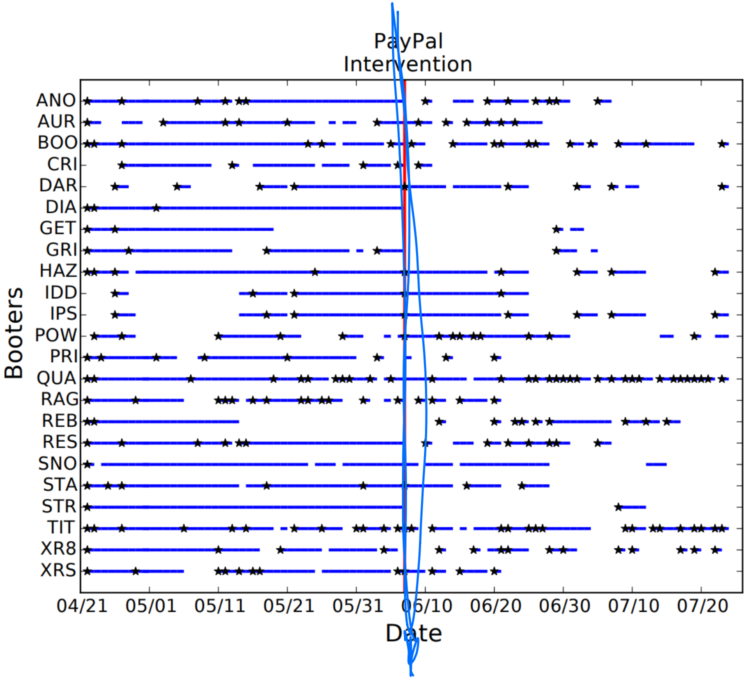
	Chargen		DNS		NTP		SSDP	
Booter	(#)	(%)	(#)	(%)	(#)	(%)	(#)	(%)
ANO	-	-	1,827	73%	-	-	-	-
BOO	370	65%	-	-	1,764	86%	-	-
CRA	-	-	43,864	56%	-	-	64,874	46%
GRI	-	-	-	-	1,701	72%	10,121	60%
HOR	-	-	-	-	8,551	58%	242,397	30%
INB	-	-	38,872	55%	4,538	92%	170,764	54%
IPS	1,636	44%	-	-	1,669	85%	90,100	29%
K-S	1,422	30%	-	-	-	-	5,982	76%
POW	-	-	-	-	-	-	1,424,099	11%
QUA	-	-	10,105	85%	-	-	39,804	67%
RES	-	-	2,260	82%	27	100%	-	-
SPE	2,358	38%	26,851	61%	6,309	35%	258,648	24%
STR	-	-	93,362	53%	-	-	7,126	74%
VDO	-	-	16,133	82%	6,325	82%	150,756	62%
XR8	-	-	44,976	52%	-	-	-	-
Total	4,565	23.46%	181,298	35.30%	17,599	42.31%	2,145,015	11.84%

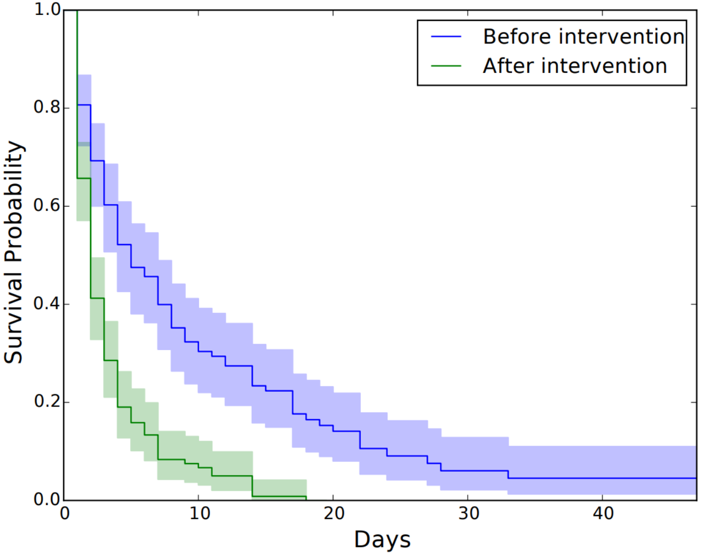
Amplifier Locations



CC	%	AS	%
		Chargen	
CN	48.78%	4134 (Chinanet)	14.46%
US	12.51%	37963 (Hangzhou Alibaba Advertising)	10.47%
KR	5.50%	4837 (CNCGROUP China169 Backbone)	6.88%
RU	4.58%	17964 (Beijing Dian-Xin-Tong Network)	2.61%
IN	2.56%	7922 (Comcast Cable Communications)	2.61%
		DNS	
US	12.38%	4134 (Chinanet)	2.68%
RU	11.58%	3462 (Data Communication Business Group)	2.15%
BR	9.19%	18881 (Global Village Telecom)	1.46%
CN	6.84%	4837 (CNCGROUP China169 Backbone)	1.45%
JP	3.61%	7922 (Comcast Cable Communications)	1.27%
		NTP	
US	31.47%	3462 (Data Communication Business Group)	14.01%
TW	15.29%	46690 (Southern New England Telephone)	12.35%
CN	10.68%	7018 (AT&T Services)	4.84%
KR	5.50%	4134 (Chinanet)	3.58%
RU	4.74%	4837 (CNCGROUP China169 Backbone)	2.18%
		SSDP	
CN	36.26%	4837 (CNCGROUP China169 Backbone)	18.98%
US	19.37%	4134 (Chinanet)	11.16%
EG	6.83%	8452 (TE Data)	6.61%
AR	5.37%	22927 (Telefonica de Argentina)	5.13%
CA	5.36%	7922 (Comcast Cable Communications)	4.60%

Payment Interventions





Mitigations

Anti-amplification

Filters

Anti-spoofing

CDNs

Avoid Becoming an Amplifier

- Filter ingress IP broadcasts at the gateway router
  - i.e. drop anything destined to *.*.*.255

Avoid Becoming an Amplifier

- Filter ingress IP broadcasts at the gateway router
  - i.e. drop anything destined to *.*.*.255
- Disable non-essential services
  - echo, chargen, NTP, etc.

Avoid Becoming an Amplifier

- Filter ingress IP broadcasts at the gateway router
  - i.e. drop anything destined to *.*.*.255
- Disable non-essential services
  - echo, chargen, NTP, etc.
- Configure services to only respond to requests from the local LAN
  - Firewall ports 53 (DNS), 123 (NTP), 11211 (memcached), etc.

Avoid Becoming an Amplifier

- Filter ingress IP broadcasts at the gateway router
  - i.e. drop anything destined to *.*.*.255
- Disable non-essential services
  - echo, chargen, NTP, etc.
- Configure services to only respond to requests from the local LAN
  - Firewall ports 53 (DNS), 123 (NTP), 11211 (memcached), etc.
- If you write a UDP service, authenticate the sources of packets
  - TCP is connection-oriented, and thus much less vulnerable

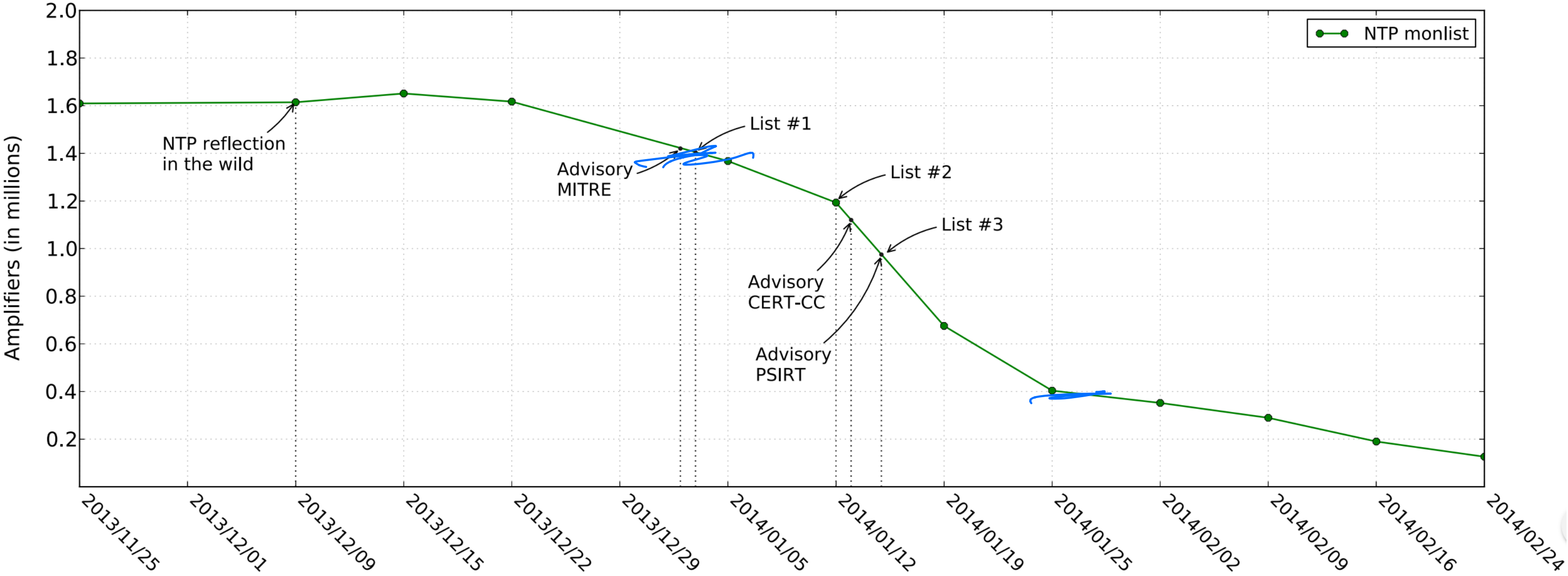
Avoid Becoming an Amplifier

- Filter ingress IP broadcasts at the gateway router
  - i.e. drop anything destined to *.*.*.255
- Disable non-essential services
  - echo, chargen, NTP, etc.
- Configure services to only respond to requests from the local LAN
  - Firewall ports 53 (DNS), 123 (NTP), 11211 (memcached), etc.
- If you write a UDP service, authenticate the sources of packets
  - TCP is connection-oriented, and thus much less vulnerable
- **Don’t be part of the problem!**
  - The behavior of your software and network impacts the well-being of others

Outreach

- Researchers are trying to clean up amplifiers
  - Scan for servers with open services that are possible amplifiers
  - Manually contact server owners, ISPs, and ASs
  - Issue public advisories
  - Get vendors to issue patches that disable services or features by default

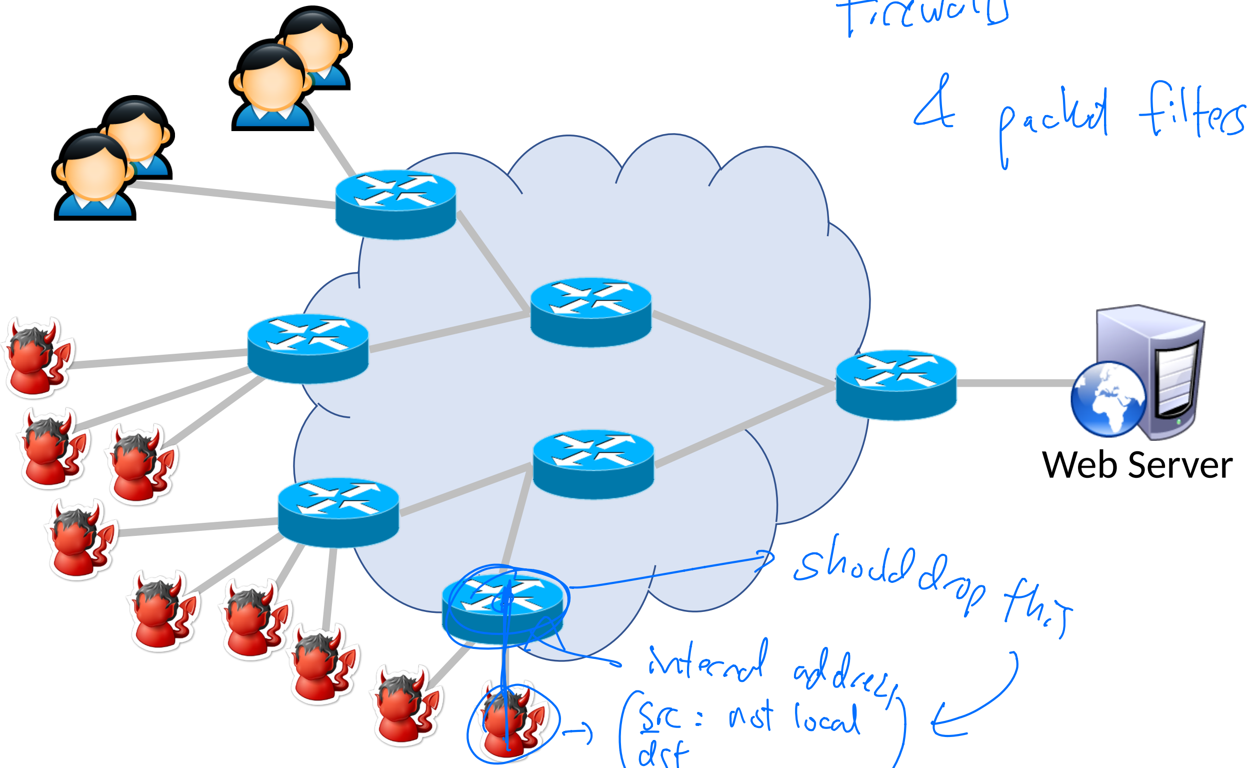
Example: NTP *monlist* Cleanup



What About Filtering?

firewalls

& packet filters

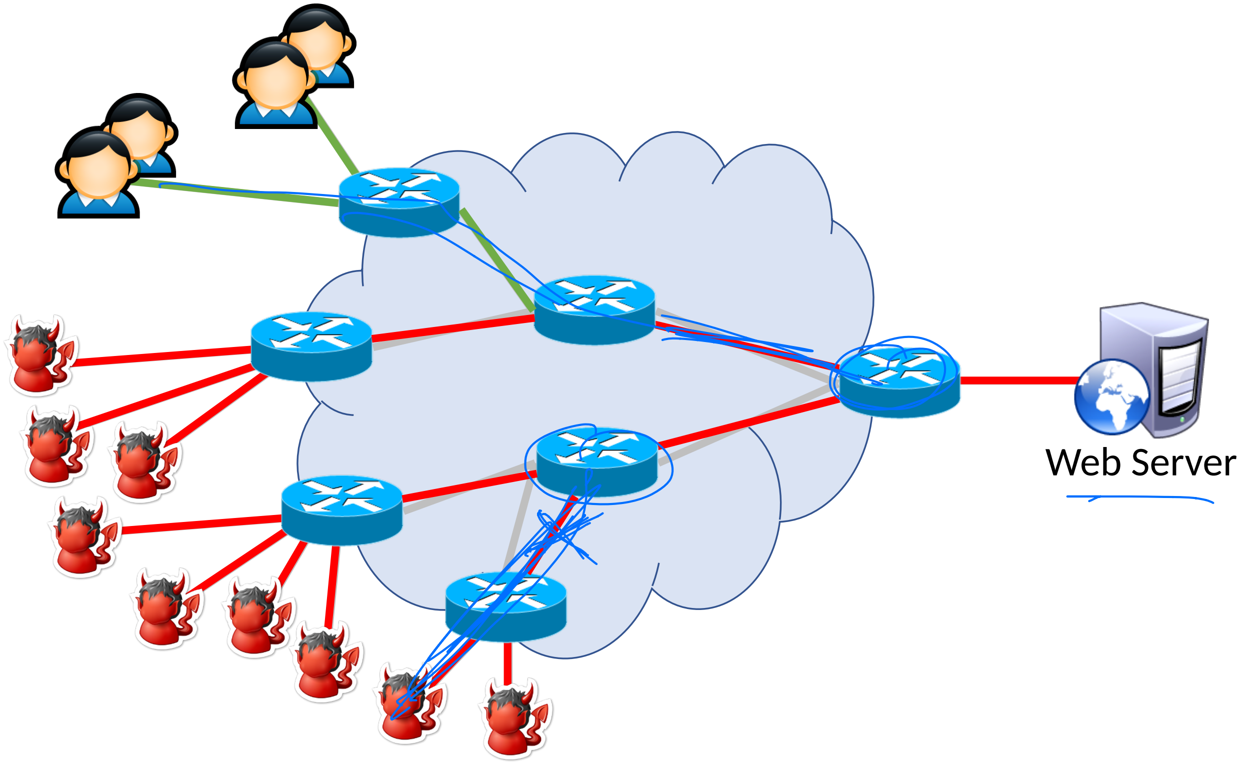


should drop this

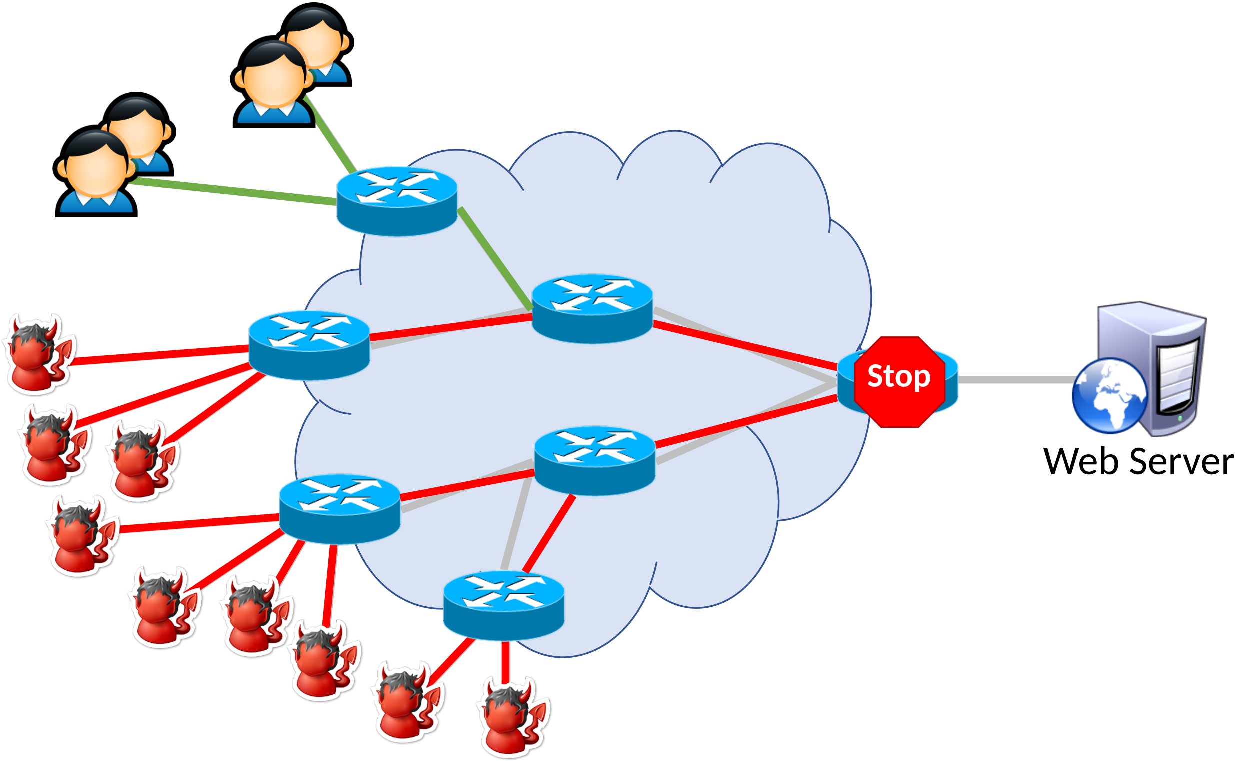
internal address

(src: not local
dst)

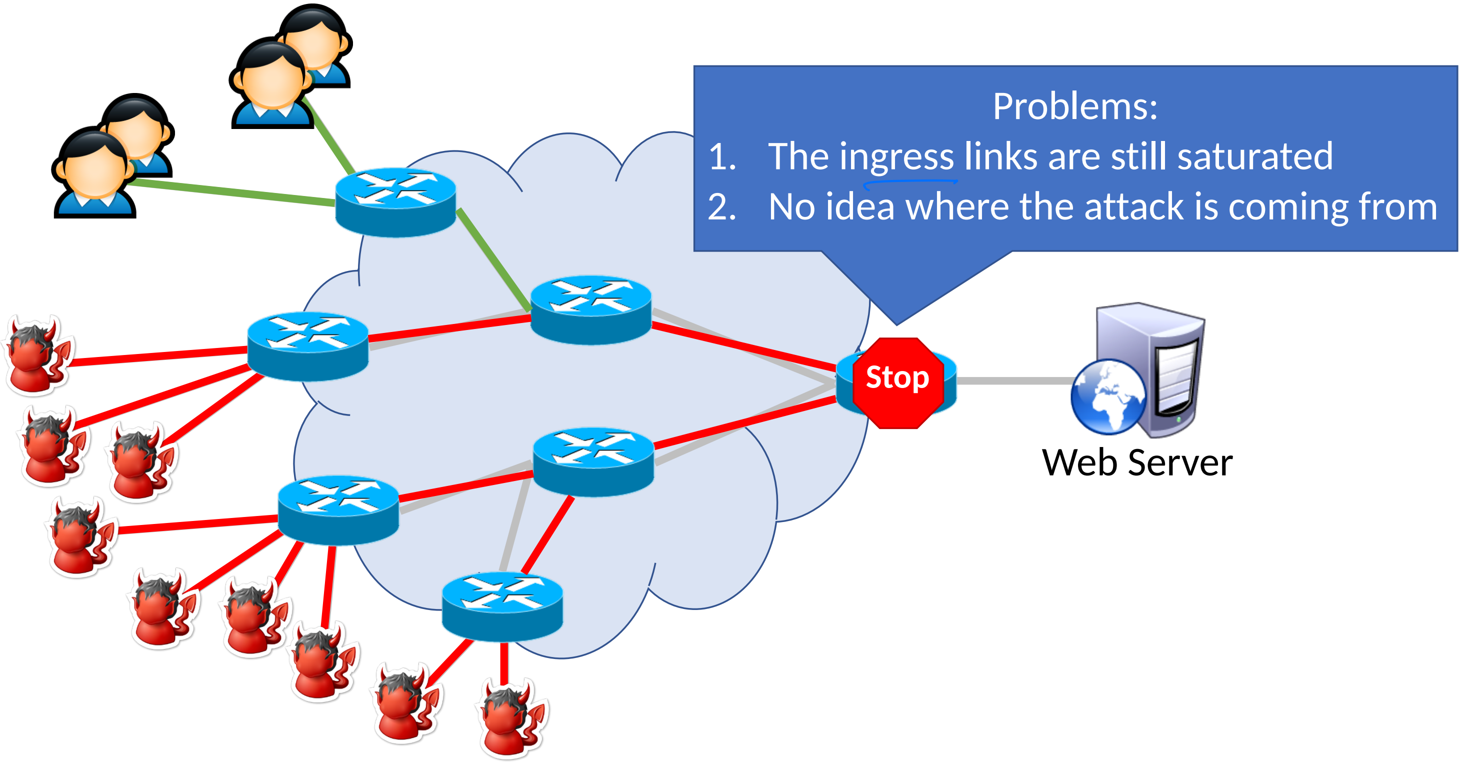
What About Filtering?



What About Filtering?



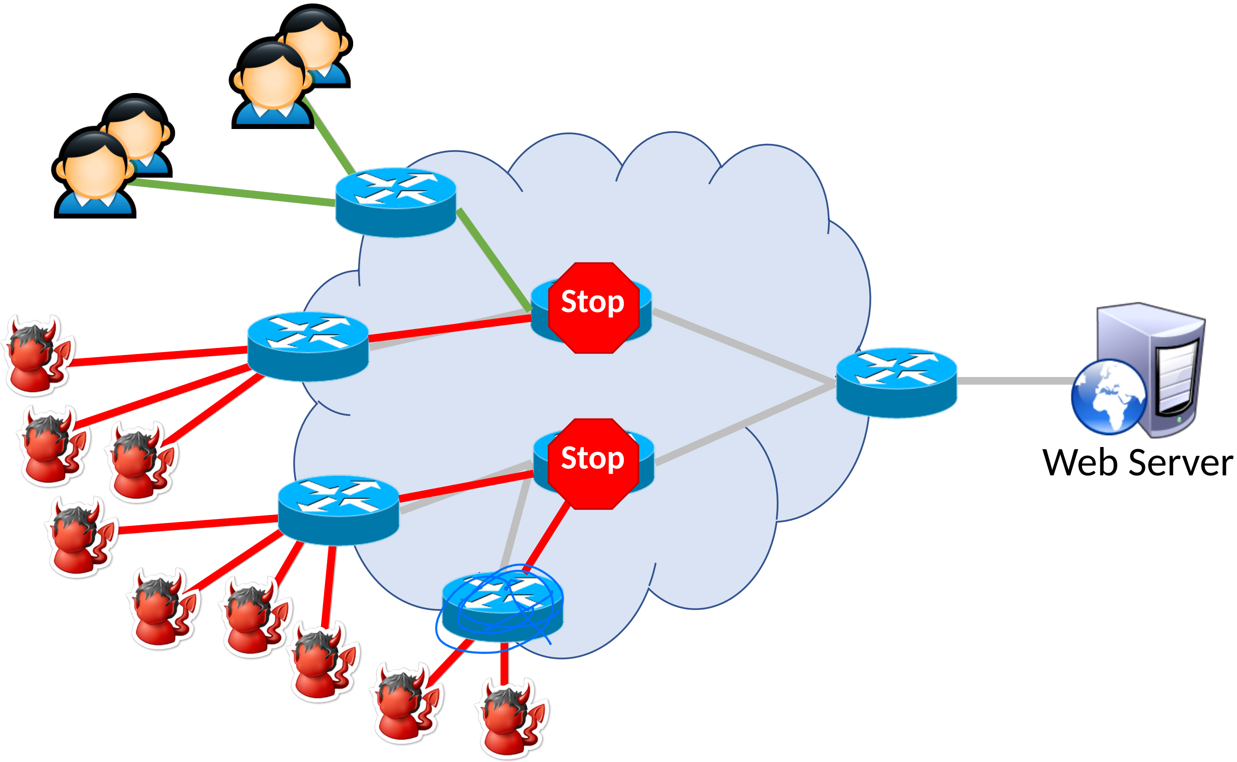
What About Filtering?



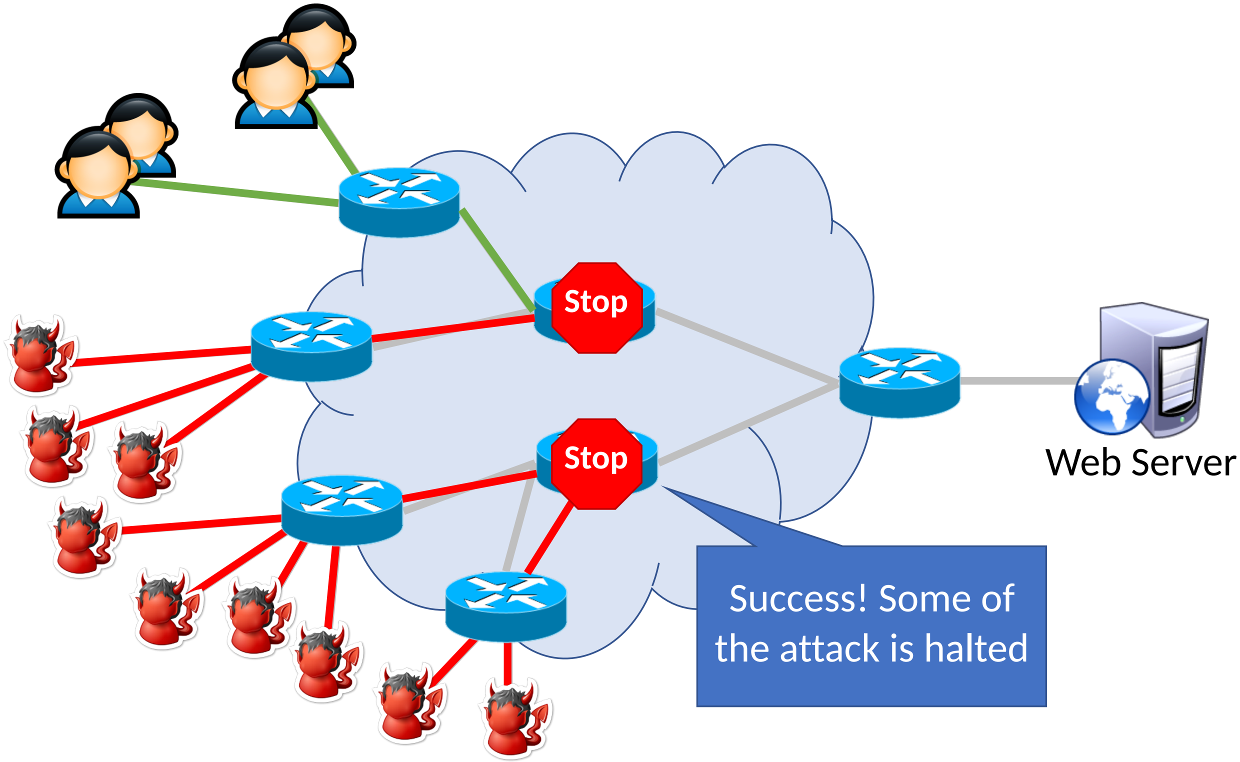
Problems:

1. The ingress links are still saturated
2. No idea where the attack is coming from

What About Filtering?

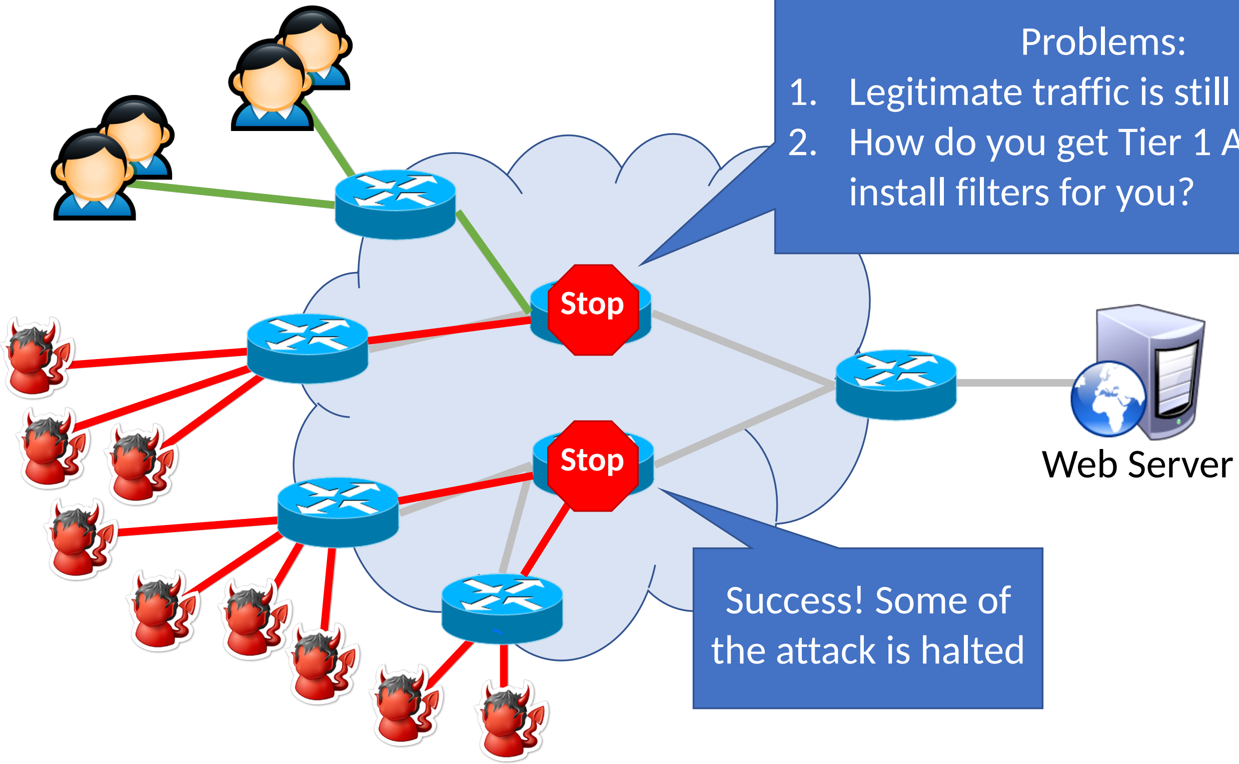


What About Filtering?



Success! Some of the attack is halted

What About Filtering?

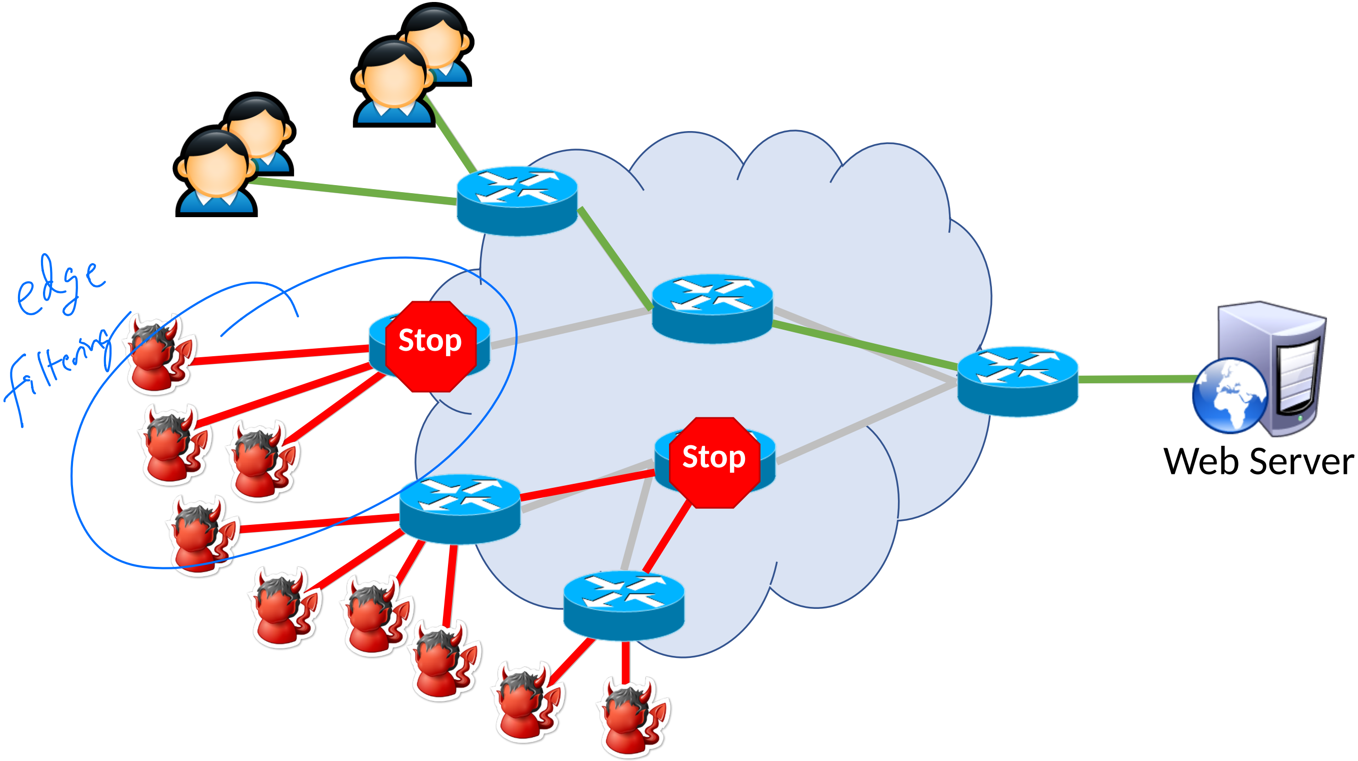


Problems:

1. Legitimate traffic is still blocked
2. How do you get Tier 1 ASs to install filters for you?

Success! Some of the attack is halted

What About Filtering?



Problems With Filters

- Packet filtering is not a viable solution
- If you install a local filter:
  - Ingress links are still saturated
  - Very hard to distinguish DDoS packets from legitimate requests, since sources are spoofed
- Remote filters work better, but:
  - You still need to track down the source of the attack
  - You have no ability to force ISPs and ASs to install filters on your behalf

In-Network Defenses

- Why don’t ISPs/ASs drop spoofed packets?

In-Network Defenses

- Why don’t ISPs/ASs drop spoofed packets?
- Unicast Reverse Path Forwarding (uRPF)
  - Routers validate the source IP addresses against routing tables
  - “Unlikely” source addresses are dropped
- uRPF modes:
  - Strict – may drop legitimate traffic (false positives)
  - Feasible – may accept spoofed traffic (false negatives)
  - Loose – only drops unroutable sources like 192.168.*.*

In-Network Defenses

- Why don’t ISPs/ASs drop spoofed packets?
- Unicast Reverse Path Forwarding (uRPF)
  - Routers validate the source IP addresses against routing tables
  - “Unlikely” source addresses are dropped
- uRPF modes:
  - Strict – may drop legitimate traffic (false positives)
  - Feasible – may accept spoofed traffic (false negatives)
  - Loose – only drops unroutable sources like 192.168.*.*
- Most ISPs/ASs don’t implement uRPF
  - Unwilling to risk false positives from strict mode
  - No incentive to implement security measures

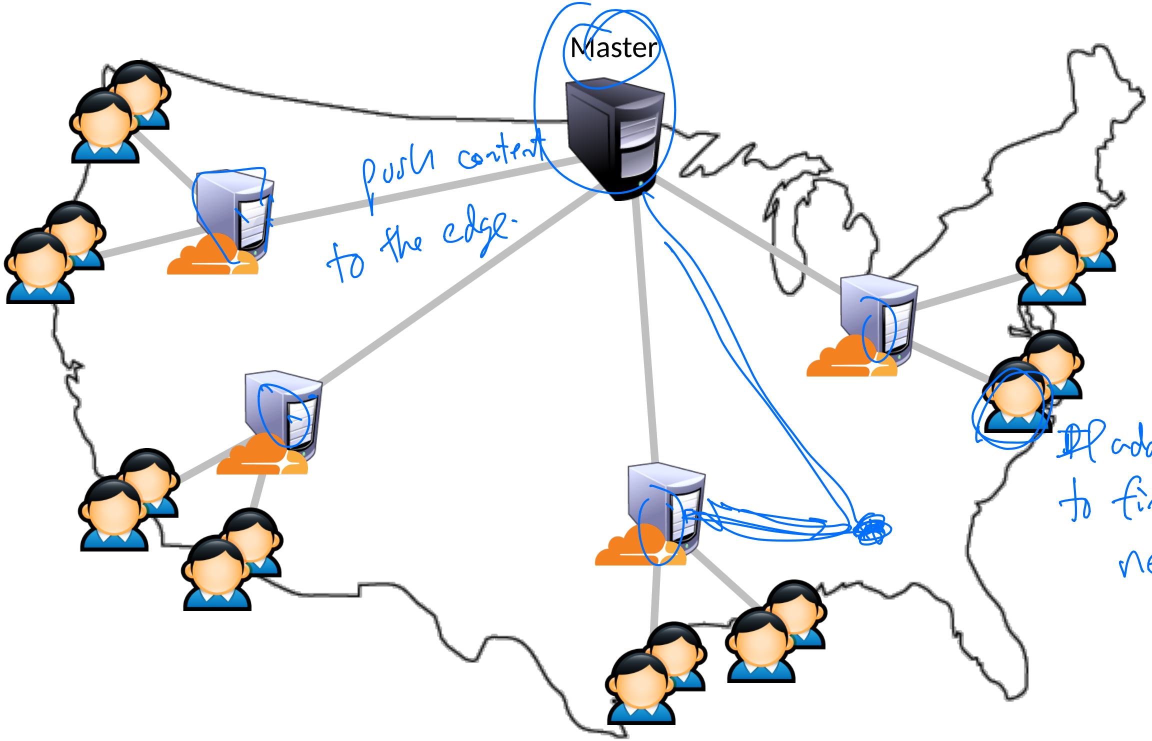
Content Delivery Networks (CDNs)

- CDNs help companies scale-up their websites
  - Cache customer content on many replica servers
  - Users access the website via the replicas
- Examples: Akamai, Cloudflare, Rackspace, Amazon Cloudfront, etc.

Content Delivery Networks (CDNs)

- CDNs help companies scale-up their websites
  - Cache customer content on many replica servers
  - Users access the website via the replicas
- Examples: Akamai, Cloudflare, Rackspace, Amazon Cloudfront, etc.
- Side-benefit: DDoS protection
  - CDNs have many servers, and a huge amount of bandwidth
  - Difficult to knock all the replicas offline
  - Difficult to saturate all available bandwidth
  - No direct access to the master server
- Cloudflare: 15 Tbps of bandwidth over 149 data centers

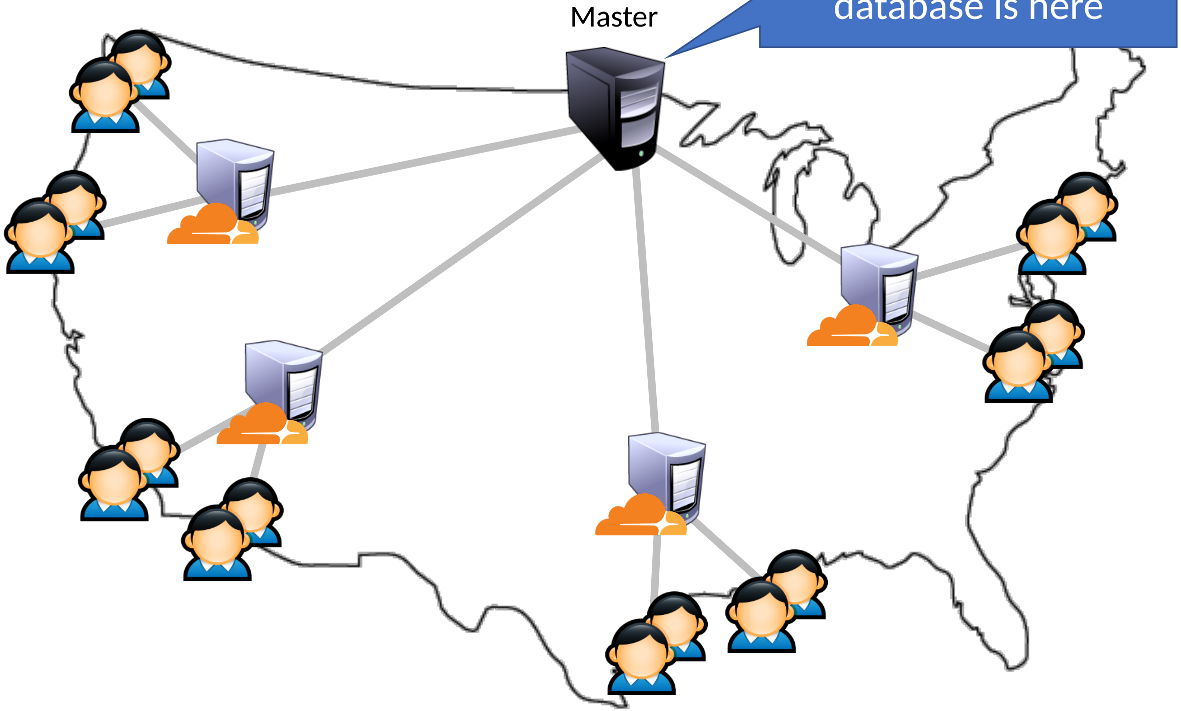
CDN Basics



push content to the edge.

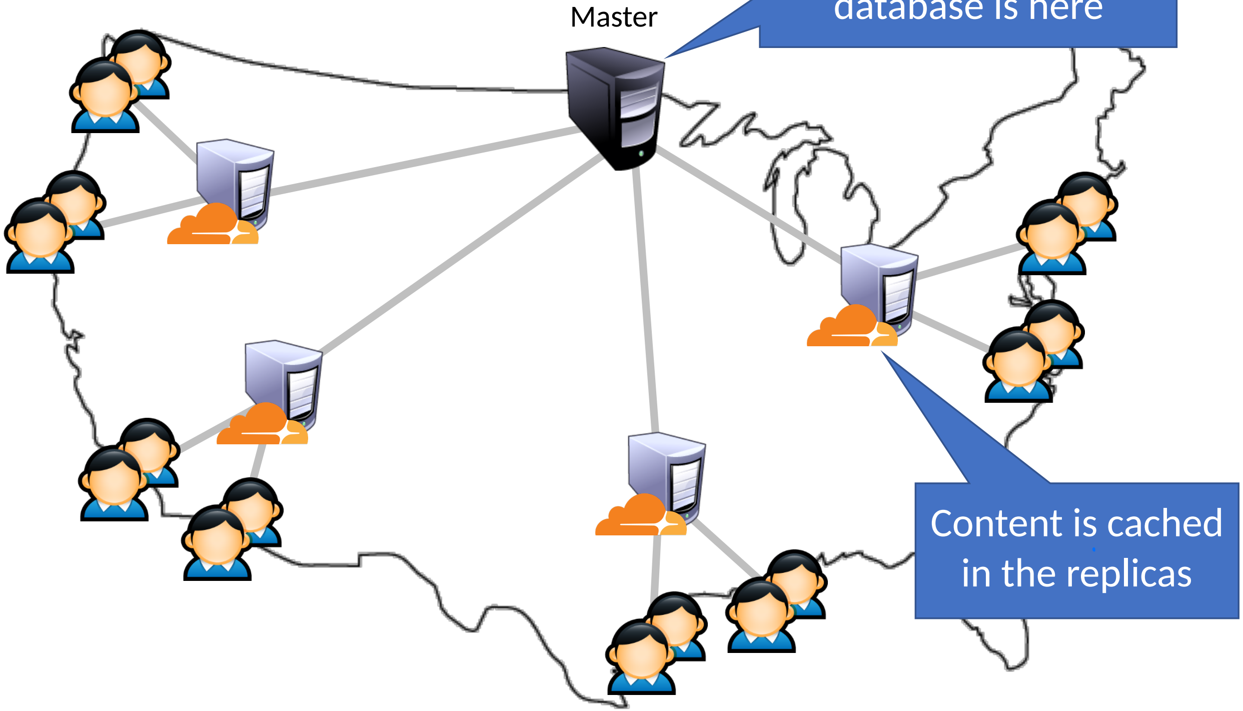
IP addr to find the nearest server

CDN Basics



Website content and database is here

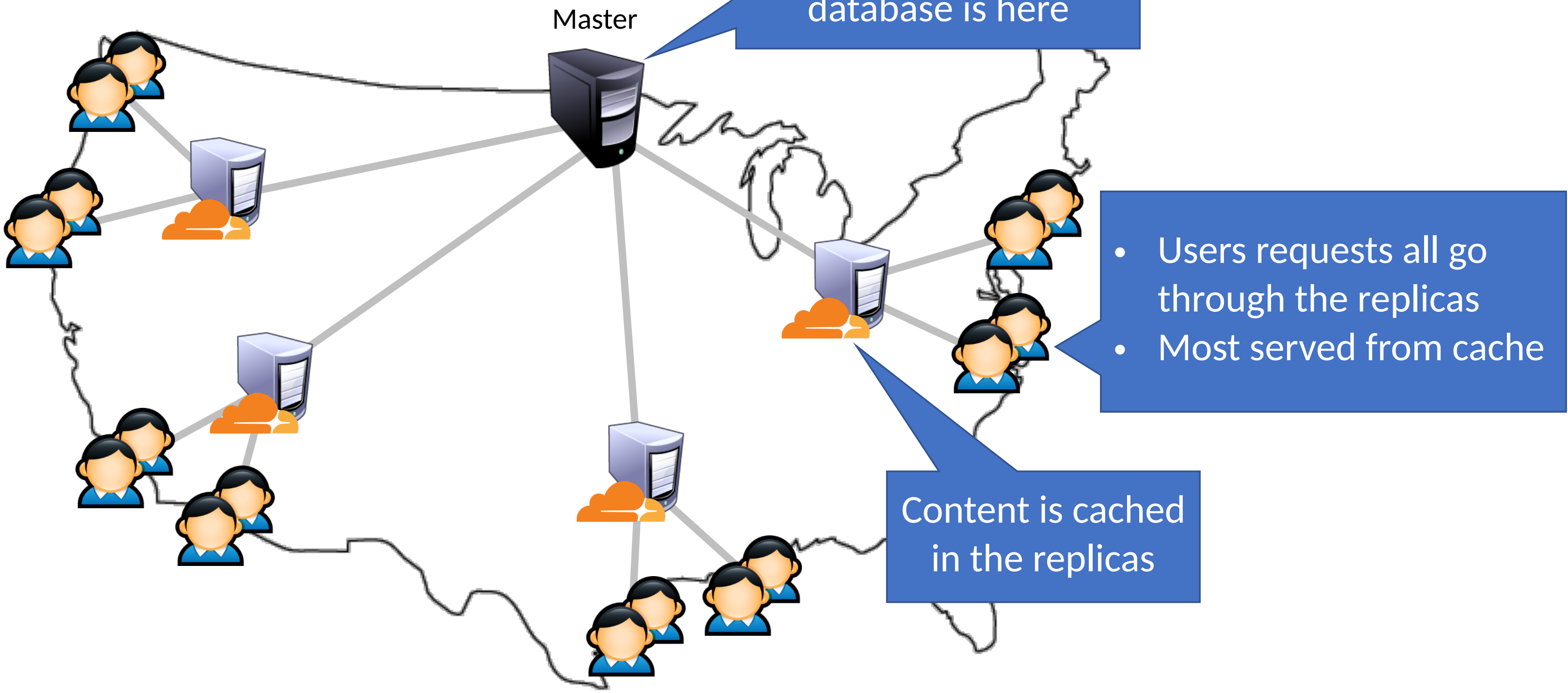
CDN Basics



Website content and database is here

Content is cached in the replicas

CDN Basics

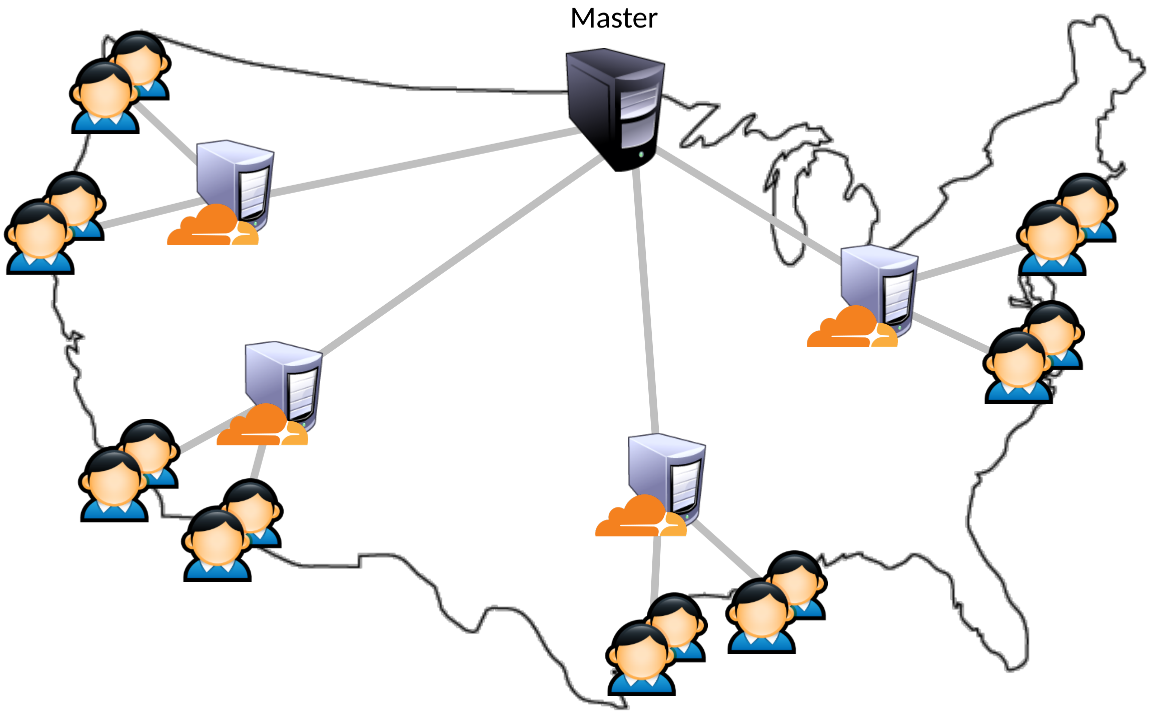


Website content and database is here

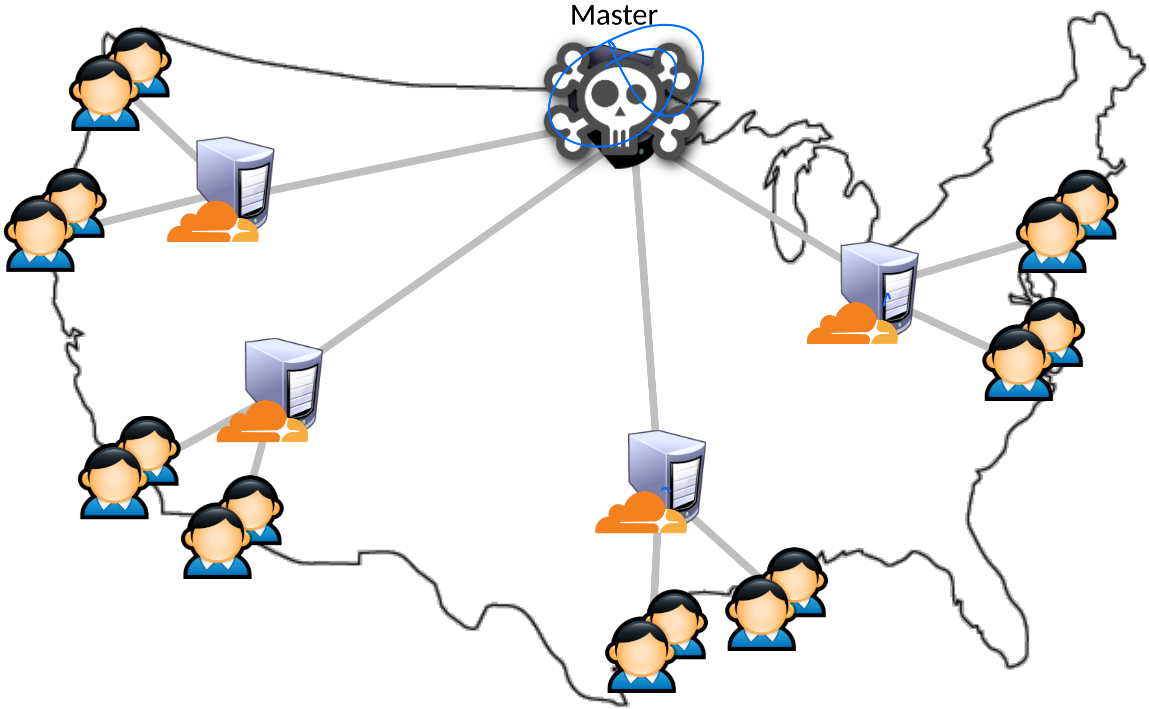
- Users requests all go through the replicas
- Most served from cache

Content is cached in the replicas

DDoS Defense via CDNs

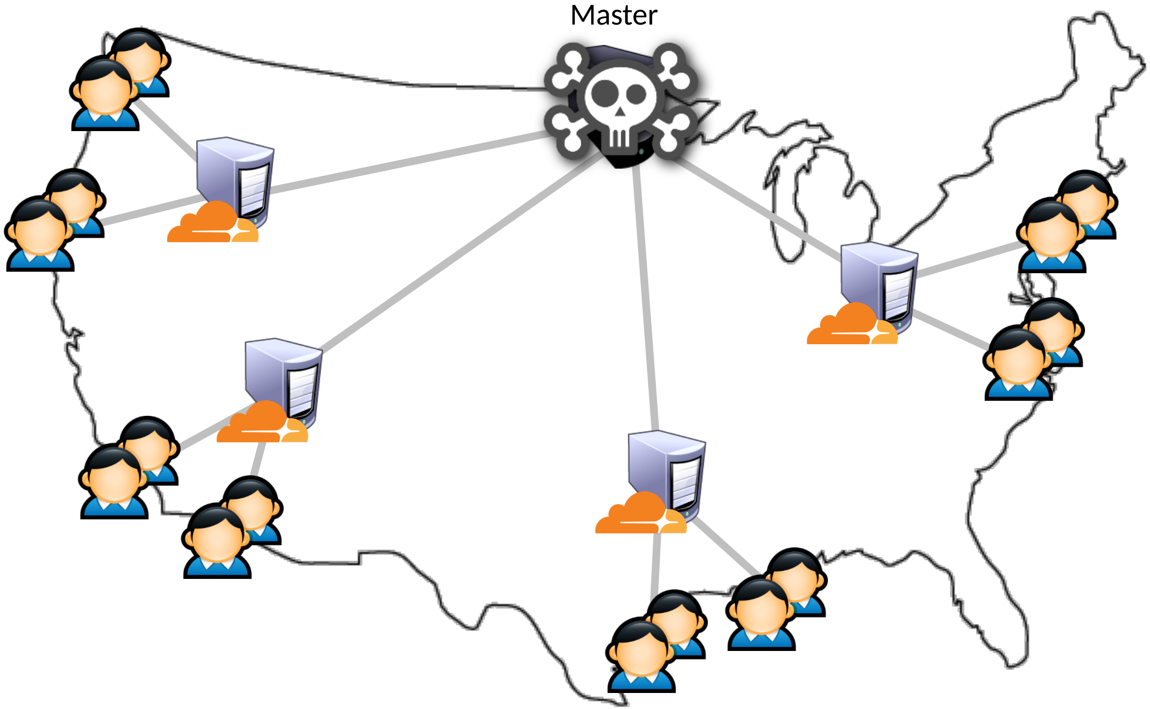


DDoS Defense via CDNs



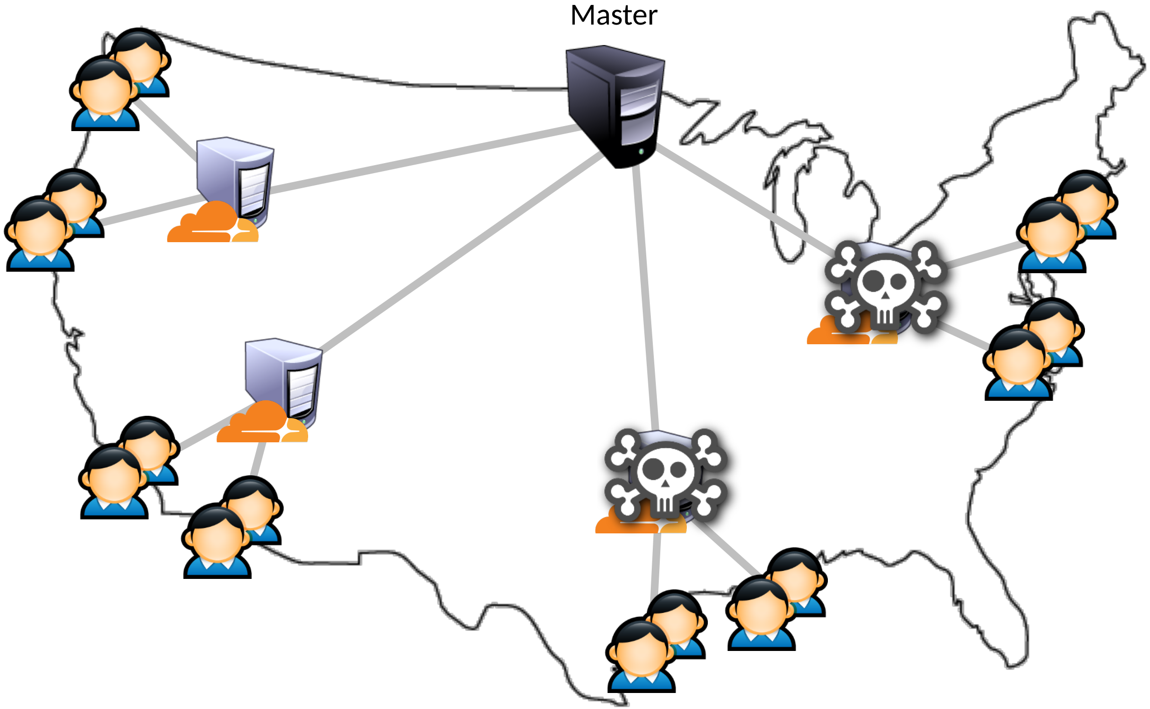
- What if you DDoS the master replica?

DDoS Defense via CDNs



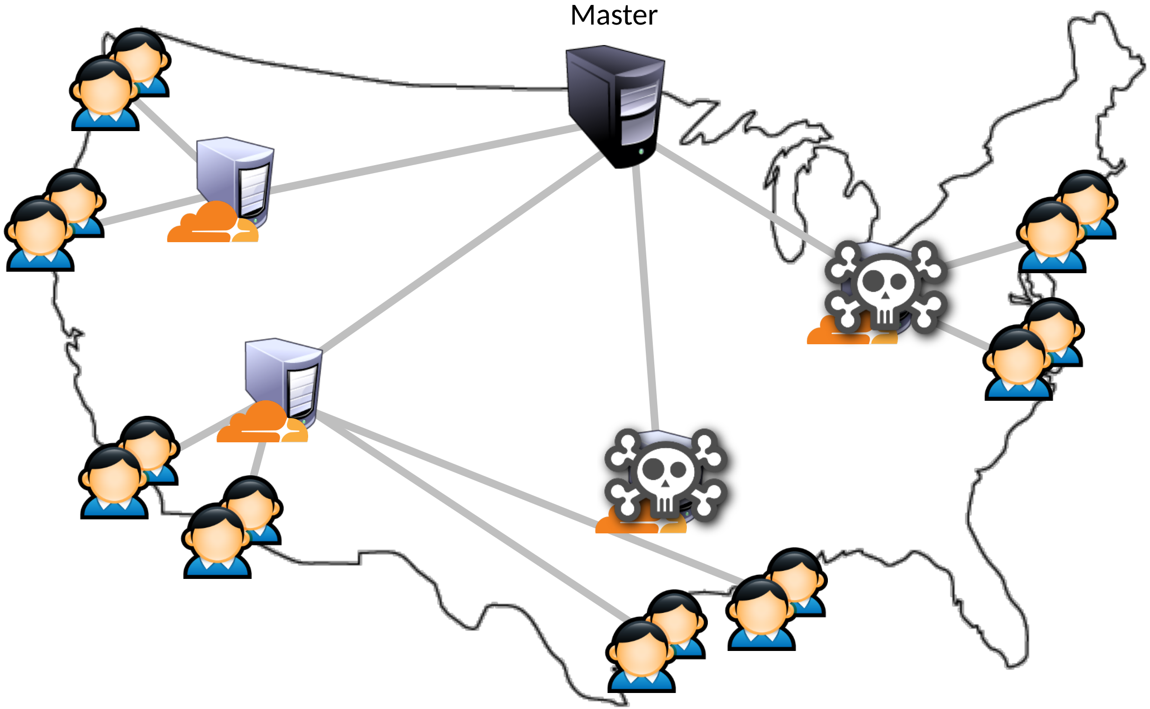
- What if you DDoS the master replica?
  - Cached copies in the CDN still available
  - Easy to do ingress filtering at the master

DDoS Defense via CDNs



- What if you DDoS the master replica?
  - Cached copies in the CDN still available
  - Easy to do ingress filtering at the master
- What if you DDoS the replicas?

DDoS Defense via CDNs



- What if you DDoS the master replica?
  - Cached copies in the CDN still available
  - Easy to do ingress filtering at the master
- What if you DDoS the replicas?
  - Difficult to kill them all
  - Dynamic DNS can redirect users to live replicas

Sources

Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services -- https://dl.acm.org/citation.cfm?id=2883004

Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks -- https://dl.acm.org/citation.cfm?id=2663717

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks -- https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-kuhrer.pdf

Review

Our main topics

- Cryptography → we spent too much time on this!!
- Authentication, passwords
- Authorization
- Ethics and cyberlaw
- Social engineering
- Systems security
- Exploits:
- Crimeware, Botnets:

Cryptography

Privacy: symmetric & public key cryptography

RSA, practitioner's knowledge

Authenticity: MACs & digital signatures.

Hashing: SHA256

collision-resistance.

Passwords and Authentication

○ What is authentication? crisp sentence

Classes of secrets? → knowledge, token, property

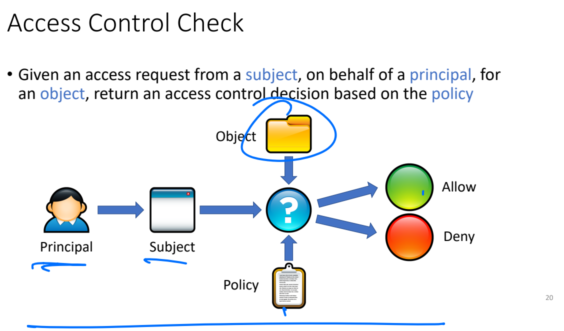
Methods and attacks against passwords?

humans are bad at pwds!!

- store pwds, best practices

Authorization

Basics of an access control check

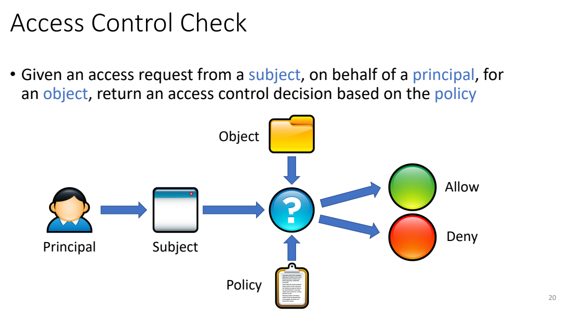


Access Control Check

- Given an access request from a subject, on behalf of a principal, for an object, return an access control decision based on the policy

Authorization

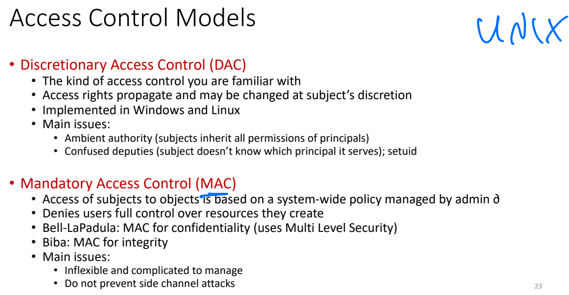
Basics of an access control check



Access Control Check

- Given an access request from a subject, on behalf of a principal, for an object, return an access control decision based on the policy

Two types



Access Control Models

- Discretionary Access Control (DAC)
  - The kind of access control you are familiar with
  - Access rights propagate and may be changed at subject’s discretion
  - Implemented in Windows and Linux
  - Main issues:
    - Ambient authority (subjects inherit all permissions of principals)
    - Confused deputies (subject doesn’t know which principal it serves); setuid
- Mandatory Access Control (MAC)
  - Access of subjects to objects is based on a system-wide policy managed by admin ∂
  - Denies users full control over resources they create
  - Bell-LaPadula: MAC for confidentiality (uses Multi Level Security)
  - Biba: MAC for integrity
  - Main issues:
    - Inflexible and complicated to manage
    - Do not prevent side channel attacks

UNIX, ACLs, capability-based

MAC

Cybersecurity and Ethics

- Many laws govern cybersecurity
  - Designed to help prosecute criminals
  - Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
  - Easy to violate these laws accidentally
  - Security professionals must be cautious and protect themselves

- Cybersecurity raises complex ethical questions
  - When and how to disclose vulnerabilities
  - How to handle leaked data
  - Line between observing and enabling crime
  - Balancing security vs. autonomy
- Ethical norms must be respected
  - Rights and expectations of individuals and companies
  - Community best-practices

Social Engineering

1. Cognitive vulnerabilities
    - Subconscious decisions may be made before you are consciously aware
    - Behavioral, social, memory biases
2. Social engineering tactics
    - Weaponizing cognitive vulnerabilities
    - Pretexting and framing
    - Elicitation and persuasion
3. Social engineering attacks
    - Baiting, Tailgating
    - Phishing, spear phishing
    - CEO fraud
    - Scareware

System Security: Attack Surfaces

- Steal the device and use it
- Social Engineering
  - Trick the user into installing malicious software
  - Spear phishing ✓
- OS-level attacks
  - Backdoor the OS
  - Direct connection via USB
  - Exploit vulnerabilities in the OS or apps (e.g. email clients, web browsers)
- Network-level attacks
  - Passive eavesdropping on the network
  - Active network attacks (e.g. man-in-the-middle)

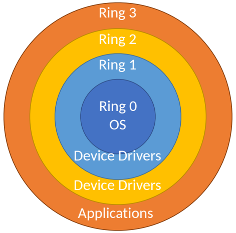
Modern defense: Isolation

Rings:

Most modern CPUs support protected mode

x86 CPUs support three rings with different privileges

- Ring 0: Operating System
  - Code in this ring may directly access any device
- Ring 1, 2: device drivers
  - Code in these rings may directly access some devices
  - May not change the protection level of the CPU
- Ring 3: userland
  - Code in this ring may not directly access devices
  - All device access must be via OS APIs
  - May not change the protection level of the CPU



why does this hw feature help security?

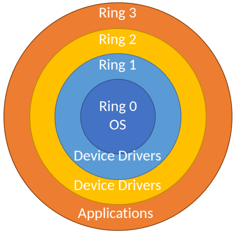
Modern defense: Isolation

Rings:

Most modern CPUs support protected mode

x86 CPUs support three rings with different privileges

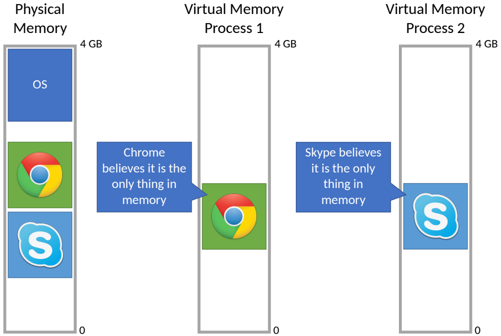
- Ring 0: Operating System
  - Code in this ring may directly access any device
- Ring 1, 2: device drivers
  - Code in these rings may directly access some devices
  - May not change the protection level of the CPU
- Ring 3: userland
  - Code in this ring may not directly access devices
  - All device access must be via OS APIs
  - May not change the protection level of the CPU



2

T

Virtual Memory:


Physical Memory
4 GB
OS
0
Chrome believes it is the only thing in memory
Virtual Memory Process 1
4 GB
0
Skype believes it is the only thing in memory
Virtual Memory Process 2
4 GB
0

Basis for tools

Security Technologies

Authentication

- Physical and remote access is restricted

Access control

- Processes cannot read/write any file
- Users may not read/write each other's files arbitrarily
- Modifying the OS and installing software requires elevated privileges

Firewall

- Unsolicited communications from the internet are blocked
- Only authorized processes may send/receive messages from the internet

Anti-virus

- All files are scanned to identify and quarantine known malicious code

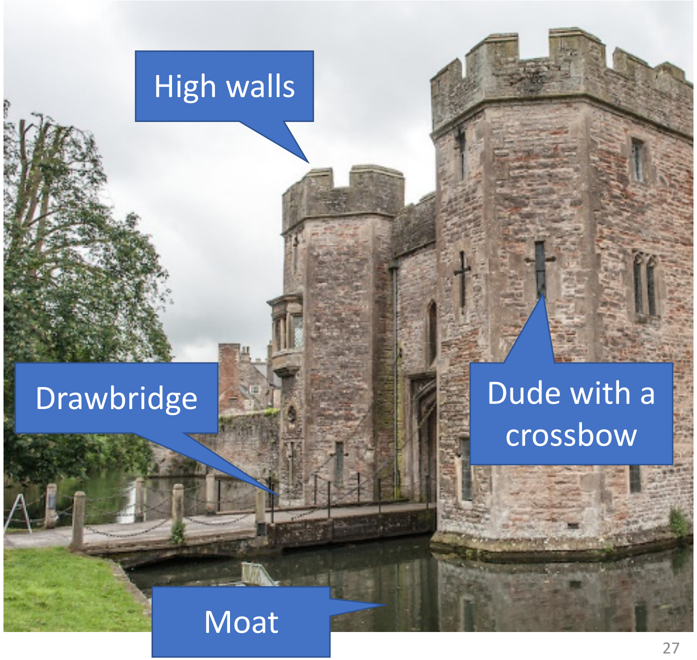
Logging

- All changes to the system are recorded
- Sensitive applications may also log their activity in the secure system log

Systems Security Principles

Defense in Depth

1. Fail-safe Defaults
2. Separation of Privilege
3. Least Privilege
4. Open Design
5. Economy of Mechanism
6. Complete Mediation
7. Compromise Recording
8. Work Factor



Exploits

- Buffer overflows
- XSS
- SQL injection
- CSRF. webmodel.

Failure of Implementation.

"failure to validate attacker-supplied input"

Anatomy of an exploit

Program Crash

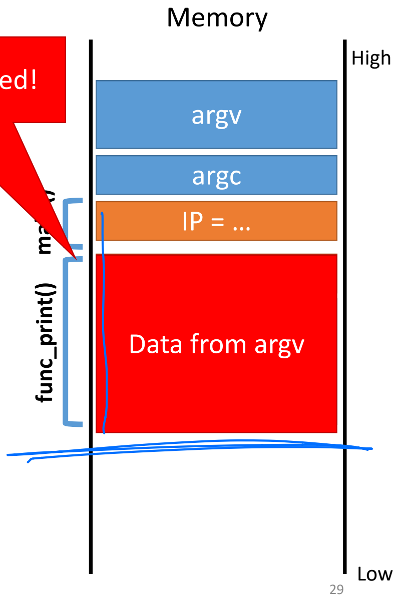
```
0:  void func_print(char s[]) {
      // only holds 32 characters, max
      char buffer[32];
1:    strcpy(buffer, s);
2:    printf("%s\n",buffer);
3:  }

4:  void main(i
5:    for (int i=1; i < argc; i++) {
6:      func_print(argv[i]);
7:    }
8:  }
```

IP

Program crashes :(

Saved IP is destroyed!



Mitigations

ROP can still bypass these.

- Stack canaries
  - Compiler adds special sentinel values onto the stack before each saved IP
  - Canary is set to a random value in each frame
  - At function exit, canary is checked
  - If expected number isn’t found, program closes with an error
- Non-executable stacks
  - Modern CPUs set stack memory as read/write, but no eXecute
  - Prevents shellcode from being placed on the stack
- Address space layout randomization
  - Operating system feature
  - Randomizes the location of program and data memory each time a program executes

SQL Injection

Pb

```
‘SELECT * FROM user_tbl WHERE user="%s" AND pw="%s";'
```

form[‘username’]	form[‘password’]	Resulting query
alice	123456	‘… WHERE user="alice" AND pw="123456";’
bob	qwerty1#	‘… WHERE user="bob" AND pw="qwery1#";’
goofy	a"bc	‘… WHERE user="goofy" AND pw="a"bc";’
weird	abc" or pw="123	‘… WHERE user=”weird" AND pw="abc" or pw="123";’
eve	" or 1=1; --	‘… WHERE user=”eve" AND pw="" or 1=1; --";’
mallory"; --		‘… WHERE user="mallory"; --" AND pw="";’

5 Lessons of fight club

verify assumption about input, reject bad/unforseen inputs

Lesson 1:

Never trust input from the user

Lesson 2:

∧ XOR

Never mix code and data

~~NX~~

$W \wedge X$. "write a page or execute a page"

~~C~~ ~~PHP~~

Lesson 3:

Use the best tools at your disposal

Lesson 4:

(get this in 2550)

Awareness and Vigilance

Lesson 5:

Patch!

Topics we did not cover

- Post-quantum cryptography ✓
- Crypto currencies and smart contracts ✓
- Protocol Security (TLS, wireless, SDN)
- Side channel attacks Spectre Meltdown
- Secure Hardware Technologies (TPM, TXT) (SGX:)
- Distributed System Security and Resilience
- Privacy and regulations
- Fuzzing and software testing
- Formal verification
- Mobile and IoT security
- Machine Learning for Security
- Adversarial Machine Learning

TAs deserve thanks!

Byron, Donald, Fiona, Kate, Martin, Matthew, Rahul, Samir, Simon

Christo Thanks!!

Please submit a TRACE course review