Raphael Hiesgen, Marcin Nawrocki, Marinho Barcellos, Daniel Kopp, Oliver Hohlfeld, Echo Chan, Roland Dobbins, Christian Doerr, Christian Rossow, Daniel R. Thomas, Mattijs Jonker, Ricky Mok, Xiapu Luo, John Kristoff, Thomas C. Schmidt, Matthias Wählisch, kc claffy

HAW Hamburg, NETSCOUT, U of Waikato, DE-CIX, U of Kassel, Akamai/Hong Kong PolyU, HPI, CISPA, U of Strathclyde, U of Twente, UCSD/CAIDA, Hong Kong PolyU, TU Dresden

# The Age of DDoScovery

## An Empirical Comparison of Industry and Academic DDoS Assessments

November 5th, 2024
raphael.hiesgen@haw-hamburg.de
IMC, Madrid, Spain

# Perspectives on DDoS

**Reality**

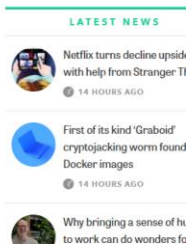
The New York Times

*Hackers Used New Weapons to Disrupt Major Websites Across U.S.*


**The truth is, most IoT devices can be turned into botnets**

*by Colm Gorey*

9 MAR 2018 1.57K VIEWS



# Perspectives on DDoS

## Reality

The New York Times

***Hackers Used New Weapons to Disrupt Major Websites Across U.S.***


**The truth is, most IoT devices can be turned into botnets**

*by Colm Gorey*

9 MAR 2018 1.57K VIEWS

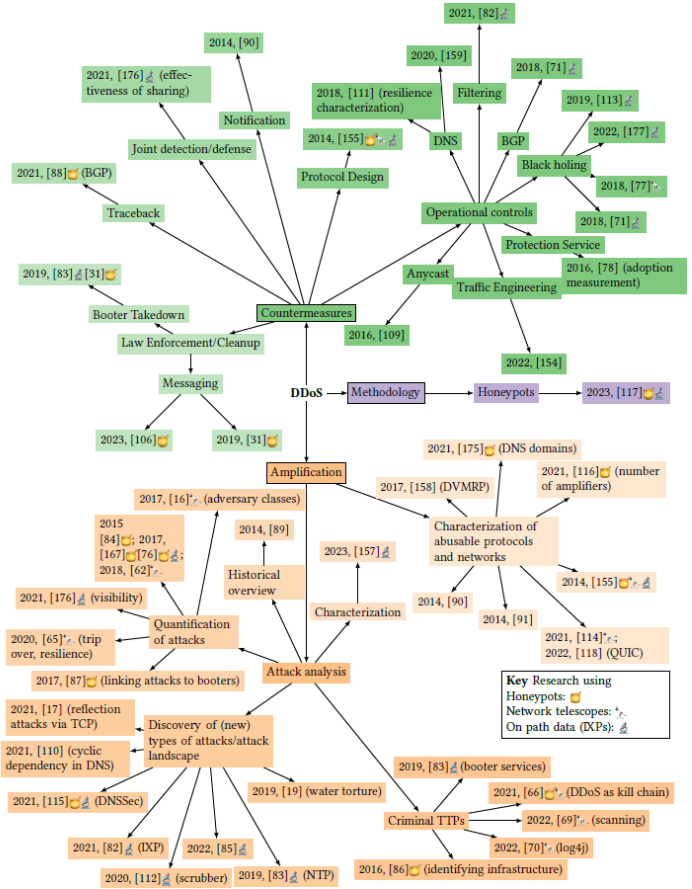
LATEST NEWS

Netflix turns decline upside with help from Stranger Th
14 HOURS AGO

First of its kind 'Graboid' cryptojacking worm found Docker images
14 HOURS AGO

Why bringing a sense of hu to work can do wonders fo

## Research



# Perspectives on DDoS

## Reality

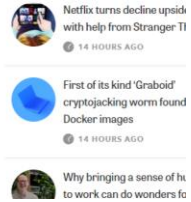
The New York Times

***Hackers Used New Weapons to Disrupt Major Websites Across U.S.***

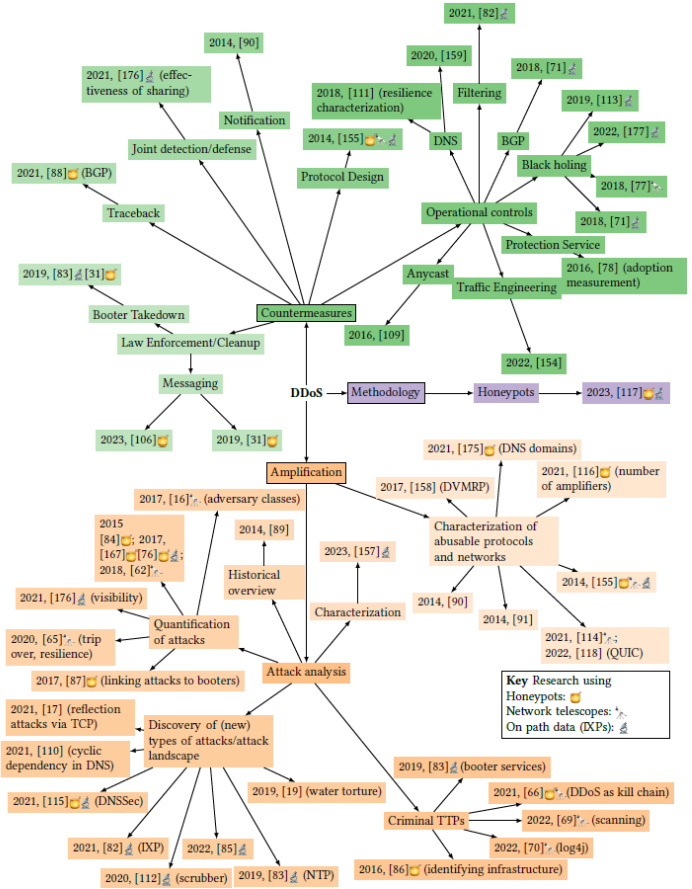

**The truth is, most IoT devices can be turned into botnets**

*by Colm Gorey*

9 MAR 2018 1.57K VIEWS




## Research




## Politics

BRIEFING

EU Legislation in Progress

European Parliament

### The NIS2 Directive

#### A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including

NIS2, by the level

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

Proposed Rule

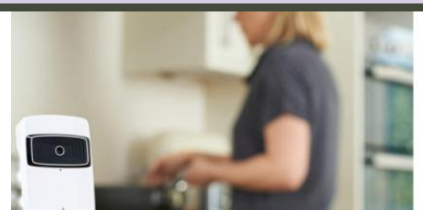
**Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements**

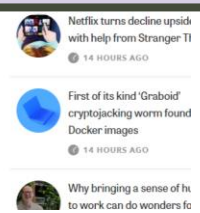
A Proposed Rule by the Homeland Security Department on 04/04/2024

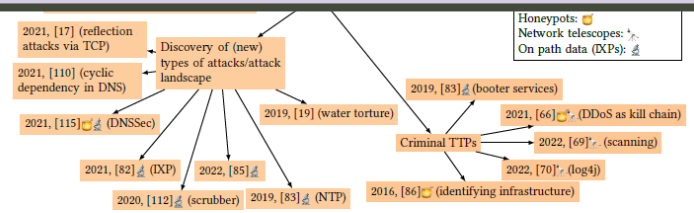
# Perspectives on DDoS

**Reality** | **Research** | **Politics**

The New York Times







The impact of actions is limited by the current understanding.

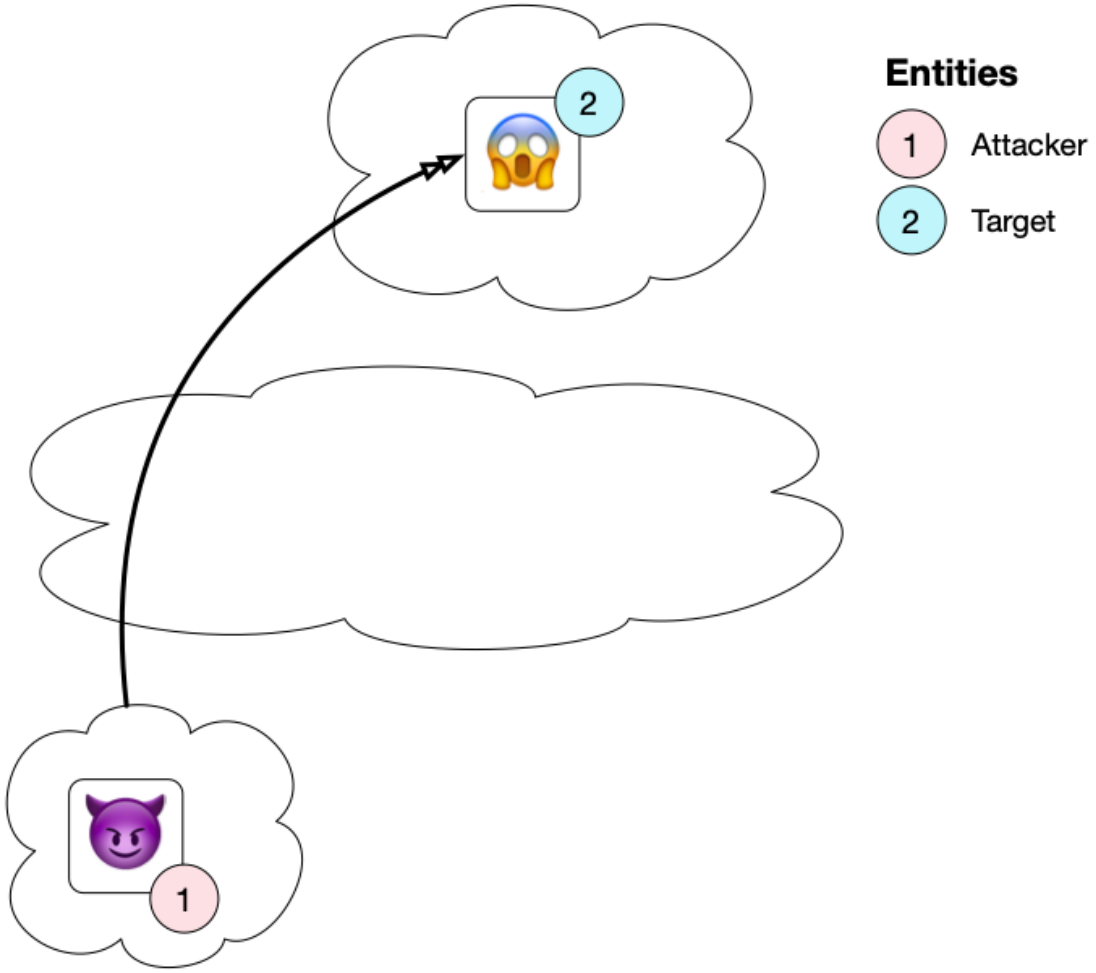
# Do observatories agree on trends in DDoS?

Analysis of 10 longitudinal DDoS datasets.

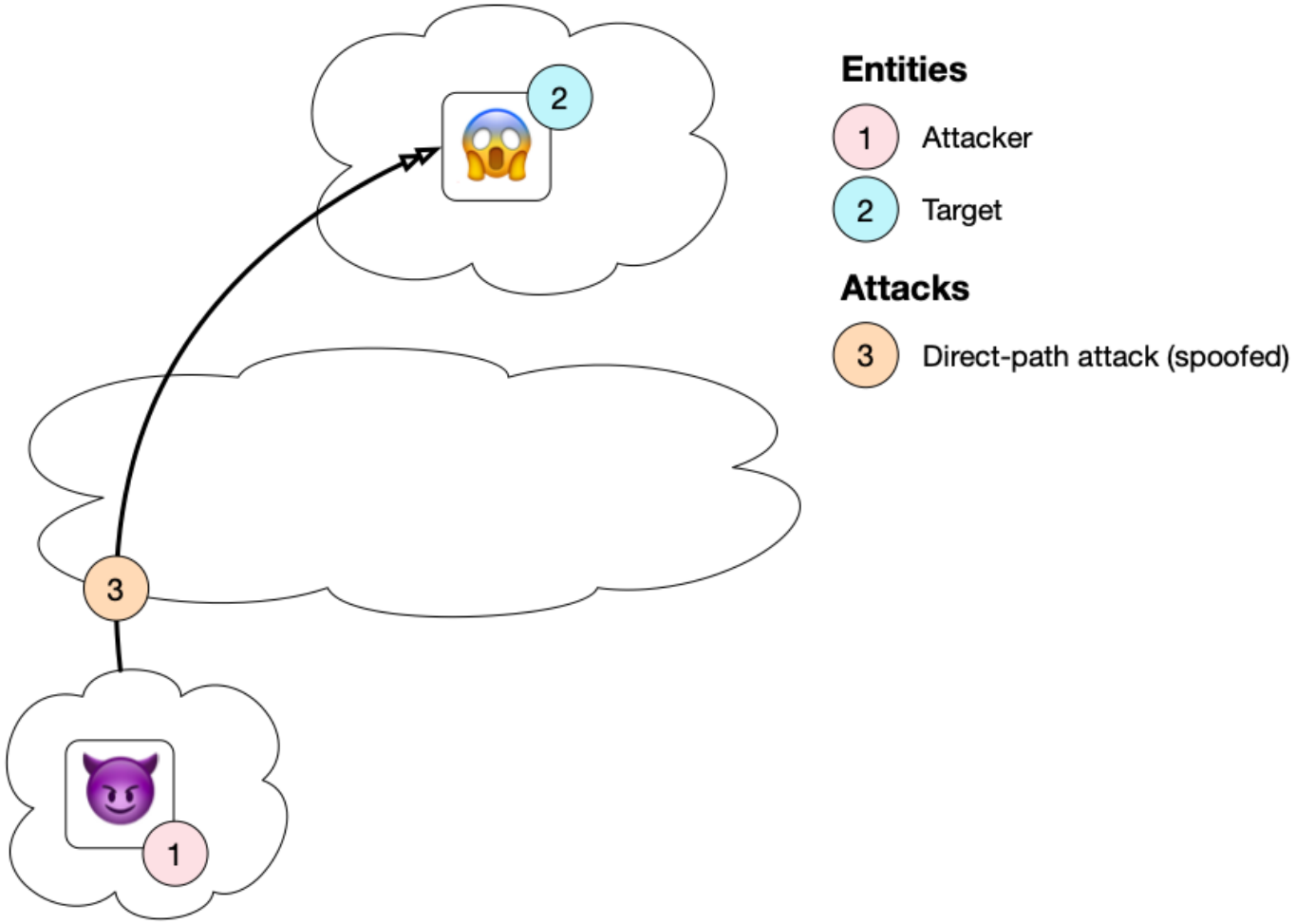
Spanning all major DDoS measurement methods.

Correlating attack trends across industry and academia.

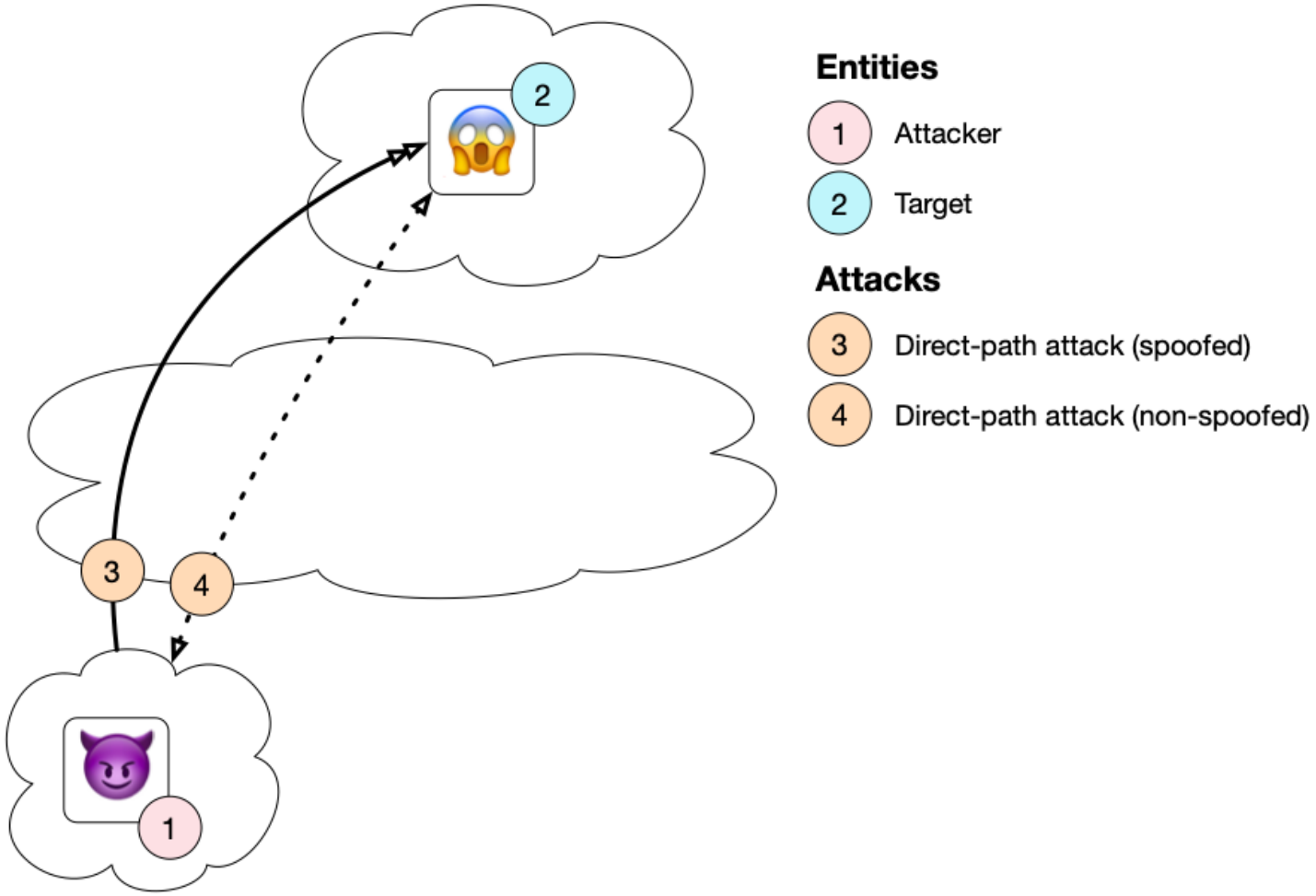
# Common DDoS Attack Types



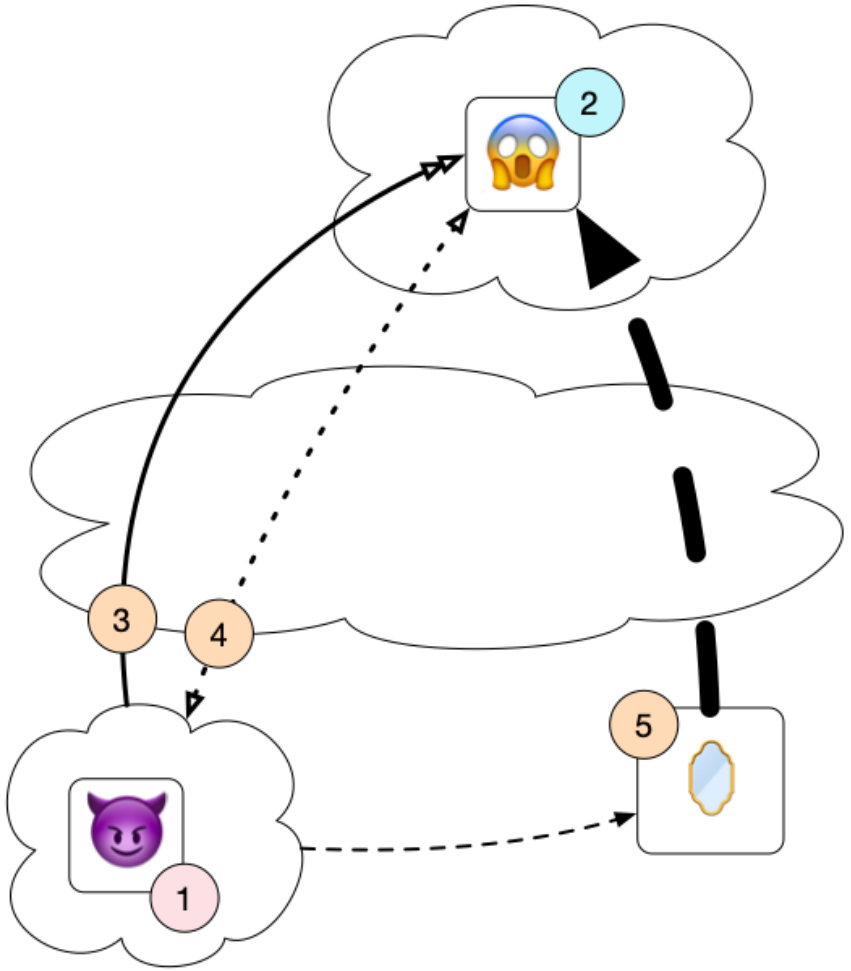
# Common DDoS Attack Types



# Common DDoS Attack Types



# Common DDoS Attack Types




**Entities**

1 Attacker

2 Target

**Attacks**

3 Direct-path attack (spoofed)

4 Direct-path attack (non-spoofed)

5 Reflection-amplification attack (spoofed)

# Prevention and Mitigation of DDoS Attacks

## Reduce attack vectors

- Examples: Disable “get monlist” (NTP) or ”ANY” (DNS) requests.

## Take down booters

- Coordinated takedowns of booter by law enforcement.

## Validate source address

- Spoofer project, industry efforts, ...

## Filter attack traffic

- Industry exists around DDoS protection.

# Prevention and Mitigation of DDoS Attacks

## Reduce attack vectors

- Examples: Disable “get monlist” (NTP) or ”ANY” (DNS) requests.
- **BUT: Attack vectors remain.**

## Take down booters

- Coordinated takedowns of booter by law enforcement.

## Validate source address

- Spoofer project, industry efforts, ...

## Filter attack traffic

- Industry exists around DDoS protection.

# Prevention and Mitigation of DDoS Attacks

## Reduce attack vectors

- Examples: Disable “get monlist” (NTP) or ”ANY” (DNS) requests.
- **BUT: Attack vectors remain.**

## Take down booters

- Coordinated takedowns of booter by law enforcement.

## Validate source address

- Spoofer project, industry efforts, ...
- **BUT: Spoofable networks remain.**

## Filter attack traffic

- Industry exists around DDoS protection.

# Prevention and Mitigation of DDoS Attacks

## Reduce attack vectors

- Examples: Disable “get monlist” (NTP) or ”ANY” (DNS) requests.
- **BUT: Attack vectors remain.**

## Take down booters

- Coordinated takedowns of booter by law enforcement.
- **BUT: Booters reappear after a while.**

## Validate source address

- Spoofer project, industry efforts, ...
- **BUT: Spoofable networks remain.**

## Filter attack traffic

- Industry exists around DDoS protection.

# Prevention and Mitigation of DDoS Attacks

## Reduce attack vectors

- Examples: Disable “get monlist” (NTP) or ”ANY” (DNS) requests.
- **BUT: Attack vectors remain.**

## Take down booters

- Coordinated takedowns of booter by law enforcement.
- **BUT: Booters reappear after a while.**

## Validate source address

- Spoofer project, industry efforts, ...
- **BUT: Spoofable networks remain.**

## Filter attack traffic

- Industry exists around DDoS protection.
- **BUT: Standardized solutions for cooperative filtering struggle with adoption.**

# Prevention and Mitigation of DDoS Attacks

**Reduce attack vectors**

- [illegible]
- [illegible]

**Va**

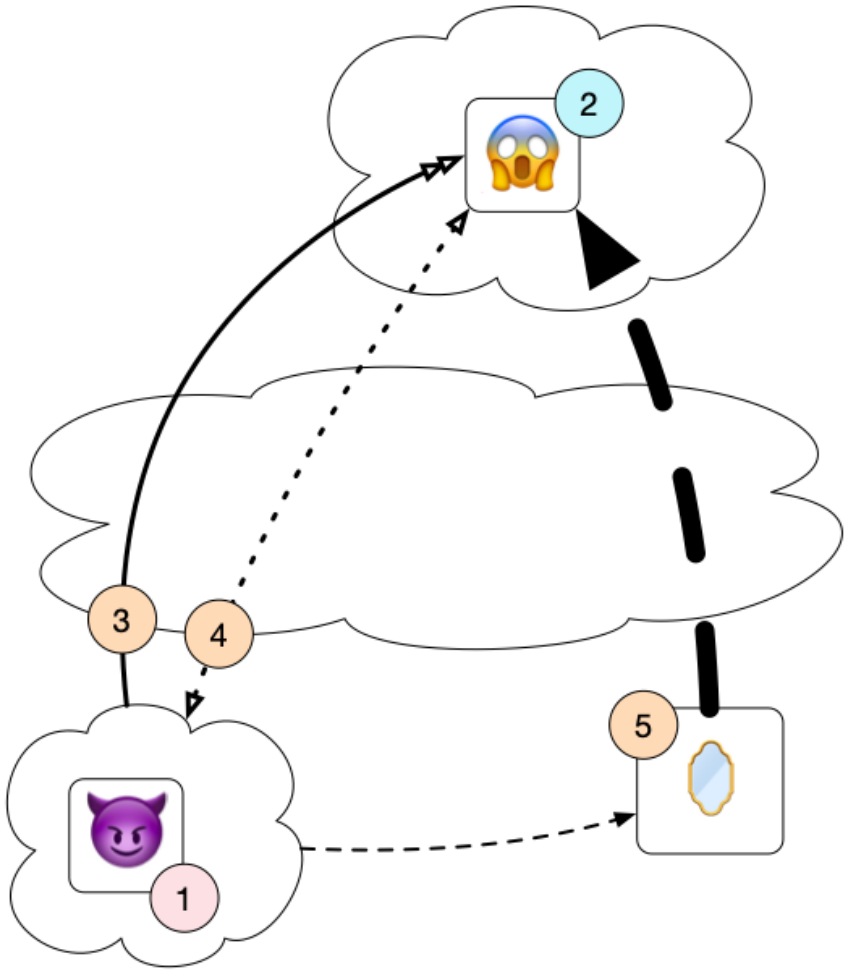
- [illegible]
- **BUT: Spoofable networks remain.**

**Take down booters**

- [illegible]
- **BUT: Standardized solutions for cooperative filtering struggle with adoption.**

DDoS attacks persist.
How well do we understand the threat landscape?

# Our DDoS Observatories




**Entities**

1 Attacker

2 Target

**Attacks**

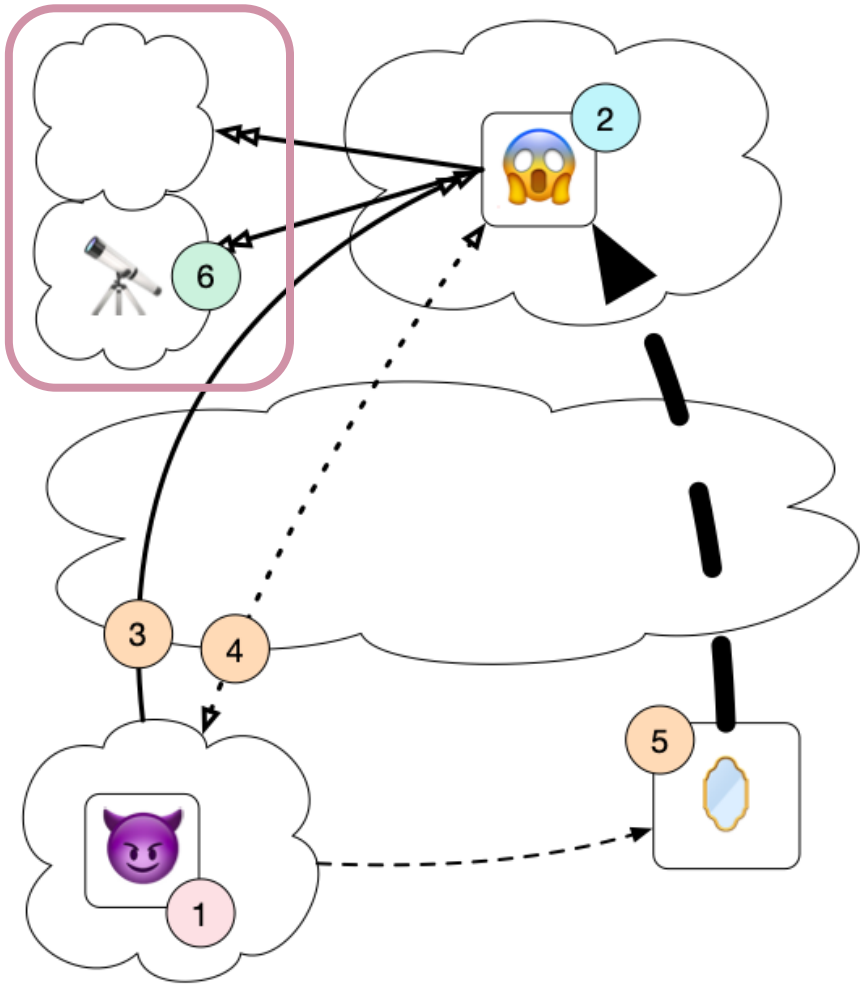
3 Direct-path attack (spoofed)

4 Direct-path attack (non-spoofed)

5 Reflection-amplification attack (spoofed)

# Our DDoS Observatories

## Network Telescopes




**Entities**

1. Attacker
2. Target

**Attacks**

3. Direct-path attack (spoofed)
4. Direct-path attack (non-spoofed)
5. Reflection-amplification attack (spoofed)

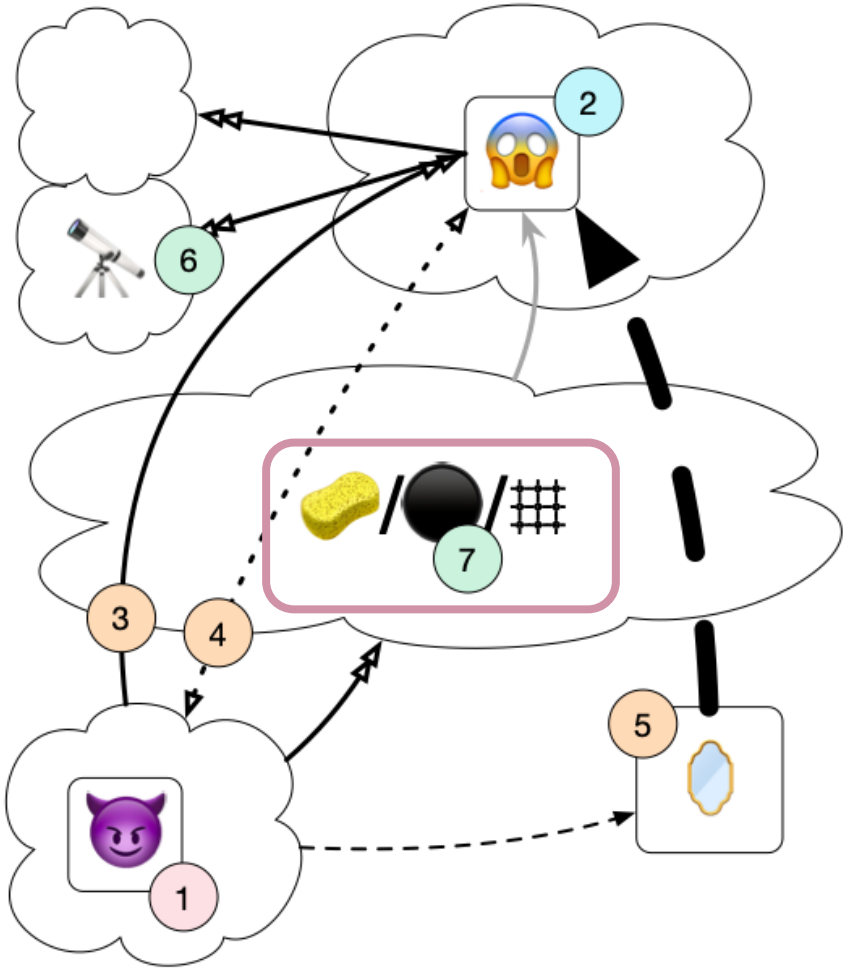
**Observation Points**

6. Network telescope

| Platform | Type | Datasets | Coverage |
|---|---|---|---|
| UCSD NT | NT | DP | 12M IPs |
| ORION NT | NT | DP | 500k IPs |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Our DDoS Observatories

## On-path Networks




**Entities**

1 Attacker

2 Target

**Attacks**

3 Direct-path attack (spoofed)

4 Direct-path attack (non-spoofed)

5 Reflection-amplification attack (spoofed)

**Observation Points**

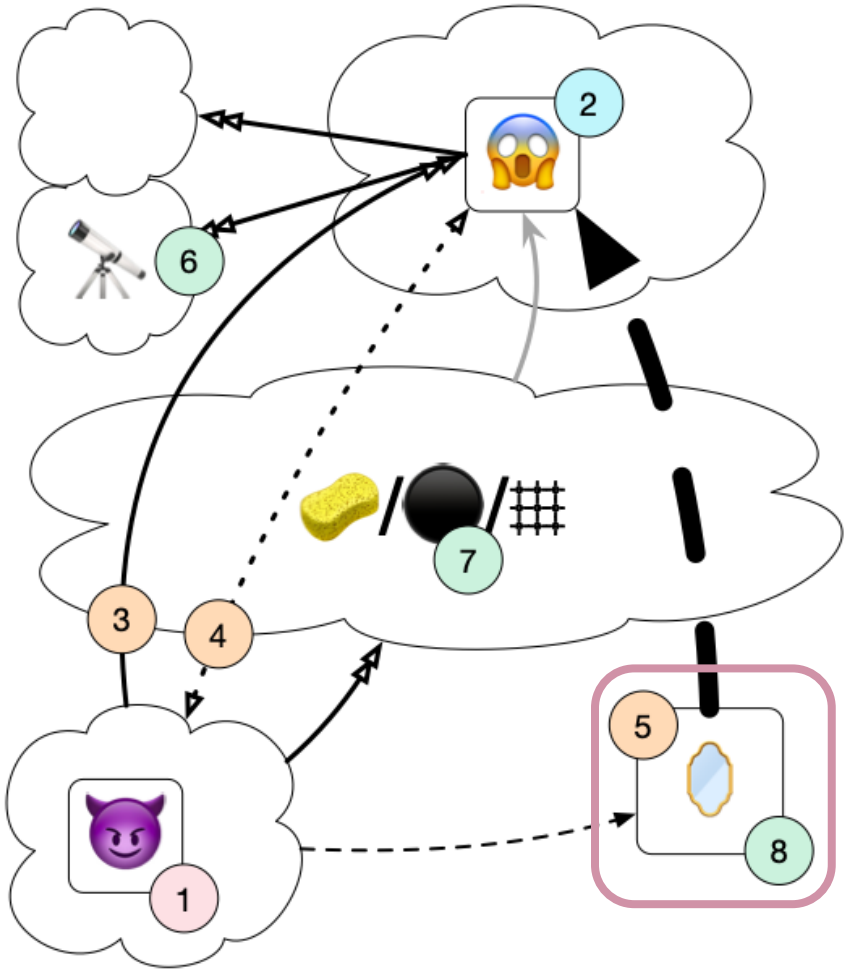
6 Network telescope

7 On-path network (e.g., DDoS mitigation, IXPs)

| Platform | Type | Datasets | Coverage |
|---|---|---|---|
| UCSD NT | NT | DP | 12M IPs |
| ORION NT | NT | DP | 500k IPs |
| Netscout | Flow | DP, RA | Confidential |
| Akamai Prolexic | Flow | DP, RA | Confidential |
| IXP Blackholing | Flow | DP, RA | Confidential |
| | | | |
| | | | |

# Our DDoS Observatories

## Honeypots




**Entities**

1. Attacker
2. Target

**Attacks**

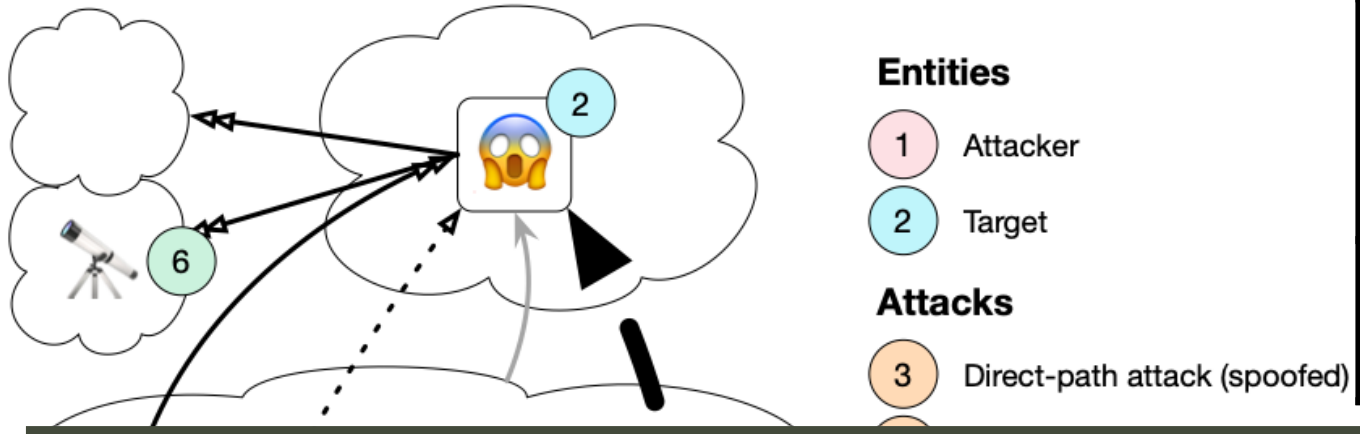
3. Direct-path attack (spoofed)
4. Direct-path attack (non-spoofed)
5. Reflection-amplification attack (spoofed)

**Observation Points**

6. Network telescope
7. On-path network (e.g., DDoS mitigation, IXPs)
8. Honeypot

| Platform | Type | Datasets | Coverage |
|---|---|---|---|
| UCSD NT | NT | DP | 12M IPs |
| ORION NT | NT | DP | 500k IPs |
| Netscout | Flow | DP, RA | Confidential |
| Akamai Prolexic | Flow | DP, RA | Confidential |
| IXP Blackholing | Flow | DP, RA | Confidential |
| AmpPot | HP | RA | ~30 IPs |
| Hopscotch | HP | RA | 65 IPs |

# Our DDoS Observatories



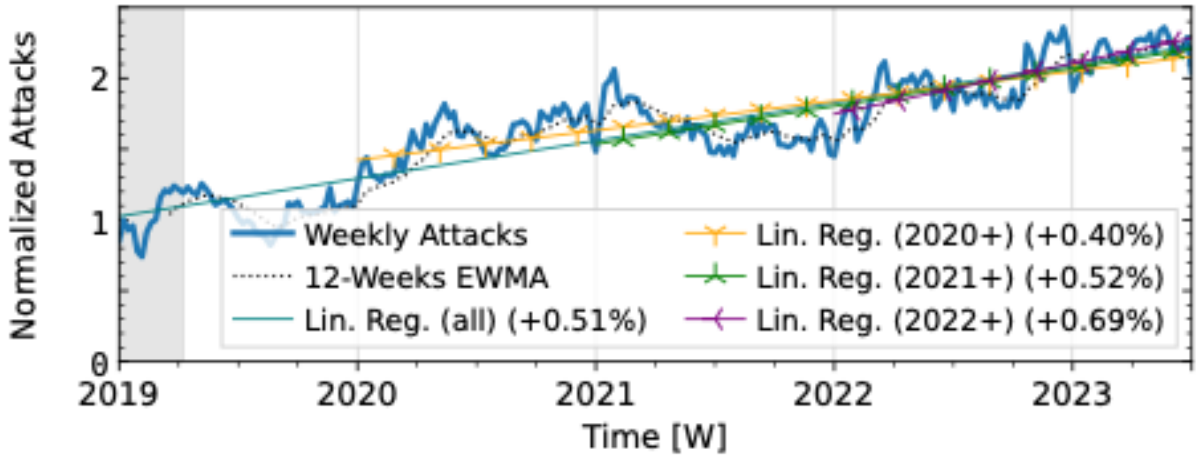

| Platform | Type | Datasets | Coverage |
|---|---|---|---|
| UCSD NT | NT | DP | 12M IPs |
| ORION NT | NT | DP | 500k IPs |
| Netscout | Flow | DP, RA | Confidential |
| Akamai Prolexic | Flow | DP, RA | Confidential |
| IXP Blackholing | Flow | DP, RA | Confidential |
| AmpPot | HP | RA | ~30 IPs |
| Hopscotch | HP | RA | 65 IPs |

10 Datasets from 7 observatories.
4.5-years measurement: ‘19 - mid ‘23.

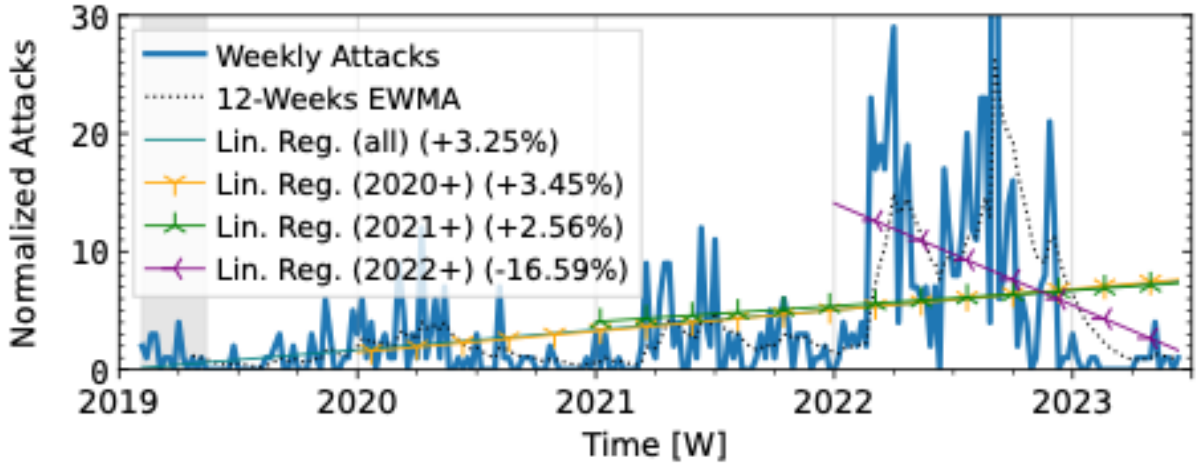
# Direct-path Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



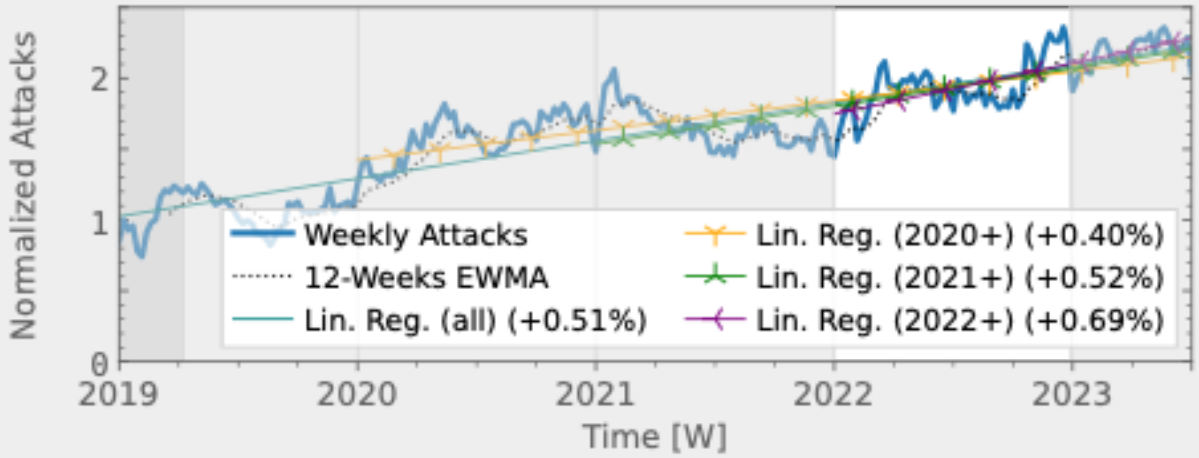

**Flow data: IXP**



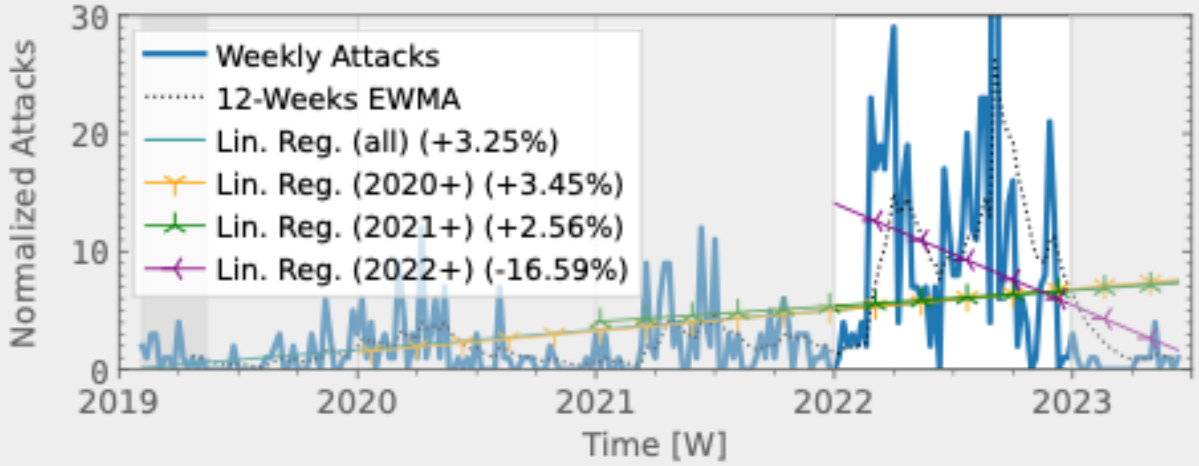
# Direct-path Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



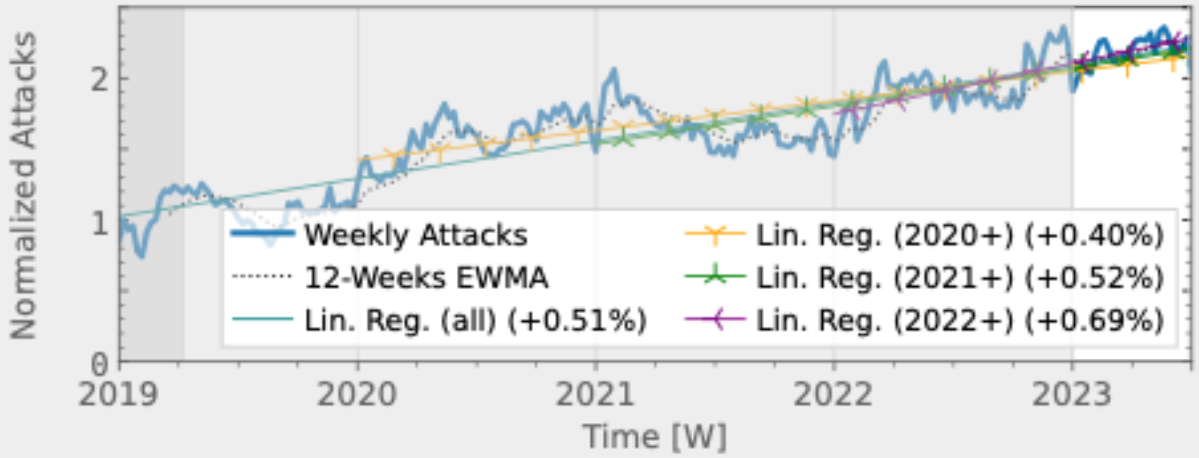

**Flow data: IXP**



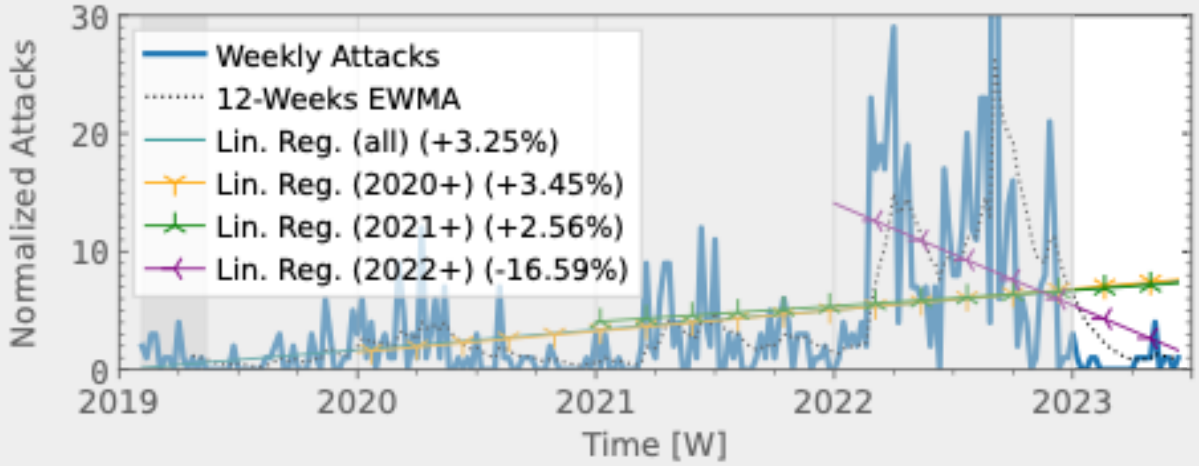
# Direct-path Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



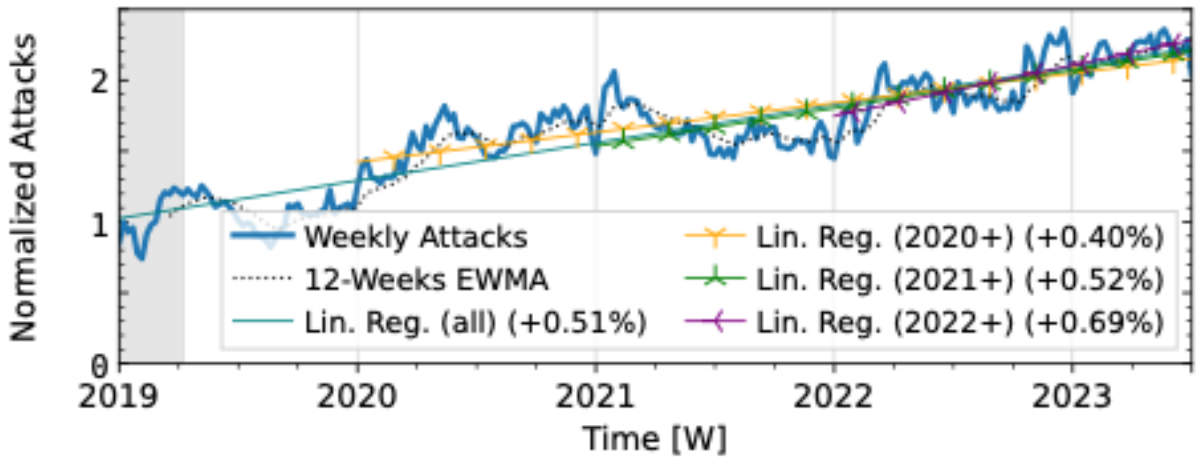

**Flow data: IXP**



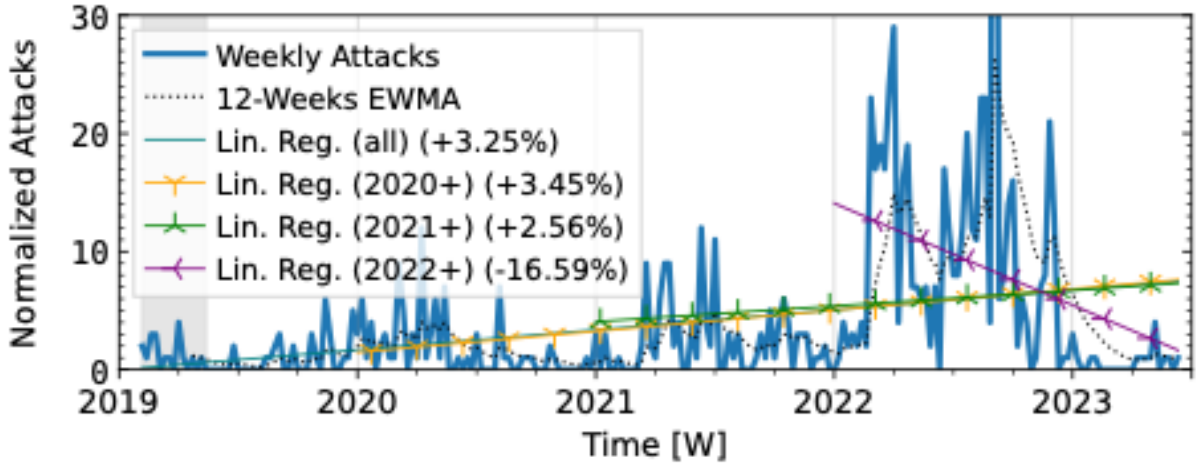
# Direct-path Attacks

## Long-term DDoS Trends

**Flow data: Netscout**




**Flow data: IXP**

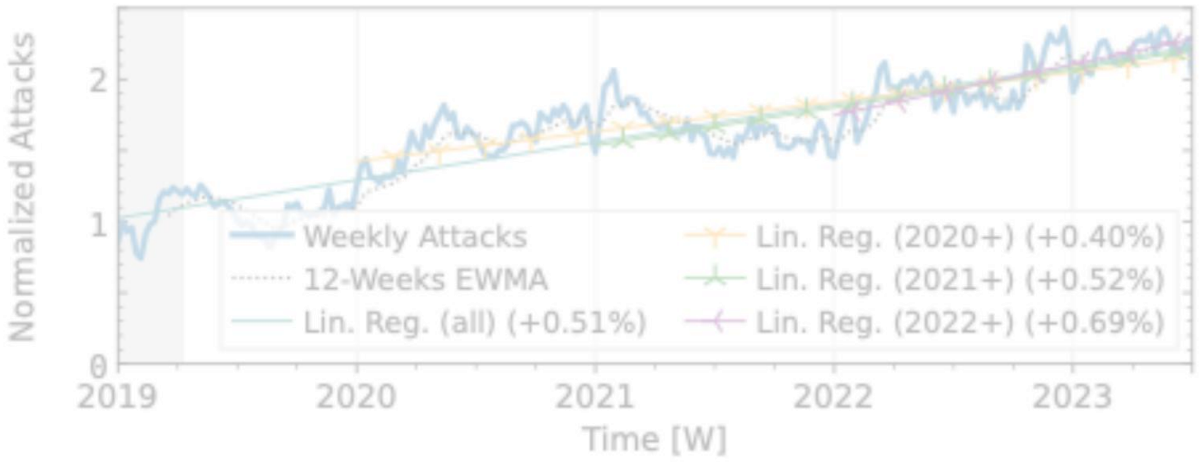



Both rise – but at different scale and trend stability.

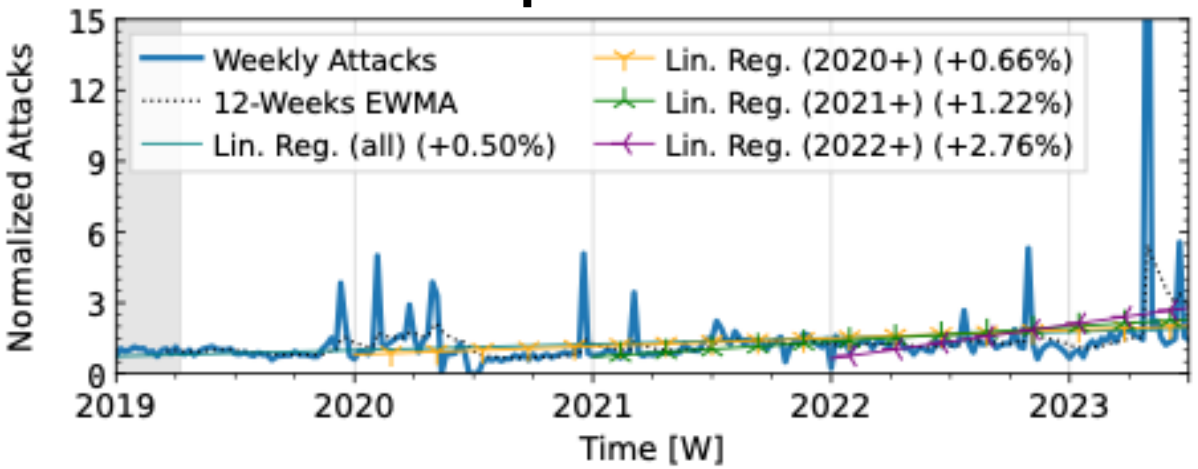
# Direct-path Attacks

## Long-term DDoS Trends

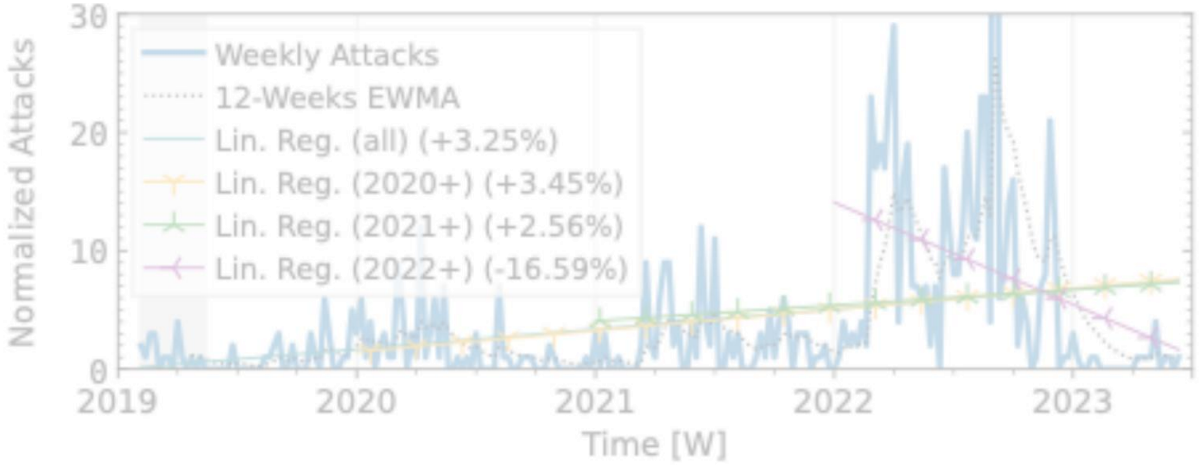
**Flow data: Netscout**



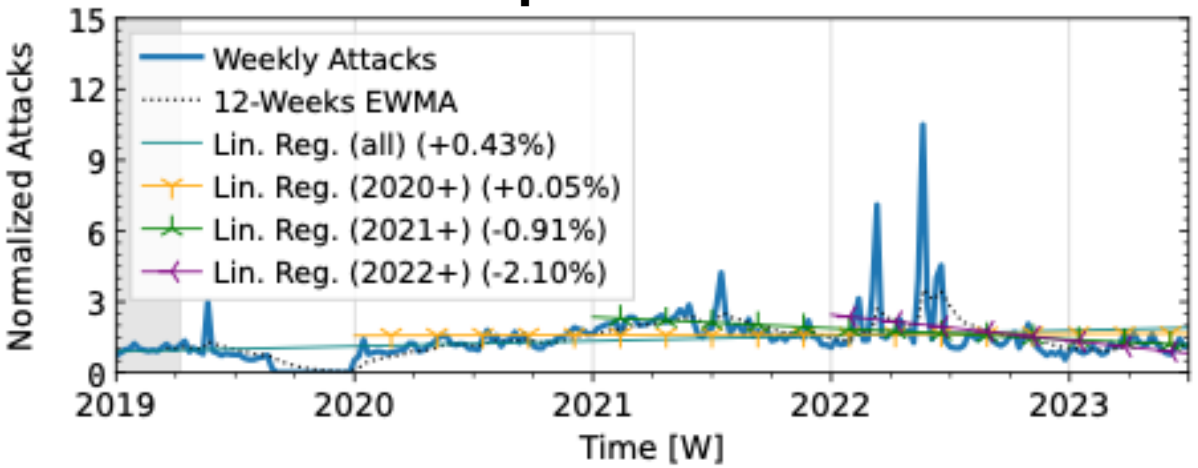

**Network telescope: UCSD**




**Flow data: IXP**




**Network telescope: ORION**



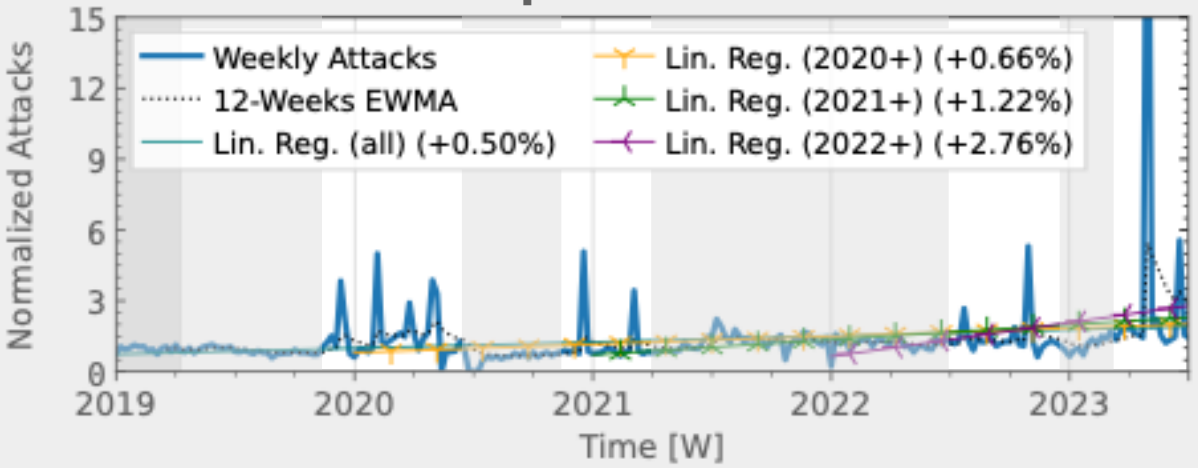
# Direct-path Attacks

## Long-term DDoS Trends

### Flow data: Netscout



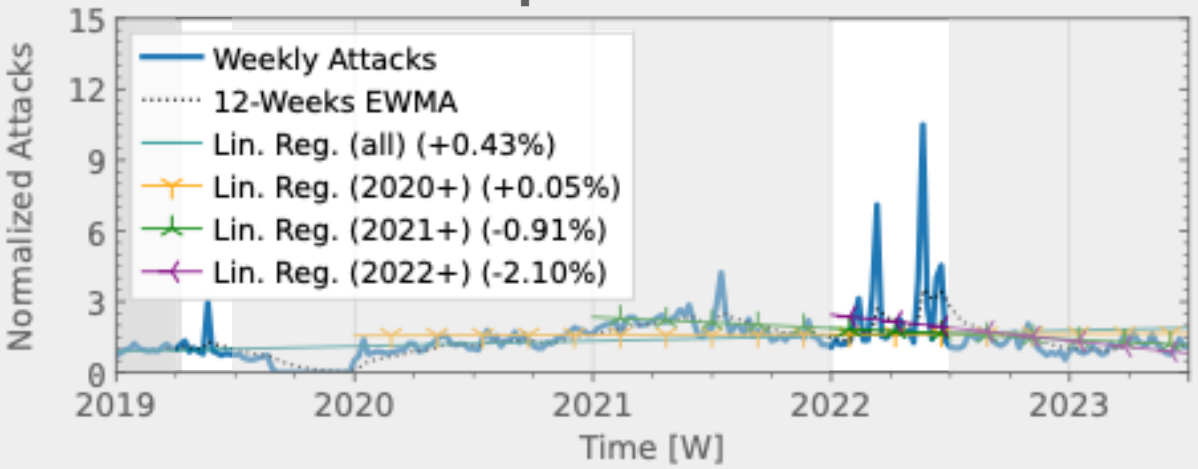

### Network telescope: UCSD




### Flow data: IXP




### Network telescope: ORION



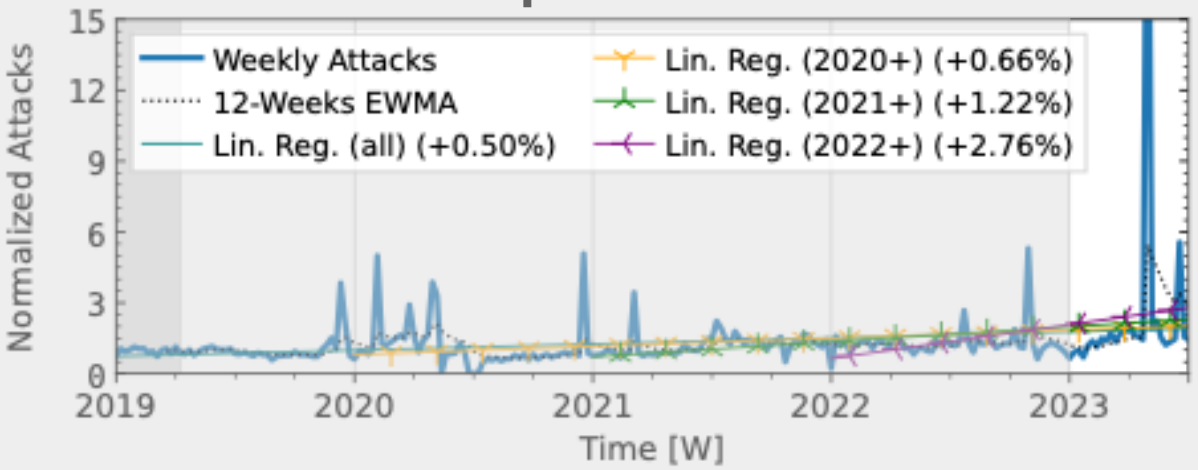
# Direct-path Attacks

## Long-term DDoS Trends

### Flow data: Netscout



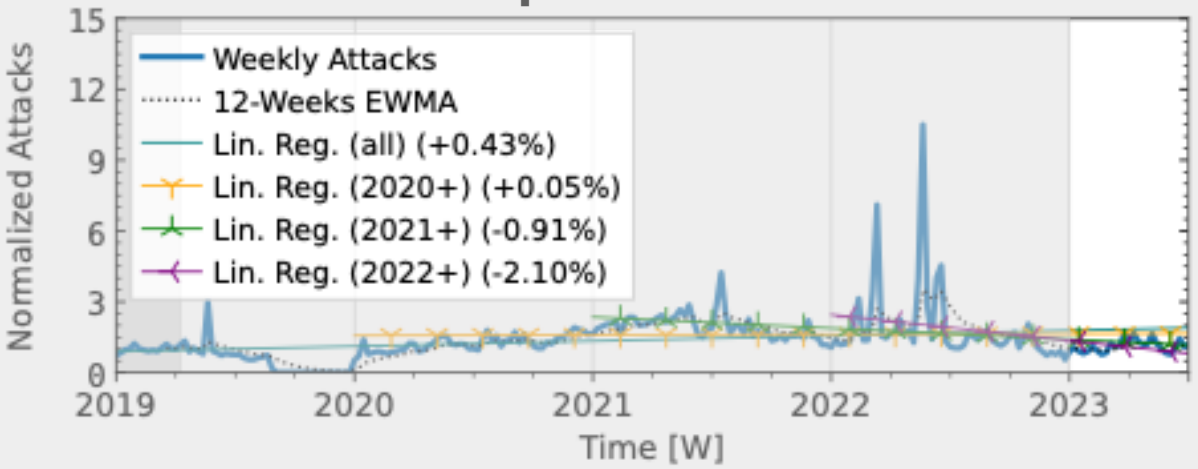

### Network telescope: UCSD




### Flow data: IXP



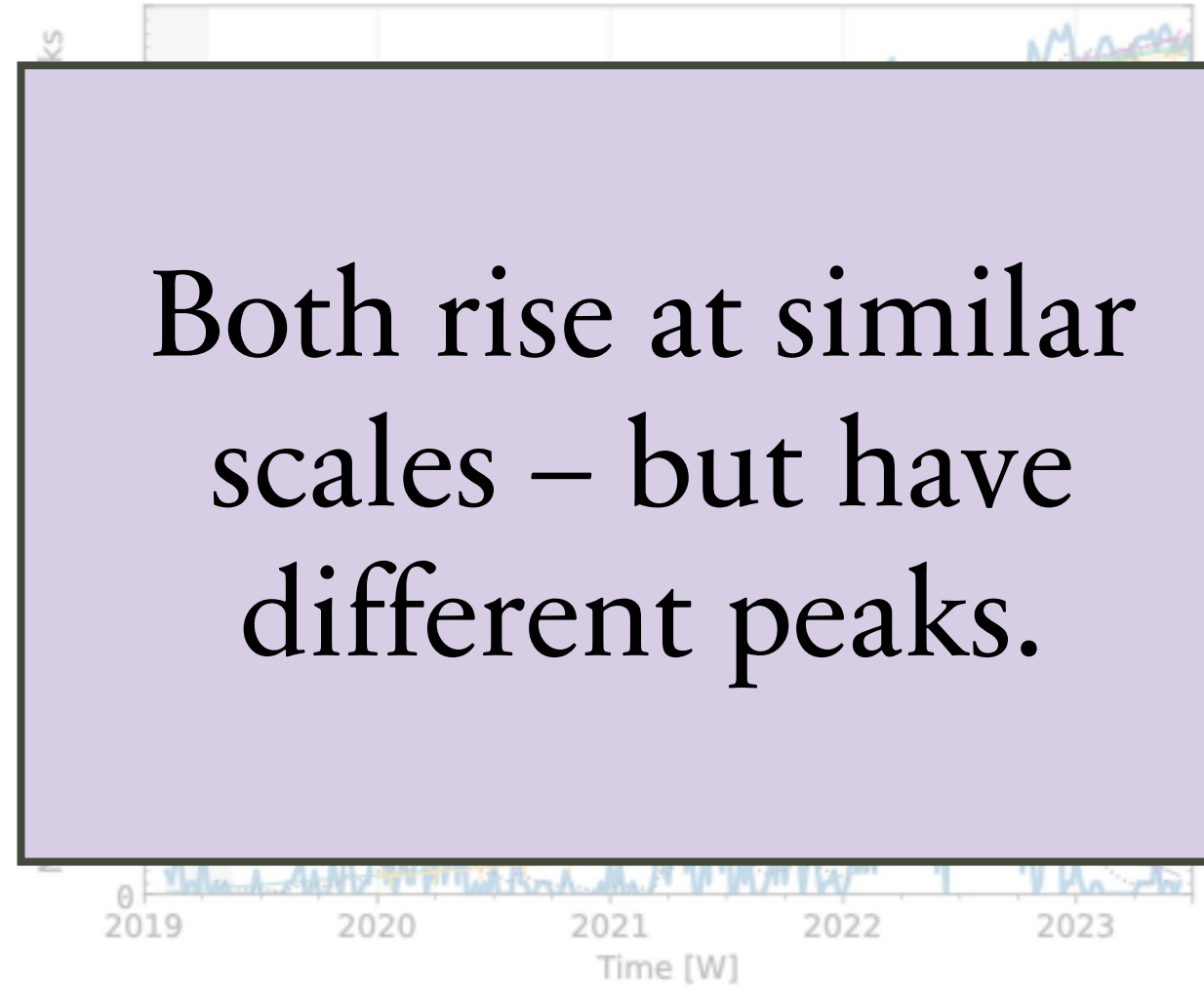

### Network telescope: ORION



# Direct-path Attacks

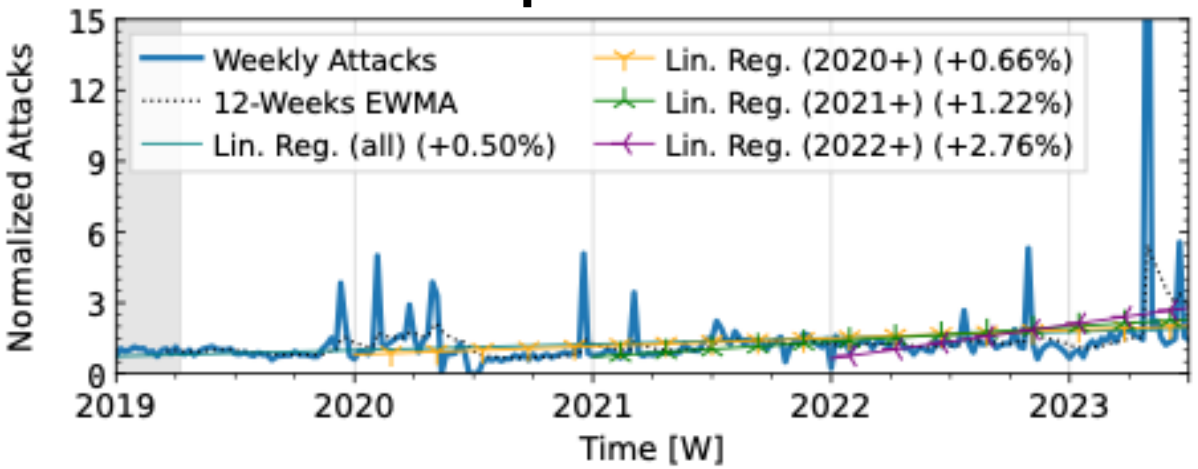
## Long-term DDoS Trends

Flow data: Netscout

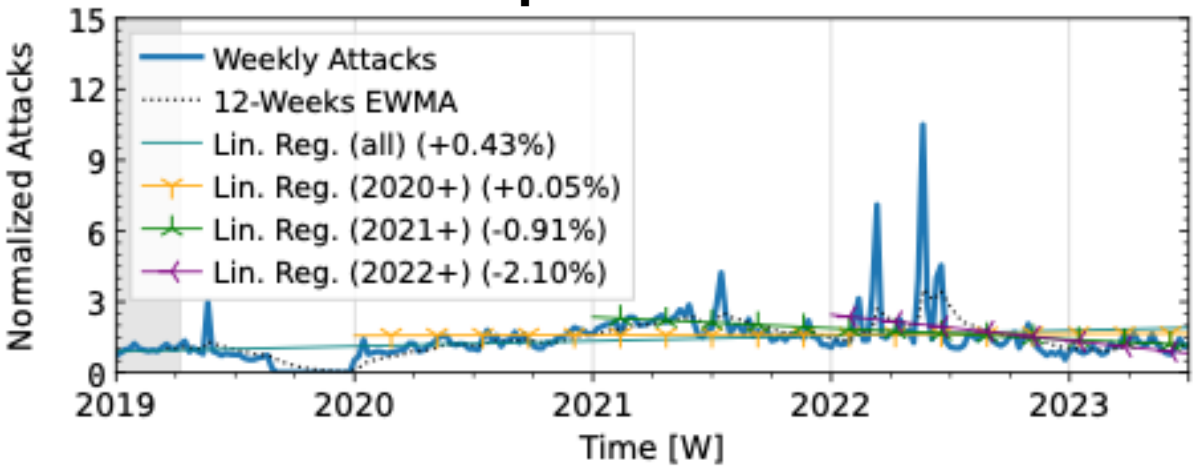



Both rise at similar scales – but have different peaks.

**Network telescope: UCSD**



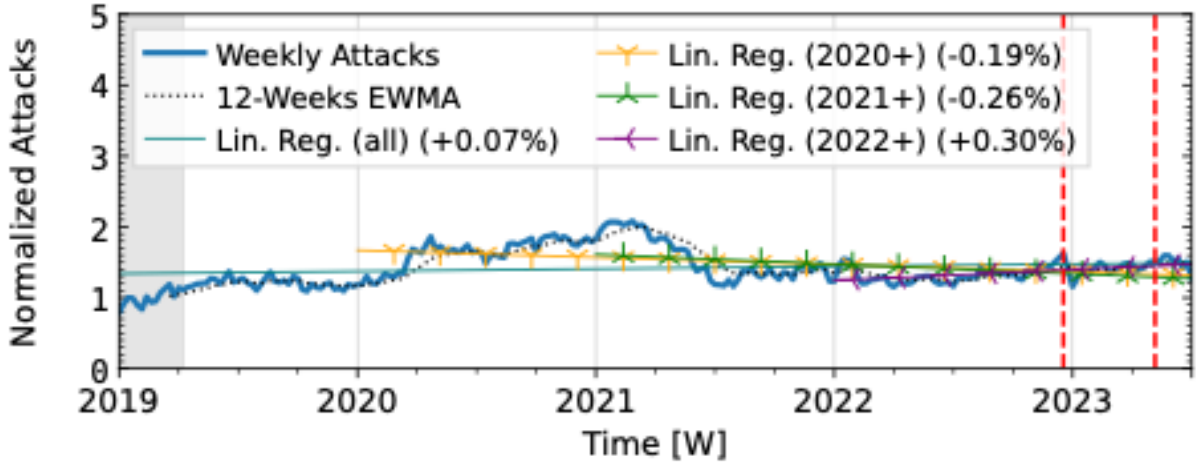

**Network telescope: ORION**



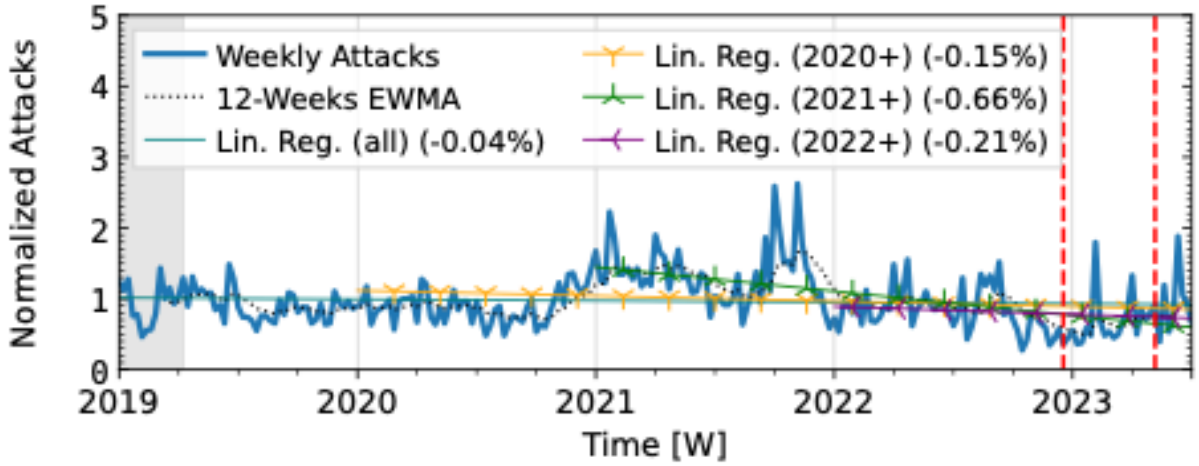
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



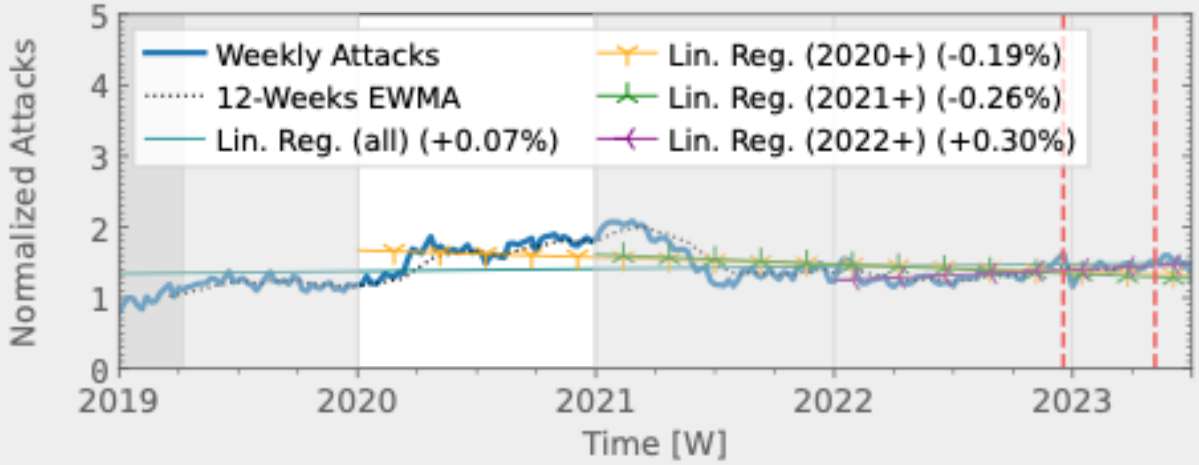

**Flow data: Akamai Prolexic**



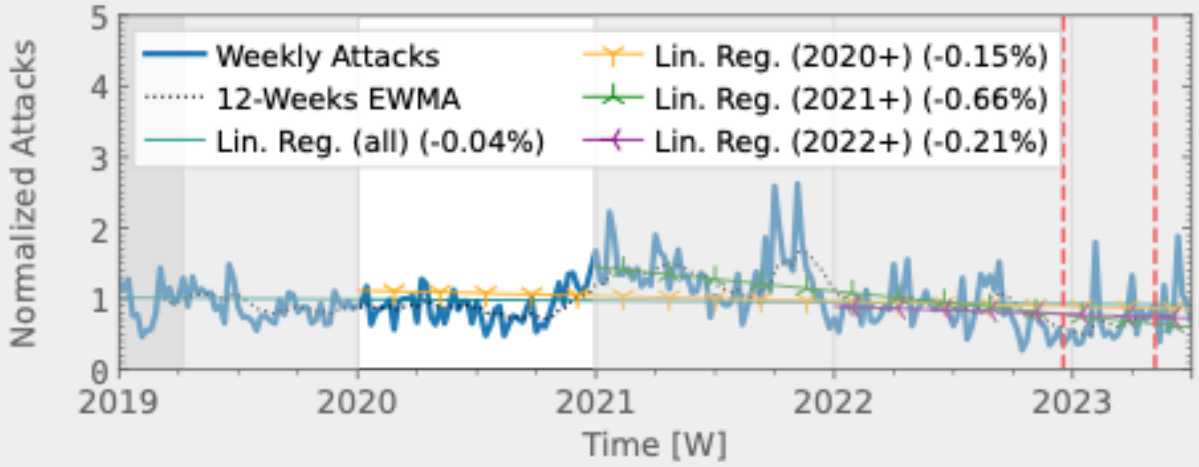
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



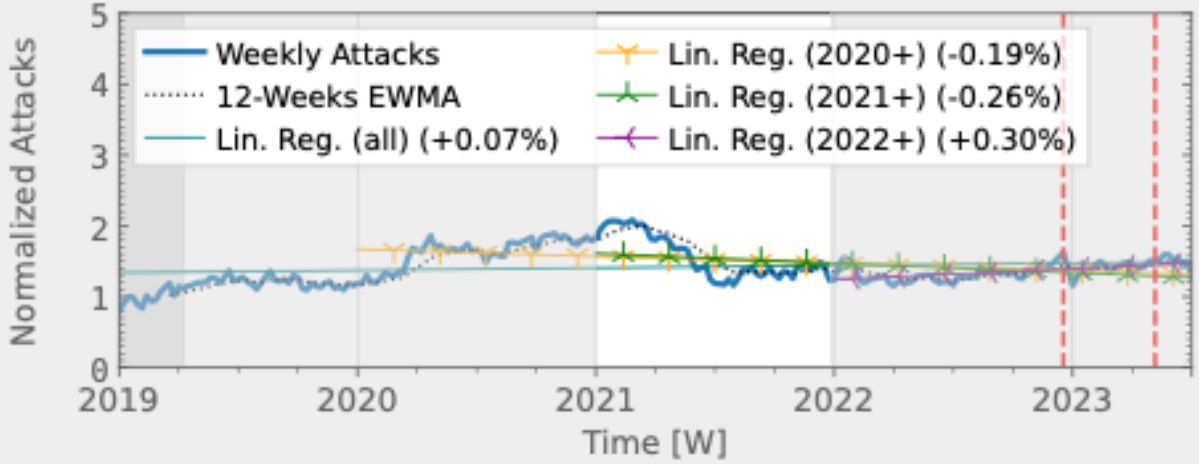

**Flow data: Akamai Prolexic**



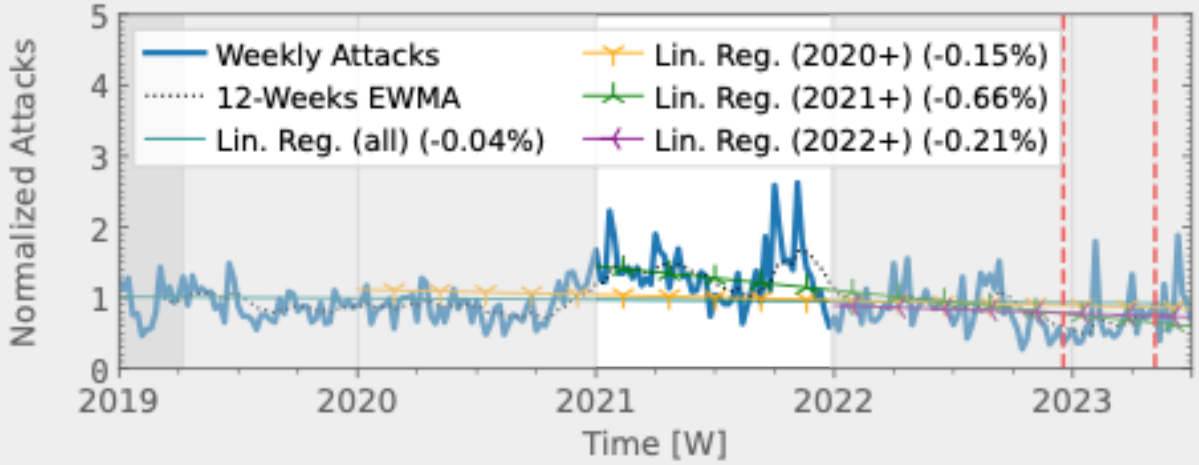
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Flow data: Netscout**



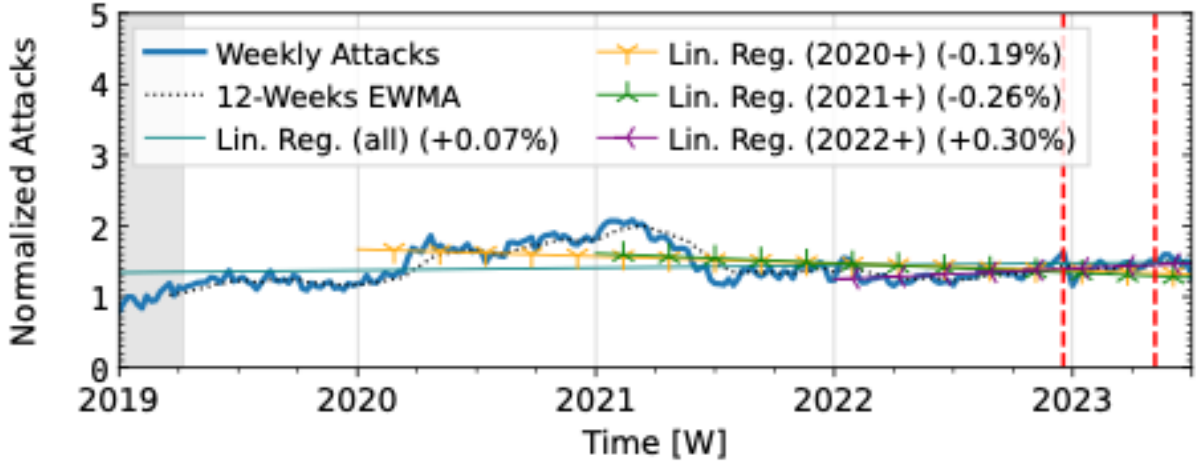

**Flow data: Akamai Prolexic**



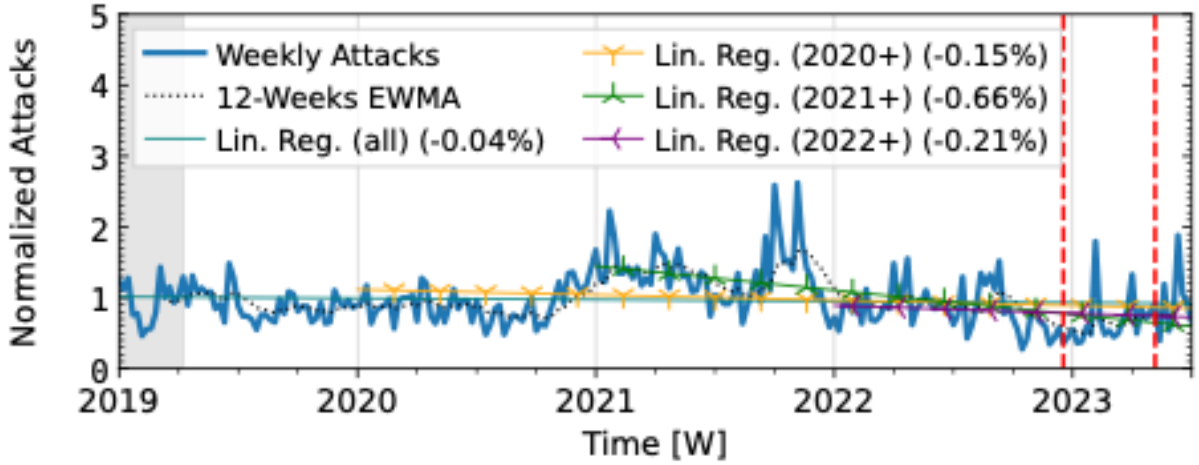
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Flow data: Netscout**




**Flow data: Akamai Prolexic**

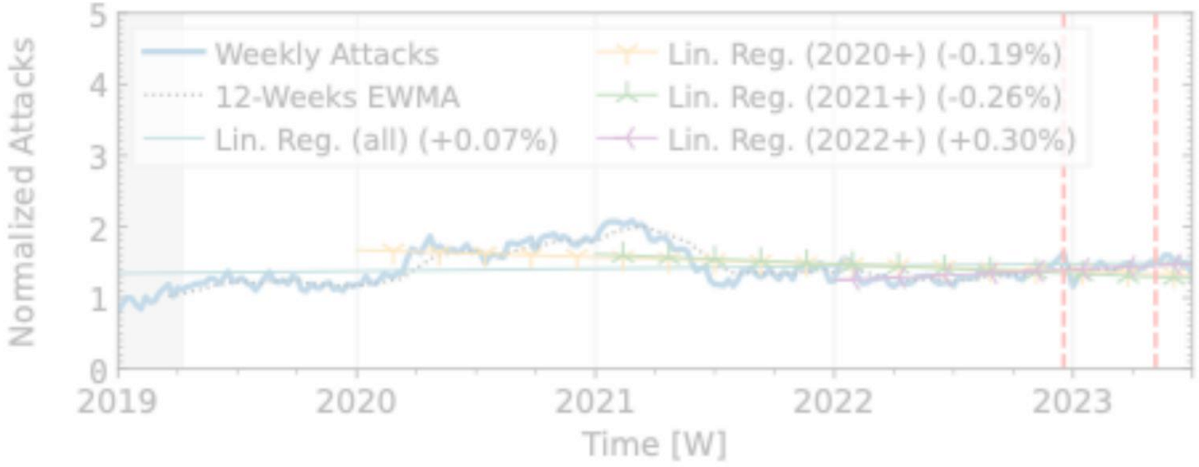



Both have similar trends and scale – but short-term behavior differs.

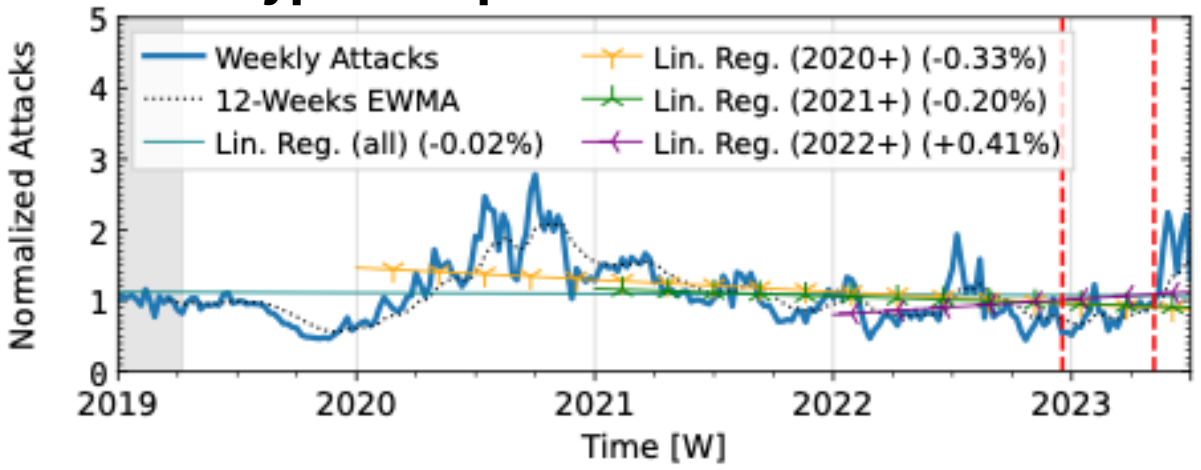
# Reflection-amplification Attacks

## Long-term DDoS Trends

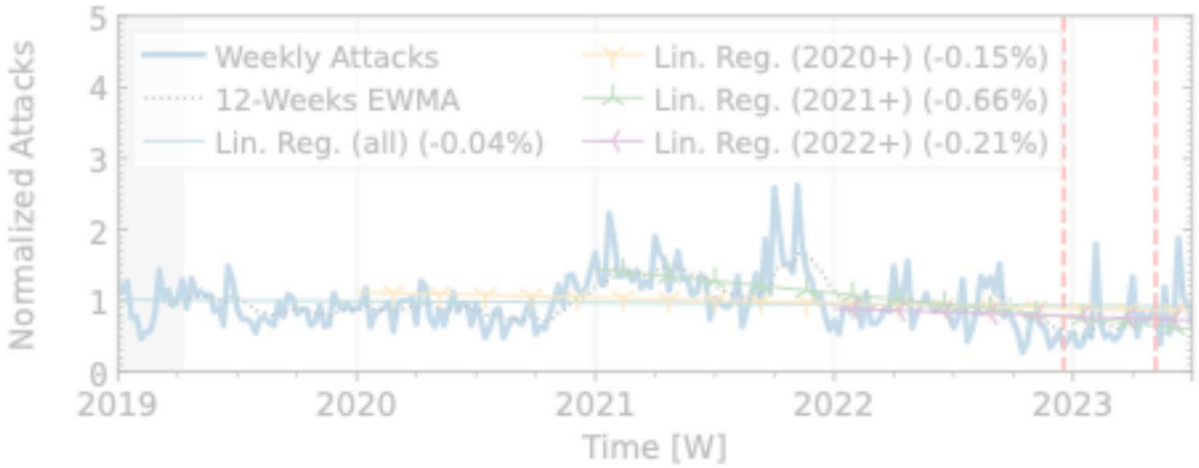
**Flow data: Netscout**



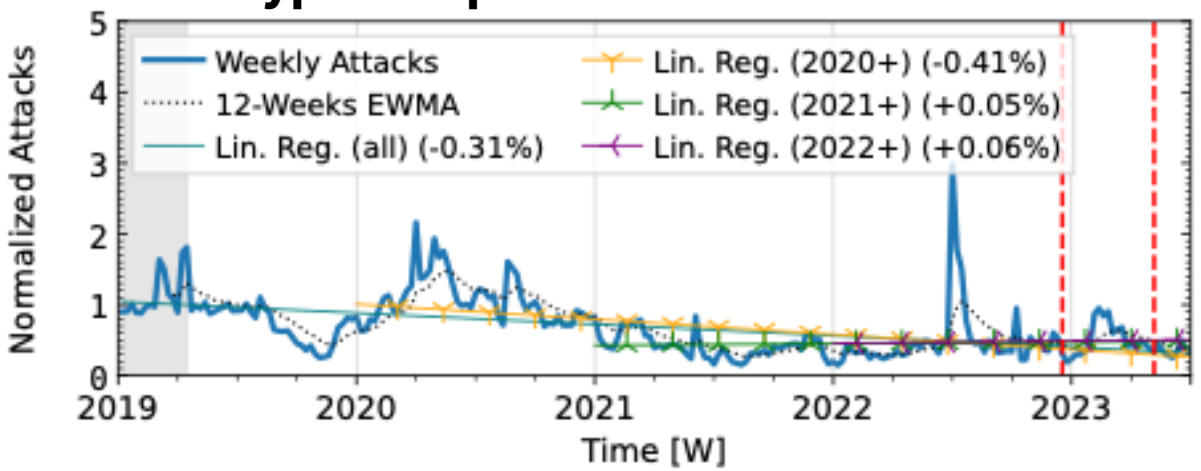

**Honeypot: AmpPot**




**Flow data: Akamai Prolexic**




**Honeypot: Hopscotch**



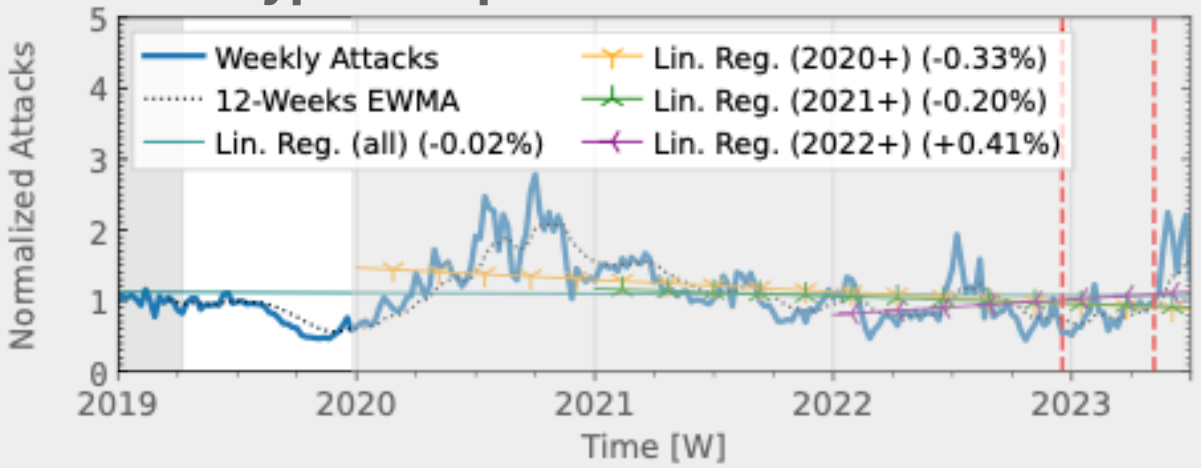
# Reflection-amplification Attacks

## Long-term DDoS Trends

### Flow data: Netscout



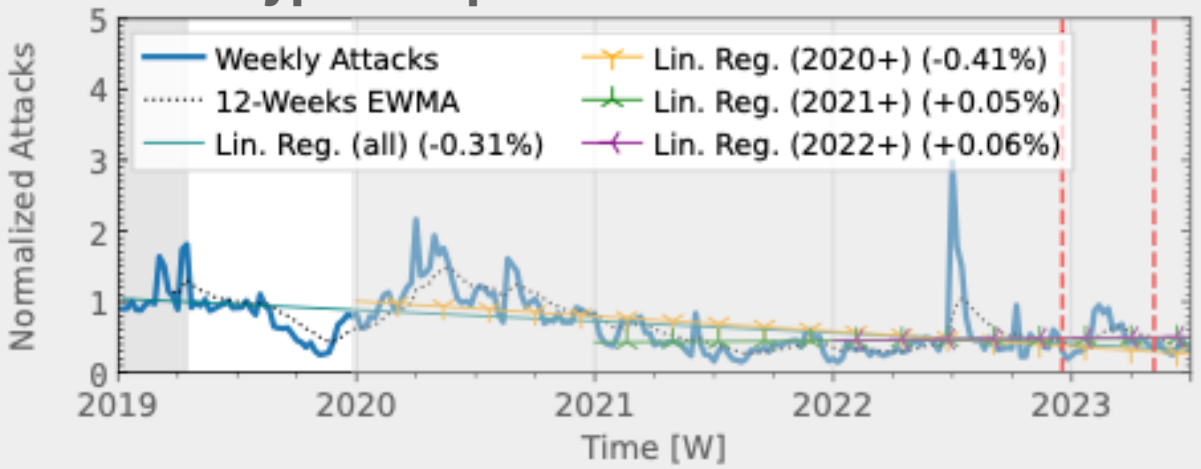

### Honeypot: AmpPot




### Flow data: Akamai Prolexic




### Honeypot: Hopscotch



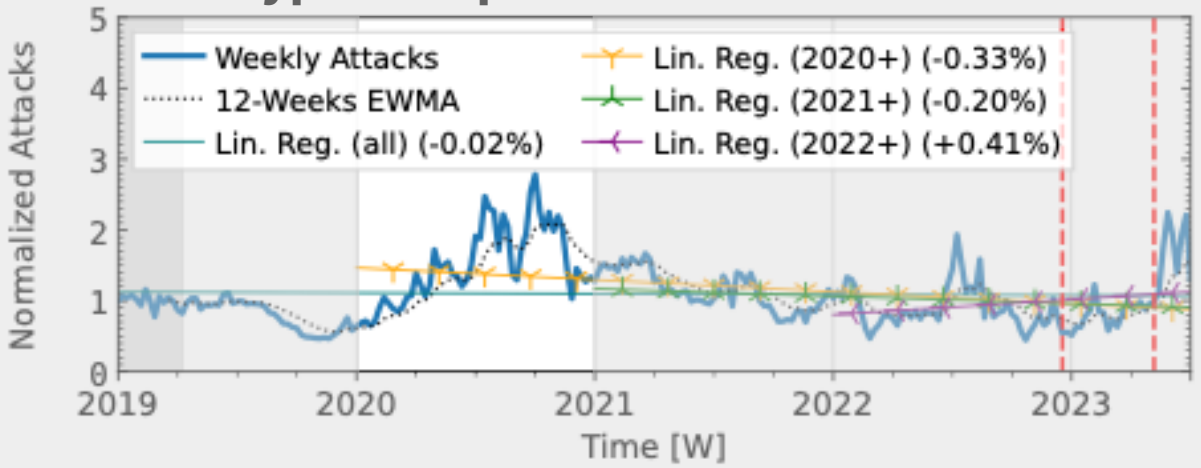
# Reflection-amplification Attacks

## Long-term DDoS Trends

### Flow data: Netscout



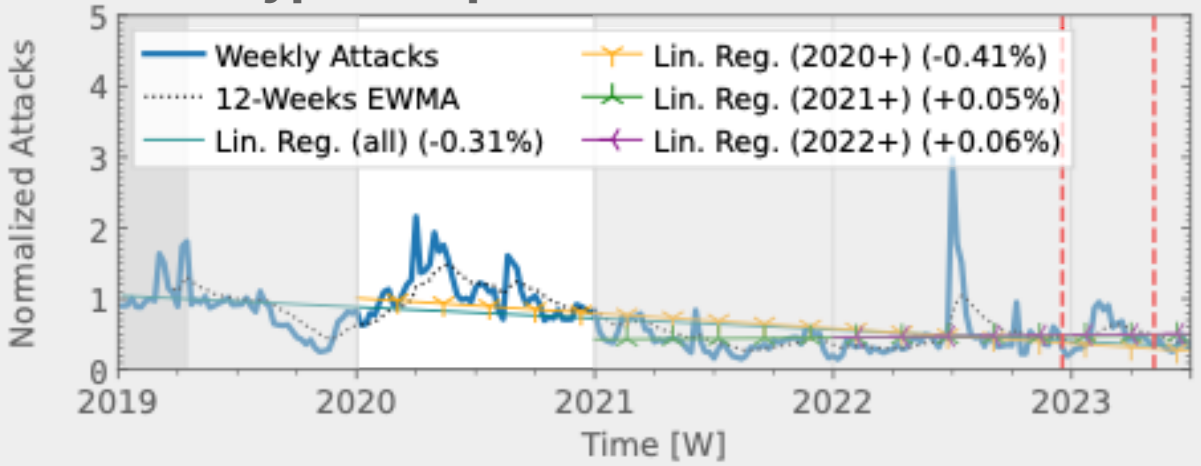

### Honeypot: AmpPot




### Flow data: Akamai Prolexic




### Honeypot: Hopscotch



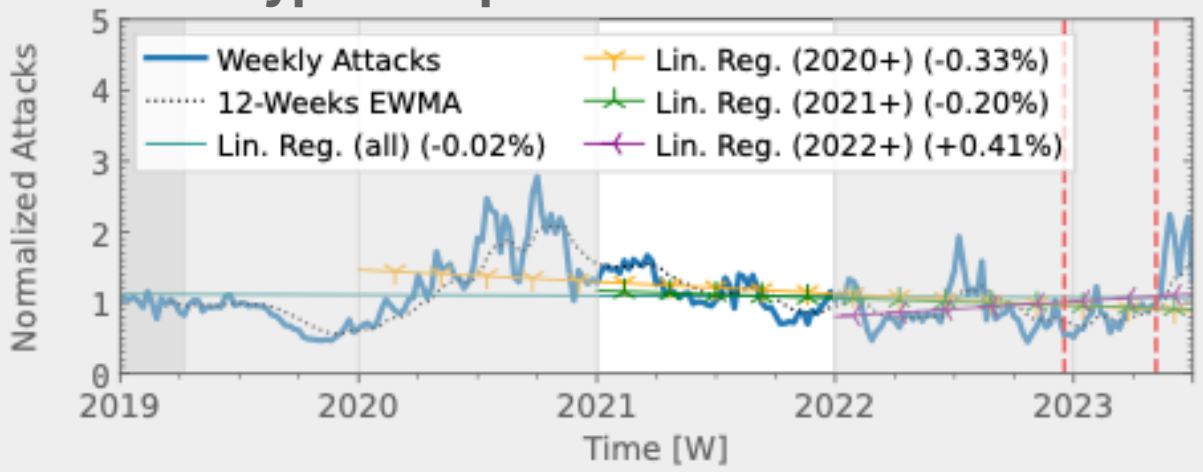
# Reflection-amplification Attacks

## Long-term DDoS Trends

### Flow data: Netscout



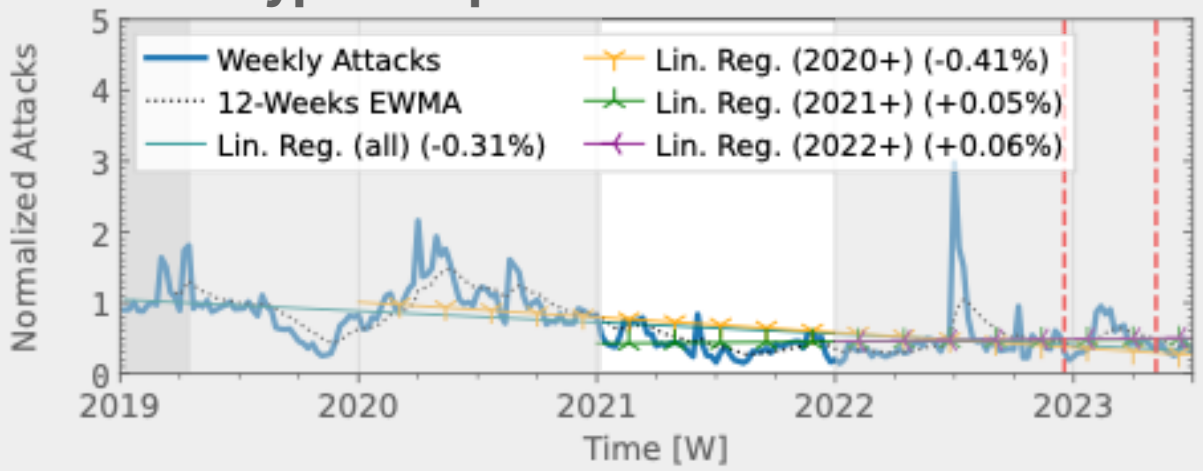

### Honeypot: AmpPot




### Flow data: Akamai Prolexic




### Honeypot: Hopscotch



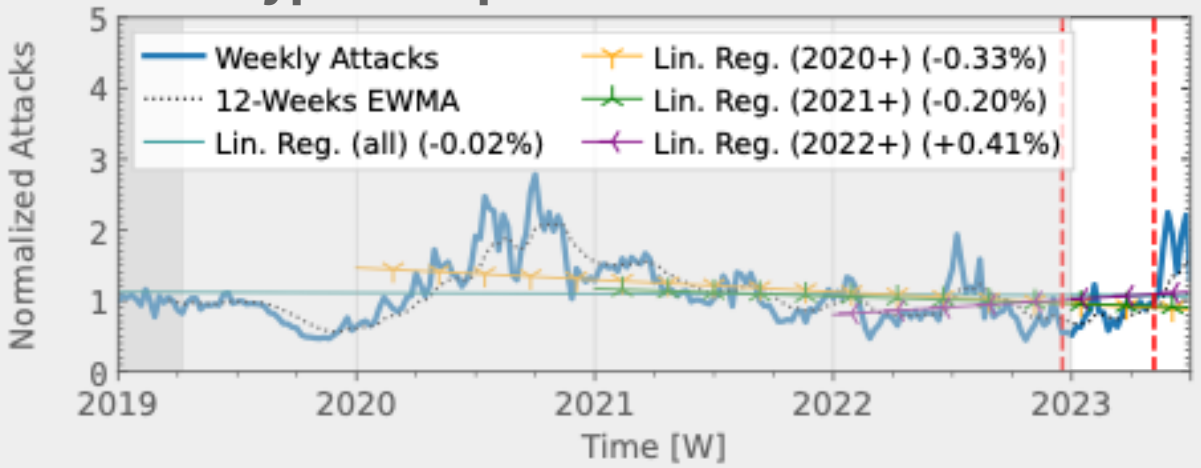
# Reflection-amplification Attacks

## Long-term DDoS Trends

### Flow data: Netscout



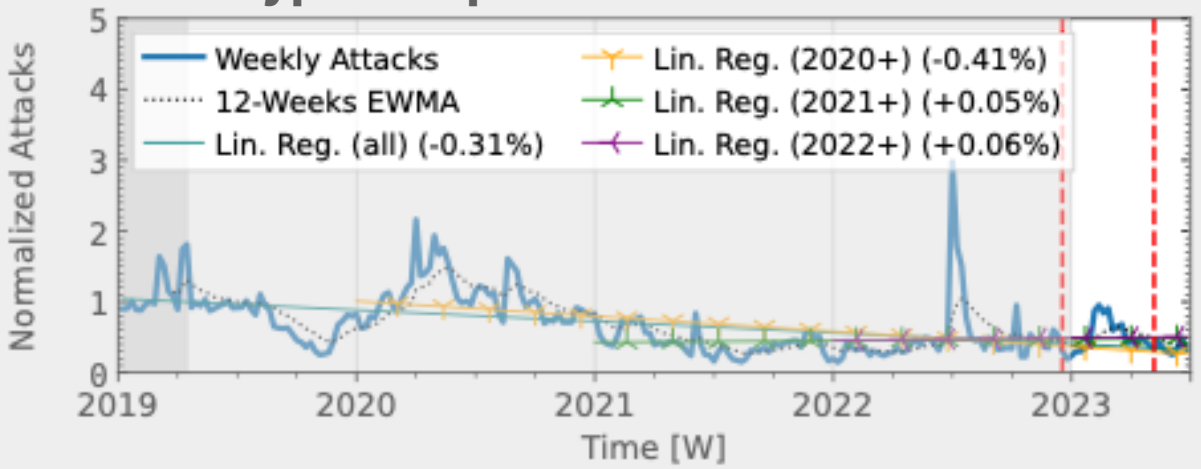

### Honeypot: AmpPot




### Flow data: Akamai Prolexic



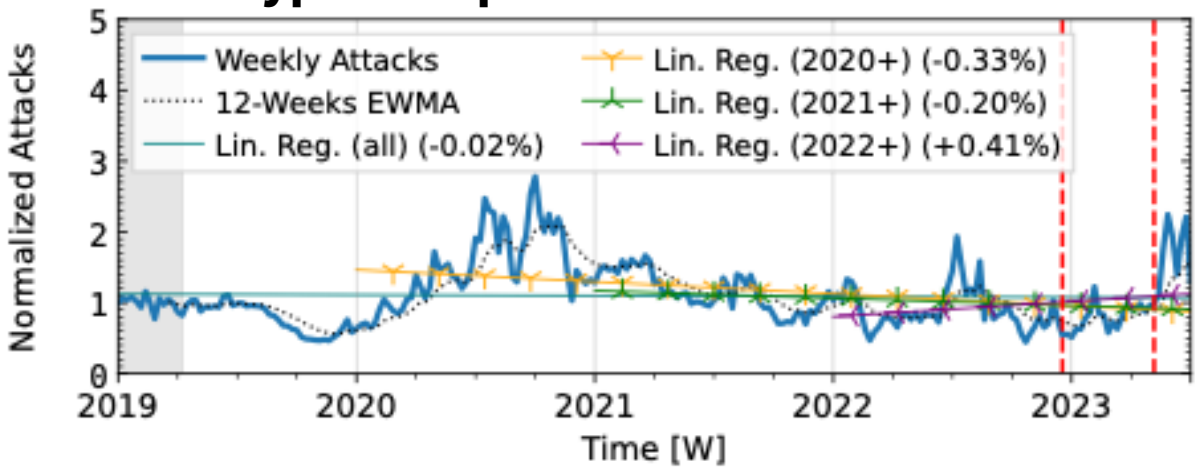

### Honeypot: Hopscotch



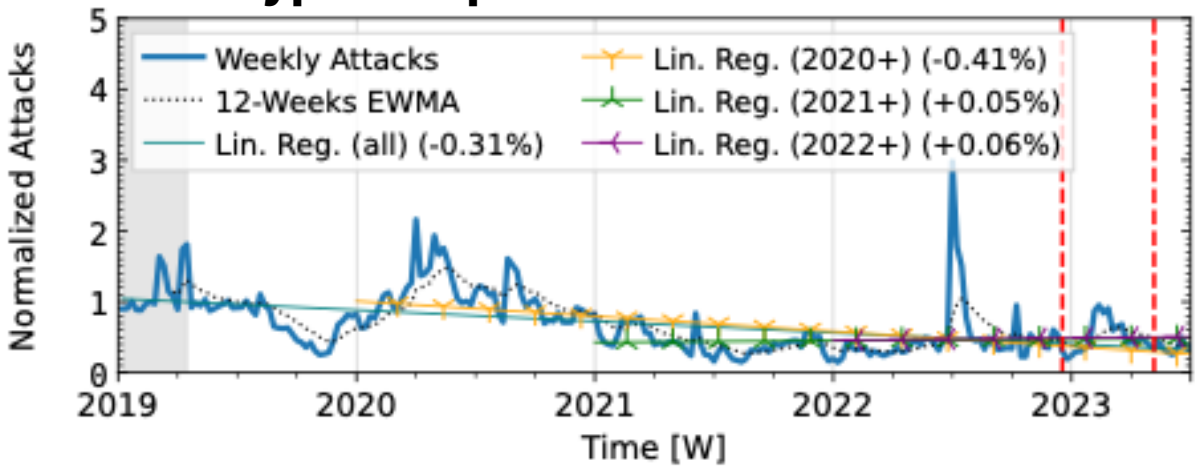
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Honeypot: AmpPot**




**Honeypot: Hopscotch**

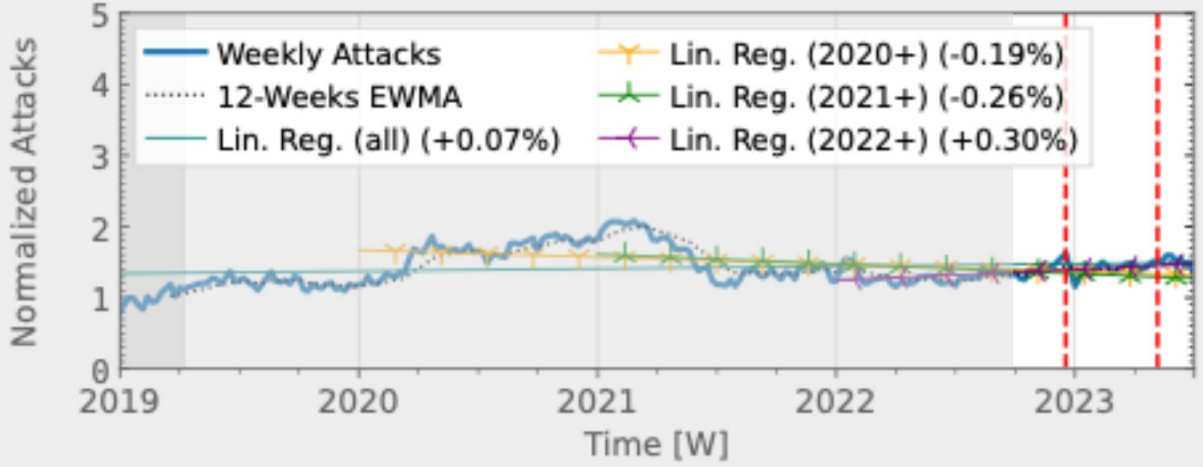



Similar only between 2019 and 2021 – still with diverging details.

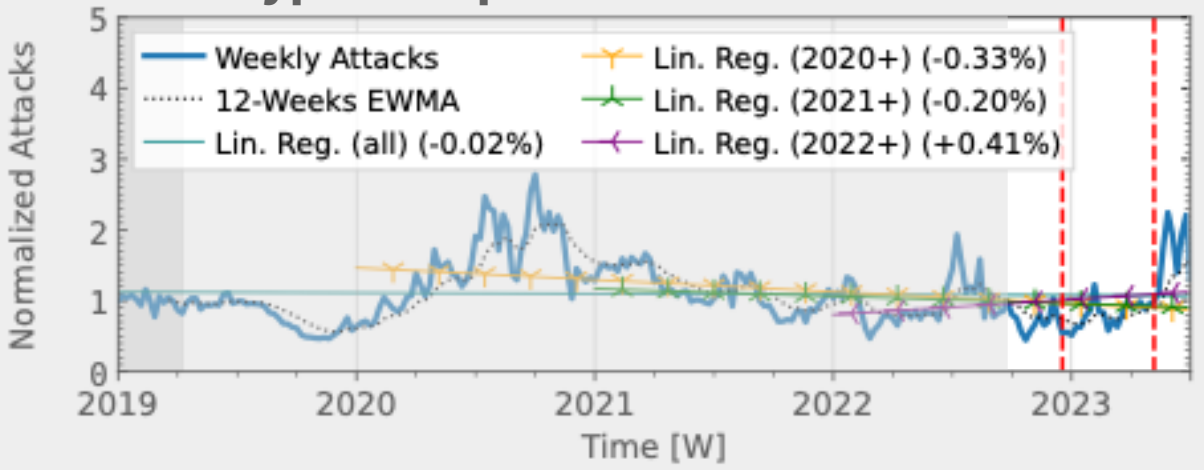
# Reflection-amplification Attacks

## Long-term DDoS Trends

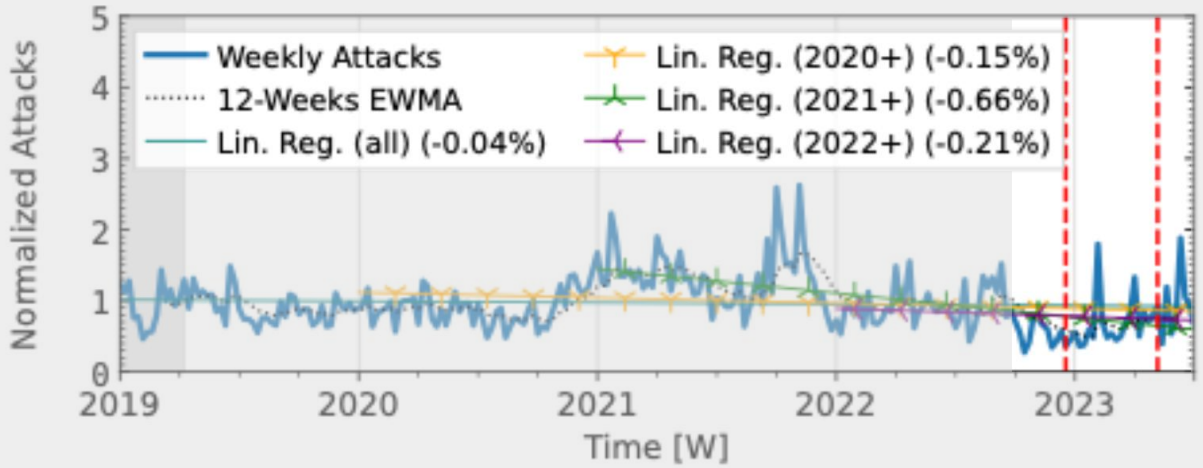
### Flow data: Netscout



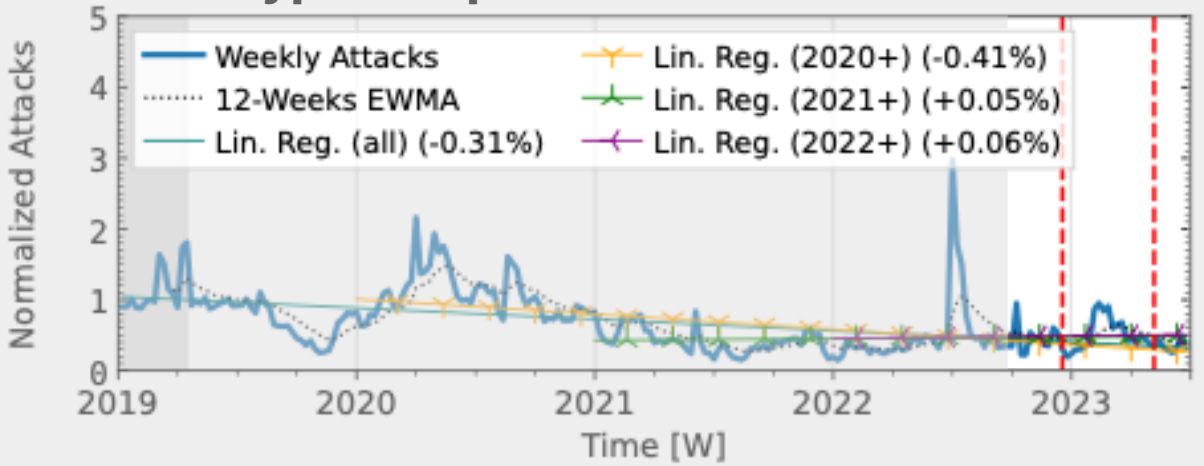

### Honeypot: AmpPot




### Flow data: Akamai Prolexic



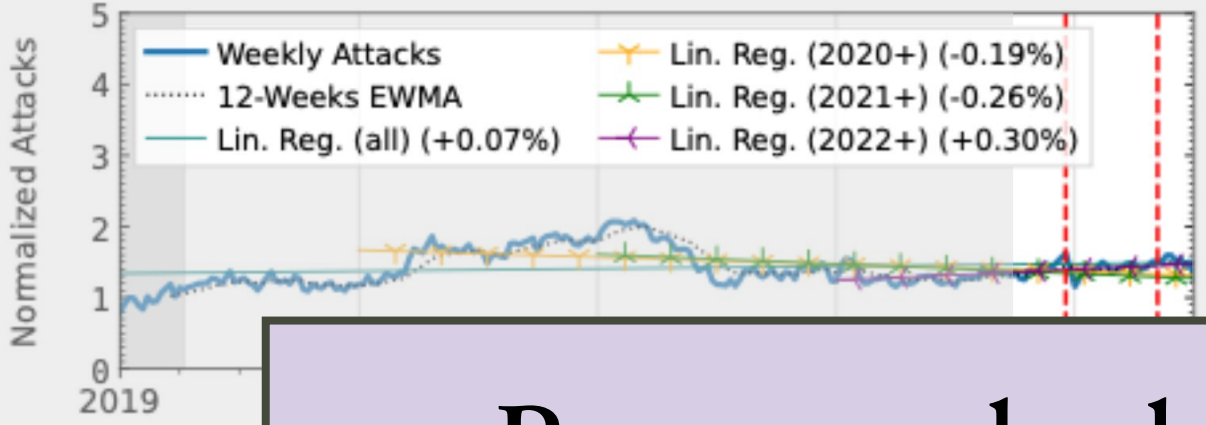

### Honeypot: Hopscotch



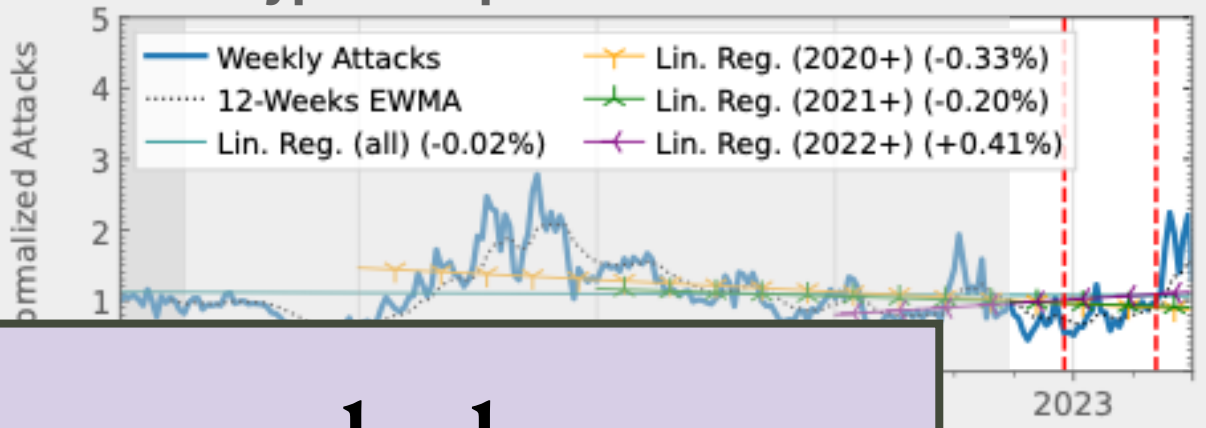
# Reflection-amplification Attacks

## Long-term DDoS Trends

**Flow data: Netscout**

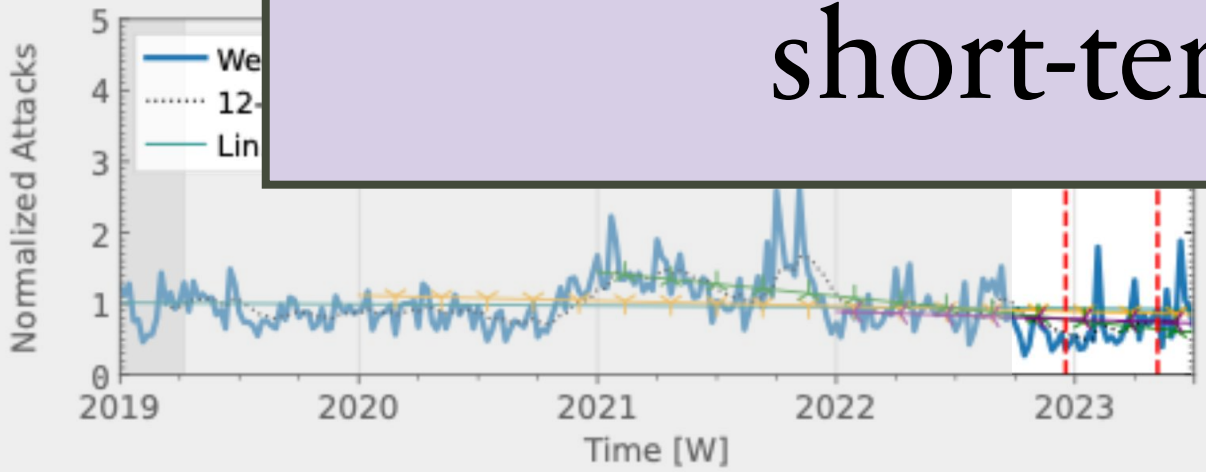


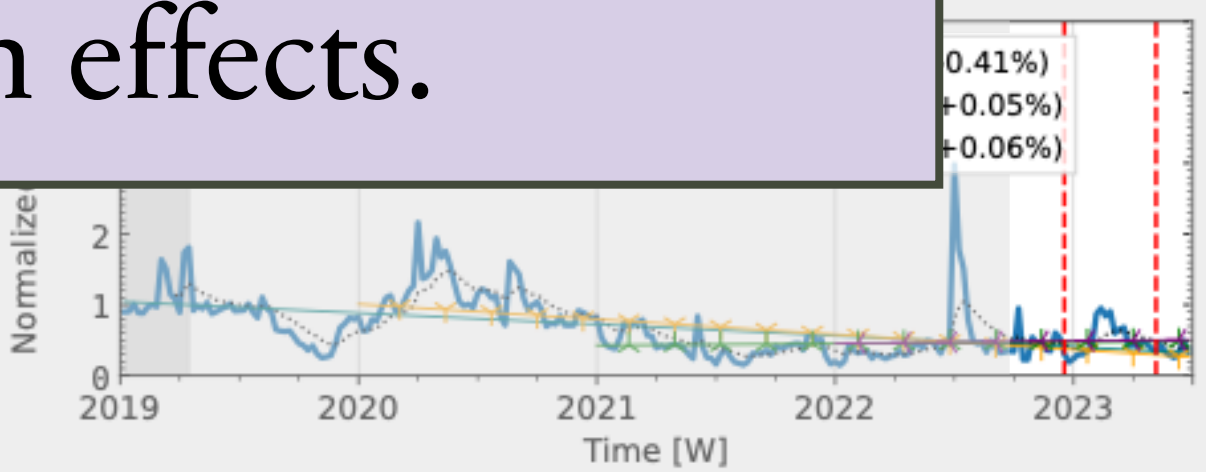

**Honeypot: AmpPot**




Booter takedowns only have short-term effects.

**Flow**



# Trend Summary

Observatories only partially agree on long-term trends.

| Attack Type | Observatories Used in This Paper (2019-2023) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Network Telescopes | | Flow Data | | | Honeypots | | |
| | UCSD | Orion | Netscout | Akamai | IXP | Hopscotch | AmpPot | NewKid |
| Direct-path | ▲ | ▲ | ▲ | ◆ | ▲ | n/a | n/a | n/a |
| Reflection-Ampl. | n/a | n/a | ▲ | ◆ | ▼ | ▼ | ◆ | ▲ |

▲ Increase
◆ Unchanged
▼ Decrease

# Trend Summary

We also analyzed 24 DDoS reports from 22 industry vendors (see our artifact).

| Attack Type | Observatories Used in This Paper (2019-2023) | | | | | | | | Industry Reports (#) (≈ 2022) |
|---|---|---|---|---|---|---|---|---|---|
| | Network Telescopes | | Flow Data | | | Honeypots | | | |
| | UCSD | Orion | Netscout | Akamai | IXP | Hopscotch | AmpPot | NewKid | |
| Direct-path | ▲ | ▲ | ▲ | ◆ | ▲ | n/a | n/a | n/a | ▲(5), ▼(0) |
| Reflection-Ampl. | n/a | n/a | ▲ | ◆ | ▼ | ▼ | ◆ | ▲ | ▲(2), ▼(3) |

# Trend Summary

**Why do observatories disagree?**
**Do they see similar DDoS events?**

| Attack Type | Observatories Used in This Paper (2019-2023) | | | | | | | | Industry Reports (#) (≈ 2022) |
|---|---|---|---|---|---|---|---|---|---|
| | Network Telescopes | | Flow Data | | | Honeypots | | | |
| | UCSD | Orion | Netscout | Akamai | IXP | Hopscotch | AmpPot | NewKid | |
| Direct-path | ▲ | ▲ | ▲ | ◆ | ▲ | n/a | n/a | n/a | ▲(5), ▼(0) |
| Reflection-Ampl. | n/a | n/a | ▲ | ◆ | ▼ | ▼ | ◆ | ▲ | ▲(2), ▼(3) |

# Target Visibility Across Observatories

**Academia**

- Each observatory contributes new targets.
  - UCSD, Hopscotch, AmpPot each exclusively observe 20% (among academia).
- A very small number of targets is observed by all four: 0.55%.

# Target Visibility Across Observatories

**Academia**

- Each observatory contributes new targets.
  - UCSD, Hopscotch, AmpPot each exclusively observe 20% (among academia).
- A very small number of targets is observed by all four: 0.55%.

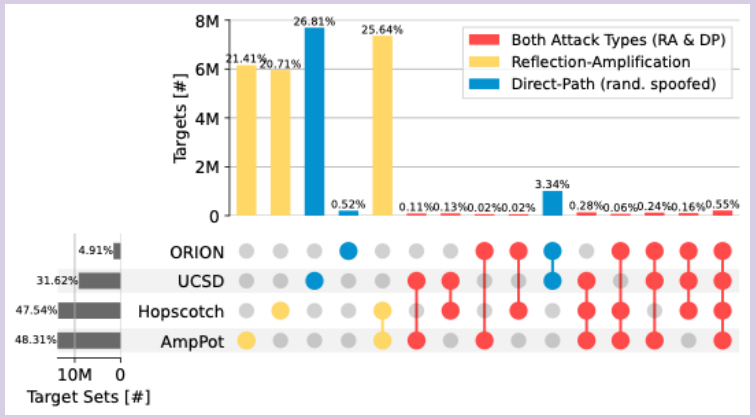
**Industry**

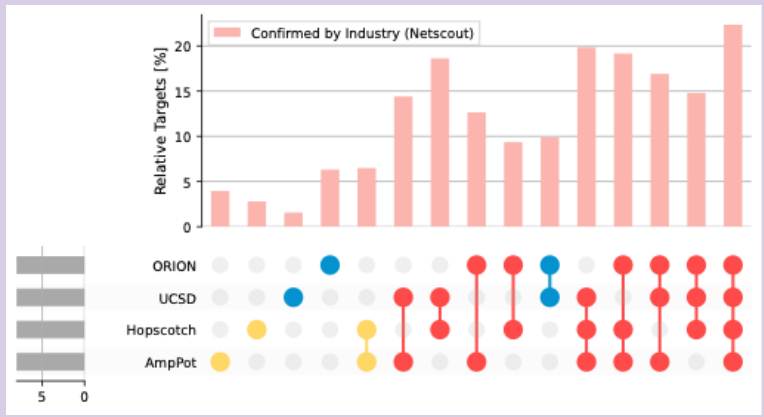
- Industry confirms few targets seen by each respective observatory from academia: *Netscout*: 2%-7%, *Akamai Prolexic*: 0.02%-0.06%
- Overlap with targets observed by all four observatories from academia is 10x higher at 20% and 0.2%!

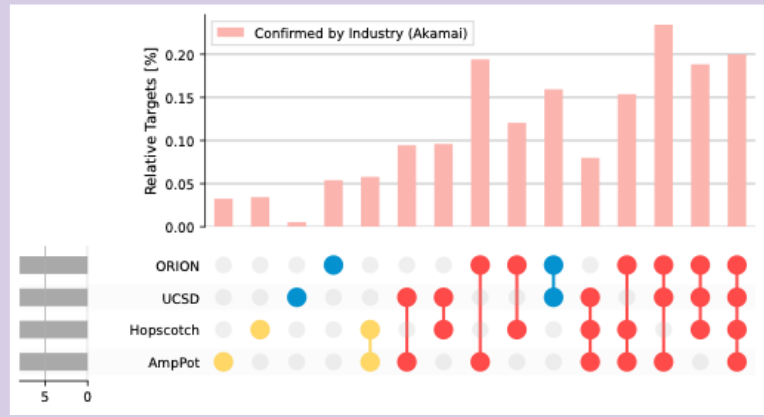
# Target Visibility Across Observatories

**Academia**

## Details in the UpSet plots of the paper!




Overlap with targets observed by all four observatories from academia is 10x higher at 20% and 0.2%!

# Target Visibility Across Observatories

**Academia**

Data sharing is required for a thorough view onto the DDoS landscape!

from academia: *Netscout*: 2%-7%, *Akamai Prolexic*: 0.02%-0.06%

- Overlap with targets observed by all four observatories from academia is 10x higher at 20% and 0.2%!

# Conclusion

- We compared 4.5 years of DDoS attack data from 7 observatories.
- Differences in trends and targets show limitations of individual views.
- Data sharing required for a comprehensive understanding of DDoS.

# Conclusion

- We compared 4.5 years of DDoS attack data from 7 observatories.
- Differences in trends and targets show limitations of individual views.
- Data sharing required for a comprehensive understanding of DDoS.

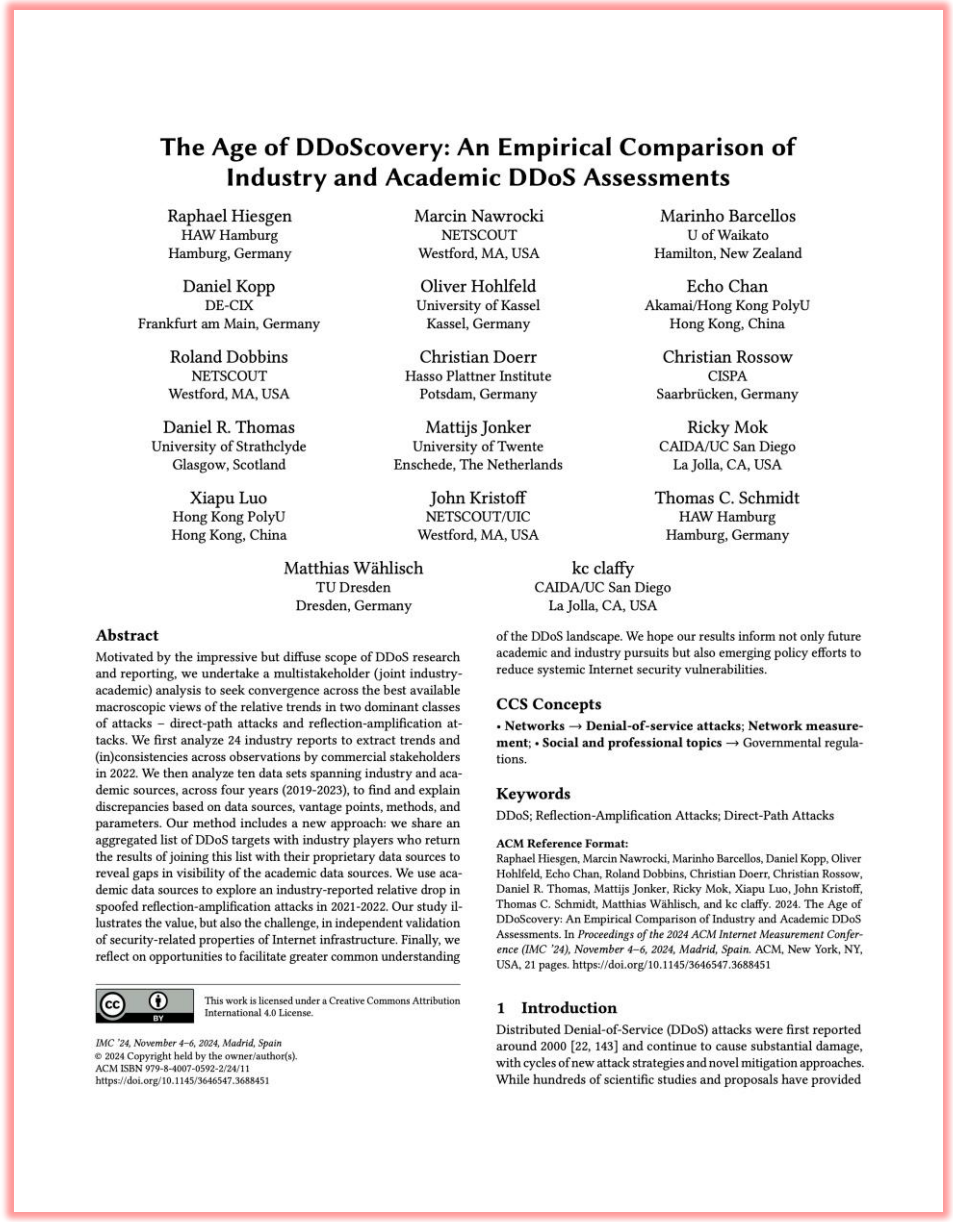
- DDoS research tries to make global inferences based on a local view.
- Acknowledging this limitation is important for accurate interpretation and accurate comparison.
- Let’s collaborate to achieve a comprehensive view of DDoS!

# Conclusion

**Thank you!**
**Artifact:** https://ddoscovery.github.io
**Me:** raphael.hiesgen@haw-hamburg.de

- We compared 4.5 years of DDoS attack data from 7 observatories.
- Differences in trends and targets show limitations of individual views.
- Data sharing required for a comprehensive understanding of DDoS.

- DDoS research tries to make global inferences based on a local view.
- Acknowledging this limitation is important for accurate interpretation and accurate comparison.
- Let's collaborate to achieve a comprehensive view of DDoS!



# The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments


Raphael Hiesgen
HAW Hamburg
Hamburg, Germany

Marcin Nawrocki
NETSCOUT
Westford, MA, USA

Marinho Barcellos
U of Waikato
Hamilton, New Zealand

Daniel Kopp
DE-CIX
Frankfurt am Main, Germany

Oliver Hohlfeld
University of Kassel
Kassel, Germany

Echo Chan
Akamai/Hong Kong PolyU
Hong Kong, China

Roland Dobbins
NETSCOUT
Westford, MA, USA

Christian Doerr
Hasso Plattner Institute
Potsdam, Germany

Christian Rossow
CISPA
Saarbrücken, Germany

Daniel R. Thomas
University of Strathclyde
Glasgow, Scotland

Mattijs Jonker
University of Twente
Enschede, The Netherlands

Ricky Mok
CAIDA/UC San Diego
La Jolla, CA, USA

Xiapu Luo
Hong Kong PolyU
Hong Kong, China

John Kristoff
NETSCOUT/UIC
Westford, MA, USA

Thomas C. Schmidt
HAW Hamburg
Hamburg, Germany

Matthias Wählisch
TU Dresden
Dresden, Germany

kc claffy
CAIDA/UC San Diego
La Jolla, CA, USA



**Abstract**

Motivated by the impressive but diffuse scope of DDoS research and reporting, we undertake a multistakeholder (joint industry-academic) analysis to seek convergence across the best available macroscopic views of the relative trends in two dominant classes of attacks – direct-path attacks and reflection-amplification attacks. We first analyze 24 industry reports to extract trends and (in)consistencies across observations by commercial stakeholders in 2022. We then analyze ten data sets spanning industry and academic sources, across four years (2019-2023), to find and explain discrepancies based on data sources, vantage points, methods, and parameters. Our method includes a new approach: we share an aggregated list of DDoS targets with industry players who return the results of joining this list with their proprietary data sources to reveal gaps in visibility of the academic data sources. We use academic data sources to explore an industry-reported relative drop in spoofed reflection-amplification attacks in 2021-2022. Our study illustrates the value, but also the challenge, in independent validation of security-related properties of Internet infrastructure. Finally, we reflect on opportunities to facilitate greater common understanding of the DDoS landscape. We hope our results inform not only future academic and industry pursuits but also emerging policy efforts to reduce systemic Internet security vulnerabilities.



**CCS Concepts**

• **Networks** → **Denial-of-service attacks**; **Network measurement**; • **Social and professional topics** → Governmental regulations.

**Keywords**

DDoS; Reflection-Amplification Attacks; Direct-Path Attacks

**ACM Reference Format:**

Raphael Hiesgen, Marcin Nawrocki, Marinho Barcellos, Daniel Kopp, Oliver Hohlfeld, Echo Chan, Roland Dobbins, Christian Doerr, Christian Rossow, Daniel R. Thomas, Mattijs Jonker, Ricky Mok, Xiapu Luo, John Kristoff, Thomas C. Schmidt, Matthias Wählisch, and kc claffy. 2024. The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3646547.3688451





*IMC '24, November 4–6, 2024, Madrid, Spain*



ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3688451


## 1 Introduction

Distributed Denial-of-Service (DDoS) attacks were first reported around 2000 [22, 143] and continue to cause substantial damage, with cycles of new attack strategies and novel mitigation approaches. While hundreds of scientific studies and proposals have provided

For more details, see our paper.
https://doi.org/10.1145/3646547.3688451

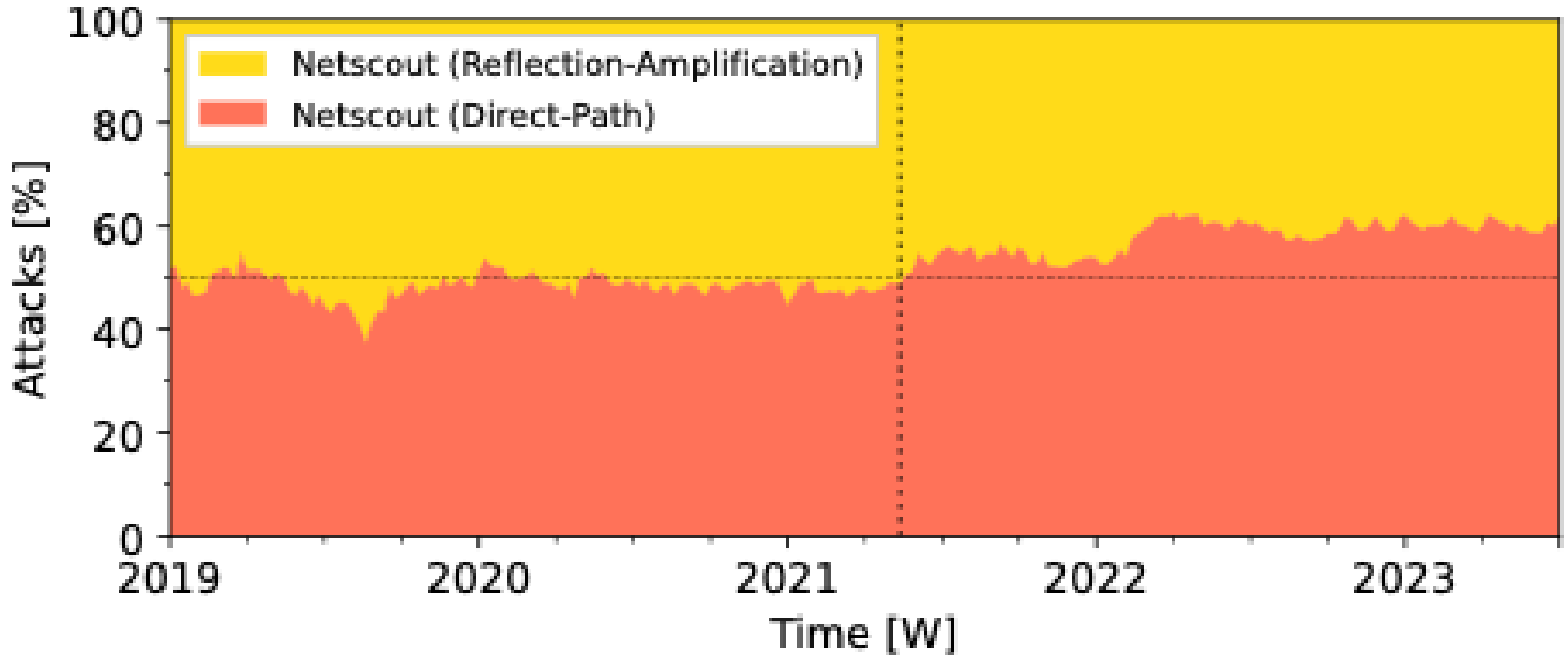
- Contact information:


**Raphael Hiesgen**
HAW Hamburg
raphael.hiesgen@haw-hamburg.de

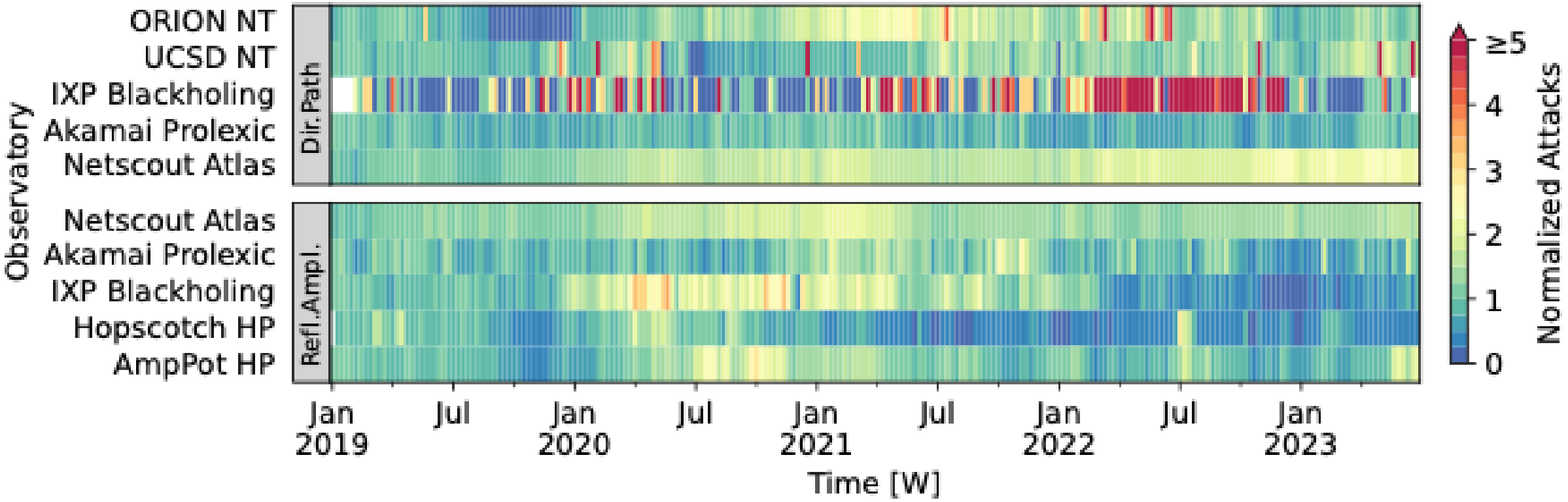

- Find our artifact at:
https://ddoscovery.github.io

# Backup Slides

# Netscout: Attack Shift



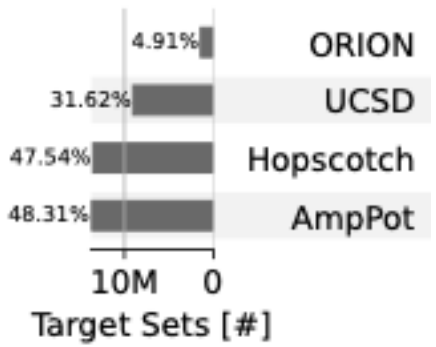
# All Attack Trends



# Targets Across Academic Observatories

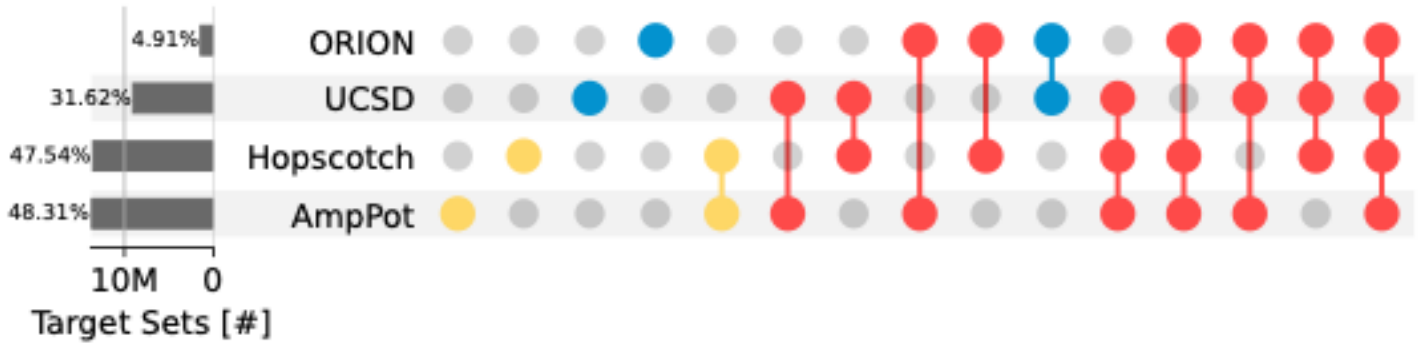
# Targets Across Observatories

Target tuples (date, IP address) seen by each observatory.

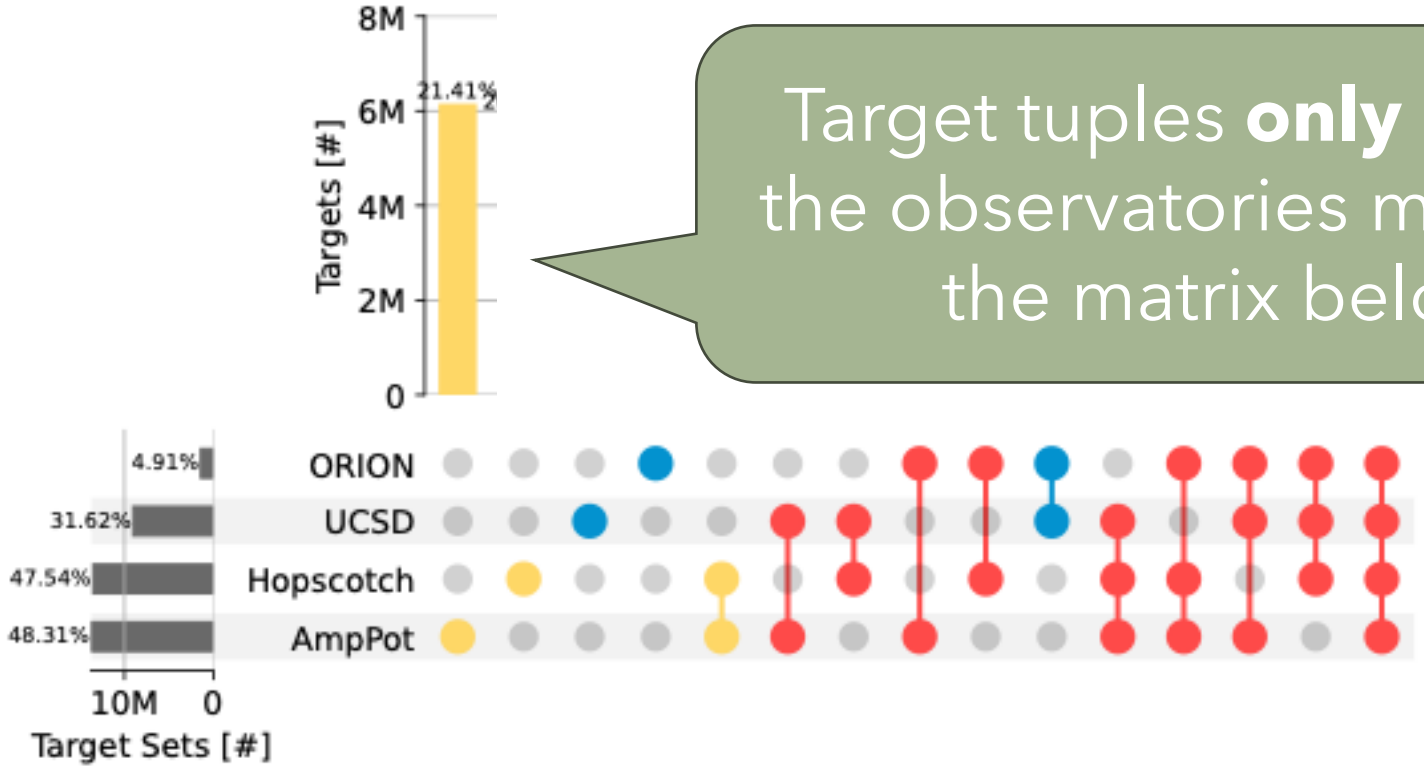


# Targets Across Academic Observatories

All combinations of observatories.

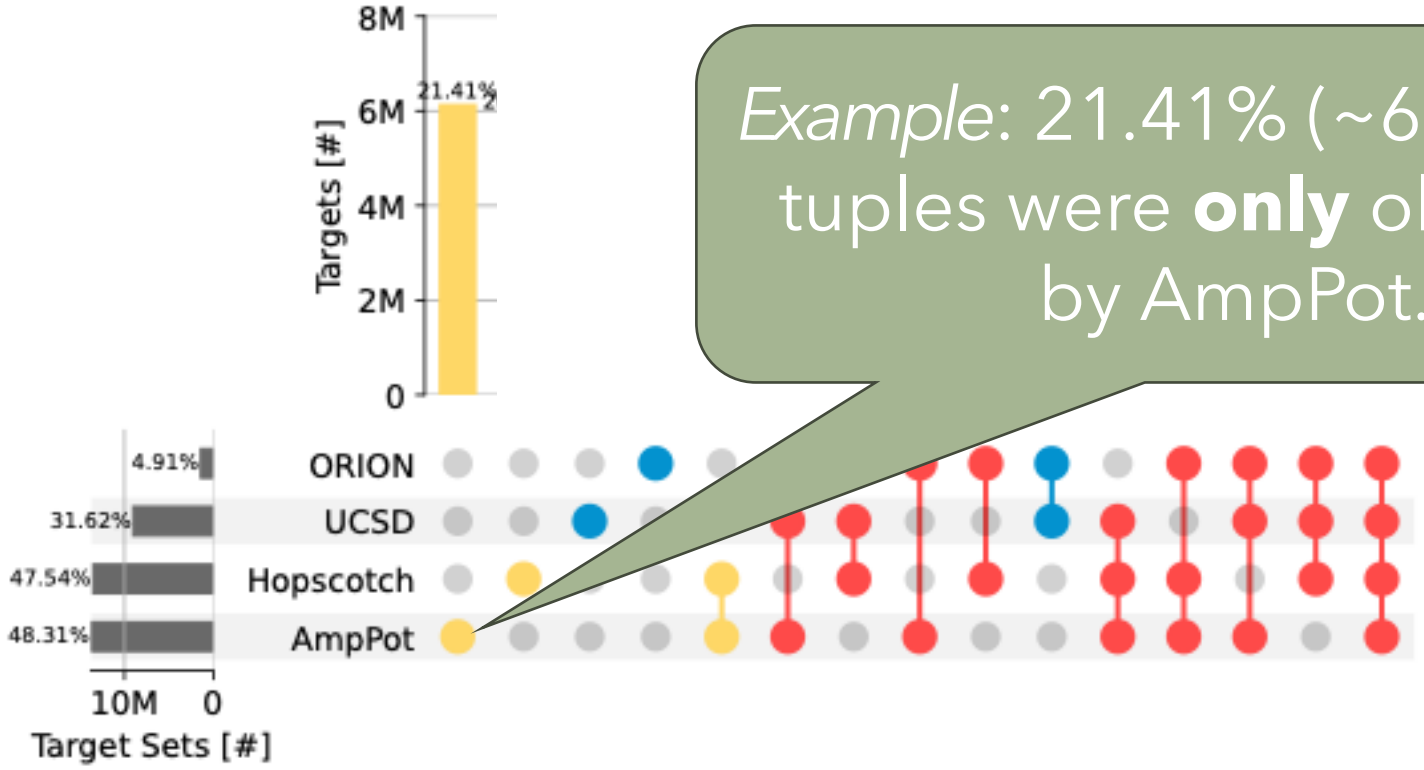


# Targets Across Academic Observatories



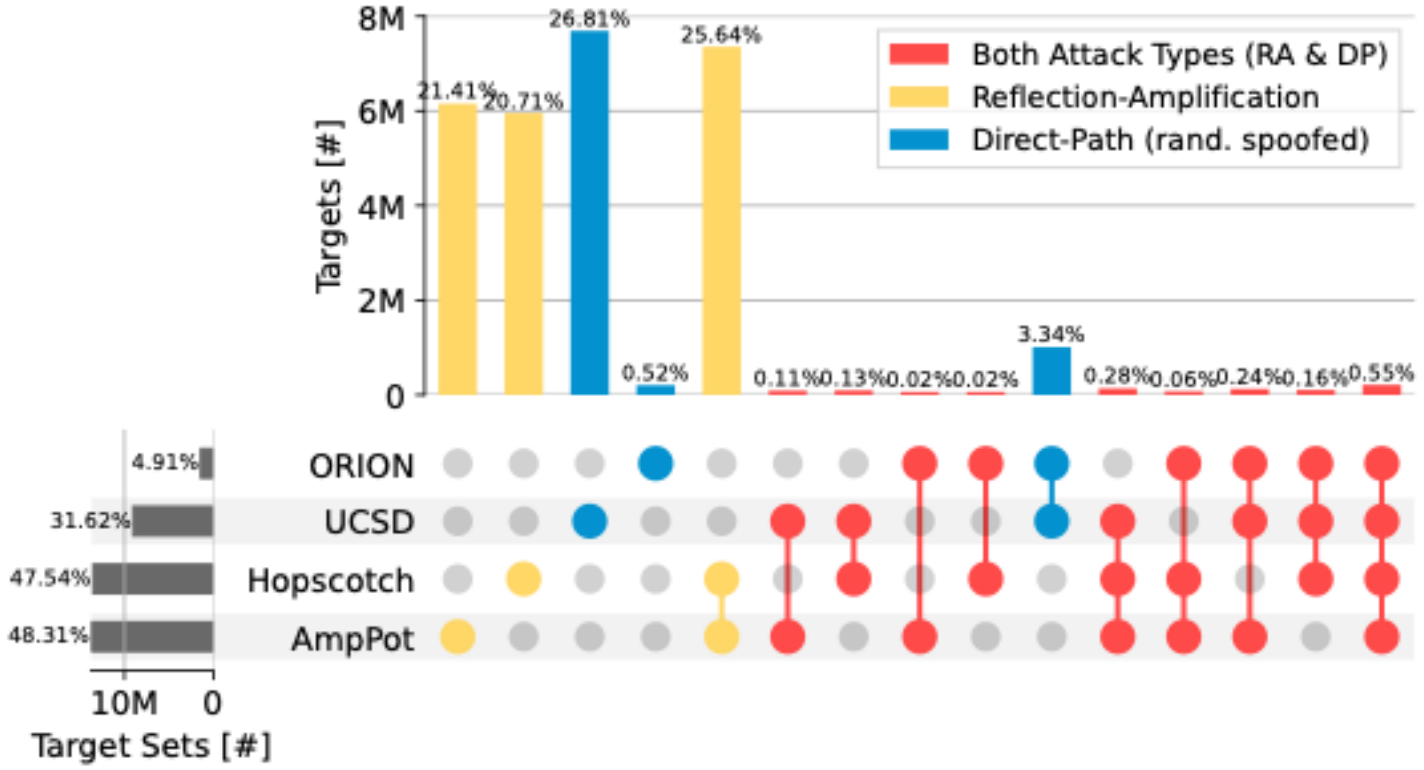

Target tuples **only** seen by the observatories marked in the matrix below.

# Targets Across Academic Observatories

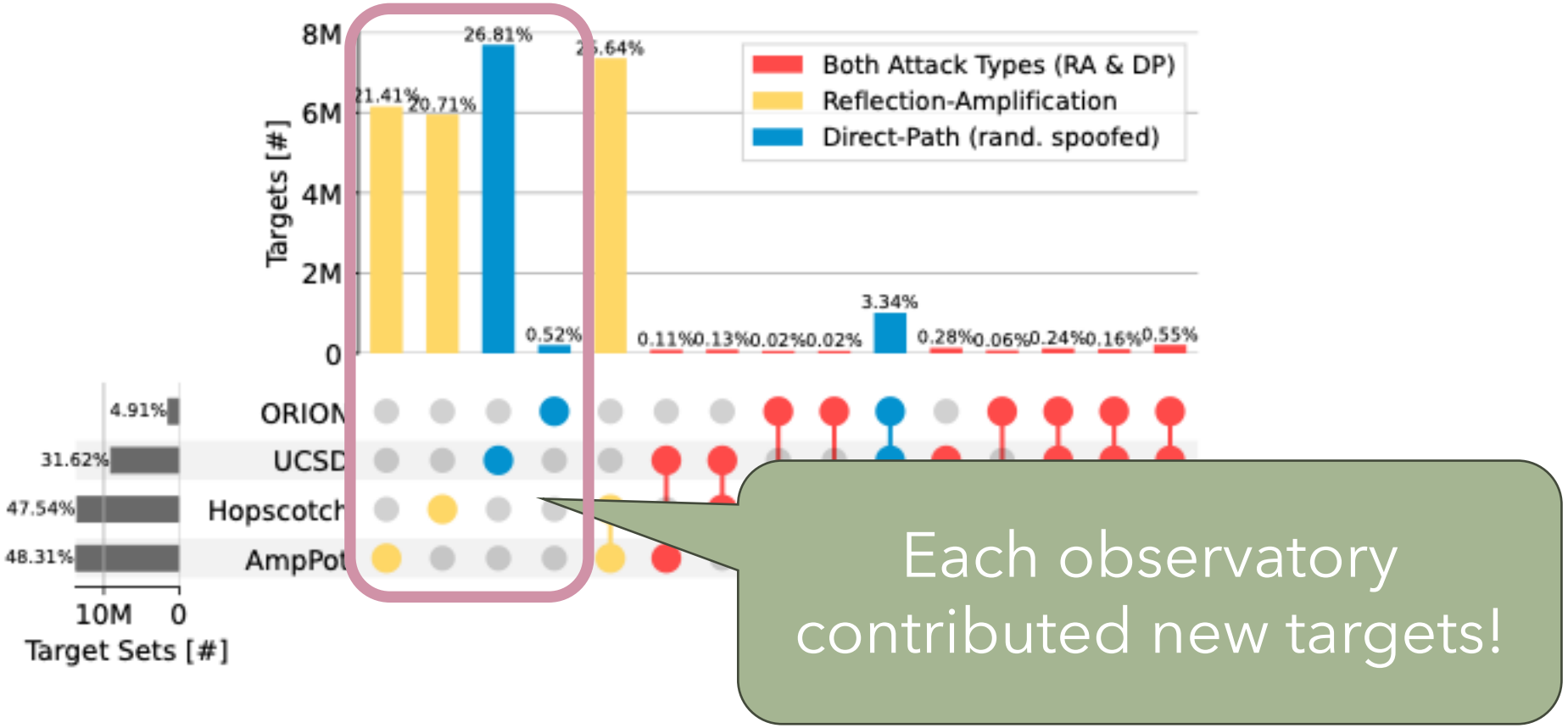



*Example*: 21.41% (~6M) target tuples were **only** observed by AmpPot.

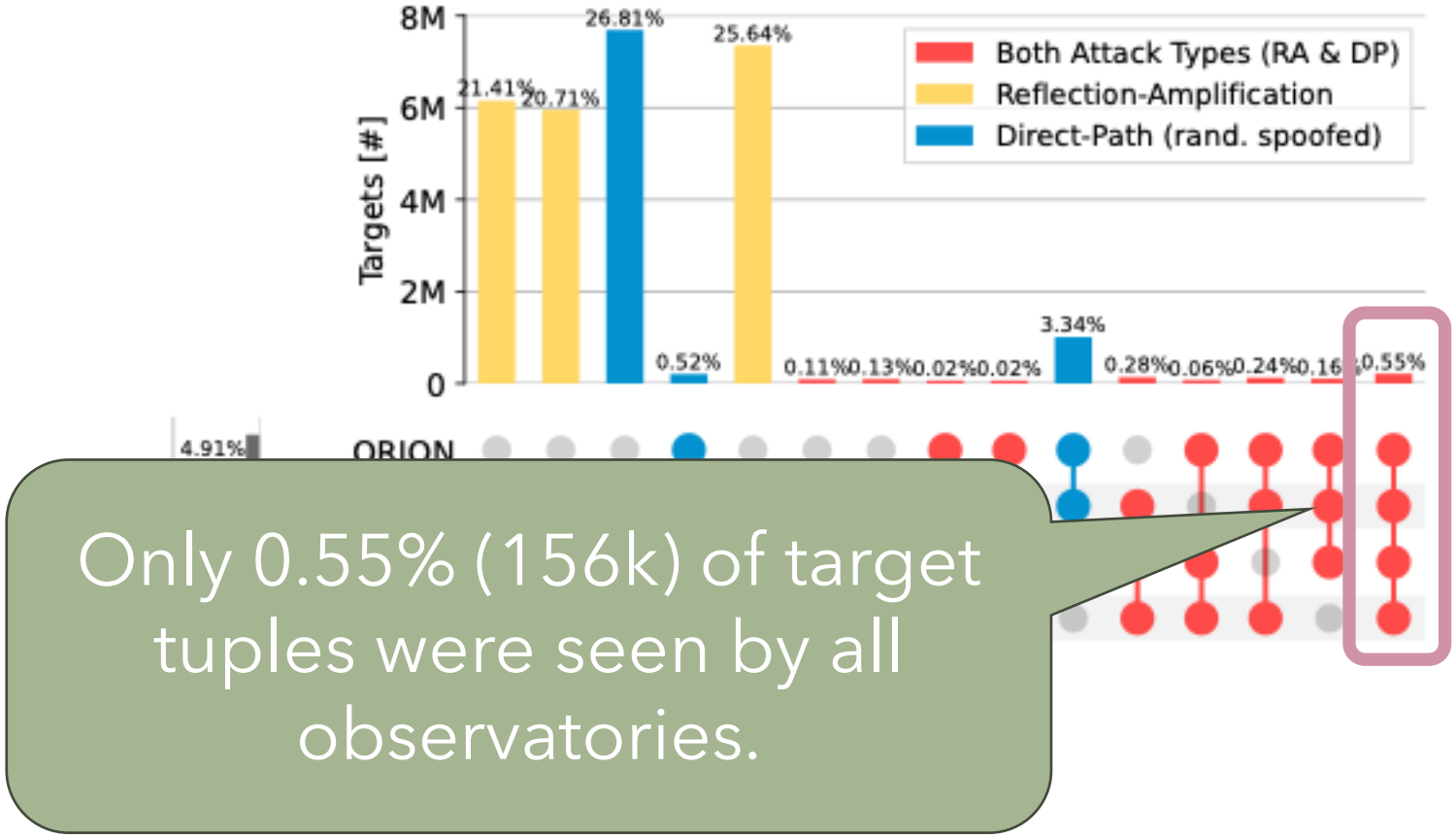
# Targets Across Academic Observatories



# Targets Across Academic Observatories

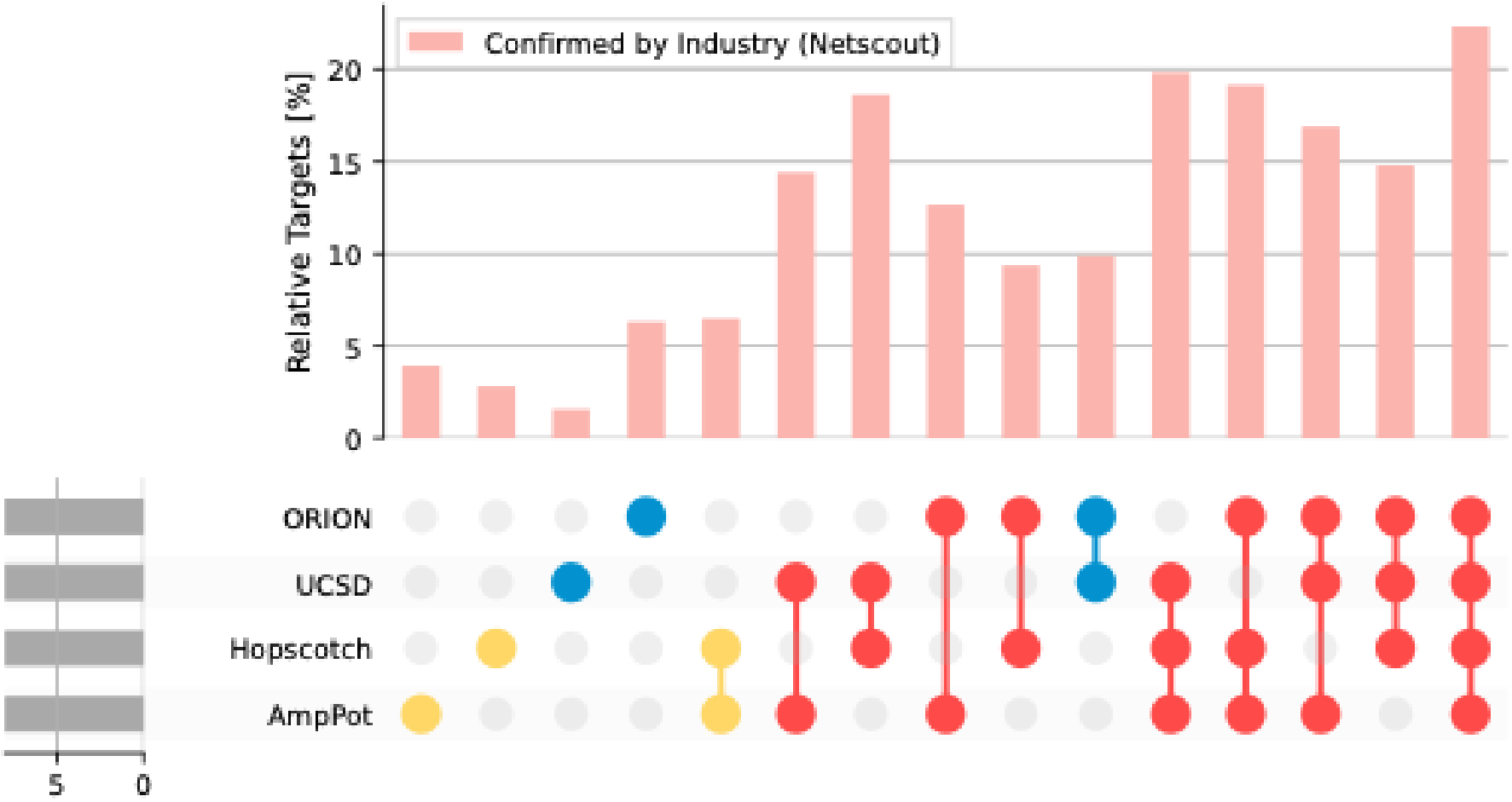


# Targets Across Academic Observatories

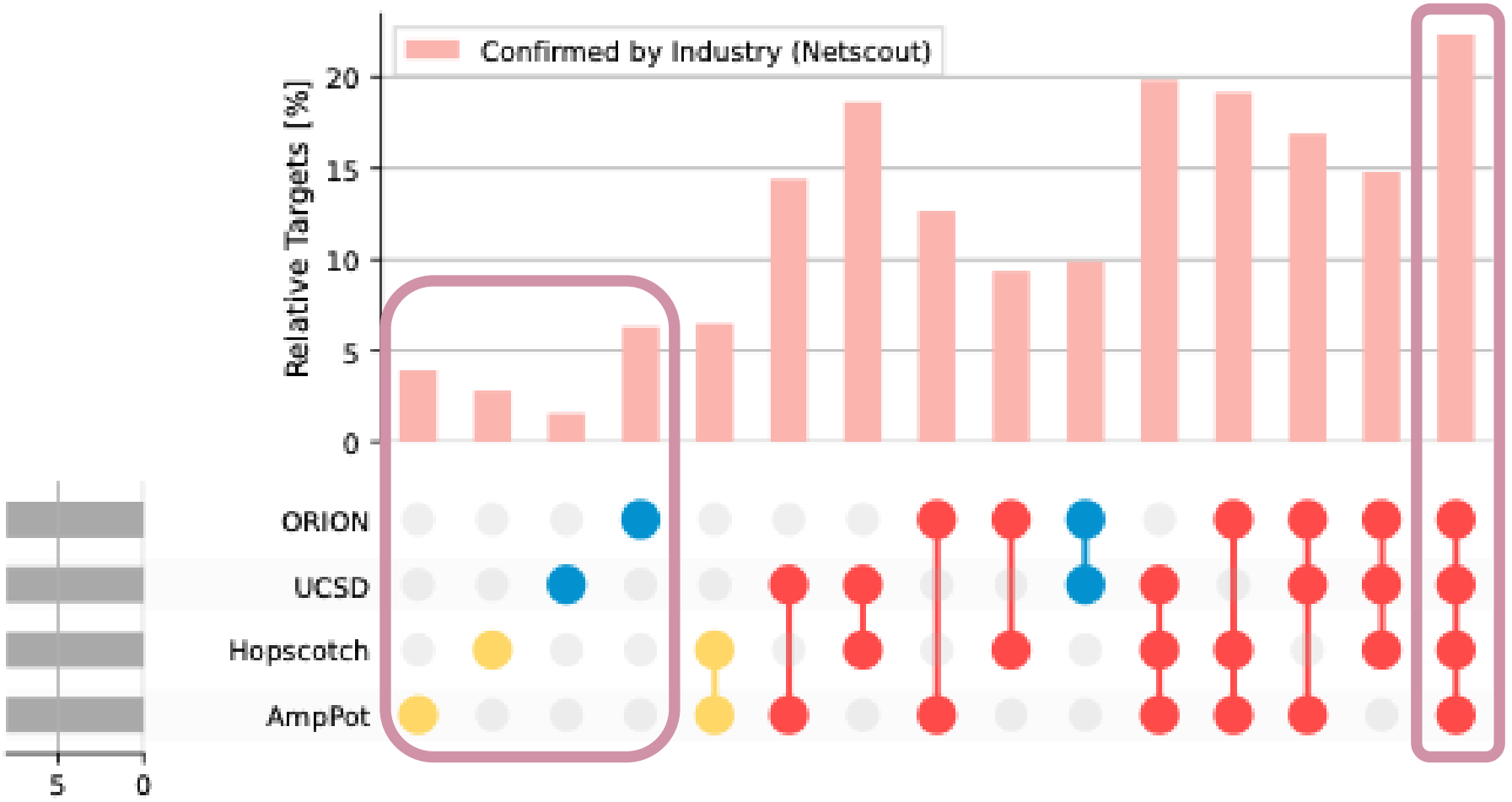



Only 0.55% (156k) of target tuples were seen by all observatories.

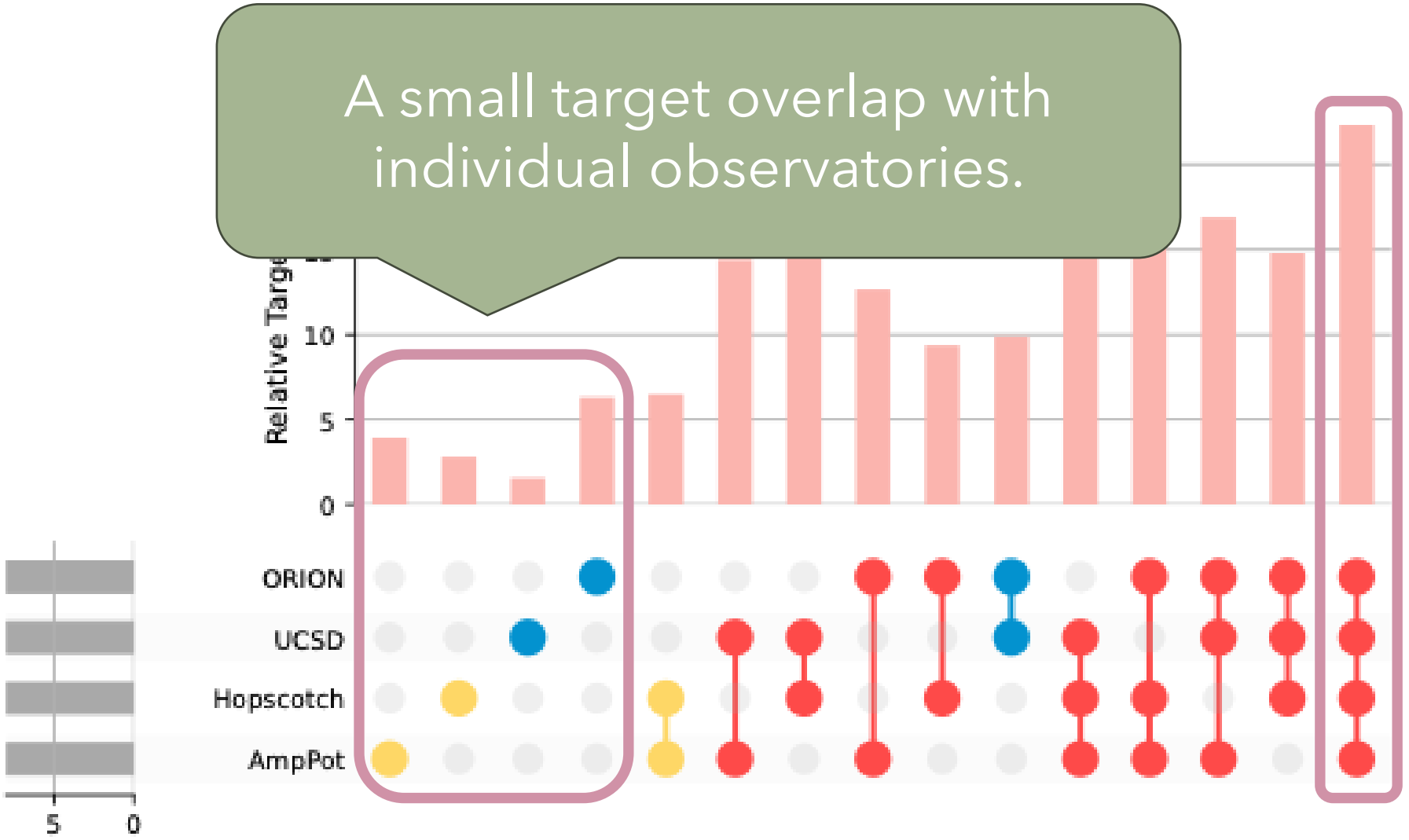
# A Quick Look at Industry



# A Quick Look at Industry

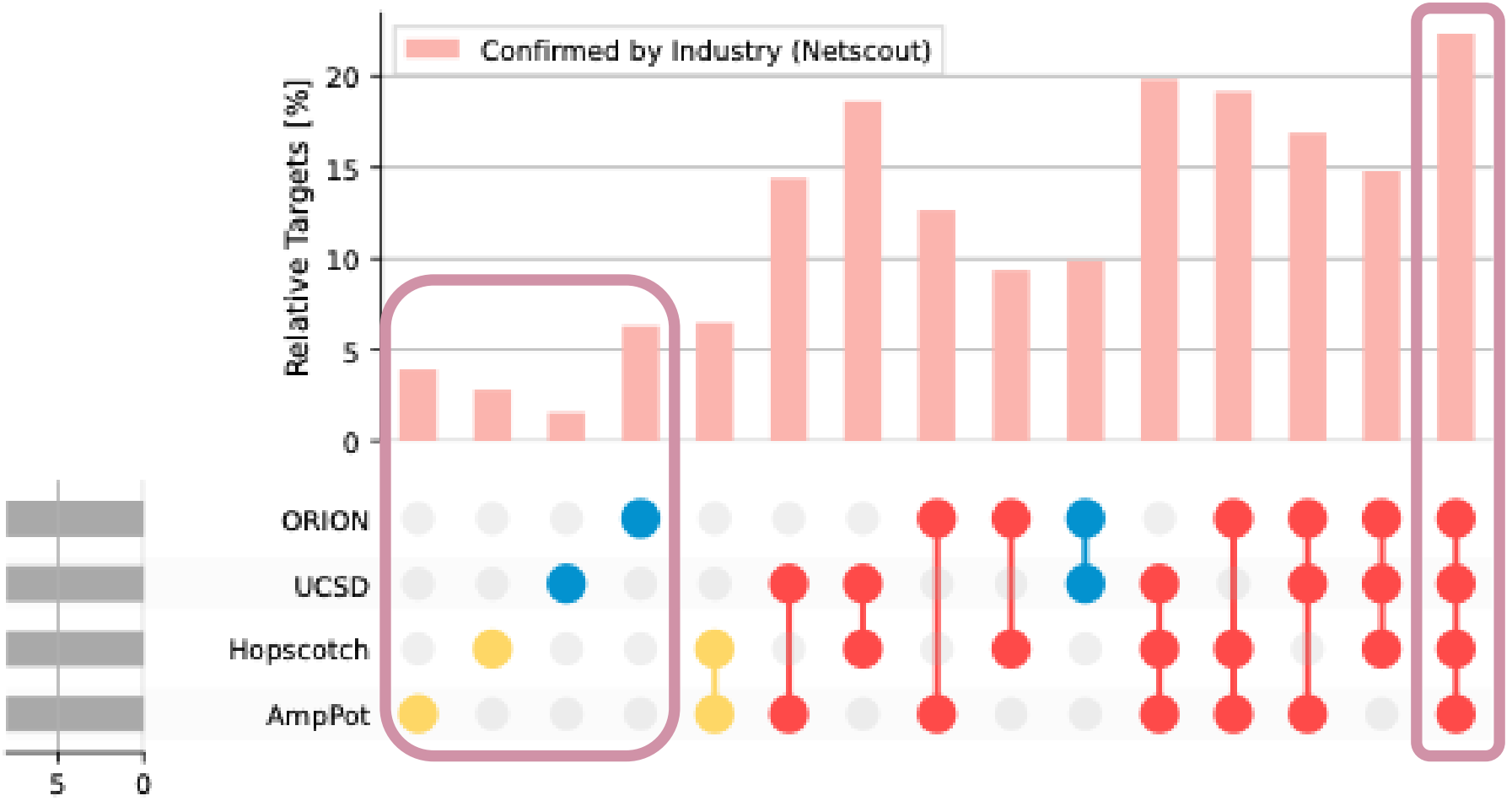


# A Quick Look at Industry

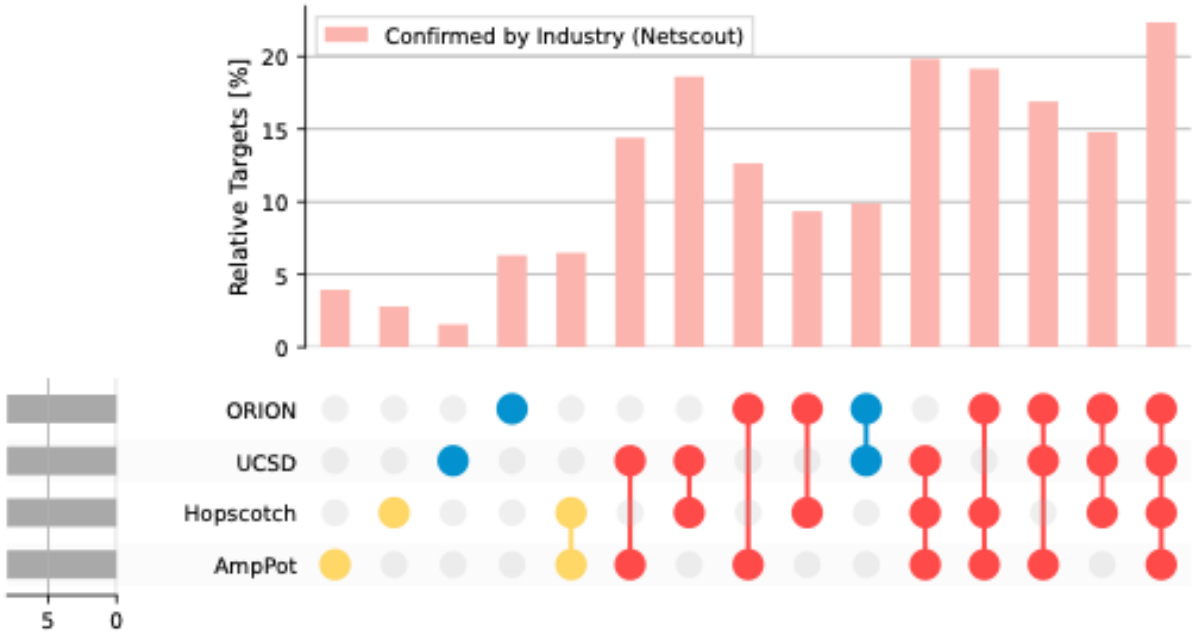


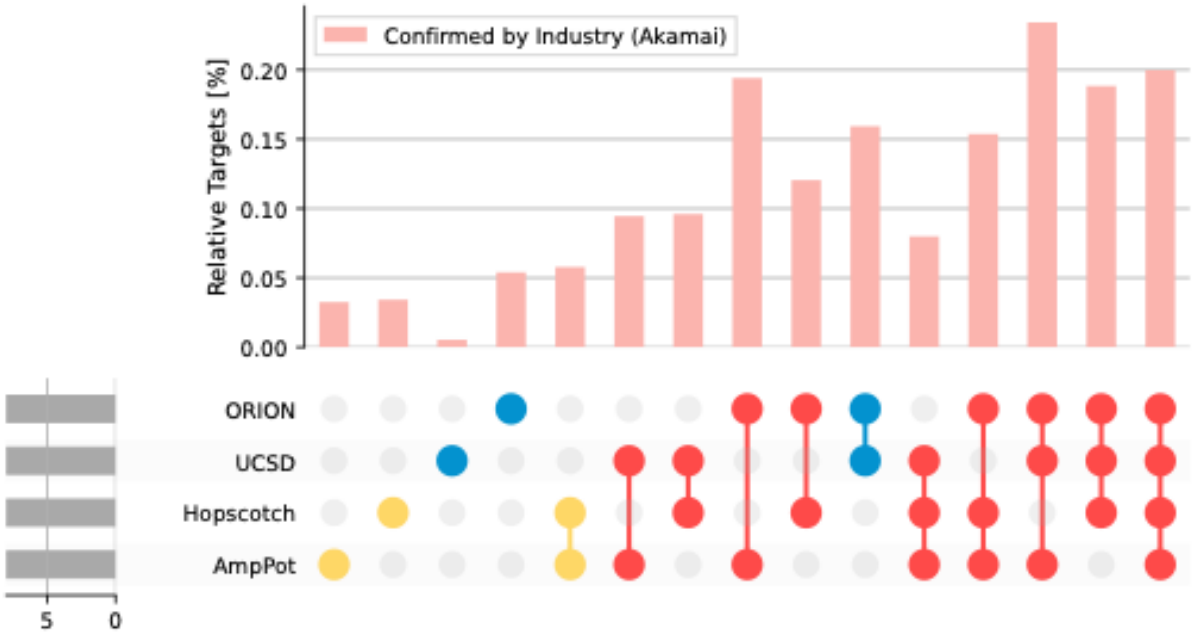
# A Quick Loo

Larger overlap among attacks observed by all of them.

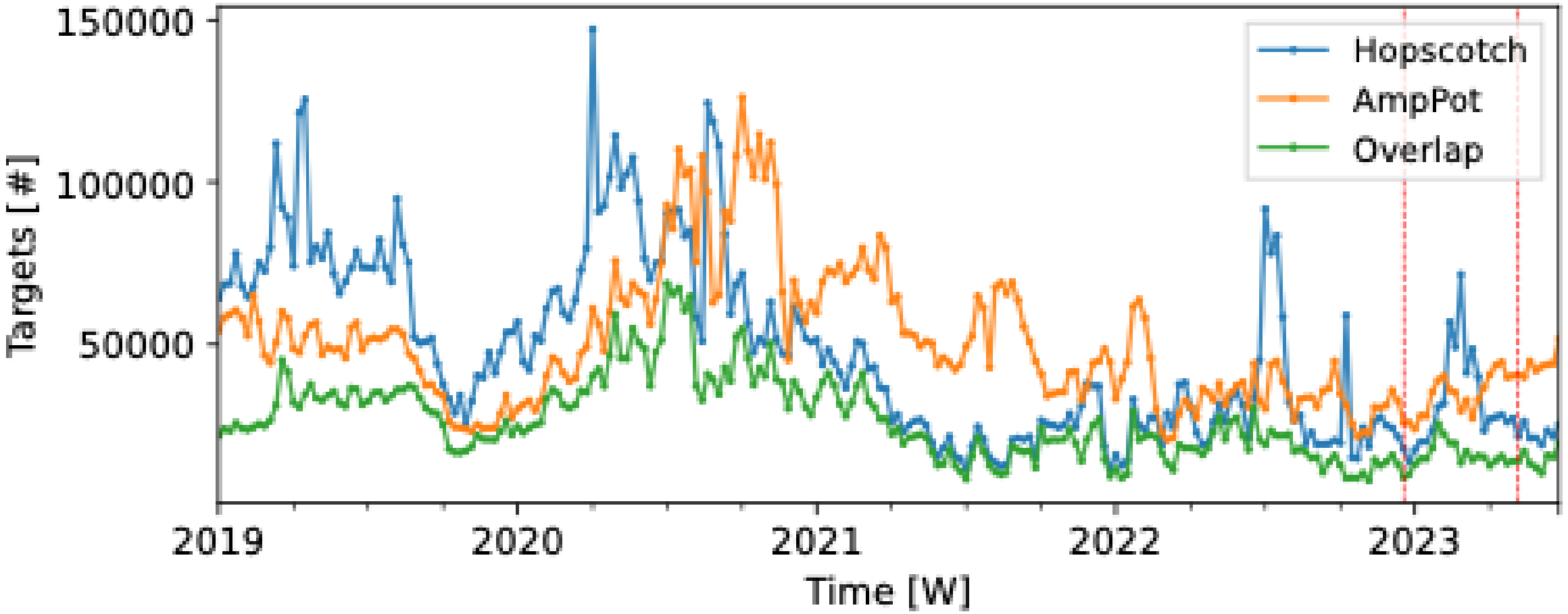


# Industry Target Overlap with Academia



# Target Overlap Timeseries : Honeypots



# Target Overlap Timeseries: Telescopes