CSE227 – Graduate Computer Security

DDoS + Botnets

UC San Diego

Housekeeping

General course things to know

- Midpoint check-in document is due **5/8 at 11:59pm PT**
  - Introduction (frame the problem)
  - Related work section (should include ~5 – 10 relevant papers)
  - Research plan, current status, what's left to do
- Midpoint check-in meetings will happen week 7! Will send out a Canvas note today.

Project goals this week

General course things to know

- By the end of this week, you should have a concrete plan that just lets you *implement* for the next four weeks!

Today's lecture

Learning Objectives

- Learn about DDoS, botnets, and mechanisms for detecting DDoS traffic on the Internet
- Discuss the "Inferring Internet DoS Activity" paper
- Discuss the "Takedown" paper

Preliminaries

What is the Internet?

What is the Internet?

A network of computer networks that lets computer talk to one another.

What is a computer network?

Interconnected computing devices that exchange data and resources via *network protocols*.

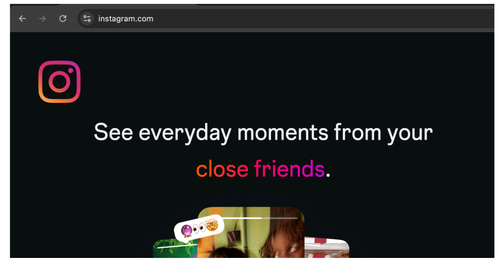
What is a network protocol?

The specification that tells you how to send, receive, and parse bytes of data you receive from an underlying network. Examples?

What is a network of networks?

- Let’s say my computer wants to talk to instagram.com. How does it do that?

my laptop



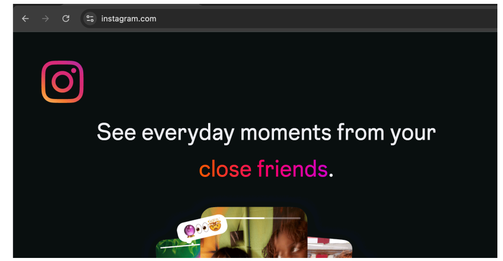
instagram.com

What is a network of networks?

- Let's say my computer wants to talk to instagram.com. How does it do that?

my laptop

router, via WiFi

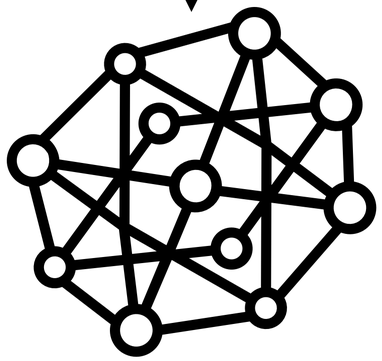


instagram.com

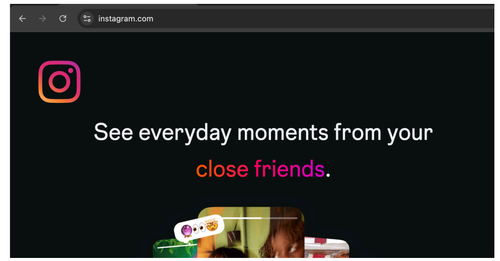
What is a network of networks?

- Let's say my computer wants to talk to instagram.com. How does it do that?

my laptop



UCSD network, via wires

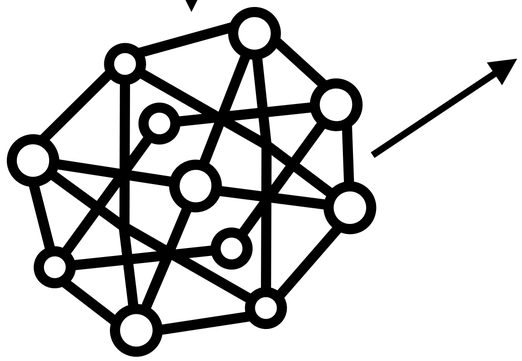


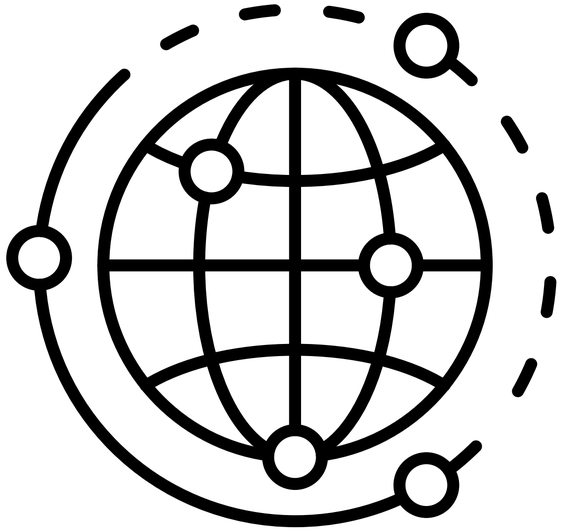
instagram.com

What is a network of networks?

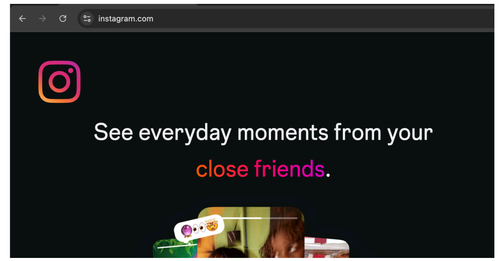
- Let's say my computer wants to talk to instagram.com. How does it do that?

my laptop





Internet, via wires



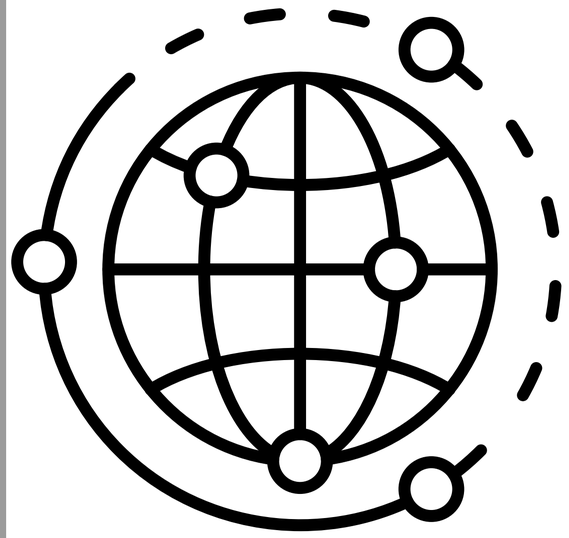
instagram.com

Internet Service Provider: An entity which enables computers access to the Internet

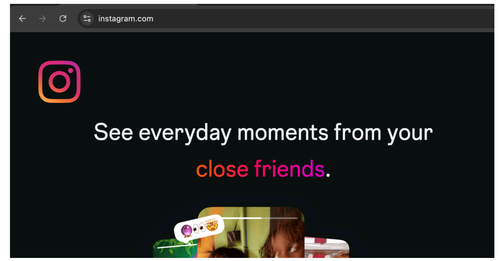
orks?

tagram.com. How does it do that?

my laptop



Internet, via wires

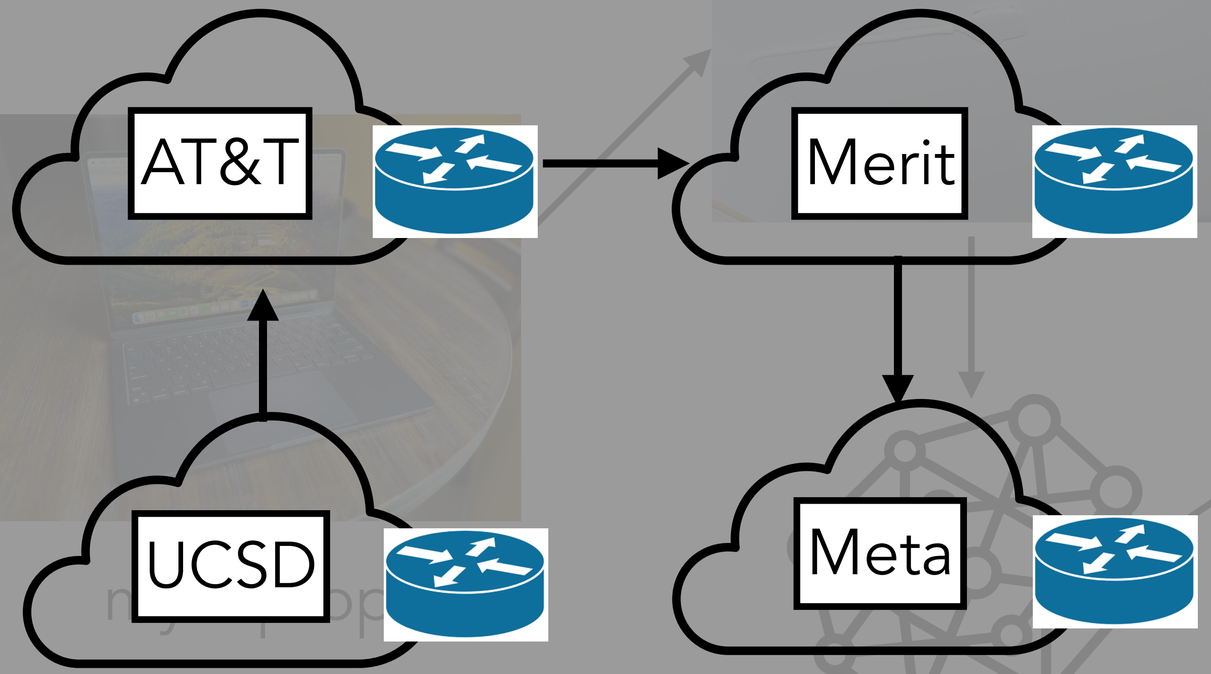


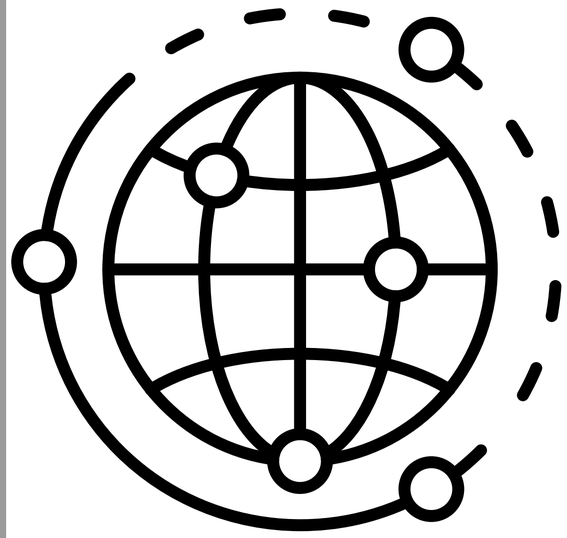
instagram.com

Internet Service Provider: An entity which enables computers access to the Internet

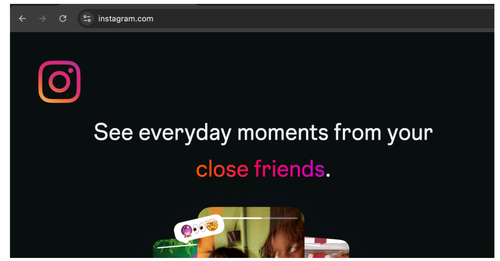
orks?

tagram.com. How does it do that?





Internet, via wires

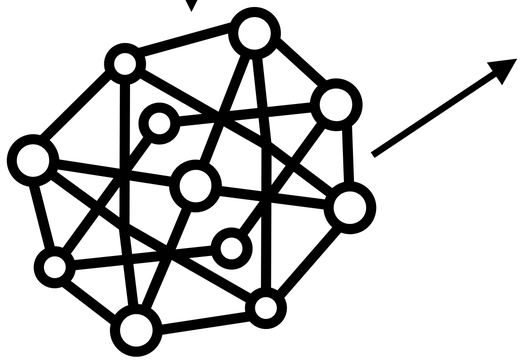


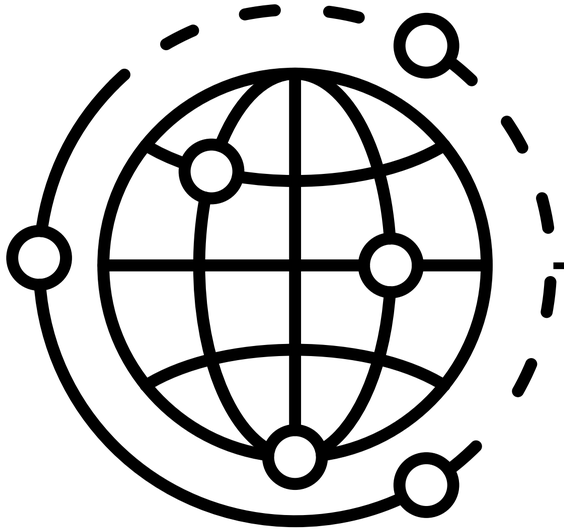
instagram.com

What is a network of networks?

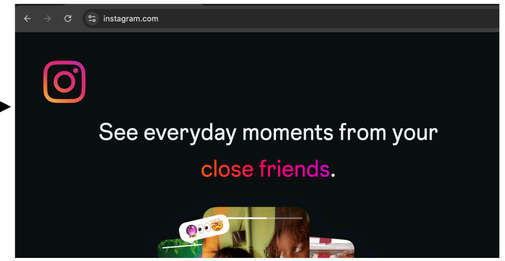
- Let's say my computer wants to talk to instagram.com. How does it do that?

my laptop





Internet, via wires

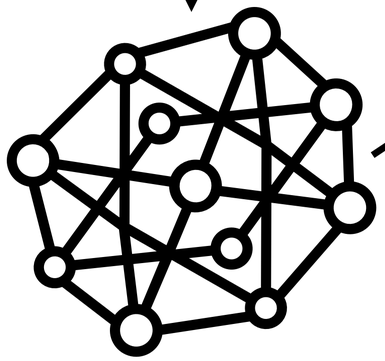


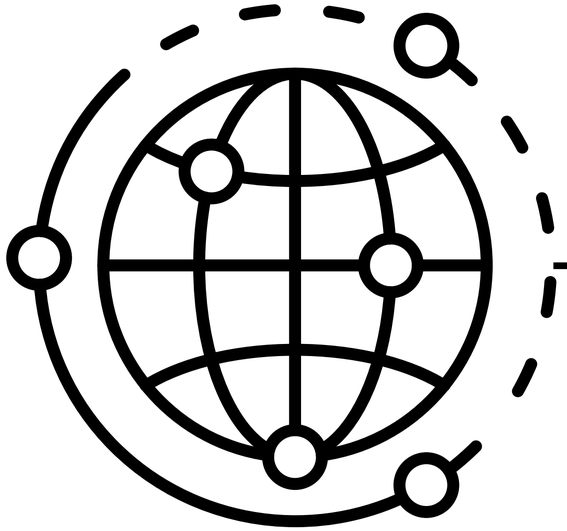
instagram.com

What is a network of networks?

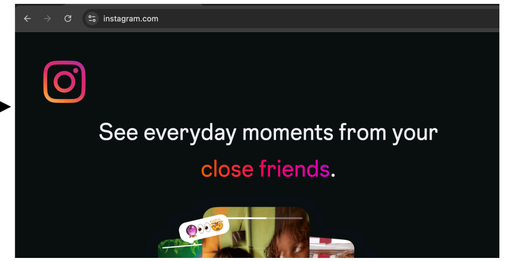
- Let's say my computer wants to talk to instagram.com. How does it do that?

my laptop





Internet, via wires



instagram.com

This all happens in < 100ms for every request.

Networking Basics

- What is an IP address?
  - How many IPv4 addresses are there? IPv6?
- What is a network *port*?
- What is TCP, and what guarantees does it provide?
- What is a TCP handshake, and how does it typically work?

What is a Denial-of-Service attack?

What is a Denial-of-Service attack?

DoS: An attack that consumes the resources of a remote host of network, making it unavailable for normal use

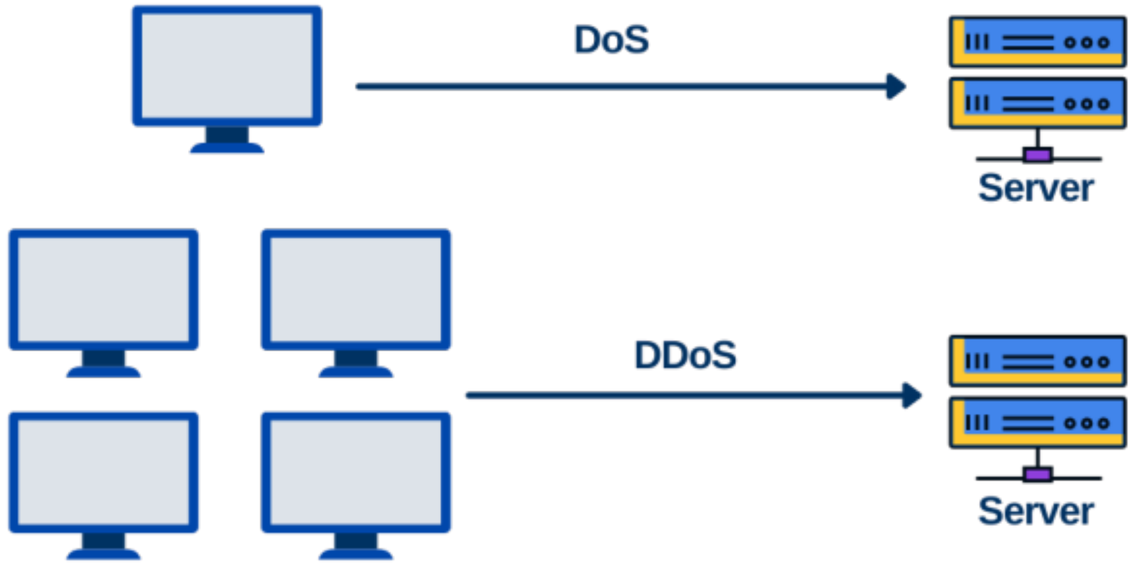
What is a Distributed Denial-of-Service attack?

What is a Distributed Denial-of-Service attack?

DDoS: DoS, but distributed across many different attacking machines making it impossible to block solely based on IP address

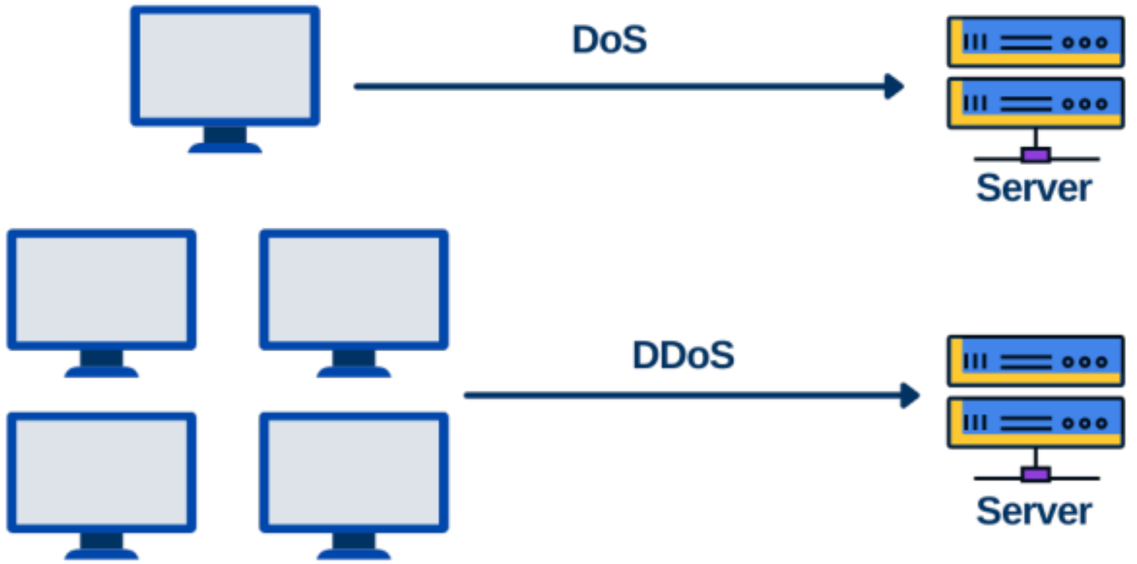
Two types of DoS

- What is a *logic-based* DoS attack?



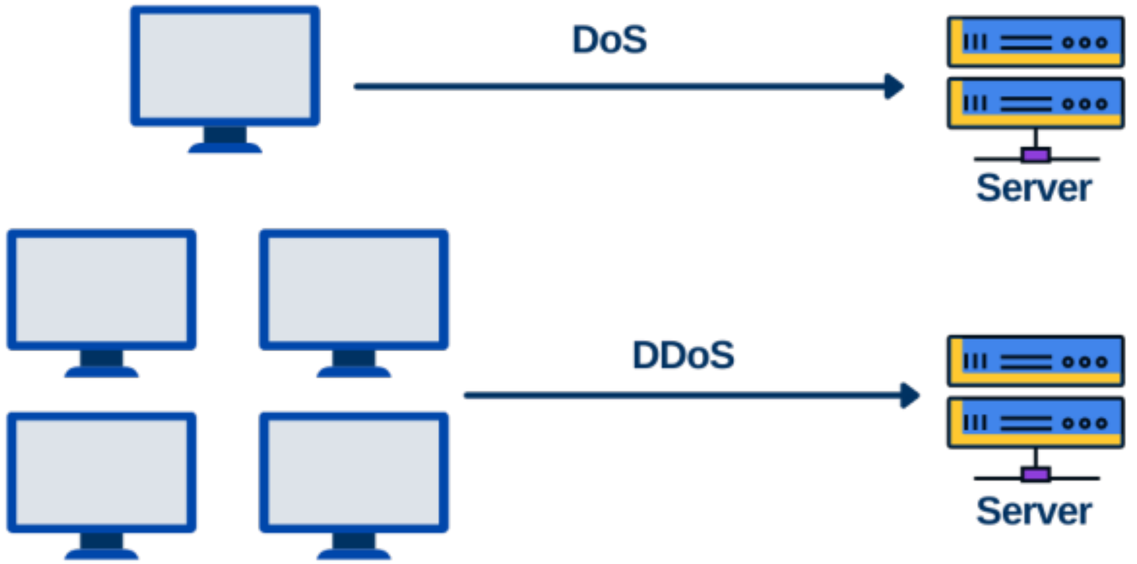
Two types of DoS

- What is a *logic-based* DoS attack?
  - Exploits some fundamental problem in the software that renders the server useless



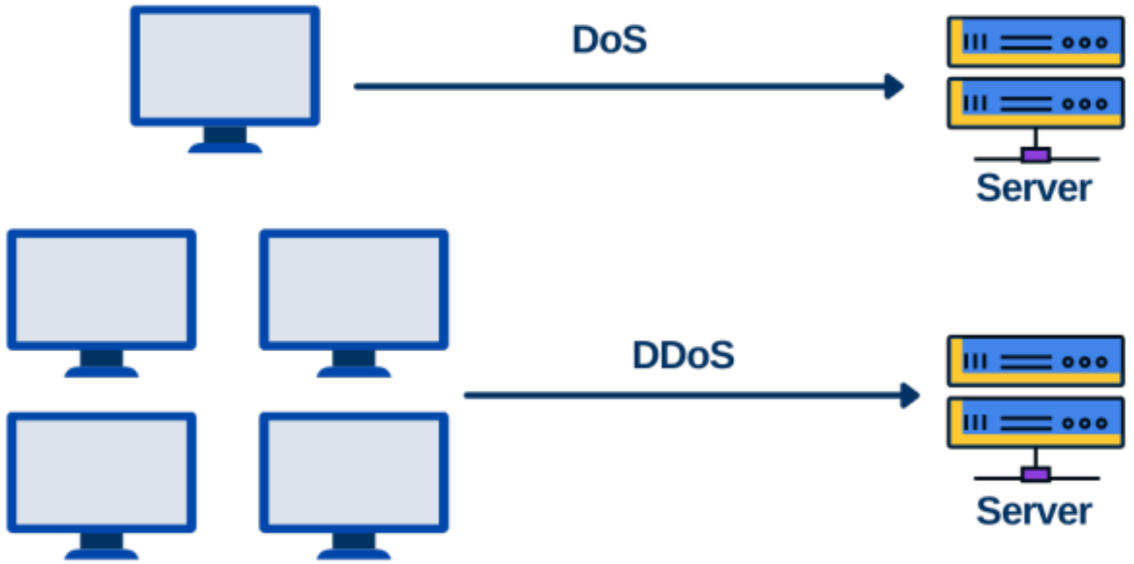
Two types of DoS

- What is a *logic-based* DoS attack?
  - Exploits some fundamental problem in the software that renders the server useless
- What is a *flooding*-based DoS attack?

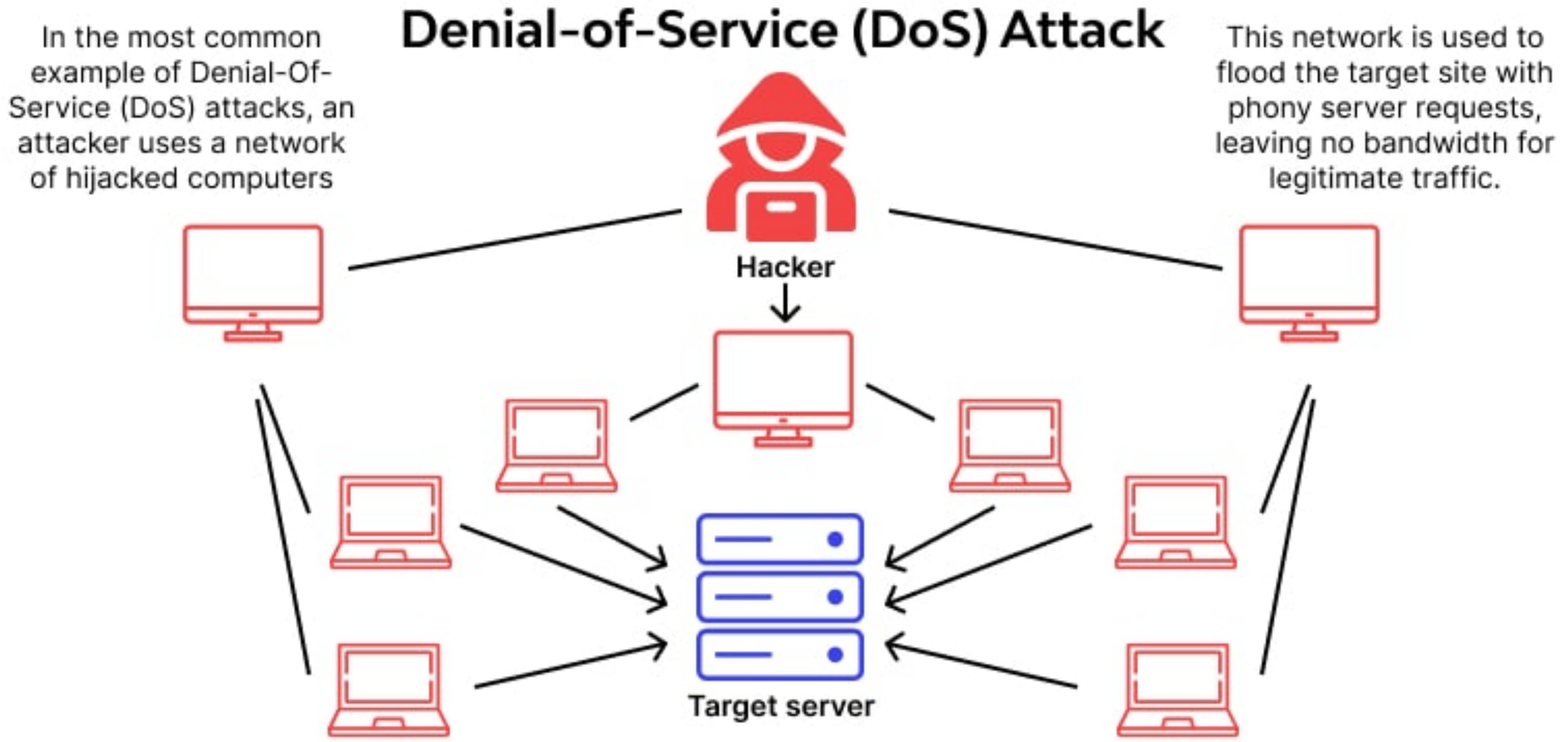


Two types of DoS

- What is a *logic-based* DoS attack?
  - Exploits some fundamental problem in the software that renders the server useless
- What is a *flooding*-based DoS attack?
  - Overwhelm resources by sending lots of packets
  - These papers: **flooding**



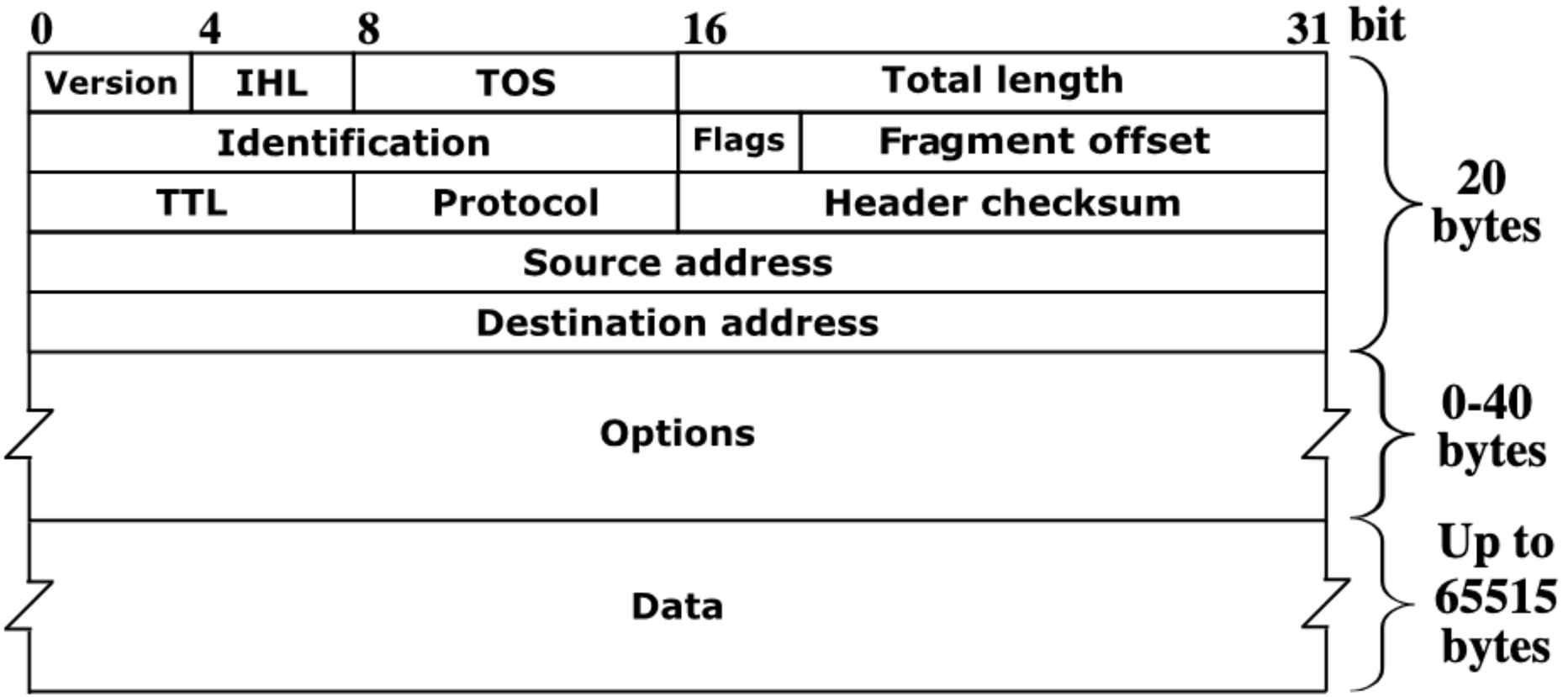
Basic Flavor of DDoS



https://www.wallarm.com/what/dos-denial-of-service-attack

What is IP spoofing?

What is IP spoofing?



What is IP spoofing?

IP: 1.1.1.1

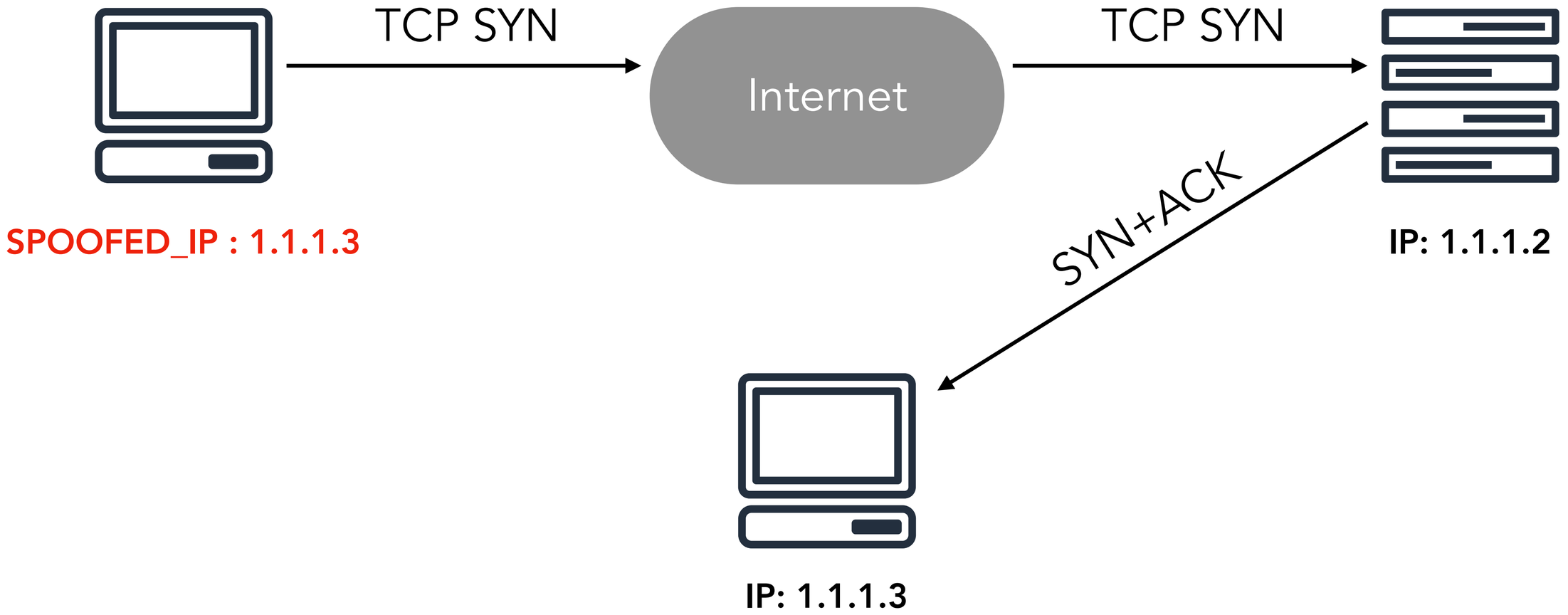
Internet

IP: 1.1.1.2

What is IP spoofing?

What is IP spoofing?

What is IP spoofing?



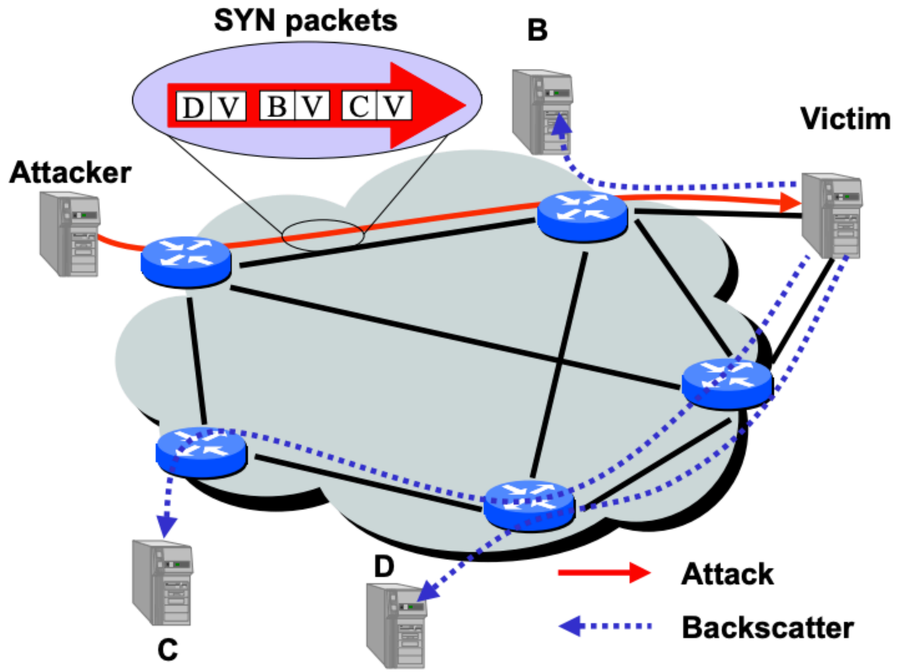
Inferring Internet Denial-of-Service Activity

A few words on this paper…

- This is a UCSD paper!
  - Stefan Savage + Geoff Voelker are the faculty authors – they do awesome work in all things cybersecurity
- This paper won best paper at USENIX Security 2001
- This paper won the USENIX Security Test-of-Time award in 2017
- First ever quantitative experiments measuring DDoS… the technique sort of started an entire field

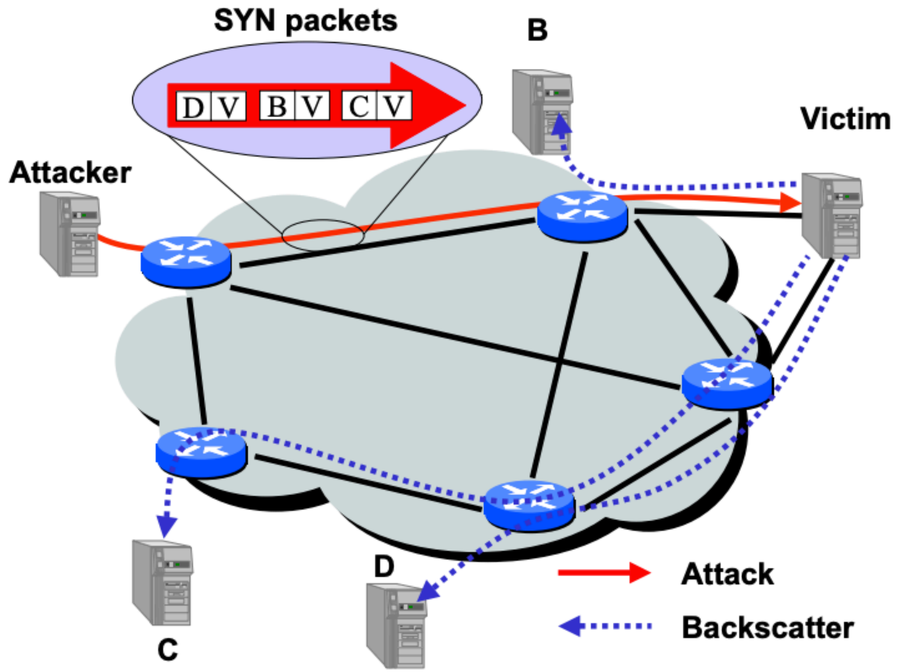
Basic Premise of the Measurement

- Most DoS and DDoS attacks employ random IP spoofing to send attack packets. Why?



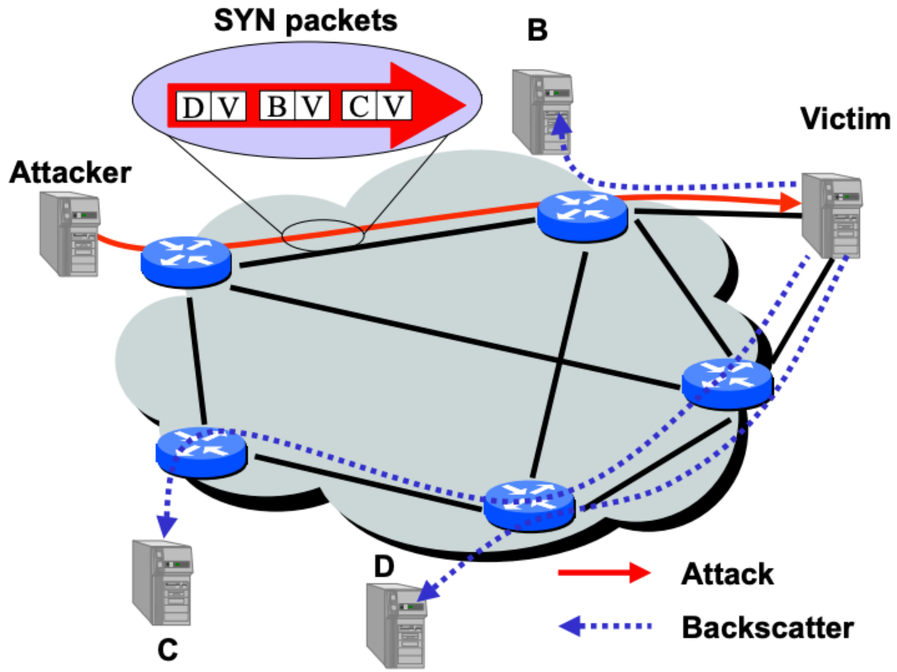
Basic Premise of the Measurement

- Most DoS and DDoS attacks employ random IP spoofing to send attack packets. Why?
- What is “backscatter?”



Basic Premise of the Measurement

- Most DoS and DDoS attacks employ random IP spoofing to send attack packets. Why?
- What is "backscatter?"
  - Responses sent from victim hosts and on-path devices to attack traffic



Assumptions in the paper

- What is address uniformity?

Assumptions in the paper

- What is address uniformity?
  - Why is uniformity not always guaranteed?

Assumptions in the paper

- What is address uniformity?
  - Why is uniformity not always guaranteed?
- What is reliable delivery?

Assumptions in the paper

- What is address uniformity?
  - Why is uniformity not always guaranteed?
- What is reliable delivery?
  - Why is reliable delivery not always guaranteed?

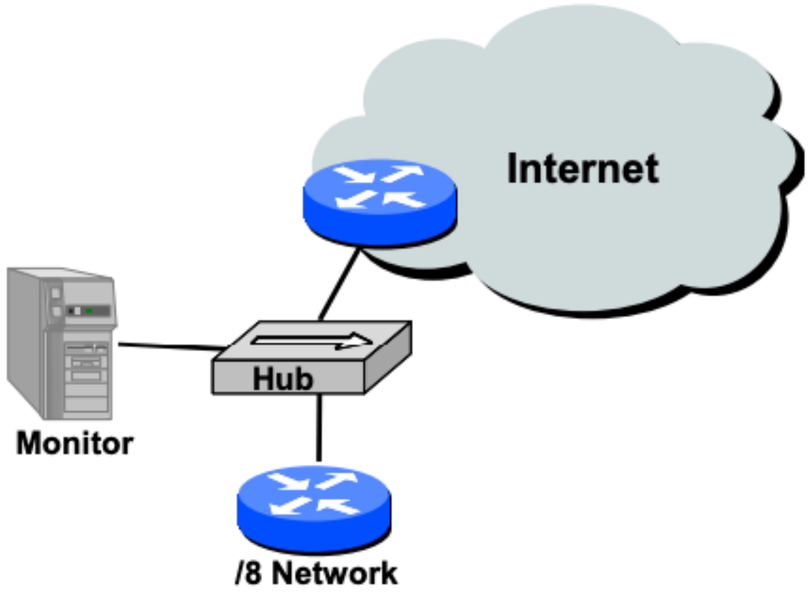
Assumptions in the paper

- What is address uniformity?
  - Why is uniformity not always guaranteed?
- What is reliable delivery?
  - Why is reliable delivery not always guaranteed?

In spite of its limitations, we believe our overall approach is sound and provides at worst a conservative estimate of current denial-of-service activity.

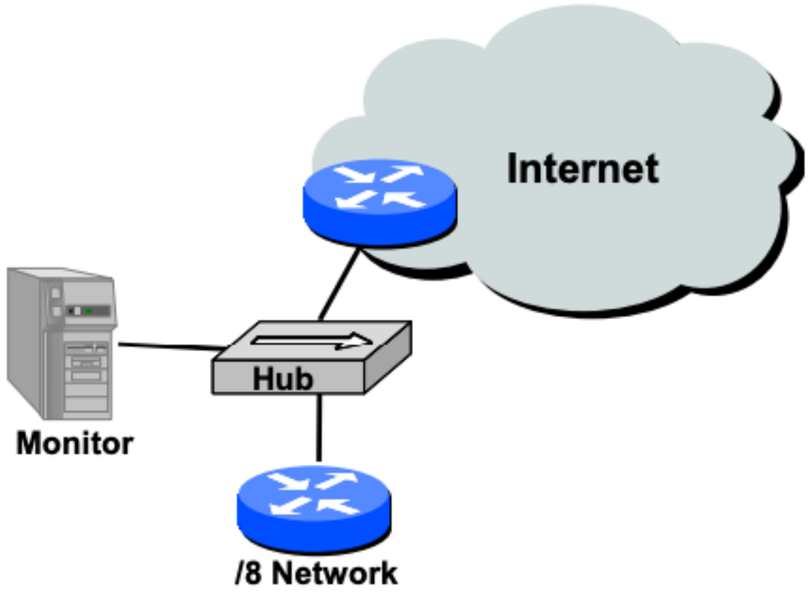
Experiments

- What did the authors monitor in order to identify DoS traffic?



Experiments

- What did the authors monitor in order to identify DoS traffic?
  - “Slash 8” (CIDR notation), which is **1/256 of all of the Internet**
  - We call this a **darknet:** globally routable address space that goes “nowhere”
  - CAIDA operates this: https://www.caida.org/projects/network_telescope/



Results

- **Authors found 12,805 attacks over the course of a week,** with 5000 distinct victim IP addresses in more than 2000 distinct DNS domains
- Characterized attacks, protocols, attack durations, strategies, and domains attacked
- My highlights
  - Hackers can have a lot of fun – reverse DNS names of the victims, is.on.the.net.illegal.ly, the.feds.cant.secure.their.shellz.ca
  - Classic ***gaming*** induced DDoS: **battle.net** is a common victim
  - Tons of attacks on Internet entities (e.g., aol.com, etc.)
  - Some attacks on core infrastructure (e.g., routers that can be central points of failure)

Meta-thoughts on the paper

- DDoS remains a problem… why is this still an issue? What remains the fundamental tension here that makes DDoS so hard to defeat?
- What did we like about this paper? What didn’t we like?
- What could we do about DoS attacks as they are described in the paper?

Story time…

- I was a first year PhD student sitting in a special topics (e.g., CSE 291) security class in my first semester, when I hear Brian Krebs' website is down due to DDoS
- Krebs writes out that it's a huge attack, 620 Gbps (at the time was very large)
- Claim is that it's powered by weak IoT devices (unverified)

Story time…

- Folks in the lab think it’s interesting, we want to investigate it
- Then, 9 days later, **the Mirai code is released online,** Internet havoc ensues

[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.

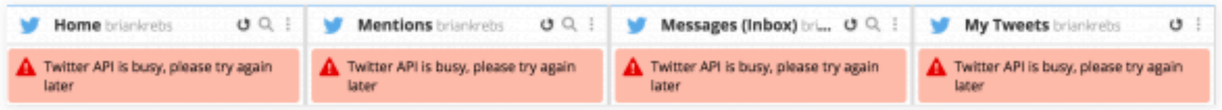
Story time…

- A few weeks later, much of the entire Internet was **down** for at least a few hours due to a Mirai DDoS attack on Dyn (dynamic DNS provider)

DDoS on Dyn Impacts Twitter, Spotify, Reddit

October 21, 2016 175 Comments

Criminals this morning massively attacked Dyn, a company that provides core Internet services for Twitter, SoundCloud, Spotify, Reddit and a host of other sites, causing outages and slowness for many of Dyn's customers.

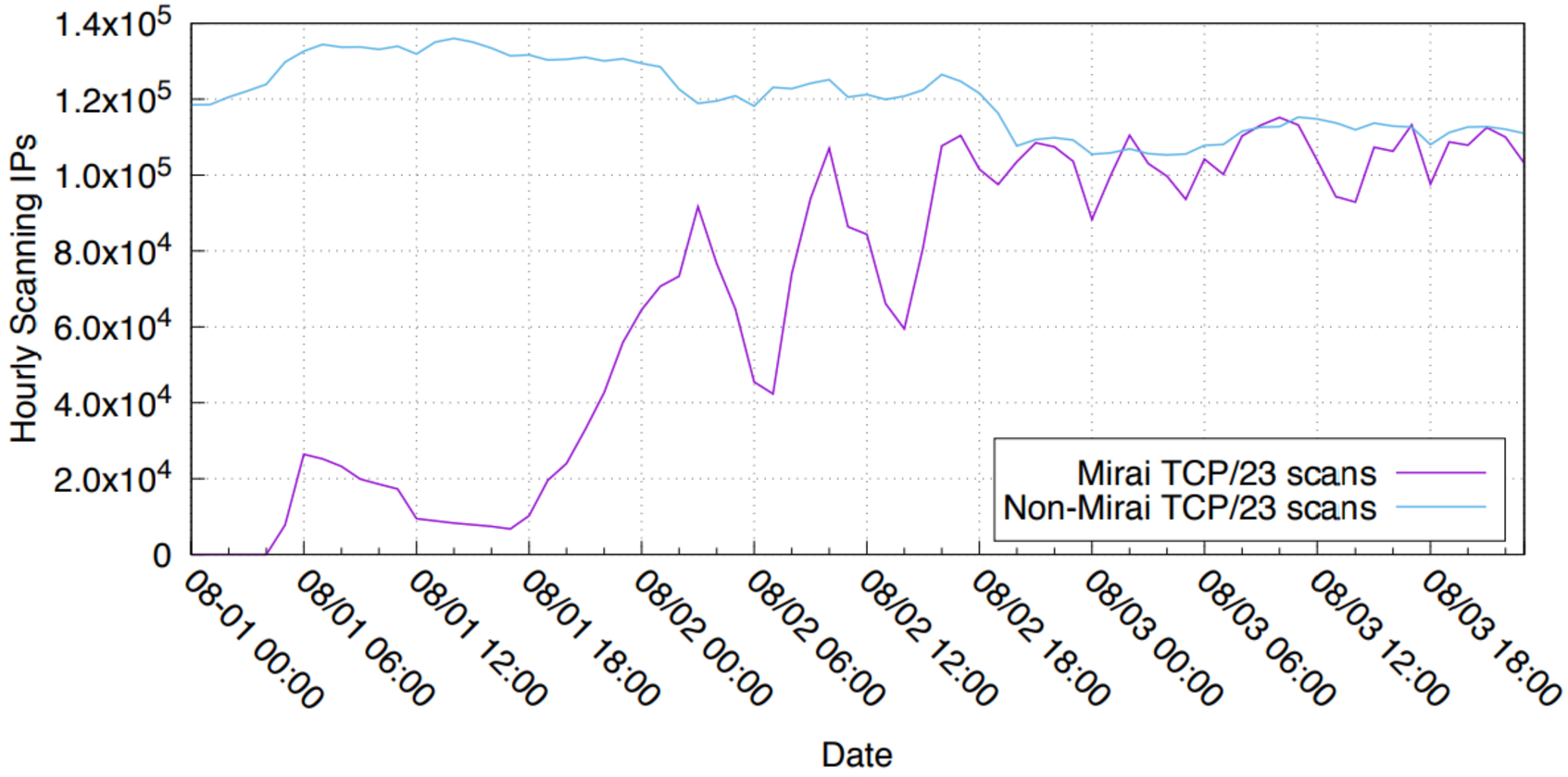


Twitter is experiencing problems, as seen through the social media platform Hootsuite.

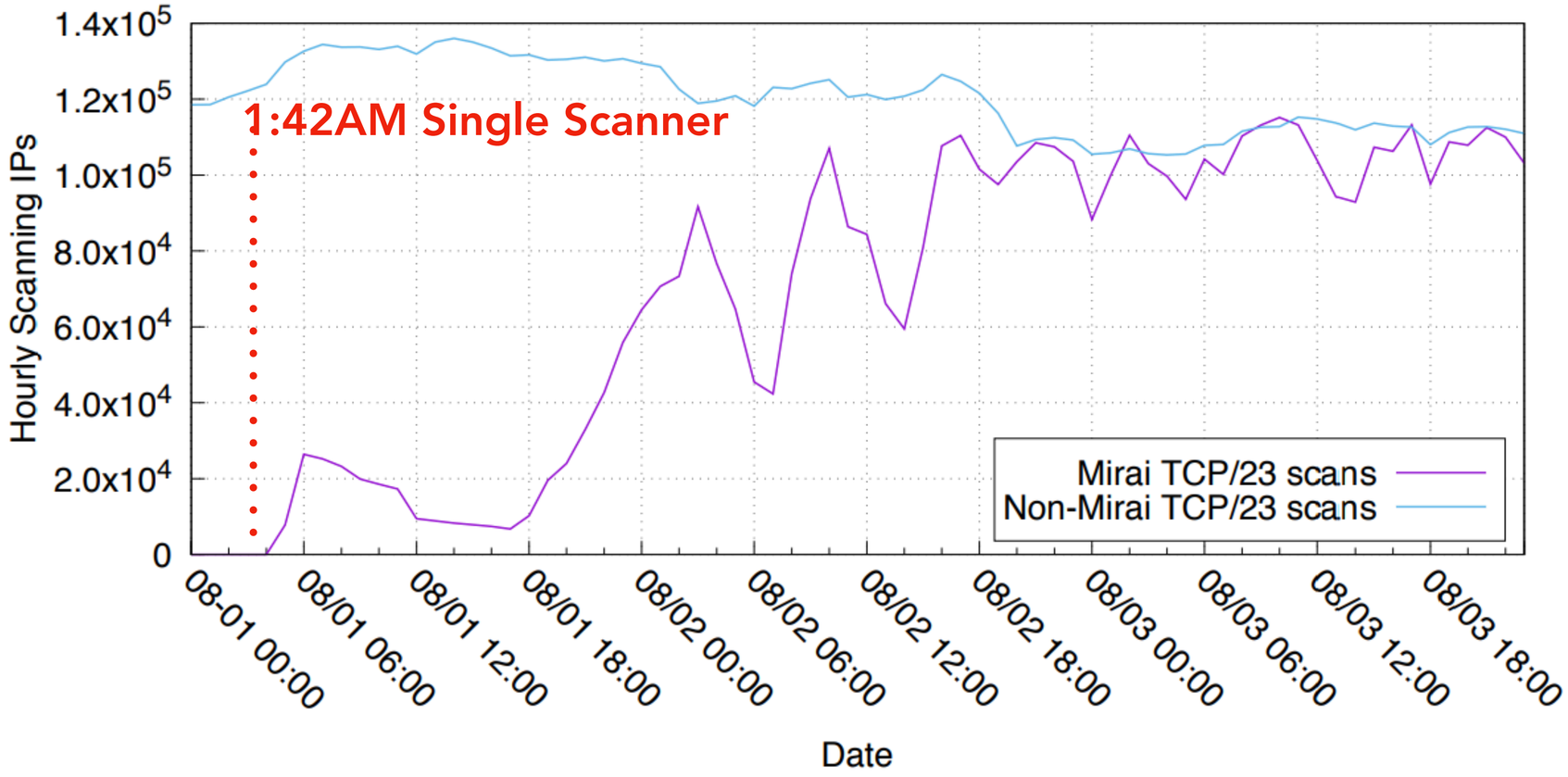
Identifying Mirai in the backscatter

- How can we distinguish Mirai scans from other DDoS traffic?
  - “Quirk” in the code that enables stateless scanning: **TCP sequence number was set to the destination IP address**
  - Expectation to see this pattern is 86 packets over our scanning period, instead we saw **116.2 billion packets**

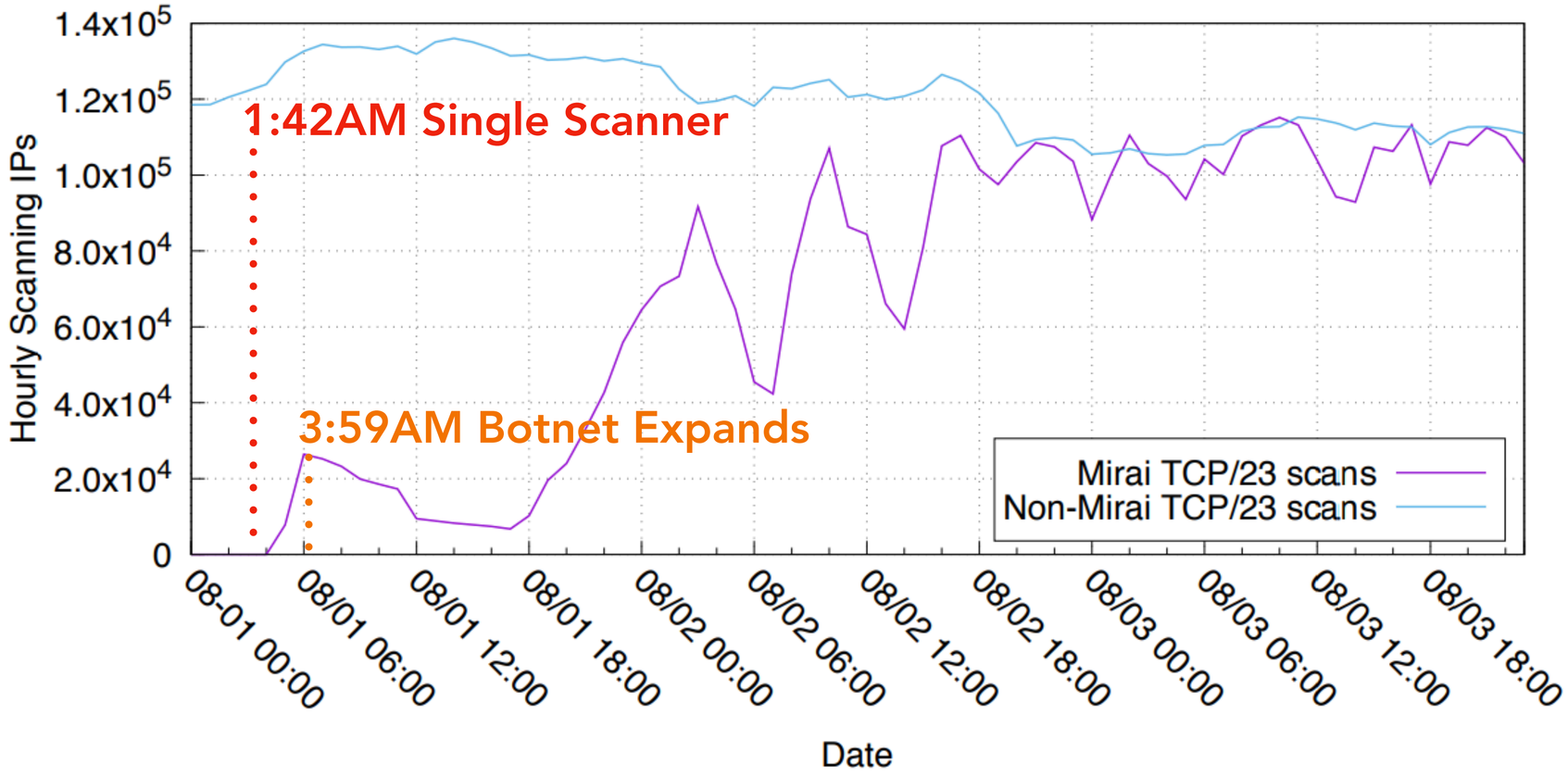
Tracking Mirai over time – Day 0



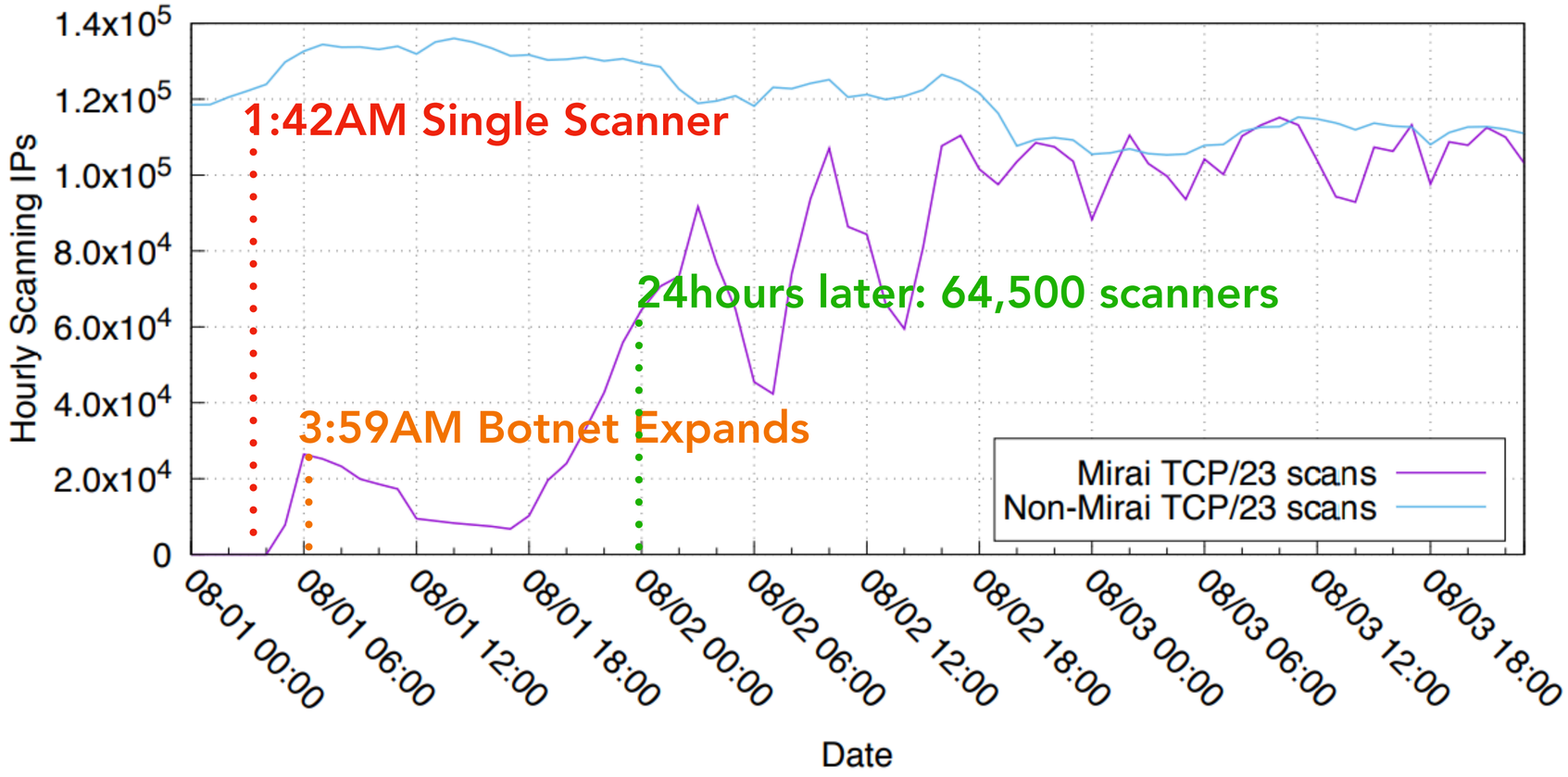
Tracking Mirai over time – Day 0



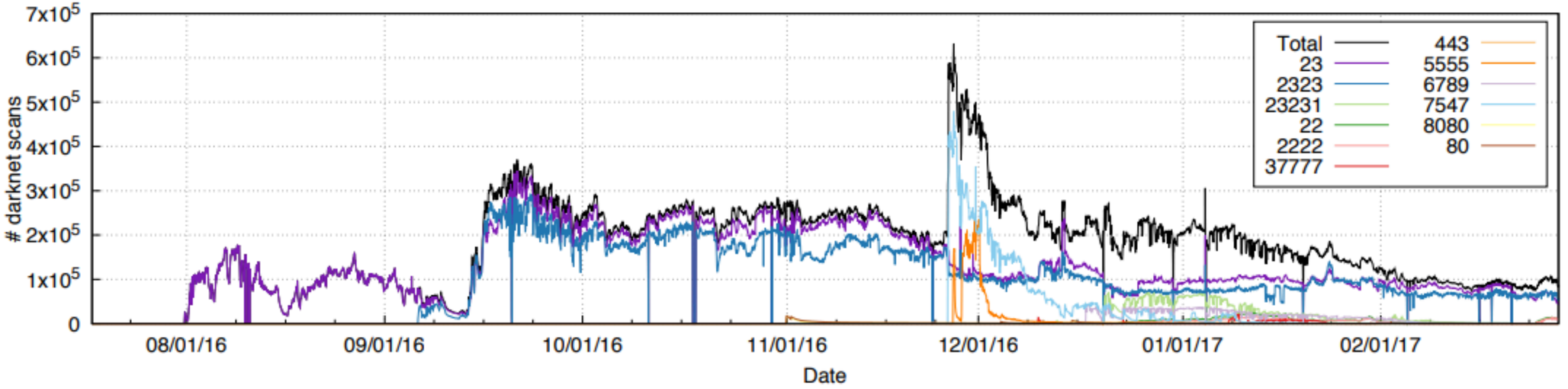
Tracking Mirai over time – Day 0



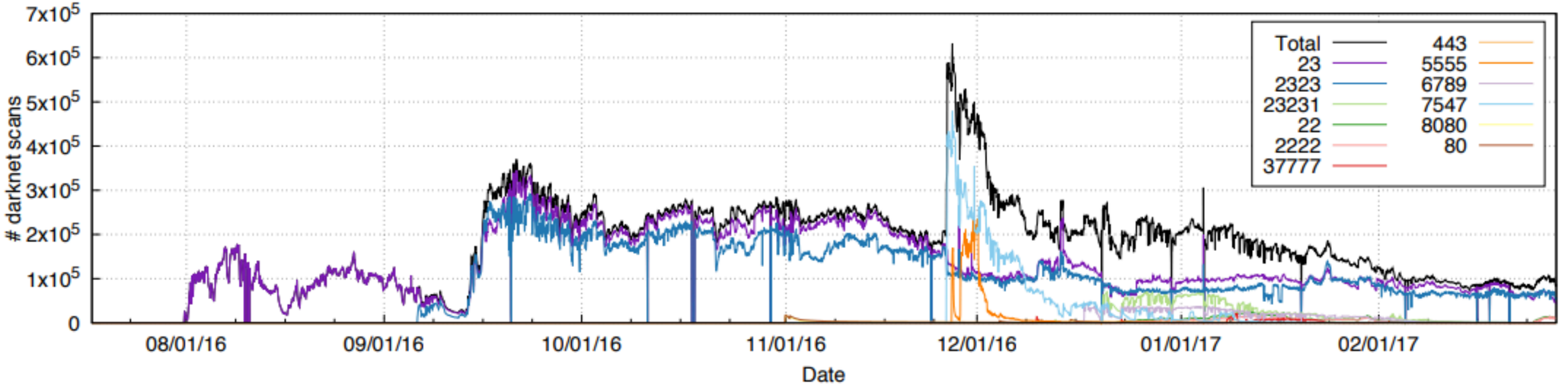
Tracking Mirai over time – Day 0



Tracking Mirai over time – the later days



Tracking Mirai over time – the later days



Steady state of 200 – 300K bots, with a spike in November 2016 of 600K, new vuln.

Myriad of Targets

- **Games:** Minecraft, Runescape, etc.
- **Politics:** Chinese political dissidents, regional Italian politician
- **Anti-DDoS:** DDoS protection services
- **Misc:** Russian cooking blog….?

Understanding the 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."

Understanding the Dyn attack

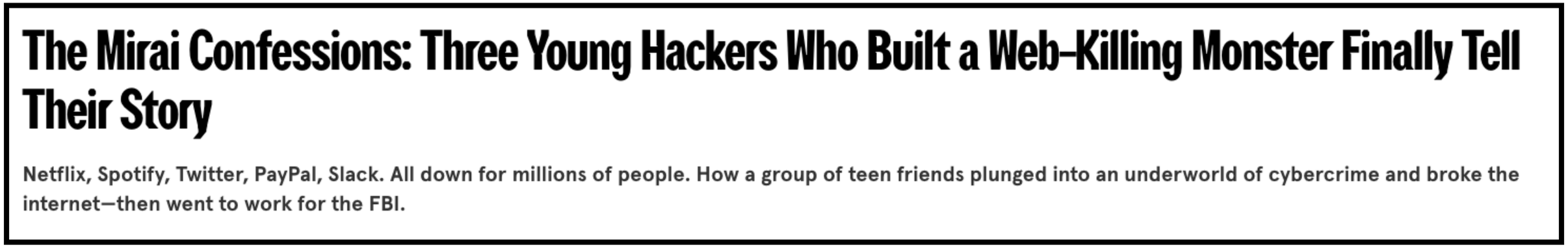
The New York Times

> "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

- Top targets are linked to Sony PlayStation
- Dyn just happened to be in the same IP block as PSN, **collateral damage**

What happened next?



The Mirai Confessions: Three Young Hackers Who Built a Web-Killing Monster Finally Tell Their Story

Netflix, Spotify, Twitter, PayPal, Slack. All down for millions of people. How a group of teen friends plunged into an underworld of cybercrime and broke the internet—then went to work for the FBI.

https://www.wired.com/story/mirai-untold-story-three-young-hackers-web-killing-monster/

Break Time + Attendance

https://tinyurl.com/cse227-attend

Codeword:
ServiceDenied

Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services

DDoS-for-hire Fundamentals

- What is a booter service?
- What do people use booter services for?
- What kinds of attacks are typically attributed to booters?

Booter Takedowns

PRESS RELEASE

U.S. authorities conduct cyber operations as part of global crackdown on DDoS-for-hire services

Thursday, April 16, 2026

Share

For Immediate Release

U.S. Attorney's Office, District of Alaska

ANCHORAGE, Alaska – The U.S. Justice Department today announced court-authorized actions taken to disrupt some of the world's leading Distributed Denial of Service (DDoS) Internet of Things (IoT) botnet services.

U.S. authorities continue to focus resources on charging DDoS botnet administrators and seizing infrastructure, like websites, that allow paying users to launch powerful DDoS attacks. These attacks flood targeted computers and servers with information to prevent them from being able to access the internet. In recent years, DDoS, aka "booter," services have continued to proliferate as they offer a low barrier to entry for users looking to engage in cybercriminal activity.

DDoS services, such as those named in this action, allegedly attacked a wide array of victims in the United States and abroad, including schools, government agencies, gaming platforms, critical infrastructure, including Department of War resources, and millions of people. In addition to affecting targeted victims, these attacks can significantly degrade internet services and completely disrupt internet connections.

- What strategies does the FBI use to conduct a booter takedown?

Booter Takedowns

PRESS RELEASE

U.S. authorities conduct cyber operations as part of global crackdown on DDoS-for-hire services

Thursday, April 16, 2026

Share

For Immediate Release

U.S. Attorney's Office, District of Alaska

ANCHORAGE, Alaska – The U.S. Justice Department today announced court-authorized actions taken to disrupt some of the world's leading Distributed Denial of Service (DDoS) Internet of Things (IoT) botnet services.

U.S. authorities continue to focus resources on charging DDoS botnet administrators and seizing infrastructure, like websites, that allow paying users to launch powerful DDoS attacks. These attacks flood targeted computers and servers with information to prevent them from being able to access the internet. In recent years, DDoS, aka "booter," services have continued to proliferate as they offer a low barrier to entry for users looking to engage in cybercriminal activity.

DDoS services, such as those named in this action, allegedly attacked a wide array of victims in the United States and abroad, including schools, government agencies, gaming platforms, critical infrastructure, including Department of War resources, and millions of people. In addition to affecting targeted victims, these attacks can significantly degrade internet services and completely disrupt internet connections.

- What strategies does law enforcement use to conduct a booter takedown?
  - Seize domains, arrest and charged people running the websites, infiltration of dark web pages
  - *Advertising* for deterrance

This paper

- **What happened to the DDoS-for-hire ecosystem post intervention?**
- How they did it…
  - How did the authors collect ground truth traffic on booter domains?
  - What is a honeypot? How did the authors use honeypot data in their analysis?
  - What social platforms helped the authors in their analysis?

Table 1: The quantitative data sources used and their origins.

Datasets	Statistics	Origins
Ground-truth traffic ◇	20.7M raw events	Our collection
Similarweb analytics ⋆	94 booter domains	Our collection
HOPSCOTCH †	4.6M records	Thomas et al. [38]
AMPPOT †	9.8M records	Krämer et al. [39]
NETSCOUT †	32.9M records	NETSCOUT [40]
Self-reported statistics †	207 booters	Our collection
Underground forums ⋆	1 704 posts	Pastrana et al. [41]
Chat channels ⋆	34 438 messages	Our collection

Data timespans covering both waves: ◇ [14 December 2022 – 31 July 2023]; ⋆ [1 October 2022 – 30 September 2023]; † [1 July 2021 – 30 June 2023]

Resurrections

- How quickly did booter services “resurrect” themselves?
  - Hours to days; **high resurrection rate!**
- First wave had ~50% resurrection, second had 100% resurrection!
  - Booters were highly resilient

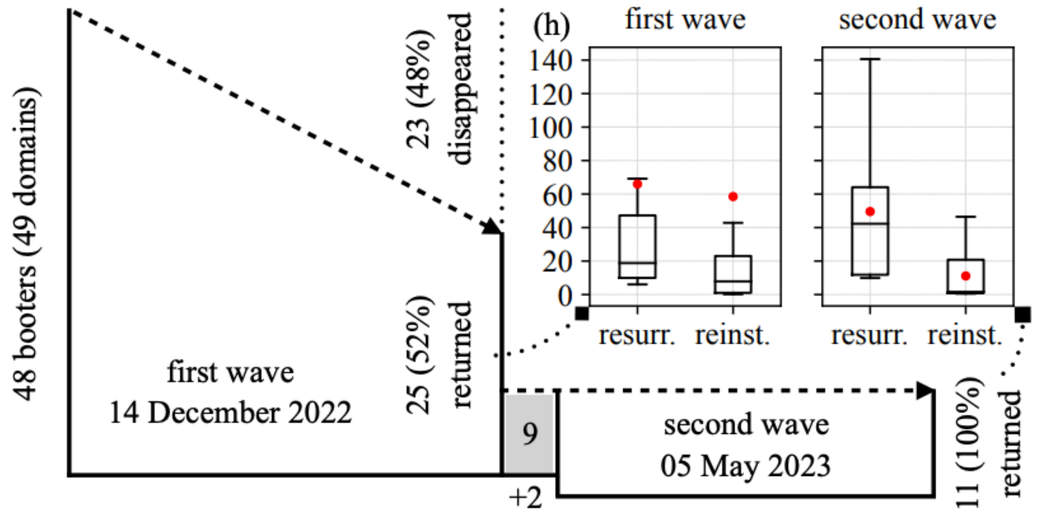
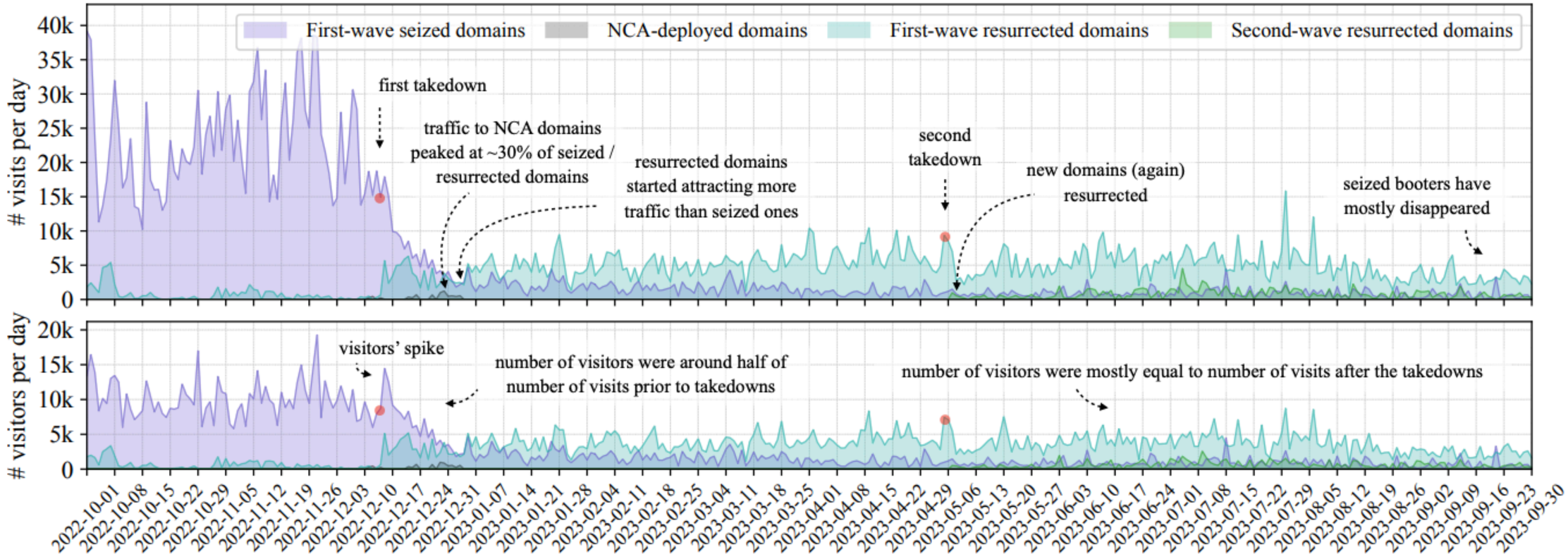


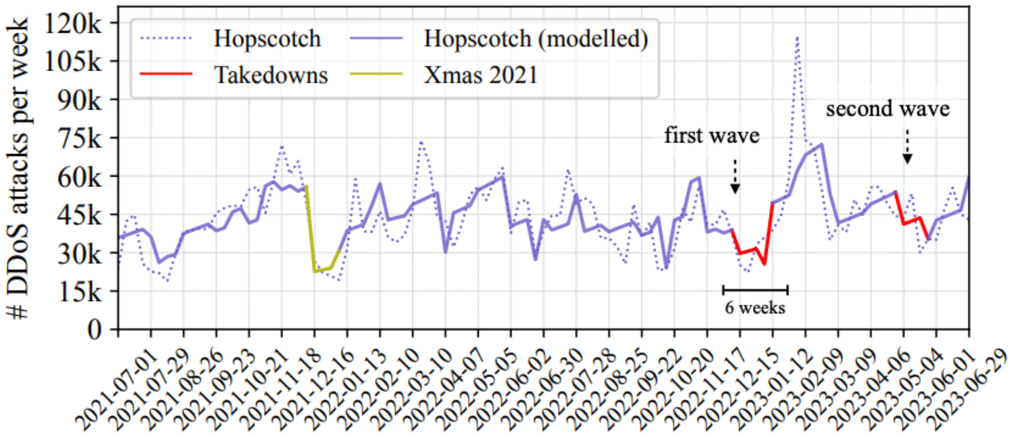
Figure 1: Overview of booter resurrections and reinstallations after two waves of takedown (hours). Red dots indicate means.

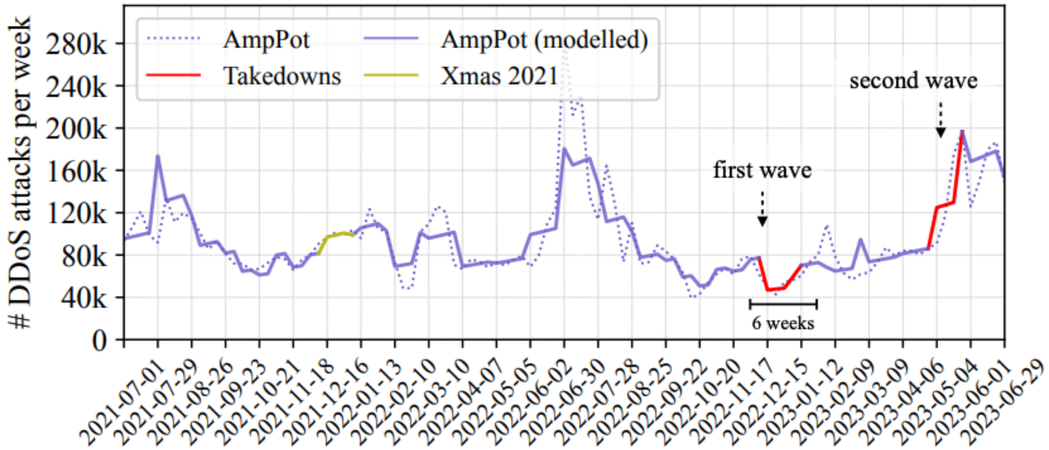
Longitudinal effects on supply-side traffic



Traffic *significantly* decreased due to the intervention (90% reduction)

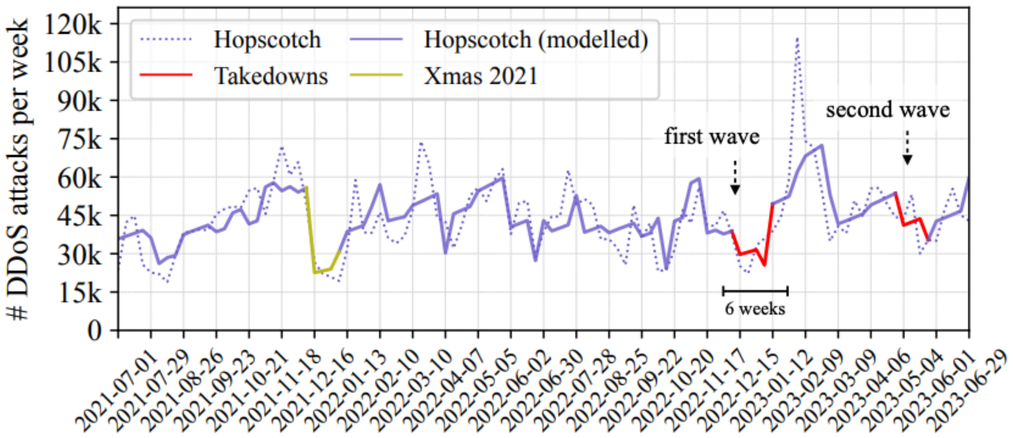
Longitudinal effects on demand

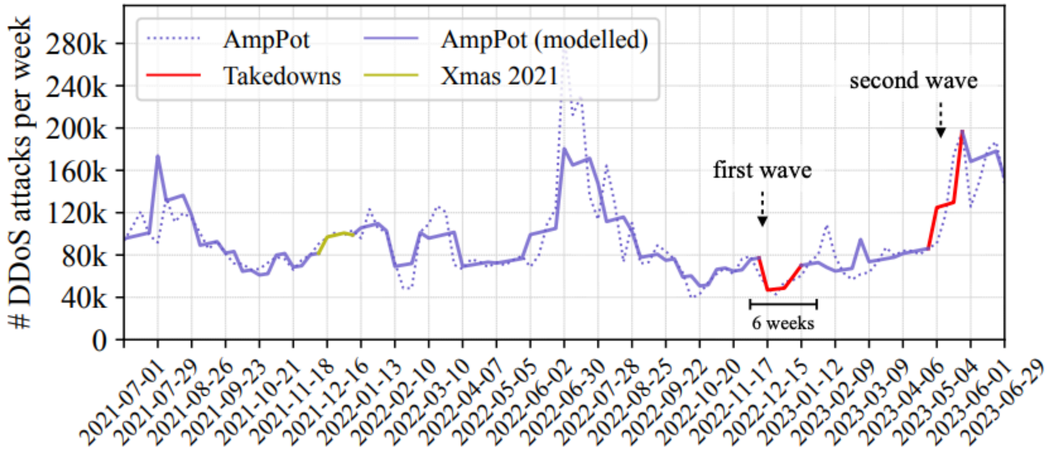




How did these interventions impact the demand for DDoS attacks?

Longitudinal effects on demand





How did these interventions impact the demand for DDoS attacks?

Immediate reduction; but regression back to mean in ~6 weeks.

Meta-thoughts

- Takedowns of supply have a *short-lived* effect in this ecosystem. Why? What does this tell us about these types of interventions?
  - Where might these interventions be useful? Where might they not be?
- What *surprised* you about this paper? What didn't surprise you at all?
- What did this paper make you think about *trust*?